2110200
DISCRETE STRUCTURE

ผศ. ดร.อรรถสิทธิ์ สุรฤกษ์

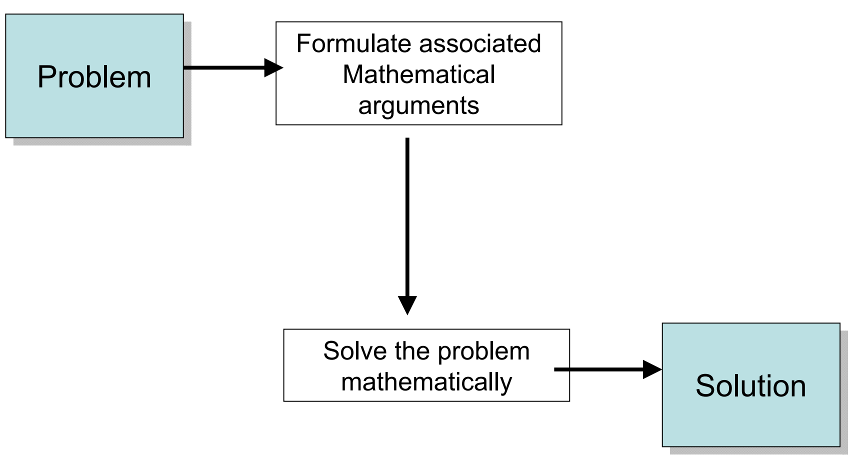
ผศ. ดร.อรรถวิทย์ สุดแสง

ผศ. ดร.อติวงศ์ สุชาโต

Course Outline

- 4 parts:
- Part1: Discrete Math Fundamentals
- Part2: Graphs and Trees
- Part3: Counting Techniques
- Part4: Number Theory

Why ???



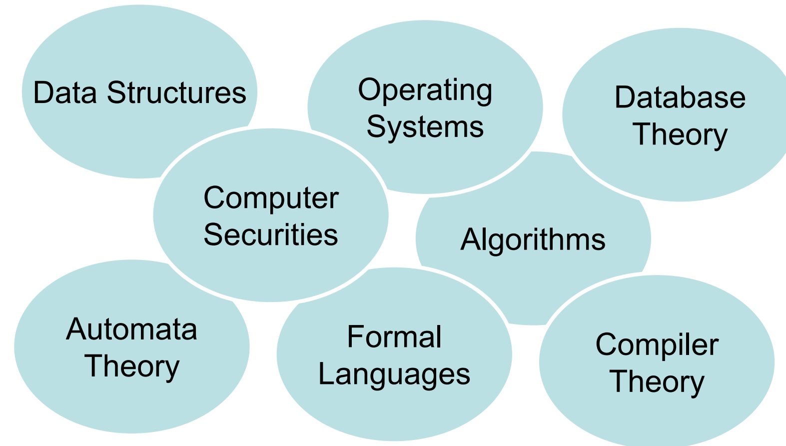
Goals of Discrete Math.

- **Mathematical Reasoning**
  - Read, comprehend, and construct mathematical arguments
- **Combinatorial Analysis**
  - Perform analysis to solve counting problems
- **Discrete Structure**
  - Able to work with discrete structures: sets, graphs, finite-state machines, etc.

Goals of Discrete Math.

- **Algorithmic Thinking**
  - Specify, verify, and analyze an algorithm
- **Applications and Modeling**
  - Apply the obtained problem-solving skills to model and solve problems in computer science and other areas, such as:
    - Business
    - Chemistry
    - Linguistics
    - Geology
    - etc

Gateway to . . .



ABET Accreditation

Programs containing the modifier "**computer**" in the title must also demonstrate that graduates have a knowledge of "**discrete mathematics**".

Foundations of Discrete Math.

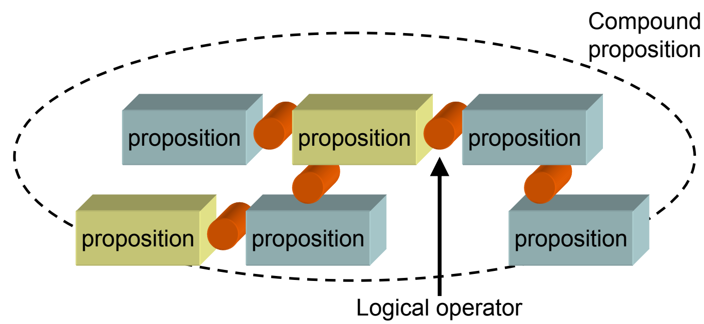
- **Logic**
  - Specify the meaning of Mathematical statements
  - Basis of all Mathematical reasoning
- **Sets**
  - Sets are collections of objects, which are used for building many important discrete structures.
- **Functions**
  - Used in the definition of some important structures
  - Represent complexity of an algorithm, and etc.

Logic

Rules of logic gives precise meaning to mathematical statements.

Proposition: Building Blocks of Logic

- Proposition =
  - Declarative sentence
  - Either *TRUE* or *FALSE* (not both)



Logical Operators

- Negation (NOT)
- Conjunction (AND)
- Disjunction (OR)
- Exclusive OR (XOR)
- Implication (IF..THEN)
- Biconditional (IF & ONLY IF)

Negation

- The negation of *p* has opposite truth value to *p*

p	$\neg p$
T	F
F	T

Conjunction

- The conjunction of *p* and *q*, is true when, and only when, both *p* and *q* are true.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction

- The disjunction of *p* and *q*, is true when at least one of *p* or *q* is true.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive OR

- Exclusive or = OR but NOT both

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

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Implication

- It is false when *p* is true and *q* is false, and true otherwise.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Biconditional

- $p \leftrightarrow q$ is true when p and q have the same truth value.
  - Intuitively, $p \leftrightarrow q$ is $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

General Compound Proposition

- Example:

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

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

Contrapositive

- The *contrapositive* of an implication $p \rightarrow q$ is:

$$\neg q \rightarrow \neg p$$

- has the same truth values as $p \rightarrow q$

Converse and Inverse

- The *converse* of an implication $p \rightarrow q$ is:

$$q \rightarrow p$$

- The *inverse* of an implication $p \rightarrow q$ is:

$$\neg p \rightarrow \neg q$$

- DO NOT have the same truth values as $p \rightarrow q$

Precedence of Logical Operators

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

$$p \wedge \neg q \vee r \rightarrow p \leftrightarrow s$$

$$\downarrow$$

$$((p \wedge (\neg q) \vee r) \rightarrow p) \leftrightarrow s$$

Translating from Natural language

- Example (Rosen):
  You cannot ride the rollercoaster if you are under 4 feet tall unless you are older than 16 years old.

q: You can ride the roller coaster
r: You are under 4 feet tall
s: You are older than 16 years old

$$(r \wedge \neg s) \rightarrow \neg q$$

q: You can ride the roller coaster
$\neg$ *r*: You are at least 4 feet tall
s: You are older than 16 years old

$$\neg(\neg r \vee s) \rightarrow \neg q$$

Consistency

- Translating natural language to logical expressions is essential to specifying system spec.
- Specifications are ***"consistent"*** when they do not conflict with one another. i.e.:

There must be an assignment of truth values to every expression that make all the expression true.

Consistency

- Whenever the system is being upgraded, users cannot access the file system.
- If users can access the file system, they can save new files.
- If users cannot save new files, the system is not being upgraded.

Consistency

- Whenever the system is being upgraded, users cannot access the file system. $p \to \neg q$
- If users can access the file system, they can save new files. $q \to r$
- If users cannot save new files, the system is not being upgraded. $\neg r \to \neg p$

p	q	r	$p \to \neg q$	$q \to r$	$\neg r \to \neg p$
T	F	T	T	T	T

These spec. are consistent.

Tautology, Contradiction, & Contingency

- A compound proposition that is always *true* is called a ***"tautology"***.
- A compound proposition that is always *false* is called a ***"contradiction"***.
- If neither a tautology nor a contradiction, it is called a ***"contingency"***.

Logical Equivalences

The propositions p and q are called "**logical equivalent**" ($p \equiv q$) if $p \leftrightarrow q$ is a tautology

Showing Logically Equivalent propositions

1 Show that the truth values of these propositions are always the same.

→ Construct truth tables.

Showing Logically Equivalent propositions

- Example (Rosen):
  Show that $p \rightarrow q \equiv \neg p \vee q$

p	q	$p \rightarrow q$	$\neg p$	$\neg p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Logically Equivalent

Showing Logically Equivalent propositions

1. Show that the truth values of these propositions are always the same.
2. Use series of established equivalences.

Logical Equivalences

- Distributive Laws
  $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- De Morgan's Laws
  $\neg (p \wedge q) \equiv \neg p \vee \neg q$
  $\neg (p \vee q) \equiv \neg p \wedge \neg q$
- More can be found in the textbook

Showing Logically Equivalent propositions

- Example (Rosen):
  Show that $\neg (p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$

$\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg(\neg p \wedge q)$ *De Morgan's*

$\equiv \neg p \wedge (\neg(\neg p) \vee \neg q)$ *De Morgan's*

$\equiv \neg p \wedge (p \vee \neg q)$ *Double negative*

$\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q)$ *Distributive*

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

$\equiv \neg p \wedge \neg q$

Predicate Logic

- In Propositional Logic, 'the atomic units' are propositions.
- E.g.:
  - *p*: John goes to school., *q*: Mary goes to school.
- In Predicate Logic, we look at each proposition as the combination of ***variables*** and ***predicates*** .
- E.g.:
  - X goes to school, where X can be John or Mary.

Predicate Logic

- The statement "*x* go to school" has two parts:
  Variable "*x*"
  The predicate "go to school"
- This statement can be denoted by *P(x)*, where *P* denotes the predicate "go to school".
- *P(x)* is said to be the value of the propositional function *P* at *x*.
- Once a value has been assigned to the variable *x*, the statement *P(x)* becomes a proposition and has a truth value.
- E.g: P(John) and P(Mary) have truth values.

Creating propositions from a propositional function

1. Assign values to all variables in a propositional function.
2. Use "Quantification"

Universal Quantifier

- $\forall x P(x)$ (read "for all x P(x)") denotes:

  P(x) is true for all values *x* in the universal of discourse.

- $\forall x P(x)$ is the same as:

  $$P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$$

  When all elements in the universe of discourse can be listed as $(x_1, x_2, \ldots, x_n)$

Universal Quantifier

- Example (Rosen):
- What is the truth value of $\forall x P(x^2 \geq x)$, when the universe of discourse consists of:
  - all real numbers?
  - all integers?

Since $x^2 \geq x$ only when $x \leq 0$ or $x \geq 1$, $\forall x P(x^2 \geq x)$ is false if the universe consists of all real numbers. However, it is true when the universe consists of only the integers.

Existential Quantifier

- $\exists x P(x)$ (read "for some x P(x)") denotes:

There exists an element x in the universe of discourse that $P(x)$ is true.

- $\exists x P(x)$ is the same as:

$$P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

When all elements in the universe of discourse can be listed as $(x_1, x_2, \ldots, x_n)$

Existential Quantifier

- Example (Rosen):
- What is the truth value of $\exists x P(x)$ where $P(x)$ is the statement $x^2 > 10$, and the universe of discourse consists of the positive integers not exceeding 4?

Since the elements in the universe can be listed as {1,2,3,4}, $\exists x P(x)$ is the same as $P(1) \vee P(2) \vee P(3) \vee P(4)$. There for $\exists x P(x)$ is true since $P(4)$ is true.

Negations

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Negation of

"Every 2nd year students loves Discrete math." is

"There is a 2nd year student who does not love Discrete math."

Negation of

"Some student in this class get 'A'." is

"None of the students in this class get 'A'."

Set

Sets

- A set is an unordered collection of objects.
  - Objects in a set are called "members" or "elements" of that set.
- Two sets are equal $\leftrightarrow$ they have the same elements

- Are {1,2,3} and {3,2,1} equal?
- Are {0,1,2} and {0,0,0,1,1,2} equal?

Set Builder Notation

- Stating the properties that all elements must have to be members.

O = {x | x is a prime number less than 100}
R = {x | x is a real number}
U = {x | x is any of the objects under consideration}

Subset

$$A \subseteq B \leftrightarrow \forall x \, (x \in A \rightarrow x \in B)$$

Proper Subset

$$A \subset B \leftrightarrow (A \subseteq B) \wedge (A \neq B)$$

For any set S, "$\varnothing \subseteq S$" and "$S \subseteq S$"

Cardinality

- For a set S, if there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a *finite set* and that n is the *cardinality* of S ($|S|=n$)
- A set is "infinite" if it is not finite.

Power Set

- Given a set S, the power set of S, ***P(S)***, is the set of all subsets of S
- If S has n elements, then $P(S)$ has 2^n elements.

- Examples (Rosen):

S	P(S)
{0,1,2}	{∅,{0},{1},{2},{0,1},{0,2},{1,2},{0,1,2}}
∅	{∅}
{∅}	{∅,{∅}}

Ordered n-tuple

- The *ordered n-tuple* $(a_1,a_2,..,a_n)$ is the ordered collection that has a_1 as its first element, a_2 as its second element,…, and an as its n^{th} element.

Two ordered n-tuples are equal ↔ each corresponding pair of their elements is equal

Cartesian Products

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

$$A_1 \times A_2 \times \ldots \times A_n = \{ (a_1,a_2,\ldots,a_n,) \mid a_i \in A_i \text{ for } i=1,2,..,n\}$$

- Examples:
- What is the Cartesian product AxBxC, where A={0,1}, B={j,k}, C={x,y,z}?

AxBxC={(0,j,x),(0,j,y),(0,j,z),(0,k,x),(0,k,y),(0,k,z),
(1,j,x),(1,j,y),(1,j,z),(1,k,x),(1,k,y),(1,k,z)}

Using Set Notation with Quantifiers

- Specify the universe of discourse .
- E.g.:

  $\forall x \in \mathbf{R}(x^2 \geq 0)$

  means "for every real number $x^2 \geq 0$"

  which is true.

Set Operations

- Union ($\cup$)
- Intersection ($\cap$)
- Difference ($-$)
- Complement ($'$)
- Symmetric difference ($\oplus$)

Symmetric Difference

- $A \oplus B$ is the set containing those elements in *either A or B* but *NOT in both A and B*.

Example:
$A = \{1,3,5\}$, $B = \{1,2,3\}$, $A \oplus B = \{2,5\}$

Principle of Inclusion-Exclusion

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

More general (Later in this course):

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \\ \Sigma|A_i| - \Sigma|A_i \cap A_j| + \Sigma|A_i \cap A_j \cap A_k| - \ldots \\ +(-1)^{n+1}| A_1 \cap A_2 \cap \ldots \cap A_n|$$

Set Identities

- Distributive Laws

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

  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- De Morgan's Laws

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

  $(A \cap B)' = A' \cup B'$
- More can be found in the textbook.

Showing that two sets have the same elements

1. Show that each set is a subset of the other.
2. Use set builder notation and logical equivalences.
3. Build membership tables.
4. Use set identities.

Proving Set Equality
Using membership table

- Example Show that $(A \cap B)' = A' \cup B'$

A	B	A′	B′	$A' \cup B'$	$(A \cap B)$	$(A \cap B)'$
0	0	1	1	1	0	1
0	1	1	0	1	0	1
1	0	0	1	1	0	1
1	1	0	0	0	1	0

Generalized Union and Intersection

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$

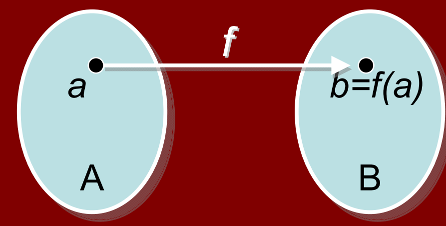
$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

Function

Functions

Definition:

- A function f from A to B is an assignment.
- assigns exactly one element of B to each of A



A: Domain
B: Codomain
b is *the image* of *a*.
a is *a pre-image* of *b*.
Range of f is the set of all images.

- Function cannot be "one-to-many".
- $\forall a \in A$, $f(a)$ must be assigned to some b.

Adding and Multiplying Functions

- Two real-valued functions *with the same domain* can be added and multiplied.

f_1, f_2 are functions from A to $\boldsymbol{R}$
$\rightarrow f_1+f_2$ and f_1f_2 are also functions from A to $\boldsymbol{R}$.

$$(f_1+f_2)(x) = f_1(x)+f_2(x)$$
$$(f_1f_2)(x) = f_1(x)f_2(x)$$

Adding and Multiplying Functions

- Example (Rosen):
- f_1, f_2 are functions from $\boldsymbol{R}$ to R. $f_1(x)=x^2$, $f_2(x)=x-x^2$. What are the functions f_1+f_2 and f_1f_2?

$$(f_1+f_2)(x) = f_1(x)+f_2(x) = x^2 + x - x^2 = x$$

$$(f_1f_2)(x) = f_1(x)f_2(x) = x^2 (x - x^2) = x^3 - x^4$$

One-to-one Functions

A function f is *one-to-one* or *injective*
$\leftrightarrow \forall x \forall y\ (\ f(x)=f(y) \rightarrow x=y\ )$

Examples (Rosen)
Determine whether these functions are one-to-one.

$f_1(x) = x^2$ from the set of integers to the set of integers
Since $f(1) = f(-1) = 1$, $f_1(x)$ is not one-to-one.

$f_2(x) = x+1$
$x+1 \neq y+1$ when $x \neq y$, then $f_2(x)$ is one-to-one.

Conditions Guaranteeing One-to-one

- Strictly increasing function:
  $\forall x\ \forall y\ (\ (x<y) \rightarrow (f(x)<f(y))\ )$
- Strictly decreasing function:
  $\forall x\ \forall y\ (\ (x<y) \rightarrow (f(x)>f(y))\ )$

where the universe of discourse = domain of *f*

Strictly increasing function
or
Strictly decreasing function
$\rightarrow$ one-to-one

Onto Functions

A function f is *onto* or *surjective*
$\leftrightarrow \forall y \exists x\ (\ f(x) = y\ )$

Examples (Rosen)
Determine whether these functions are onto.

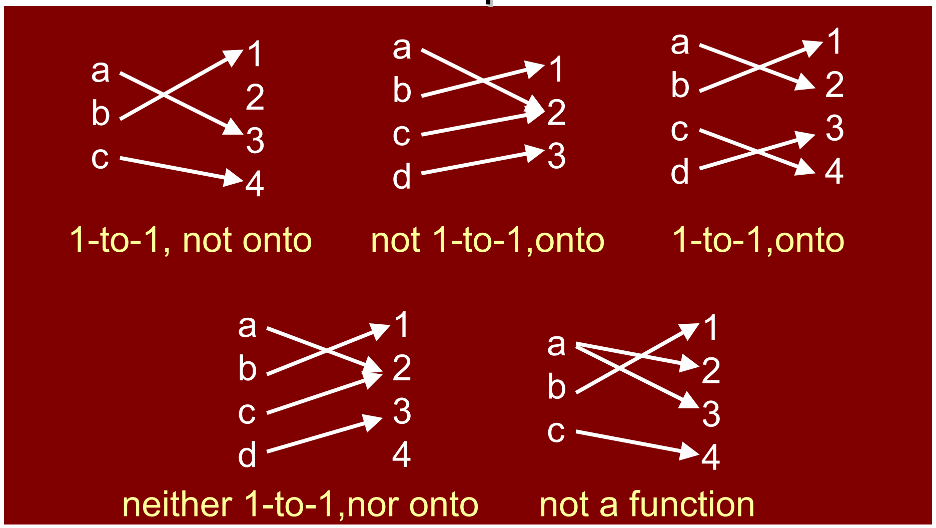
$f_1(x) = x^2$ from the set of integers to the set of integers
No, since there is no integer x that $f_1(x)=-1$

$f_2(x) = x+1$
Yes, for every $f_2(x)=y$, there is an integer $x=y-1$

One-to-one Correspondence

- *One-to-one* AND *Onto*
- Also called ***"bijection"***

Examples



Inverse Functions

- Let f be a *one-to-one correspondent* function from A to B.
- $f^{-1}(b)$ assigns to b, belonging to B, the unique element a, belonging to A, such that $f(a)=b$.

$$f^{-1}(b)=a \leftrightarrow f(a)=b$$

A function that is *NOT one-to-one correspondent* is *NOT invertible*.

Composite Functions

- $(f \bullet g)(a) = f(\ g(a)\ )$
- $f \bullet g$ cannot be defined unless the range of g is a subset of the domain of f.
- If f is a one-to-one correspondent function from A to B

$$(\ f^{-1} \bullet f\ )(a) = a, \quad a \in A$$
$$(\ f \bullet f^{-1}\ )(b) = b, \quad b \in B$$

Some Important Functions

- Floor function $\lfloor\ \rfloor$

  $\lfloor x \rfloor$ = the largest integer $\leq x$

- Ceiling function $\lceil\ \rceil$

  $\lceil x \rceil$ = the smallest integer $\geq x$

Examples

- Example (Rosen):
- Each byte is made up of 8 bits. How many bytes are required to encoded 100 bits of data?

$$\lceil 100/8 \rceil = \lceil 12.5 \rceil = 13 \text{ bytes}$$

Factorial Function

- $f(n) = n!$ is the product of the first n positive integers, so that

$$f(n) = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$$

$$\text{and } f(0) = 0! = 1$$

Logic: Key Terms

- Proposition
- Truth value
- Negation
- Logical Operator
- Compound proposition
- Truth table
- Disjunction
- Conjunction
- Exclusive or
- Implication
- Inverse
- Converse
- Contrapositive
- Biconditional
- Tautology
- Contradiction
- Contingency
- Consistency
- Logical equivalence
- Predicate
- Propositional function
- Universe of discourse
- Existential quantifier
- Universal quantifier

Sets: Key Terms

- Set
- Element
- Member
- Empty/Null set
- Universal set
- Venn diagram
- Set equality
- Subset
- Proper subset
- Finite set
- Infinite set
- Cardinality
- Power set
- Union
- Intersection
- Difference
- Complement
- Symmetric difference
- Membership table

Functions: Key Terms

- Function
- Domain
- Codomain
- Image
- Pre-image
- Range
- Onto / Surjection
- One-to-one / Injection
- One-to-one correspondence / bijection
- Inverse
- Composition
- Floor function
- Ceiling function
- Factorial

Relation

Relations

- A (binary) relation form A to B is a subset of AxB
- A *relation on the set A* is a *relation from A to A*
- A function from A to B is a relation from A to B
- Examples:

  $R_1 = \{(1,1),(1,2),(2,1),(2,3)\}$

  $R_2 = \{(a,b) \mid a = b \text{ or } a = -b\}$

  a and b are integers

Properties of Relations

- R on the set A is *reflexive* $\leftrightarrow \forall a\ ((a,a) \in R)$

Example: Consider relations on {1,2,3,4}

R must contain (1,1),(2,2),(3,3),(4,4)

R1 = {(1,1),(1,2),(1,3),(2,2),(3,3),(4,1),(4,4)} 

R2 = {(1,1),(2,1),(2,3),(3,1),(3,2),(3,3),(3,4),(4,4)} 

Symmetric and Antisymmetric

- R on a set A is *symmetric*
  $\leftrightarrow \forall a \forall b((a,b) \in R \rightarrow (b,a) \in R)$
- R on a set A is *antisymmetric*
  $\leftrightarrow \forall a \forall b(((a,b)\in R \land (b,a)\in R) \rightarrow (a=b))$
- These two are NOT opposite.

Symmetric and Antisymmetric

- *Symmetric* $\leftrightarrow \forall a \forall b((a,b) \in R \rightarrow (b,a) \in R)$
- *Antisym* $\leftrightarrow \forall a \forall b(((a,b)\in R \land (b,a)\in R) \rightarrow (a=b))$

<u>Example</u>:

	Sym	Antisym
$R_1 = \{(1,1),(1,2),(2,1)\}$		
$R_2 = \{(1,1),(1,2)\}$		
$R_3 = \{(a,b) \mid a = b \}$ (on Int.)		
$R_4 = \{(2,1)\}$		
$R_5 = \{(a,b) \mid a + b \leq 3\}$ (on Int.)		

Transitive Relations

- R on a set A is *transitive*
  $\leftrightarrow \forall a \forall b \forall c(((a,b)\in R \land (b,c)\in R) \rightarrow (a,c)\in R)$

$R_1 = \{(1,2),(2,3),(1,3),(1,4)\}$
$R_2 = \{(1,1),(1,2),(1,3),(2,4)\}$
$R_3 = \{(a,b) \mid a < b\}$

Combining Relations

- Since a relation is a set, we can apply all set operators to relations.
- <u>Example</u> (Rosen)
  $R_1 = \{(1,1),(2,2),(3,3)\}$,
  $R_2 = \{(1,1),(1,2),(1,3),(1,4)\}$

  $R_1 \cap R_2 = \{(1,1)\}$
  $R_1 - R_2 = \{(2,2),(3,3)\}$

Composite Relations

- R is a relation from A to B
- S is a relation from B to C
- $S \circ R$ = {(a,c)| $a \in A, c \in C$, and there exists $b \in B$ such that $(a,b) \in R$ and $(b,c) \in S$}

Composite Relations

- Example (Rosen):

  R is a relation from {1,2,3} to {1,2,3,4} with R={(1,1),(1,4),(2,3),(3,1),(3,4)} and S is a relation from {1,2,3,4} to {0,1,2} with S={(1,0),(2,0),(3,1),(3,2),(4,1)}.

  What is the composite of R and S?

  SoR = {(1,0),(1,1),(2,1),(2,2),(3,0),(3,1)}