

- ~~I am very available to students.~~
- ~~Start the homework assignments early~~
 - ~~Homework in this class requires “thinking time”~~
- ~~Read the textbook.~~
 - ~~Ask Questions! The textbook can be hard to follow—reading a dense, technical work is a “learning outcome” for this class~~

01-6: ~~Class Goals~~

- ~~Prove that there are some problems that cannot be solved~~
- ~~Show that there are some problems that (are believed to) require an exponential amount of time to solve (NP-Complete)~~
 - ~~Examine some strategies for dealing with these problems~~
- ~~Along the way, learn how to model computation mathematically, and pick up some useful formalisms & techniques~~
 - ~~DFA, regular expressions, CFGs, etc.~~

01-7: ~~Review of the Basics~~

- ~~Most (but perhaps not all) of the following material is review from discrete mathematics~~
- ~~I will go fairly fast, assuming it is review~~
 - ~~Ask me to slow down if you have any questions!~~

01-8: Sets – Definition

- A **set** is an unordered collection of objects
- $S = \{a, b, c\}$
 - a, b, c are **elements** or **members** of the set S

01-9: Sets – Definition

- A **set** is an unordered collection of objects
- $S = \{a, b, c\}$
 - a, b, c are **elements** or **members** of the set S
- Elements in a set need have no relation to each other
 - $S_1 = \{1, 2, 3\}$
 - $S_2 = \{\text{red, farmhouse, } \pi, -32\}$

01-10: Sets – Definition

- Sets can contain other sets as elements
 - $S_1 = \{3, \{3, 4\}, \{4, \{5, 6\}\}\}$

- $S_2 = \{\{1, 2\}, \{\{4\}\}\}$
- Sets do not contain duplicates
 - $\text{NotASet} = \{4, 2, 4, 5\}$

01-11: Sets – Cardinality

- **Cardinality** of a set is the number of elements in the set
 - $|\{a, b, c\}| = 3$
 - $|\{\{a, b\}, c\}| = ?$

01-12: Sets – Cardinality

- **Cardinality** of a set is the number of elements in the set
 - $|\{a, b, c\}| = 3$
 - $|\{\{a, b\}, c\}| = 2$ ($\{a, b\}$ and c)

01-13: Sets – Empty, Singleton

- **Empty Set:** $\{\}$ or \emptyset , $|\{\}| = |\emptyset| = 0$
- **Singleton set** – set with one element
 - $\{1\}$
 - $\{4\}$
 - $\{\}$?
 - $\{\{\}\}$?
 - $\{\{3, 1, 2\}\}$?

01-14: Sets – Empty, Singleton

- **Empty Set:** $\{\}$ or \emptyset , $|\{\}| = |\emptyset| = 0$
- **Singleton set** – set with one element
 - $\{1\}$
 - $\{4\}$
 - $\{\}$ NO! Set contains 0 elements
 - $\{\{\}\}$
 - $\{\{3, 1, 2\}\}$

01-15: Sets – Membership

- Set membership: $x \in S$
 - $3 \in \{1, 3, 5\}$
 - $a \notin \{b, c, d\}$
 - $3 \in \{1, \{2, 3\}\}$?
 - $\{\} \in \{1, 2, 3\}$?
 - $\{\} \in \{1, \{\}, 4\}$?

01-16: Sets – Membership

- Set membership: $x \in S$
 - $3 \in \{1, 3, 5\}$
 - $a \notin \{b, c, d\}$
 - $3 \notin \{1, \{2, 3\}\}$
 - $\{\} \notin \{1, 2, 3\}$
 - $\{\} \in \{1, \{\}, 4\}$

01-17: Sets – Describing

- Referring to sets
 - List all members
 - $\{3, 4, 5\}, \quad \{0, 1, 2, 3, \dots\}$
 - $S = \{x : x \text{ has a certain property}\}$
 $S = \{x \mid x \text{ has a certain property}\}$
 - $S = \{x : x \in \mathbf{N} \wedge x < 10\}$
 \mathbf{N} is the set of natural numbers $\{0, 1, 2, \dots\}$
 - $S = \{x : x \text{ is prime}\}$
 - $A \cup B = \{x : x \in A \vee x \in B\}$
 - $A \cap B = \{x : x \in A \wedge x \in B\}$
 - $A - B = \{x : x \in A \wedge x \notin B\}$

01-18: Sets – \cup, \cap

- More Union & Intersection
 - A and B are **disjoint** if $A \cap B = \{\}$
 - S is a collection of sets (set of sets)
 - $\bigcup S = \{x : x \in A \text{ for some } A \in S\}$
 - $\bigcup\{\{1, 2\}, \{2, 3\}\} = \{1, 2, 3\}$
 - $\bigcap S = \{x : x \in A \text{ for all } A \in S\}$
 - $\bigcap\{\{1, 2\}, \{2, 3\}\} = \{2\}$

01-19: Sets – Subset

- Subsets & Supersets
 - A is a subset of B , $A \subseteq B$ if:
 - $\forall x, x \in B \implies x \in A$
 - $\forall (x \in B), x \in A$
 - A is a proper subset of B , $A \subset B$ if:
 - $A \subseteq B \wedge (\exists x, x \in B \wedge x \notin A)$
 - $\{\}$ is a subset of any set (including itself)
 - $\{\}$ is the only set that does not have a proper subset

01-20: **Sets – Power Set**

- Power set: Set of all subsets
- $2^S = \{x : x \subseteq S\}$
 - $2^{\{a,b\}} = \{\{\}, \{a\}, \{b\}, \{a,b\}\}$
 - $2^{\{1\}} = \{\{\}\}$
- $|2^S| = ?$

01-21: **Sets – Power Set**

- Power set: Set of all subsets
- $2^S = \{x : x \subseteq S\}$
 - $2^{\{a,b\}} = \{\{\}, \{a\}, \{b\}, \{a,b\}\}$
 - $2^{\{1\}} = \{\{\}\}$
- $|2^S| = 2^{|S|}$

01-22: **Sets – Partition**

Π is a **partition** of S if:

- $\Pi \subset 2^S$
- $\{\} \notin \Pi$
- $\forall (X, Y \in \Pi), X \neq Y \implies X \cap Y = \{\}$
- $\bigcup \Pi = S$

$\{\{a, c\}, \{b, d, e\}, \{f\}\}$ is a partition of $\{a,b,c,d,e,f\}$

$\{\{a, b, c, d, e, f\}\}$ is a partition of $\{a,b,c,d,e,f\}$

$\{\{a, b, c\}, \{d, e, f\}\}$ is a partition of $\{a,b,c,d,e,f\}$

01-23: **Ordered Pair**

- (x, y) is an *ordered pair*
- Order matters – $(x, y) \neq (y, x)$ if $x \neq y$
 - hence *ordered*
- x and y are the **components** of the ordered pair (x, y)

01-24: **Cartesian Product**

$$A \times B = \{(x, y) : x \in A \wedge y \in B\}$$

- $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
- $\{1, 2\} \times \{1, 2\} = ?$
- $2^{\{a\} \times \{b\}} = ?$
- $2^{\{a\}} \times 2^{\{b\}} = ?$

01-25: **Cartesian Product**

$$A \times B = \{(x, y) : x \in A \wedge y \in B\}$$

- $\{1, 2\} \times \{3, 4\} = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$
- $\{1, 2\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$
- $2^{\{a\} \times \{b\}} = \{\{(a, b)\}, \{\}\}$
- $2^{\{a\}} \times 2^{\{b\}} = \{\{\{a\}, \{b\}\}, \{\{a\}, \{\}\}, \{\{\}, \{b\}\}, \{\{\}, \{\}\}\}$

01-26: **Cartesian Product**

Which of the following is true:

- $\forall(A, B) \quad A \times B = B \times A$
- $\forall(A, B) \quad A \times B \neq B \times A$
- None of the above

01-27: **Cartesian Product**

Which of the following is true:

- $\forall(A, B) \quad A \times B = B \times A$
 - If and only if $A = B$
- $\forall(A, B) \quad A \times B \neq B \times A$
 - If and only if $A \neq B$

01-28: **Cartesian Product**

- Why “Cartesian”?
 - Think “Cartesian Coordinates” (standard coordinate system)
 - $\mathbf{R} \times \mathbf{R}$ is the real plane
 - Set of all points (x, y) where $x, y \in \mathbf{R}$
 - \mathbf{R} is the set of real numbers (think “floats” if you’re CS)

01-29: **Cartesian Product**

- Can take the Cartesian product of > 2 sets.
- $A \times B \times C = \{(x, y, z) : x \in A, y \in B, z \in C\}$
- $\{a\} \times \{b, c\} \times \{d\} = \{(a, b, d), (a, c, d)\}$
- (Technically, $A \times B \times C = (A \times B) \times C$)
 - $\{a\} \times \{b, c\} \times \{d\} = \{((a, b), d), ((a, c), d)\}$
 - Often drop the extra parentheses for readability

01-30: **Relations**

- A **relation** R is a set of ordered pairs

- For example the relation $<$ over the Natural Numbers is the set:

$$\left\{ \begin{array}{l} (0,1), (0,2), (0,3), \dots \\ (1,2), (1,3), (1,4), \dots \\ (2,3), (2,4), (2,5), \dots \\ \dots \end{array} \right\}$$

01-31: **Relations**

- Often, relations are over the same set
 - that is, a subset of $A \times A$ for some set A
- Not all relations are over the same set, however
 - Relation describing prices of computer components
 $\{(Hard\ drive, \$55), (WAP, \$49), (256M\ DDR, \$44), \dots\}$

01-32: **Functions**

- A **function** is a special kind of relation (all functions are relations, but not all relations are functions)
- A relation $R \subseteq A \times B$ is a function if:
 - For each $a \in A$, there is exactly one ordered pair in R with the first component a

01-33: **Functions**

- A function f that is a subset of $A \times B$ is written: $f : A \mapsto B$
 - $(a, b) \in f$ is written $f(a) = b$
 - A is the domain of the function
 - if $A' \subseteq A$, $f(A') = \{b : a \in A' \wedge f(a) = b\}$ is the **image** of A'
 - The **range** of a function is the image of its domain

01-34: **Functions**

A function $f : A \mapsto B$ is:

- **one-to-one** if no two elements in A match to the same element in B
- **onto** Each element in B is mapped to by at least one element in A
- a **bijection** if it is both one-to-one and onto

The **inverse** of a binary relation $R \subset A \times B$ is denoted R^{-1} , and defined to be $\{(b, a) : (a, b) \in R\}$

- A function only has an inverse if ...

01-35: **Functions**

A function $f : A \mapsto B$ is:

- **one-to-one** if no two elements in A match to the same element in B
- **onto** Each element in B is mapped to by at least one element in A
- a **bijection** if it is both one-to-one and onto

The **inverse** of a binary relation $R \subset A \times B$ is denoted R^{-1} , and defined to be $\{(b, a) : (a, b) \in R\}$

- A function only has an inverse if it is a bijection

01-36: **Functions**

- What if we want to take the inverse of a function that is not a bijection – what can we do?
 - Want to preserve full information about the original function
 - Resulting inverse must be an actual function

01-37: **Functions**

- What if we want to take the inverse of a function that is not a bijection – what can we do?
 - Want to preserve full information about the original function
 - Resulting inverse must be an actual function
- How can we have an element map to 0, 1, or more elements, and still have a function? *HINT: If we modified the range ...*

01-38: **Functions**

- What if we want to take the inverse of a function that is not a bijection – what can we do?
 - Want to preserve full information about the original function
 - Resulting inverse must be an actual function

$$f : A \mapsto B \quad f^{-1} : B \mapsto 2^A$$

(example on chalkboard) 01-39: **Relations**

- Q and R are two relations
- The composition of Q and R , $Q \circ R$ is:

$$\{(a, b) : (a, c) \in Q, (c, b) \in R \text{ for some } c\}$$

$$Q = \{(a, c), (b, d), (c, a)\}$$

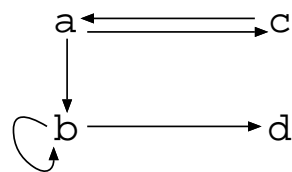
$$R = \{(a, c), (b, c), (c, a)\}$$

$$Q \circ R = \{(a, a), (c, c)\}$$

$Q \circ Q?$ $(Q \circ R) \circ Q?$ 01-40: **Relation Graph**

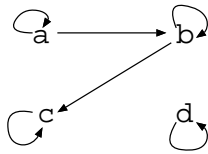
- Each element is a node in the graph
- if $(a, b) \in R$, then there is an edge from a to b in the graph

$$R = \{(a, b), (a, c), (c, a), (b, b), (b, d)\}$$

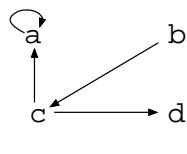


01-41: **Relation Types**

- A relation $R \subseteq A \times A$ is **reflexive** if
 - $(a, a) \in R$ for each $a \in A$
 - $\forall(a \in A), (a, a) \in R$
 - Each node has a self loop



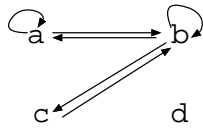
Reflexive



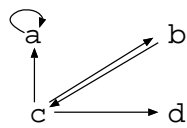
Not Reflexive

01-42: **Relation Types**

- A relation $R \subseteq A \times A$ is **symmetric** if
 - $(a, b) \in R$ whenever $(b, a) \in R$
 - $(a, b) \in R \implies (b, a) \in R$
 - Every edge goes “both ways”



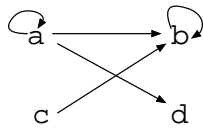
Symmetric



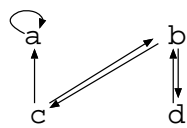
Not Symmetric

01-43: **Relation Types**

- A relation $R \subseteq A \times A$ is **antisymmetric** if
 - whenever $(a, b) \in R$, a, b are distinct $(b, a) \notin R$
 - $(a, b) \in R \wedge a \neq b \implies (b, a) \notin R$
 - No edge goes “both ways”



Antisymmetric

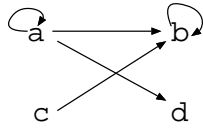


Not Antisymmetric

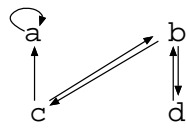
- Can a relation be neither symmetric nor antisymmetric?

01-44: **Relation Types**

- A relation $R \subseteq A \times A$ is **antisymmetric** if
 - whenever $(a, b) \in R$, a, b are distinct $(b, a) \notin R$
 - $(a, b) \in R \implies (b, a) \notin R$
 - No edge goes “both ways”



Antisymmetric

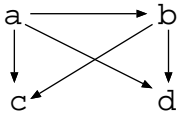


Not Antisymmetric

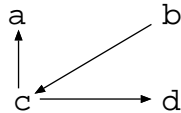
- Can a relation be both symmetric and antisymmetric?

01-45: **Relation Types**

- A relation $R \subseteq A \times A$ is **transitive** if
 - whenever $(a, b) \in R$, and $(b, c) \in R$, $(a, c) \in R$
 - $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$
 - Every path of length 2 has a direct edge



Transitive



Not Transitive

01-46: **Closure**

- A set $A \subseteq B$ is closed under a relation $R \subseteq ((B \times B) \times B)$ if:
 - $a_1, a_2 \in A \wedge ((a_1, a_2), c) \in R \implies c \in A$
 - That is, if a_1 and a_2 are both in A , and $((a_1, a_2), c)$ is in the relation, then c is also in A
- \mathbb{N} is closed under addition
- \mathbb{N} is not closed under subtraction or division

01-47: **Closure**

- Relations are also sets (of ordered pairs)
- We can talk about a relation R being closed over another relation R'
 - Each element of R' is an ordered triple of ordered pairs!

01-48: **Closure**

- Relations are also sets (of ordered pairs)
- We can talk about a relation R being closed over another relation R'
 - Each element of R' is an ordered triple of ordered pairs!
- Example:
 - $R \subseteq A \times A$
 - $R' = \{(((a, b), (b, c)), (a, c)) : a, b, c \in A\}$

- If R is closed under R' , then . . .

01-49: **Closure**

- Relations are also sets (of ordered pairs)
- We can talk about a relation R being closed over another relation R'
 - Each element of R' is an ordered triple of ordered pairs!
- Example:
 - $R \subseteq A \times A$
 - $R' = \{((a, b), (b, c)), (a, c) : a, b, c \in A\}$
 - If R is closed under R' , then R is transitive!

01-50: **Closure**

- **Reflexive closure** of a relation $R \subseteq A \times A$ is the smallest possible superset of R which is reflexive
 - Add self-loop to every node in relation
 - Add (a, a) to R for every $a \in A$
- **Transitive Closure** of a relation $R \subseteq A \times A$ is the smallest possible superset of R which is transitive
 - Add direct link for every path of length 2.
 - $\forall (a, b, c \in A)$ if $(a, b) \in R \wedge (b, c) \in R$ add (a, c) to R .

(examples on board) 01-51: **Relation Types**

- Equivalence Relation
 - Symmetric, Transitive, Reflexive
- Examples:
 - Equality ($=$)
 - A is the set of English words, $(w_1, w_2) \in R$ if w_1 and w_2 start with the same letter

(example graphs) 01-52: **Relation Types**

- Equivalence Relation
 - Symmetric, Transitive, Reflexive
- Separates set into equivalence classes (all words that start with a, for example)
- If $a \in A$, then $[a]$ represents equivalence class that contains a .

01-53: **Relation Types**

- Partial Order
 - Antisymmetric, Transitive, Reflexive
- Examples:

- \leq for integers

A is the set of integers, $(a, b) \in R$ if $a \leq b$

- Ancestor

$R \subseteq A \times A = \{(x, y) : x \text{ is an ancestor of } y, \text{ or } x = y\}$

(example graphs) 01-54: **Relation Types**

- Total Order

- $R \subseteq A \times A$ is a total order if:

- R is a partial order
- For all $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$
- Is \leq a total order?
- Is Ancestor a total order?

(example graphs) 01-55: **Cardinality**

- How can we tell if two sets A and B have the same cardinality?

01-56: **Cardinality**

- How can we tell if two sets A and B have the same cardinality?
 - Calculate $|A|$ and $|B|$, make sure numbers are the same
 - Match each element in A to an element in B
 - Create a bijection $f : A \mapsto B$
(or $f : B \mapsto A$)

01-57: **Cardinality**

- What about infinite sets? Are they all equinumerous (that is, have the same cardinality)?
- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .

01-58: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Even elements of \mathbb{N} ?

01-59: **Countable Sets**

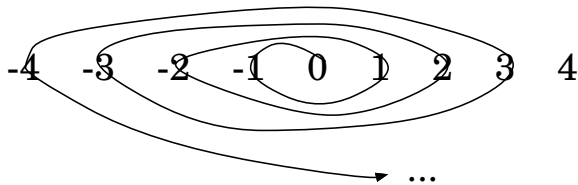
- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Even elements of \mathbb{N} ?
 - $f(x) = 2x$

01-60: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Integers (\mathbb{Z})?

01-61: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Integers (\mathbb{Z})?
 - $f(x) = \lceil \frac{x}{2} \rceil - 1^x$

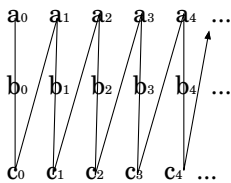


01-62: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Union of 3 (disjoint) countable sets A, B, C?

01-63: **Countable Sets**

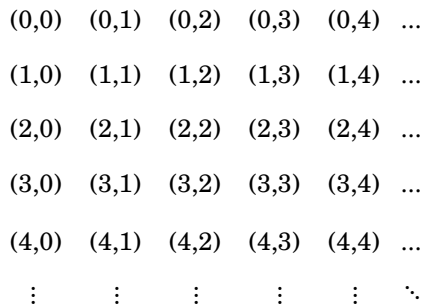
- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Union of 3 (disjoint) countable sets A, B, C?



- $f(x) = \begin{cases} a_{\frac{x}{3}} & \text{if } x \bmod 3 = 0 \\ b_{\frac{x-1}{3}} & \text{if } x \bmod 3 = 1 \\ c_{\frac{x-2}{3}} & \text{if } x \bmod 3 = 2 \end{cases}$

01-64: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - $\mathbb{N} \times \mathbb{N}$?



01-65: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .

- $\mathbb{N} \times \mathbb{N}$?

(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	...
(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	...
(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	...
(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	...
(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	...
⋮	⋮	⋮	⋮	⋮	⋮

- $f((x, y)) = \frac{(x+y)*(x+y+1)}{2} + x$

01-66: **Countable Sets**

- A set is **countable infinite** (or just **countable**) if it is equinumerous with \mathbb{N} .
 - Real numbers between 0 and 1 (exclusive)?

01-67: **Uncountable \mathbb{R}**

- Proof by contradiction
 - Assume that \mathbb{R} between 0 and 1 (exclusive) is countable
 - (that is, assume that there is some bijection from \mathbb{N} to \mathbb{R} between 0 and 1)
 - Show that this leads to a contradiction
 - Find some element of \mathbb{R} between 0 and 1 that is not mapped to by any element in \mathbb{N}

01-68: **Uncountable \mathbb{R}**

- Assume that there is some bijection from \mathbb{N} to \mathbb{R} between 0 and 1

0	0.3412315569...
1	0.0123506541...
2	0.1143216751...
3	0.2839143215...
4	0.2311459412...
5	0.8381441234...
6	0.7415296413...
⋮	⋮

01-69: **Uncountable \mathbb{R}**

- Assume that there is some bijection from \mathbb{N} to \mathbb{R} between 0 and 1

0	0.3412315569...
1	0.0123506541...
2	0.1143216751...
3	0.2839143215...
4	0.2311459412...
5	0.8381441234...
6	0.7415296413...
⋮	⋮

Consider: 0.425055...

01-70: **Proof Techniques**

- Three basic proof techniques used in this class
 - Induction
 - Diagonalization
 - Pigeonhole Principle

01-71: **Induction**

Can create exact postage for any amount $\geq \$0.08$ using only 3 cent and 5 cent stamps

01-72: **Induction**

Can create exact postage for any amount $\geq \$0.08$ using only 3 cent and 5 cent stamps

- Base case

Can create postage for 0.08 using one 5-cent and one 3-cent stamp

01-73: **Induction**

Can create exact postage for any amount $\geq \$0.08$ using only 3 cent and 5 cent stamps

- Inductive case
 - To show: if we can create exact postage for $\$x$ using only 3-cent and 5-cent stamps, we can create exact postage for $\$x + \0.01 using 3-cent and 5-cent stamps
 - Two cases:
 - Making change for $\$x$ uses at least one 5-cent stamp
 - Making change for $\$x$ uses no 5-cent stamps

01-74: **Induction**

- To show: if we can create exact postage for $\$x$ using only 3-cent and 5-cent stamps, we can create exact postage for $\$x + \0.01 using 3-cent and 5-cent stamps
 - Making change for $\$x$ uses at least one 5-cent stamp
 - Replace a 5-cent stamp with two 3-cent stamps to get $\$x + \0.01
 - Making change for $\$x$ uses no 5-cent stamps
 - Replace three 3-cent stamps with two 5-cent stamps to get $\$x + \0.01

01-75: **Pigeonhole Principle**

- A, B are finite sets, with $|A| > |B|$, then there is no one-to-one function from A to B
- If you have n pigeonholes, and $> n$ pigeons, and every pigeon is in a pigeonhole, there must be at least one hole with > 1 pigeon.

01-76: **Pigeonhole Principle**

- Show that in a relation R over a set A , if there is a path from a_i to a_j in R , then there is a path from a to b whose length is at most $|A|$.

01-77: **Pigeonhole Principle**

Proof by Contradiction

- Assume that there exists some shortest path from a_i to a_j of length $> |A|$.
- By pigeonhole principle, some element must repeat:
 - $\{a_i, \dots, a_k, \dots, a_k \dots a_j\}$
- We can create a shorter path by removing elements between a_k s.
- We've just found a shorter path from a_i to a_j – a contradiction