Graphs
(And Review)

Lecture 11

Register your i>Clicker!

<u>Exam</u>

Bring your ID!

More preparation material:
to be posted

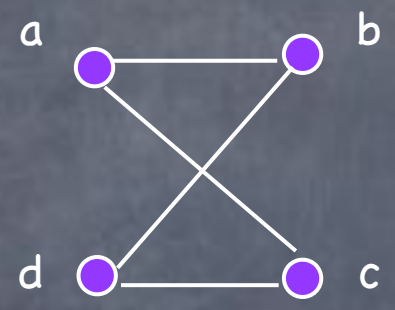
Graph Isomorphism

Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$

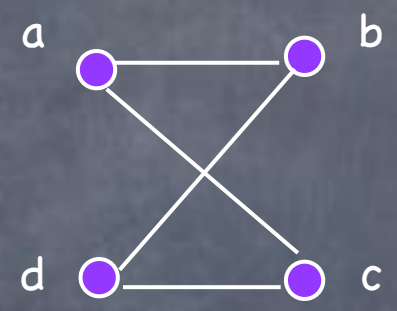
Graph Isomorphism

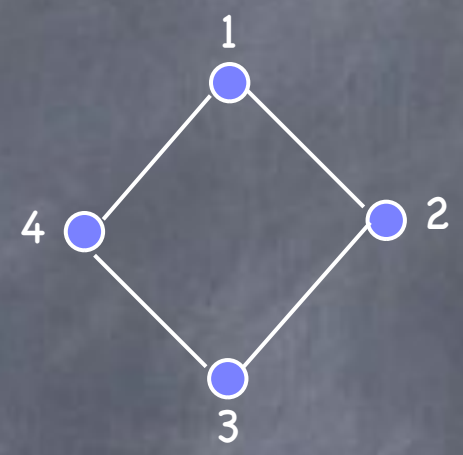
- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



Graph Isomorphism

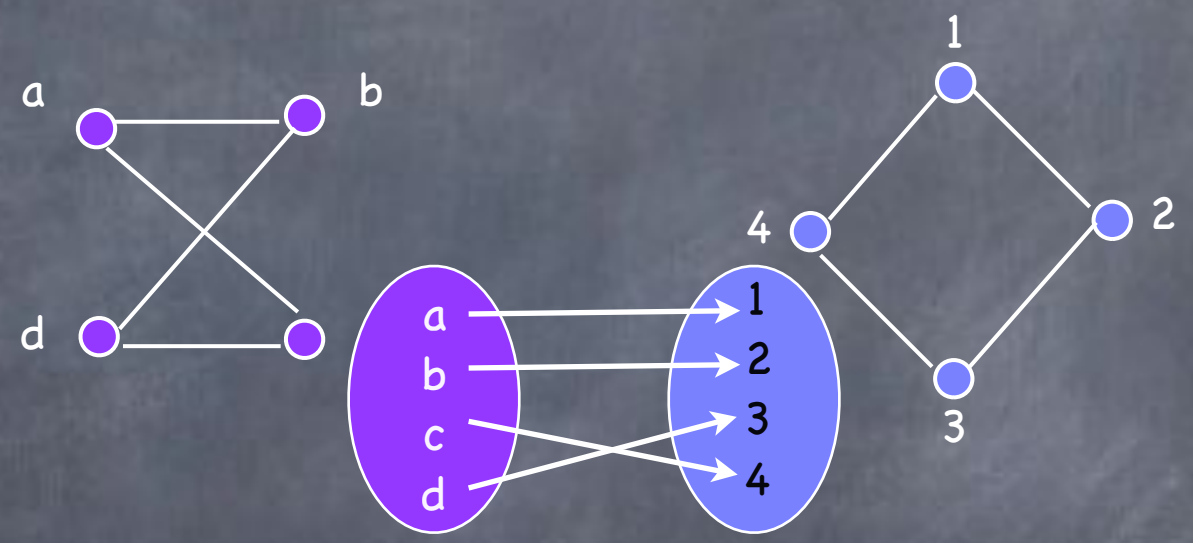
- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$





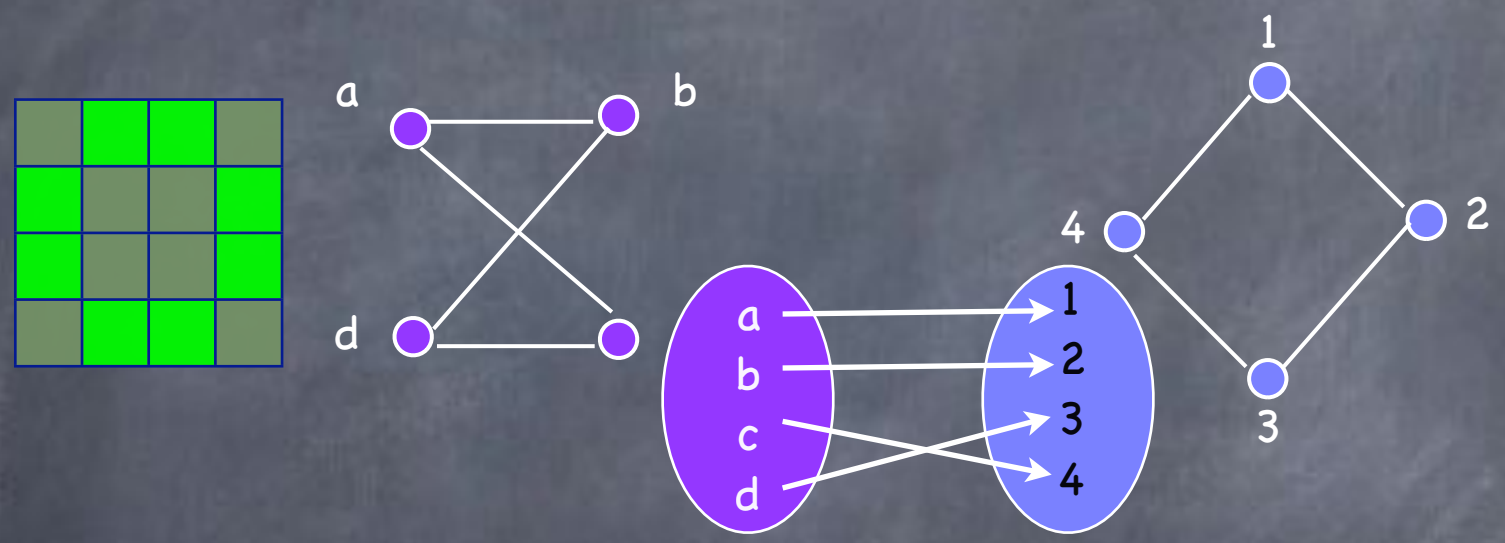
Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



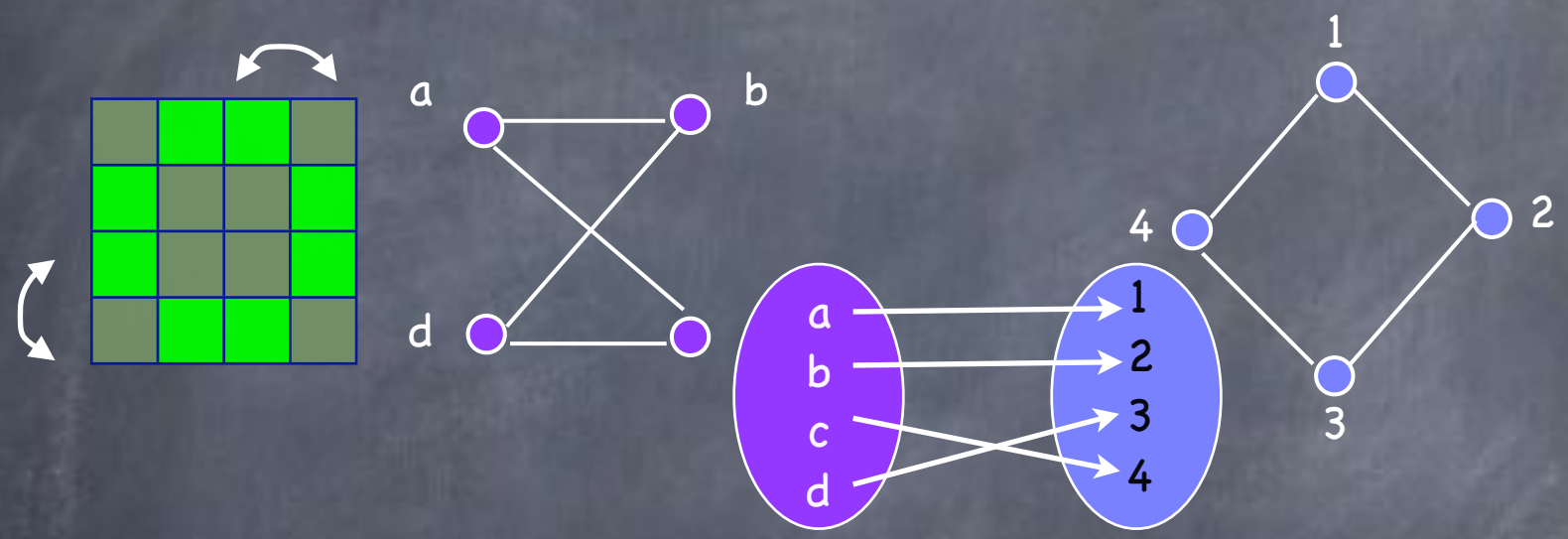
Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



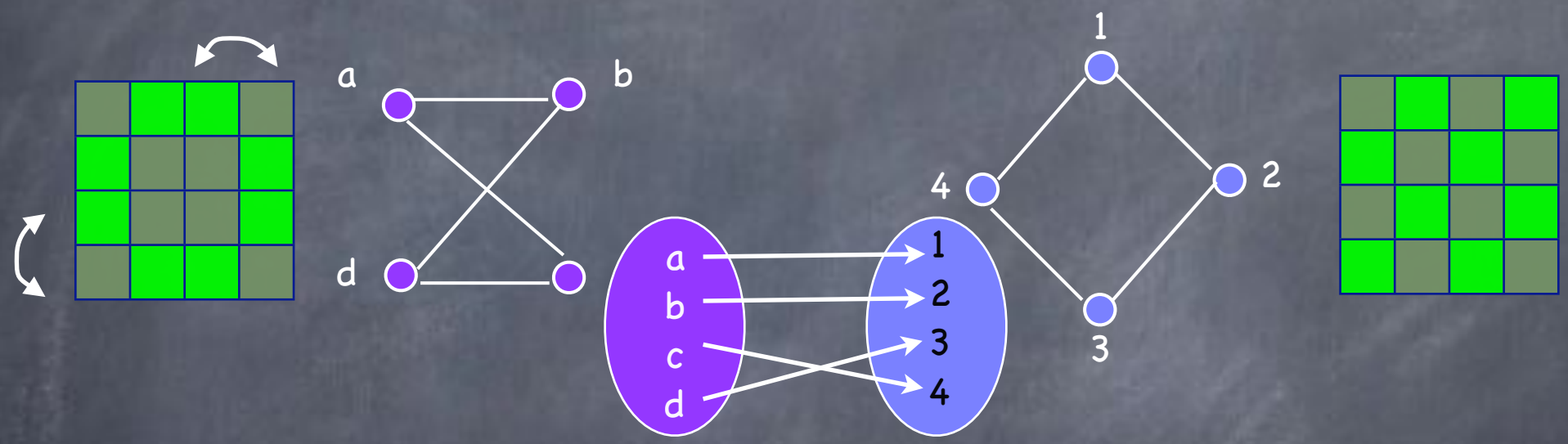
Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



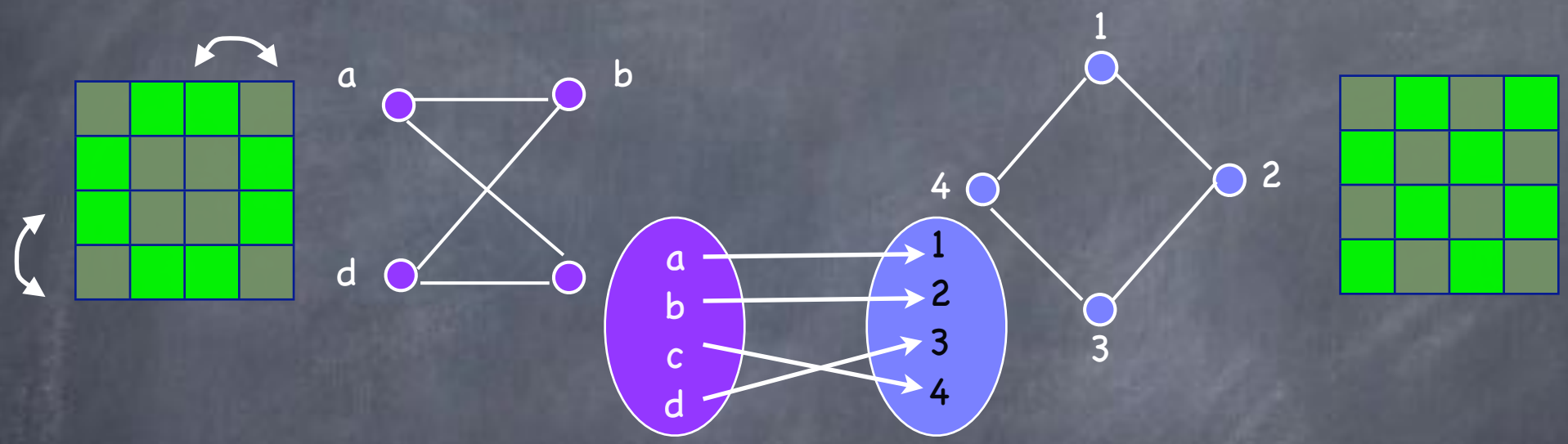
Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



Graph Isomorphism

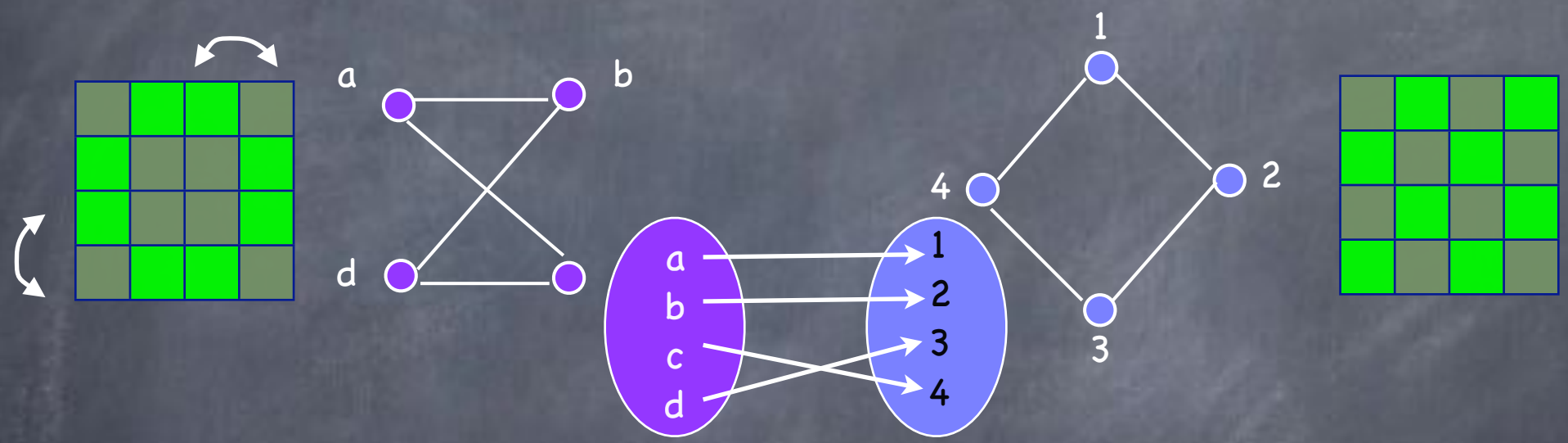
- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



- Computational problem: check if two graphs (given as adjacency matrices) are isomorphic

Graph Isomorphism

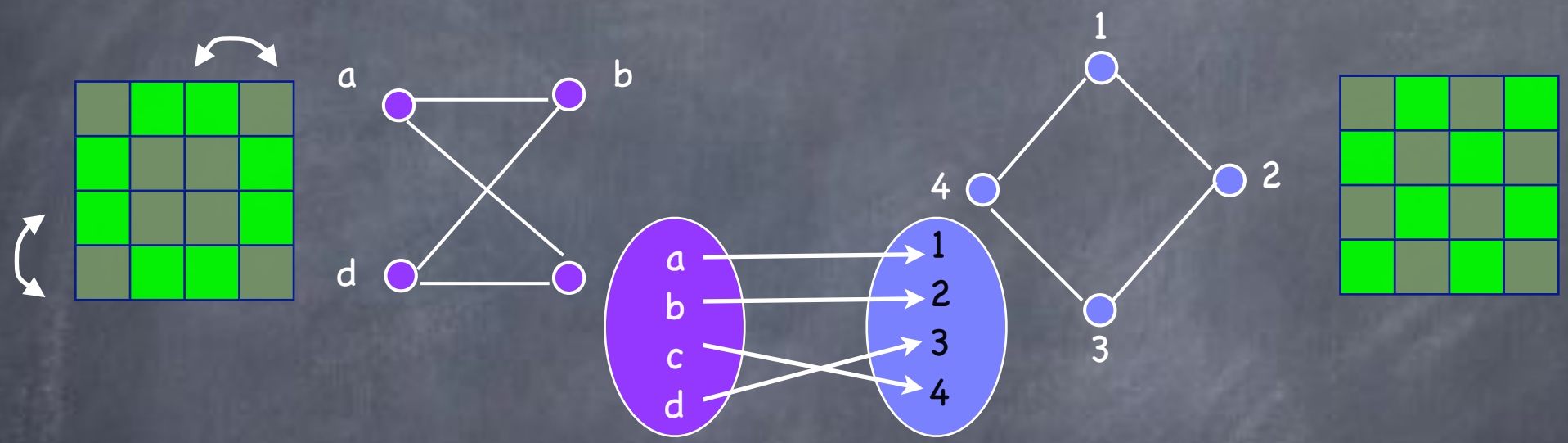
- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



- Computational problem: check if two graphs (given as adjacency matrices) are isomorphic
  - Can rule out if certain "invariants" are not preserved (e.g. $|V|,|E|$)

Graph Isomorphism

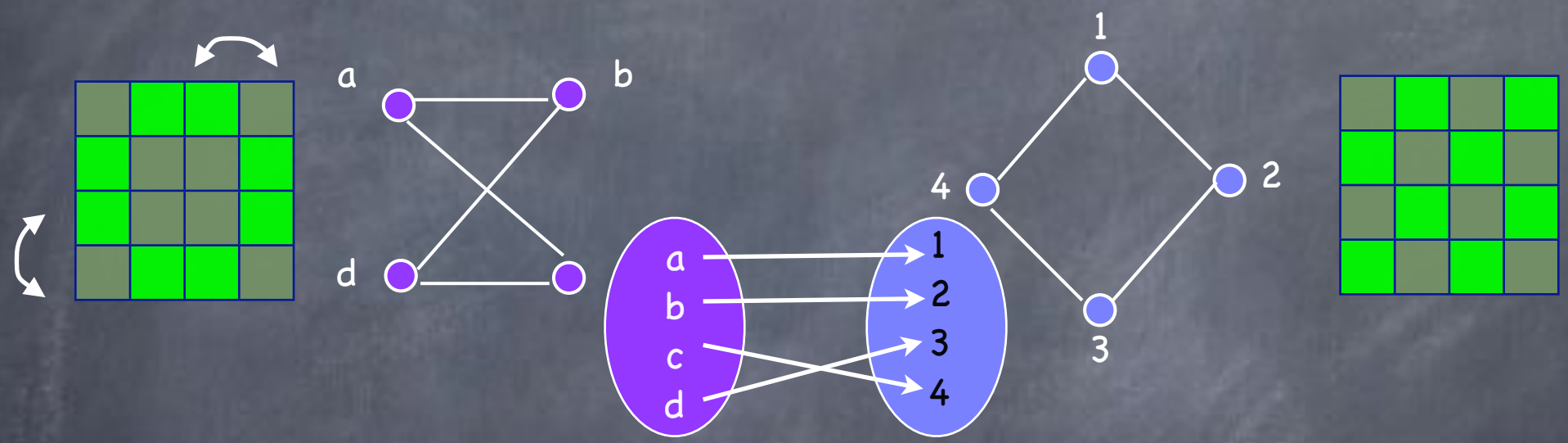
- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



- Computational problem: check if two graphs (given as adjacency matrices) are isomorphic
  - Can rule out if certain "invariants" are not preserved (e.g. $|V|,|E|$)
- In general, no "efficient" algorithm known, when graph is large

Graph Isomorphism

- $G_1 = (V_1,E_1)$ and $G_2 = (V_2,E_2)$ are isomorphic if there is a bijection $f:V_1 \rightarrow V_2$ such that $\{u,v\} \in E_1$ iff $\{f(u),f(v)\} \in E_2$



- Computational problem: check if two graphs (given as adjacency matrices) are isomorphic
  - Can rule out if certain "invariants" are not preserved (e.g. $|V|,|E|$)
- In general, no "efficient" algorithm known, when graph is large
  - Some believe no efficient algorithm "exists"

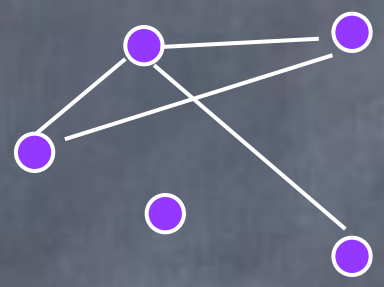
Degree of a node

Degree of a node

- Given a simple graph $G = (V,E)$, for each node $v \in V$, the degree of v is the number of edges incident on v

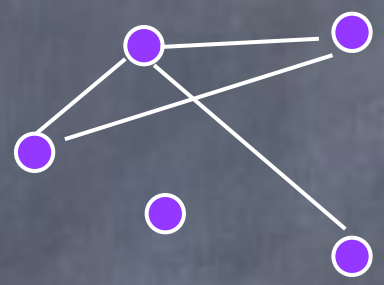
Degree of a node

- Given a simple graph G = (V,E), for each node v∈V, the degree of v is the number of edges incident on v



Degree of a node

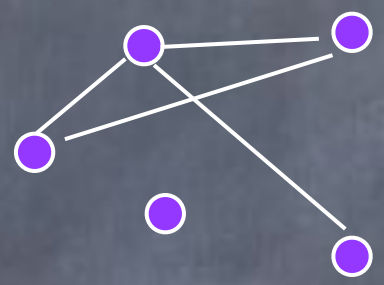
- Given a simple graph $G = (V,E)$, for each node $v \in V$, the degree of v is the number of edges incident on v



- Formally, $\deg(v) = |\{ u : \{u,v\} \in E \}|$

Degree of a node

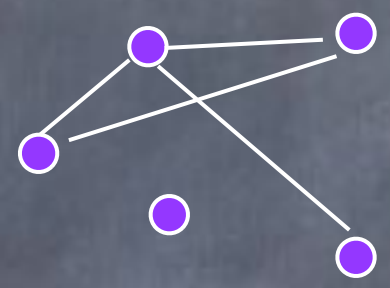
- Given a simple graph $G = (V,E)$, for each node $v \in V$, the degree of v is the number of edges incident on v



- Formally, $\deg(v) = |\{ u : \{u,v\} \in E \}|$
- Counting edges in two different ways: $2 \cdot |E| = \sum_{v \in V} \deg(v)$

Degree of a node

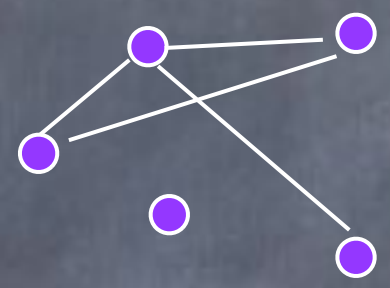
- Given a simple graph $G = (V,E)$, for each node $v \in V$, the degree of v is the number of edges incident on v



- Formally, $\deg(v) = |\{ u : \{u,v\} \in E \}|$
- Counting edges in two different ways: $2 \cdot |E| = \sum_{v \in V} \deg(v)$
- Degree sequence: sorted list of degrees. (e.g.: 0,1,2,2,3)

Degree of a node

- Given a simple graph $G = (V,E)$, for each node $v \in V$, the degree of v is the number of edges incident on v



- Formally, $\deg(v) = |\{ u : \{u,v\} \in E \}|$
- Counting edges in two different ways: $2 \cdot |E| = \sum_{v \in V} \deg(v)$
- Degree sequence: sorted list of degrees. (e.g.: 0,1,2,2,3)
- Degree sequence invariant under isomorphism

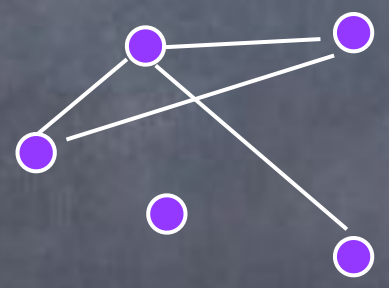
Subgraphs

Subgraphs

- A subgraph of $G = (V,E)$ is a graph $G' = (V',E')$ such that $V' \subseteq V$ and $E' \subseteq E$

Subgraphs

- A subgraph of $G = (V,E)$ is a graph $G' = (V',E')$ such that $V' \subseteq V$ and $E' \subseteq E$



Subgraphs

- A subgraph of $G = (V,E)$ is a graph $G' = (V',E')$ such that $V' \subseteq V$ and $E' \subseteq E$

Subgraphs

- A subgraph of $G = (V,E)$ is a graph $G' = (V',E')$ such that $V' \subseteq V$ and $E' \subseteq E$

- If G_1 and G_2 are isomorphic, then every subgraph of G_1 is isomorphic to some subgraph of G_2

Walks, Paths & Cycles

Walks, Paths & Cycles

- A walk (of length k, $k \geq 0$) from node a to node b is a sequence of nodes $(v_0, v_1, \ldots, v_k)$ such that

Walks, Paths & Cycles

- A walk (of length k, $k \geq 0$) from node a to node b is a sequence of nodes $(v_0, v_1, \ldots, v_k)$ such that
  - $v_0 = a$, $v_k = b$

Walks, Paths & Cycles

- A <u>walk</u> (of length k, $k \geq 0$) from node a to node b is a sequence of nodes $(v_0, v_1, \ldots, v_k)$ such that
  - $v_0 = a$, $v_k = b$
  - for all $i \in \{0,\ldots,k-1\}$, the edge $\{v_i,v_{i+1}\} \in E$

Walks, Paths & Cycles

- A <u>walk</u> (of length k, $k \geq 0$) from node a to node b is a sequence of nodes $(v_0, v_1, \ldots, v_k)$ such that
  - $v_0 = a$, $v_k = b$
  - for all $i \in \{0,\ldots,k-1\}$, the edge $\{v_i,v_{i+1}\} \in E$
- If a walk has no node repeating, then it is called a <u>path</u>

Walks, Paths & Cycles

- A walk (of length k, $k \geq 0$) from node a to node b is a sequence of nodes $(v_0, v_1, \ldots, v_k)$ such that
  - $v_0 = a$, $v_k = b$
  - for all $i \in \{0,\ldots,k-1\}$, the edge $\{v_i,v_{i+1}\} \in E$
- If a walk has no node repeating, then it is called a path
- If a walk of length > 2 has $v_0=v_k$, but no other two nodes are equal, then it is called a cycle

Walks, Paths & Cycles

- A <u>walk</u> (of length k, $k \geq 0$) from node a to node b is a sequence of nodes (v_0, v_1, … , v_k) such that
  - $v_0 = a$, $v_k = b$
  - for all $i \in \{0,\ldots,k-1\}$, the edge $\{v_i,v_{i+1}\} \in E$
- If a walk has no node repeating, then it is called a <u>path</u>
- If a walk of length > 2 has $v_0=v_k$, but no other two nodes are equal, then it is called a <u>cycle</u>
  - In a simple graph, a cycle is of length at least 3

Walks, Paths & Cycles

- A walk (of length k, $k \geq 0$) from node a to node b is a sequence of nodes (v_0, v_1, … , v_k) such that
  - $v_0 = a$, $v_k = b$
  - for all $i \in \{0,\ldots,k-1\}$, the edge $\{v_i,v_{i+1}\} \in E$
- If a walk has no node repeating, then it is called a path
- If a walk of length > 2 has $v_0=v_k$, but no other two nodes are equal, then it is called a cycle
  - In a simple graph, a cycle is of length at least 3
- A graph is acyclic if it has no cycles (i.e., no C_k is a subgraph of G)

Connectivity

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v
- Relation Connected(u,v) is an equivalence relation

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v
- Relation Connected(u,v) is an equivalence relation
  - Reflexive, Symmetric and Transitive

Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v
- Relation Connected(u,v) is an equivalence relation
  - Reflexive, Symmetric and Transitive

Walks can be spliced together to get walks

Connectivity

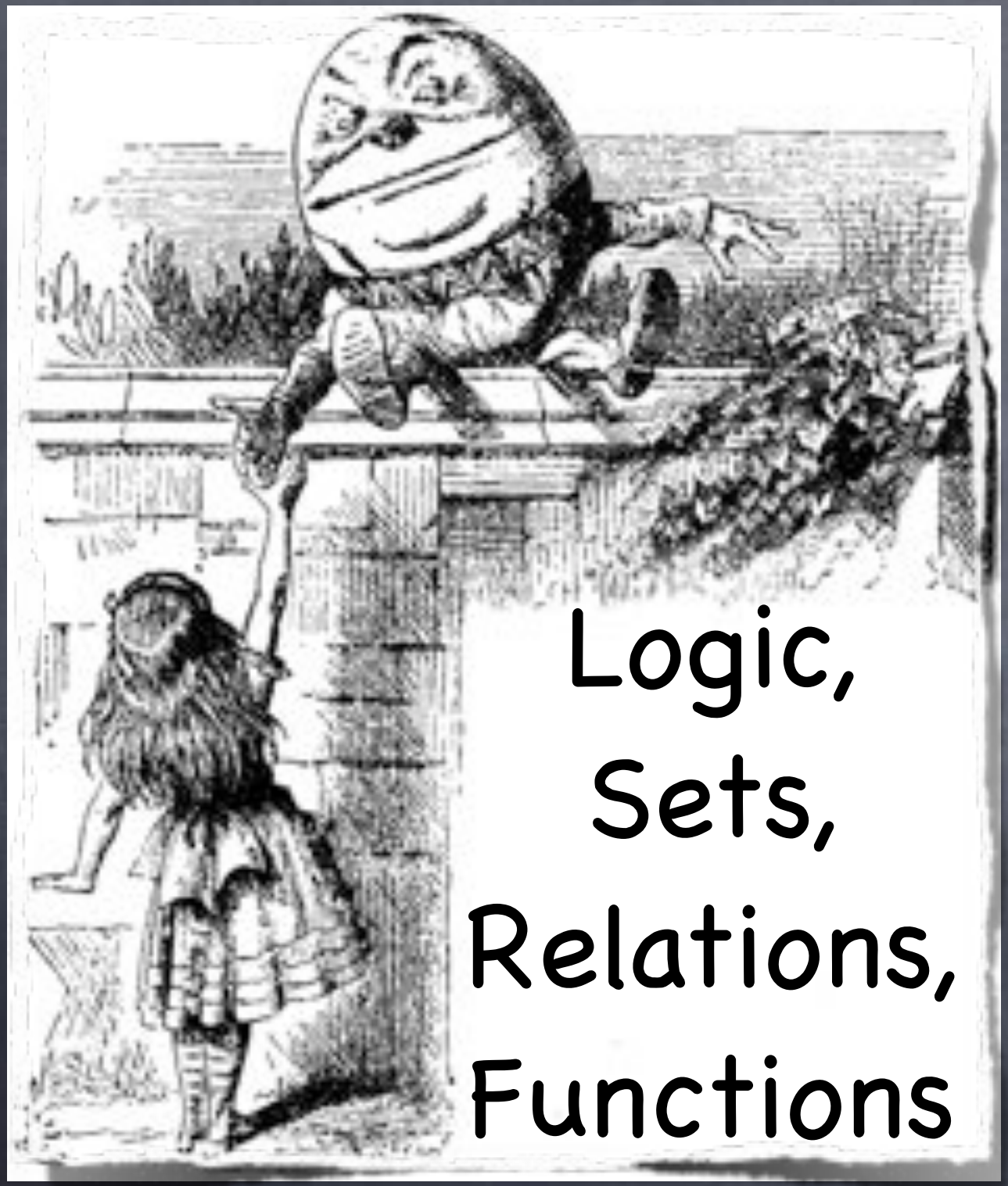
- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v
- Relation Connected(u,v) is an equivalence relation
  - Reflexive, Symmetric and Transitive

    Walks can be spliced together to get walks
  - Equivalence classes of this relation are called the connected components of G

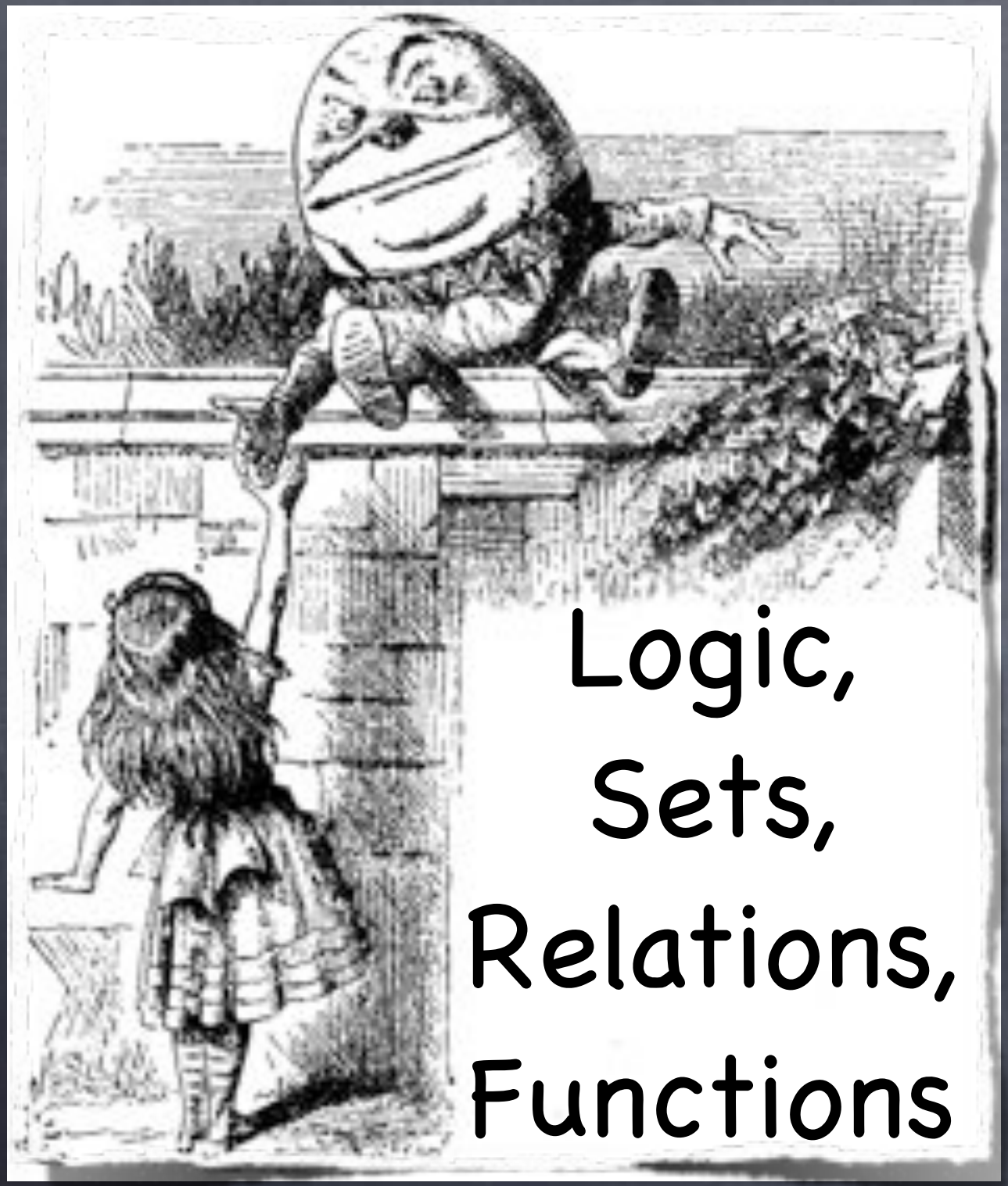
Connectivity

- Given a graph G, whether there is a path between two nodes u and v is an important question regarding G
  - u is said to be connected to v if there is such a path
  - u connected to v iff there is a walk from u to v
- Relation Connected(u,v) is an equivalence relation
  - Reflexive, Symmetric and Transitive

    Walks can be spliced together to get walks
  - Equivalence classes of this relation are called the connected components of G
- Number of edges in the shortest path between u and v is called the distance between u and v



Logic, Sets, Relations, Functions



Logic, Sets, Relations, Functions

Review
(continued)

Question

Question

- $\overline{R \cup (S \cap T)}$ =

  A. $\overline{R} \cap \overline{S} \cap \overline{T}$
  B. $(\overline{R} \cap \overline{S}) \cup (\overline{R} \cap \overline{T})$
  C. $(\overline{R} \cup \overline{S}) \cap (\overline{R} \cup \overline{T})$
  D. $\overline{R} \cup (\overline{S} \cap \overline{T})$
  E. None of the above

Question

- $\overline{R \cup (S \cap T)} =$

$\overline{R} \cap (\overline{S \cap T}) = \overline{R} \cap (\overline{S} \cup \overline{T})$

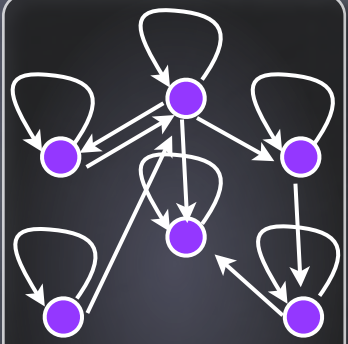
A. $\overline{R} \cap \overline{S} \cap \overline{T}$
B. $(\overline{R} \cap \overline{S}) \cup (\overline{R} \cap \overline{T})$
C. $(\overline{R} \cup \overline{S}) \cap (\overline{R} \cup \overline{T})$
D. $\overline{R} \cup (\overline{S} \cap \overline{T})$
E. None of the above

Question

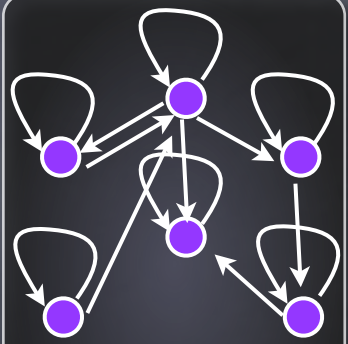
Question

- For two sets S,T, which is a valid proof approach for showing that S = T

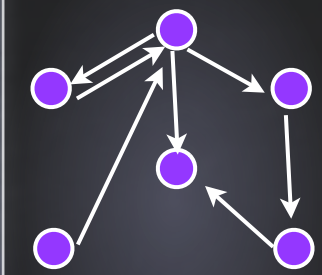
  A. Suppose $x \in S$. Then argue $x \in T$.
  B. Suppose $x \notin S$. Then argue $x \notin T$.
  C. Either A or B
  D. A & B together
  E. None of the above



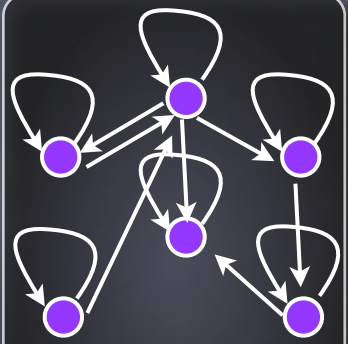
Reflexive:
All self-loops



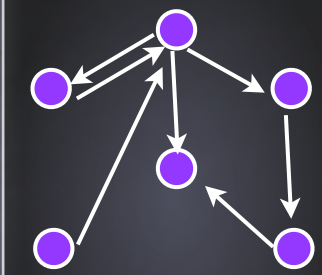
Reflexive:
All self-loops



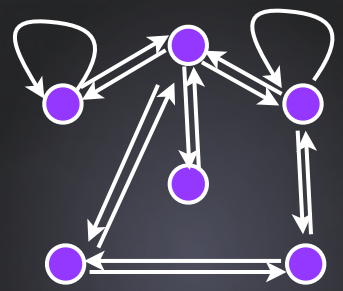
Irreflexive:
No self-loops



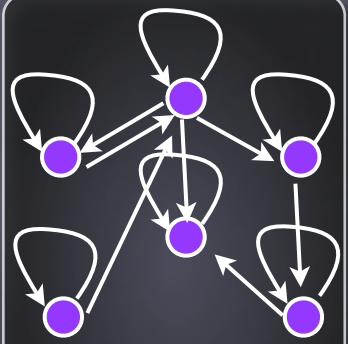
Reflexive:
All self-loops



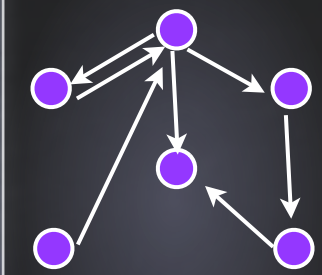
Irreflexive:
No self-loops



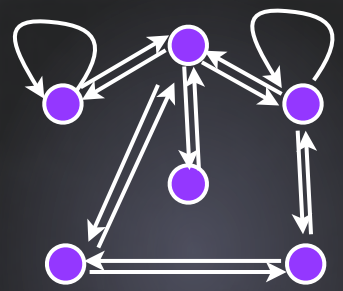
Symmetric:
Only self-loops &
bidirectional edges



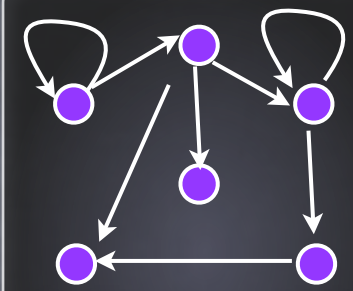
Reflexive:
All self-loops



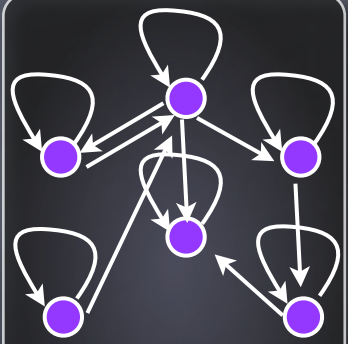
Irreflexive:
No self-loops



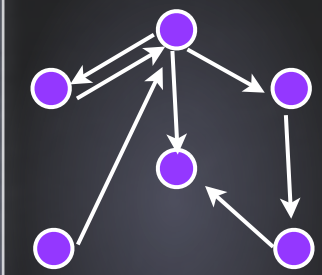
Symmetric:
Only self-loops &
bidirectional edges



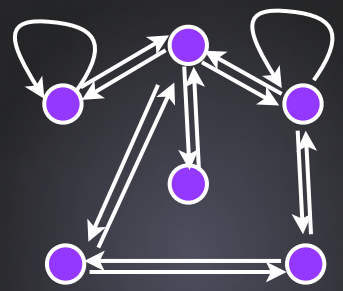
Anti-symmetric:
No bidirectional
edges



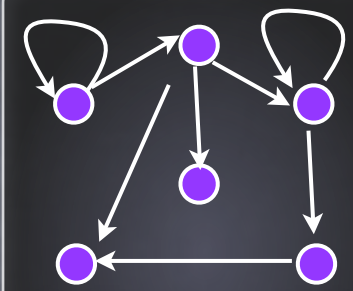
Reflexive:
All self-loops



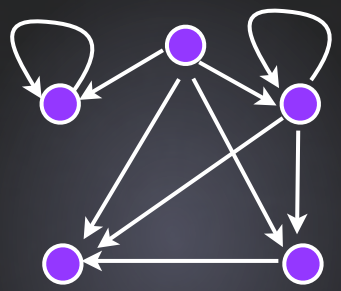
Irreflexive:
No self-loops



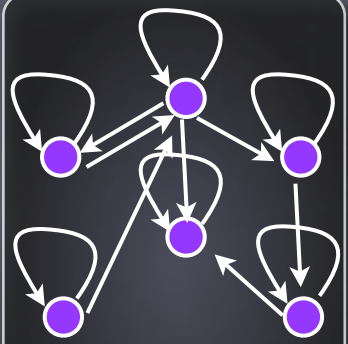
Symmetric:
Only self-loops &
bidirectional edges



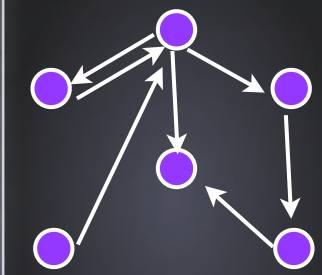
Anti-symmetric:
No bidirectional
edges



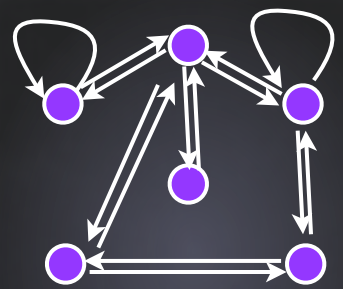
Transitive:
Path from a to b
implies edge (a,b)



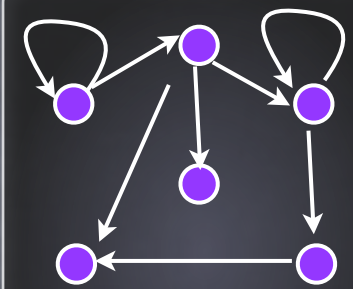
Reflexive:
All self-loops



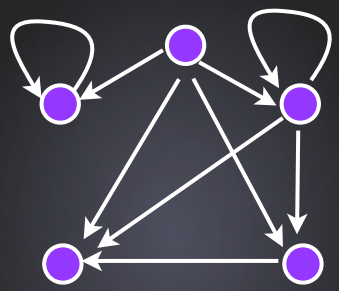
Irreflexive:
No self-loops



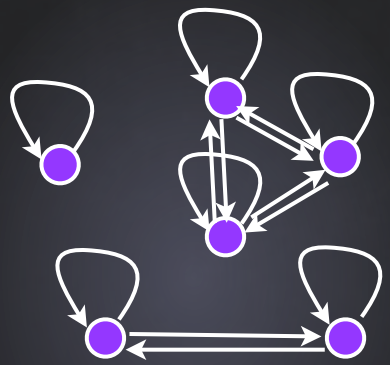
Symmetric:
Only self-loops & bidirectional edges



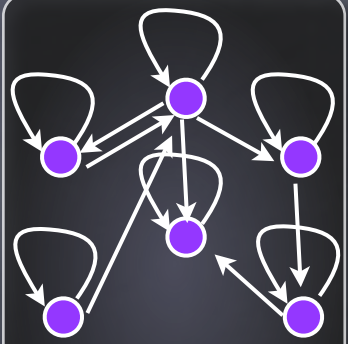
Anti-symmetric:
No bidirectional edges



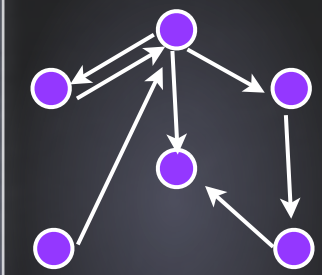
Transitive:
Path from a to b implies edge (a,b)



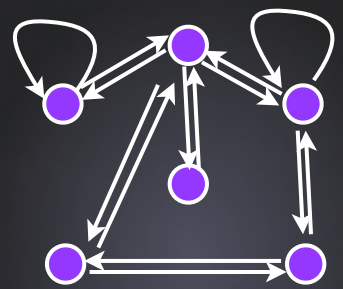
Equivalence:
Cliques, disconnected from each other



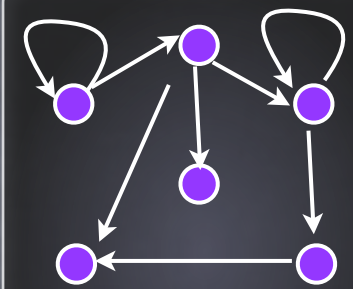
Reflexive:
All self-loops



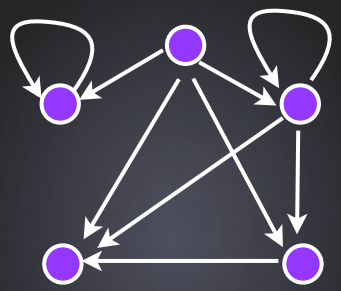
Irreflexive:
No self-loops



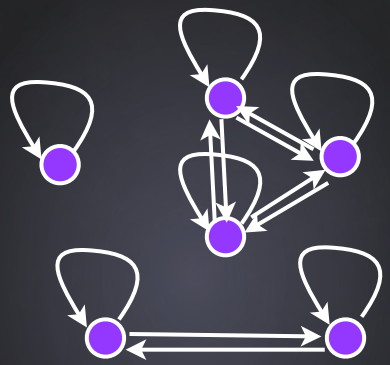
Symmetric:
Only self-loops & bidirectional edges



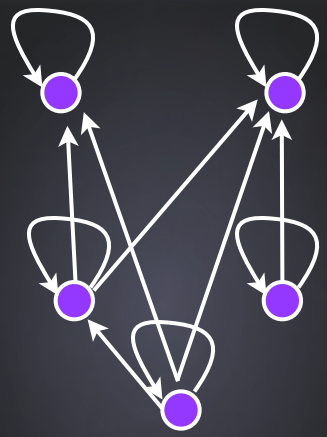
Anti-symmetric:
No bidirectional edges



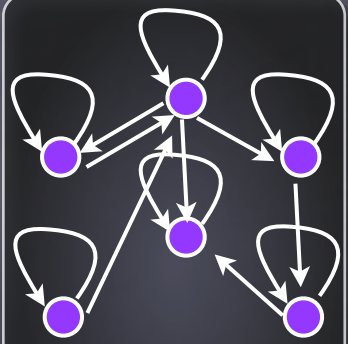
Transitive:
Path from a to b implies edge (a,b)



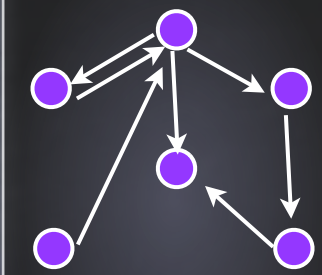
Equivalence:
Cliques, disconnected from each other



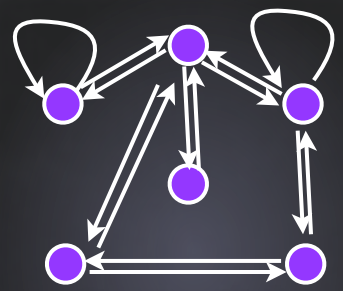
Partial Order:
Reflexive, with no cycles



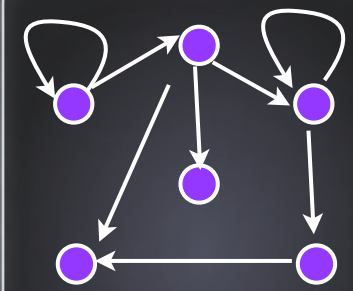
Reflexive:
All self-loops



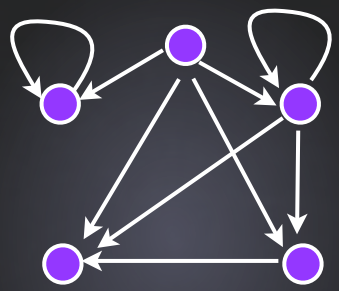
Irreflexive:
No self-loops



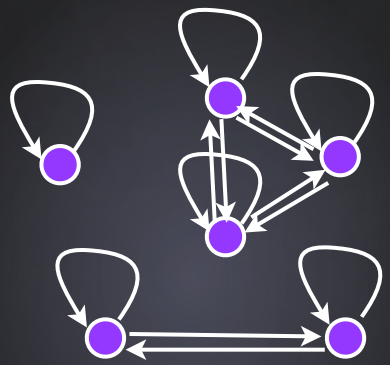
Symmetric:
Only self-loops & bidirectional edges



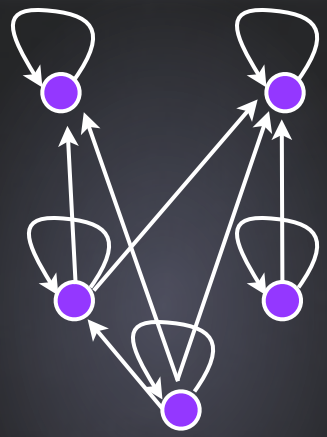
Anti-symmetric:
No bidirectional edges



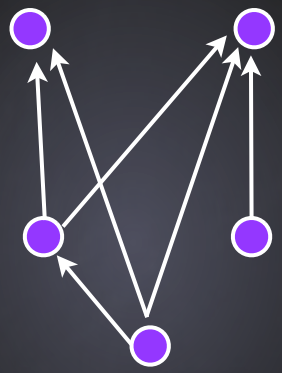
Transitive:
Path from a to b implies edge (a,b)



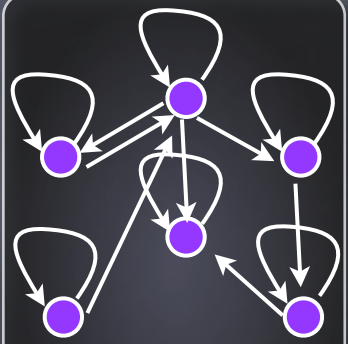
Equivalence:
Cliques, disconnected from each other



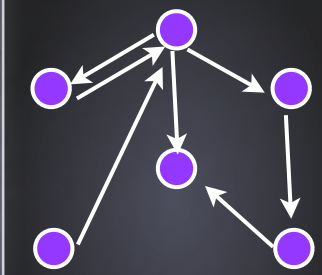
Partial Order:
Reflexive, with no cycles



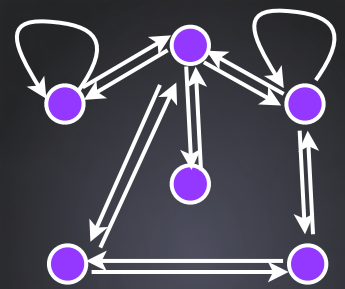
Strict partial Order:
Irreflexive, with no cycles



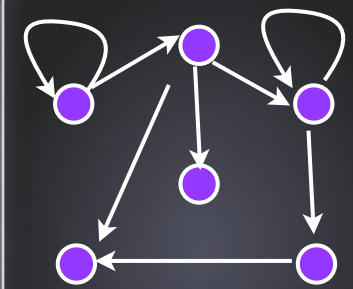
Reflexive:
All self-loops



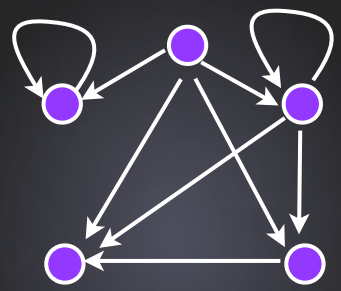
Irreflexive:
No self-loops



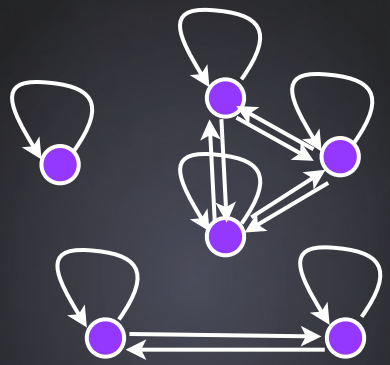
Symmetric:
Only self-loops &
bidirectional edges



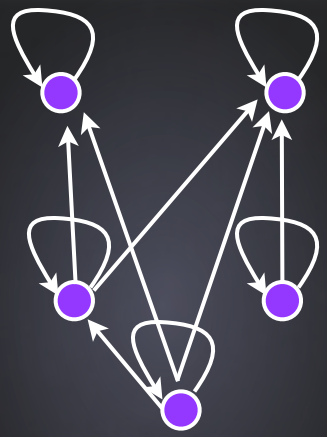
Anti-symmetric:
No bidirectional
edges



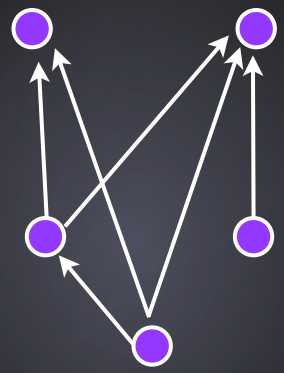
Transitive:
Path from a to b
implies edge (a,b)



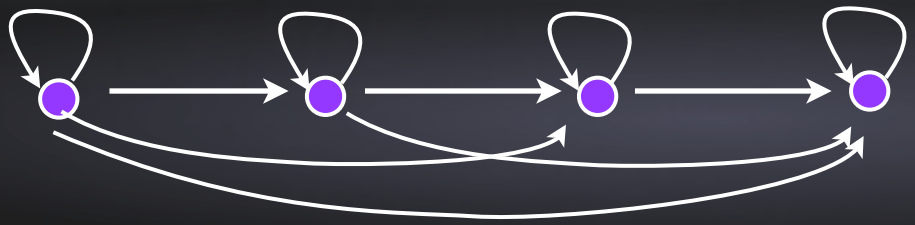
Equivalence:
Cliques, disconnected
from each other



Partial Order:
Reflexive, with no
cycles



Strict partial Order:
Irreflexive, with no
cycles



Total (or Linear) Order:
Partial order, with
an edge between every pair

Question

- Find the wrong statement

  A. $(\forall a,b \quad a \sqsubset b) \rightarrow \sqsubset$ is an equivalence relation
  B. $(\forall a,b \quad \neg(a \sqsubset b)) \rightarrow \sqsubset$ is a partial order
  C. if $\sqsubset$ is a strict partial order, it is not a partial order
  D. if $\sqsubset$ is a linear order, it is a partial order
  E. None of the above

Types of Functions

Types of Functions

- Function $f:A \to B$. Every $x \in A$ has exactly one image $f(x)$
- Onto Function: Every $y \in B$ has <u>at least</u> one pre-image (x s.t. $y=f(x)$)
  - $|Im(f)| = |B| \leq |A|$
- One-to-One function: Every $y \in B$ has <u>at most</u> one pre-image
  - $|Im(f)| = |A| \leq |B|$
- Bijection: Every $y \in B$ has <u>exactly</u> one pre-image
  - $|Im(f)| = |A| = |B|$
- Strictly increasing/strictly decreasing functions are one-to-one
- Function Composition: $g \circ f : Dom_f \to CoDom_g$, $g \circ f(x) = g(f(x))$
- A one-to-one function f is invertible: $\exists g$ s.t. $g \circ f \equiv Id$
- A bijection f has a unique inverse f^{-1}. f and f^{-1} are inverses of each other

Question

- Below $f:\mathbb{Z}\rightarrow\mathbb{Z}$ and $g:\mathbb{Z}\rightarrow\mathbb{Z}$ defined as follows:

  $f(x) = 5x$, and $g(x)=\lfloor x/5 \rfloor$. Then:

  A. $f\circ g$ is identity over $\mathbb{Z}$
  B. $g\circ f$ is identity over $\mathbb{Z}$
  C. $f\circ g$ is not well-defined
  D. $g\circ f$ is not well-defined
  E. None of the above

Question

- Below $f:\mathbb{Z}\to\mathbb{Z}$ and $g:\mathbb{Z}\to\mathbb{Z}$ defined as follows:

  $f(x) = 5x$, and $g(x)=\lfloor x/5 \rfloor$. Then:

  A. $f\circ g$ is identity over $\mathbb{Z}$

  $f\circ g(x) = 5 \lfloor x/5 \rfloor \in [x-4,x]$

  B. $g\circ f$ is identity over $\mathbb{Z}$

  C. $f\circ g$ is not well-defined

  D. $g\circ f$ is not well-defined

  E. None of the above

Question

- Below $f:\mathbb{Z}\to\mathbb{Z}$ and $g:\mathbb{Z}\to\mathbb{Z}$ defined as follows:

  $f(x) = 5x$, and $g(x)=\lfloor x/5 \rfloor$. Then:

  A. $f\circ g$ is identity over $\mathbb{Z}$

  $f\circ g(x) = 5 \lfloor x/5 \rfloor \in [x-4,x]$

  B. $g\circ f$ is identity over $\mathbb{Z}$

  $g\circ f(x) = \lfloor 5x/5 \rfloor = x$

  C. $f\circ g$ is not well-defined

  D. $g\circ f$ is not well-defined

  E. None of the above

Numb3rs

Review

Division

- For any two integers a and b, $a \neq 0$, there is a <u>unique</u> quotient q and remainder r, such that
$$b = q \cdot a + r, \quad \text{and } 0 \leq r < |a|$$

-2	-14	-13	-12	-11	-10	-9	-8
-1	-7	-6	-5	-4	-3	-2	-1
	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	7	8	9	10	11	12	13
2	14	15	16	17	18	19	20

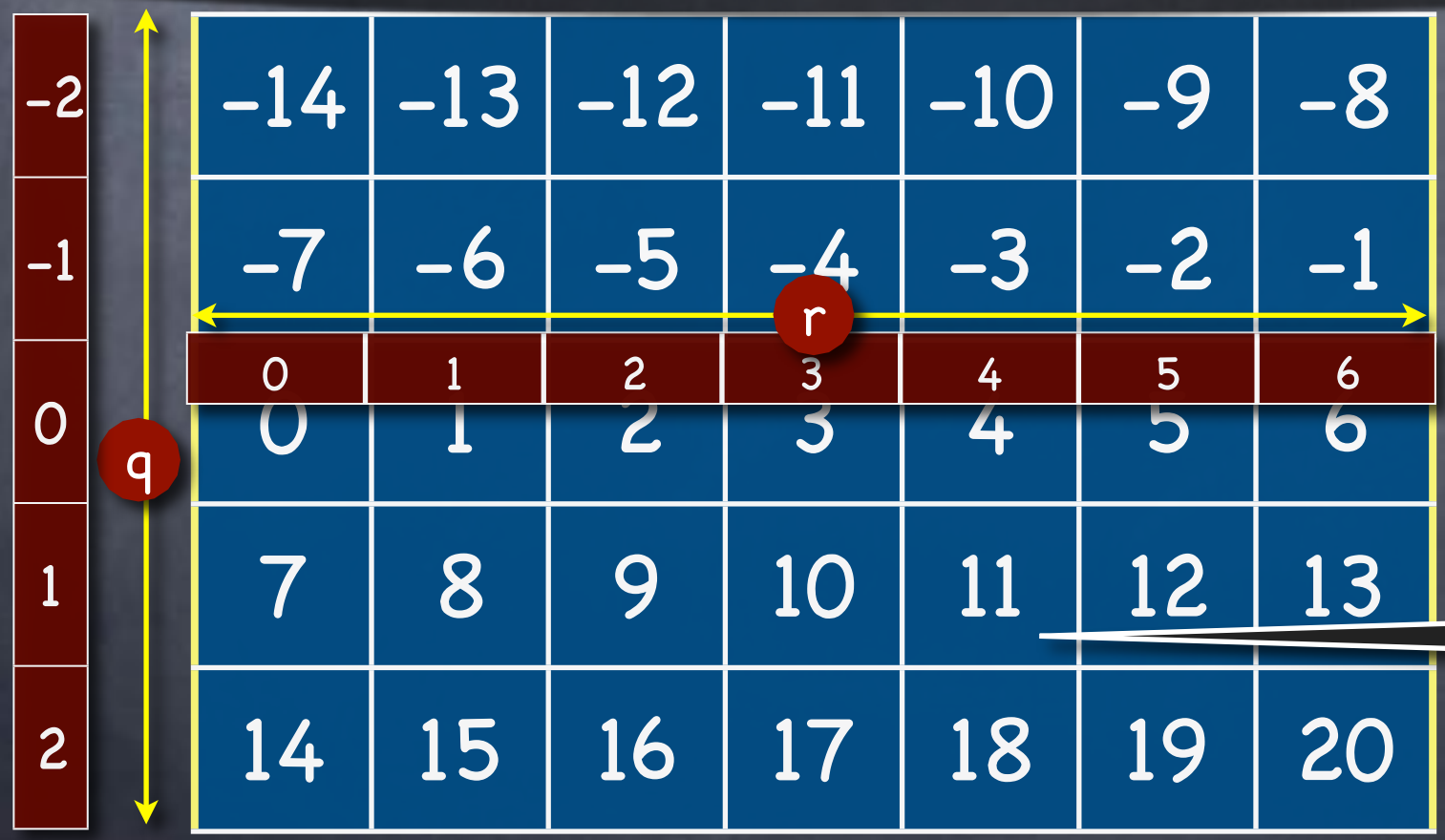
r

q

a=7

Division

- For any two integers a and b, $a \neq 0$, there is a <u>unique</u> quotient q and remainder r, such that
$$b = q \cdot a + r, \quad \text{and } 0 \leq r < |a|$$



a=7

e.g.
b=11
q=1, r=4

Division

$q = \lfloor b/a \rfloor$

- For any two integers a and b, $a \neq 0$, there is a <u>unique</u> quotient q and remainder r, such that
$$b = q \cdot a + r, \quad \text{and } 0 \leq r < |a|$$

-2	-14	-13	-12	-11	-10	-9	-8
-1	-7	-6	-5	-4	-3	-2	-1
	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	7	8	9	10	11	12	13
2	14	15	16	17	18	19	20

r

q

a=7

e.g.
b=11
q=1, r=4

Common Divisors & Multiples

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b.
  Smallest positive number d s.t. $\exists u,v\in\mathbb{Z}$ $d = ua+vb$

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b.
  Smallest positive number d s.t. $\exists u,v\in\mathbb{Z}$ $d = ua+vb$

coprimes:
gcd(a,b)=1

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b.
  Smallest positive number d s.t. $\exists u,v\in\mathbb{Z}$ $d = ua+vb$

coprimes: gcd(a,b)=1

$d|(ua+vb)$

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b.
  Smallest positive number d s.t. $\exists u,v\in\mathbb{Z}$ $d = ua+vb$

coprimes: gcd(a,b)=1

$d|(ua+vb)$

- Least Common Multiple (for $a\neq0$ and $b\neq0$)
  lcm(a,b) = smallest positive integer among the common multiples of a and b

Common Divisors & Multiples

- Common Divisor: c is a common divisor of integers a and b if $c|a$ and $c|b$. [a.k.a. common factor]

- Common Multiple: c is a common multiple of a and b if $a|c$ and $b|c$.

- Greatest Common Divisor (for $(a,b)\neq(0,0)$)
  gcd(a,b) = largest among common divisors of a and b.
  Smallest positive number d s.t. $\exists u,v\in\mathbb{Z}$ $d = ua+vb$

  coprimes: $\gcd(a,b)=1$

  $d|(ua+vb)$

- Least Common Multiple (for $a\neq0$ and $b\neq0$)
  lcm(a,b) = smallest positive integer among the common multiples of a and b

- $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = |a\cdot b|$ [Why?]

Congruence

-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

modulus=7

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

modulus=7

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

p&q on same column: <u>distance</u> between p&q is a multiple of m

	3	-12	-11	-10	-9	-8
	6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

modulus=7

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

p&q on same column: <u>distance</u> between p&q is a multiple of m

modulus=7

	3	-12	-11	-10	-9	-8
	6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

p&q on same column: <u>distance</u> between p&q is a multiple of m

modulus=7

	3	-12	-11	-10	-9	-8
	6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	
14	15	16	17	18	19	20

<u>$11 \equiv 18 \pmod{7}$</u>

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

p&q on same column: <u>distance</u> between p&q is a multiple of m

modulus=7

	3	-12	-11	-10	-9	-8
	6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	
14	15	16	17	18	19	20

$11 \equiv 18 \pmod{7}$

$11 \equiv -10 \pmod{7}$

Congruence

- For a "modulus" m and two integers p and q, we say $p \equiv q \pmod{m}$ if $m|(p-q)$

p&q on same column: <u>distance</u> between p&q is a multiple of m

Each column is an equivalence class of the relation $\cdot \equiv \cdot \pmod{m}$

	3	-12	-11	-10	-9	-8
	6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
0	1	2	3	4	5	6
7	8	9	10	11	12	
14	15	16	17	18	19	20

modulus=7

$11 \equiv 18 \pmod{7}$

$11 \equiv -10 \pmod{7}$

Modular Arithmetic

- $[a]_m$: the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular addition: $[a]_m +_m [b]_m \triangleq [a+b]_m$
- Modular multiplication: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$
- Multiplicative Inverse! a has a multiplicative inverse modulo m iff a is co-prime with m.
  - $\gcd(a,m)=1 \leftrightarrow \exists u,v\ au+mv=1 \leftrightarrow \exists u\ [a]_m \times_m [u]_m = [1]_m$
  - e.g. $[2]_9 \times_9 [5]_9 = [1]_9$ so $[2]_9^{-1} = [5]_9$ and $[5]_9^{-1} = [2]_9$
  - For a prime modulus p, all except $[0]_p$ have inverses!

Question

Question

- Let $a = 31^3 + 374 \times 12 + 5 \times 121$. Then

  A. $a \equiv 0 \pmod 3$
  B. $a \equiv 1 \pmod 3$
  C. $a \equiv 2 \pmod 3$
  D. None of the above

Question

- Let $a = 31^3 + 374\times12 + 5\times121$. Then

  A. $a \equiv 0 \pmod 3$
  B. $a \equiv 1 \pmod 3$
  C. $a \equiv 2 \pmod 3$
  D. None of the above

$\equiv 1^3 + 0 + 2\times1 \pmod 3$

Question

Question

- Let $a = 11^7$

  A. $a \equiv 0 \pmod{12}$
  B. $a \equiv 1 \pmod{12}$
  C. $a \equiv 7 \pmod{12}$
  D. $a \equiv 11 \pmod{12}$
  E. None of the above

Question

- Let $a = 11^7$

  A. $a \equiv 0 \pmod{12}$
  B. $a \equiv 1 \pmod{12}$
  C. $a \equiv 7 \pmod{12}$
  D. $a \equiv 11 \pmod{12}$
  E. None of the above

$(-1)^7 \equiv -1 \pmod{12}$