CS 207: Discrete Structures

Abstract algebra and Number theory

Lecture 34

Oct 12 2015

Topic 3: Graph theory

Some basic notions

- Basics: graphs, paths, cycles, walks, trails, ...
- Cliques and independent sets.
- Graph representations, isomorphisms and automorphisms.
- Matchings: perfect, maximal and maximum.
- Directed graphs, trees...

Topic 3: Graph theory

Some characterizations

1. Basics concepts and definitions.
2. Eulerian graphs: Using degrees of vertices.
3. Bipartite graphs: Using odd length cycles.
4. Connected components: Using cycles.
5. Maximum matchings: Using augmenting paths.
6. Perfect matchings in bipartite graphs: Using neighbour sets. – Hall's theorem
7. Maximum matchings in bipartite graphs: Minimum vertex covers. – Konig-Egervary's theorem
8. Stable matchings and the Gale-Shapley algorithm.

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Some questions

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Some questions

- What is abstract algebra?

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Some questions

- What is abstract algebra?
- What is number theory?

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Some questions

- What is abstract algebra?
- What is number theory?
- What is the link?

Topic 4: Abstract algebra and number theory

Today onwards

Start of next topic: Abstract algebra and number theory.

Some questions

- What is abstract algebra?
- What is number theory?
- What is the link?
- Why study either of these?

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$
  - Identity function is an automorphism.
  - Inverse of an automorphism is an automorphism.
  - Composition of two automorphisms is an automorphism
  - Composition of automorphisms satisfies associativity.

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$
  - Identity function is an automorphism.
  - Inverse of an automorphism is an automorphism.
  - Composition of two automorphisms is an automorphism
  - Composition of automorphisms satisfies associativity.
- The set of all automorphisms is called the automophism group.

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$
  - Identity function is an automorphism.
  - Inverse of an automorphism is an automorphism.
  - Composition of two automorphisms is an automorphism
  - Composition of automorphisms satisfies associativity.
- The set of all automorphisms is called the automophism group.
- Is this really a property of edge relation?
- What if we say (V, E') where E' is a set of ordered pairs?

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$
  - Identity function is an automorphism.
  - Inverse of an automorphism is an automorphism.
  - Composition of two automorphisms is an automorphism
  - Composition of automorphisms satisfies associativity.
- The set of all automorphisms is called the automophism group.
- Is this really a property of edge relation?
- What if we say (V, E') where E' is a set of ordered pairs?
- What if we say (V, R) where R is set of paths of length 3?

Some properties of discrete structures

Why not start with something we already know?

- Automorphisms of a graph:
  - An automorphism of a graph $G = (V, E)$ is a bijection $f : V \to V$ which preserves the edges, i.e.,
    - $uv \in E$ iff $f(u)f(v) \in E$
  - Identity function is an automorphism.
  - Inverse of an automorphism is an automorphism.
  - Composition of two automorphisms is an automorphism
  - Composition of automorphisms satisfies associativity.
- The set of all automorphisms is called the automophism group.
- Is this really a property of edge relation?
- What if we say (V, E') where E' is a set of ordered pairs?
- What if we say (V, R) where R is set of paths of length 3?
- Basically, we can have (V, R) where for any bijection g on V, there is a natural way of applying g on R and $g(R) = (R)$.

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!
- The group of all permutations is called the symmetric group.

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!
- The group of all permutations is called the symmetric group.
- What about a subset of the permutations? If it satisfies these properties it is called a permutation group.

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!
- The group of all permutations is called the symmetric group.
- What about a subset of the permutations? If it satisfies these properties it is called a permutation group.

- The set of automorphisms on any (V, R) (for a graph) satisfies all the properties.

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!
- The group of all permutations is called the symmetric group.
- What about a subset of the permutations? If it satisfies these properties it is called a permutation group.

- The set of automorphisms on any (V, R) (for a graph) satisfies all the properties.
- Which subsets of permutations satisfy can be determined as automorphisms of $G = (V, E)$?

Something even easier?

Consider the set of all bijections on $X = \{1, \ldots, n\}$ – i.e., permutations of X

- What is an operation on X?
- This satisfies all the properties mentioned above!
- The group of all permutations is called the symmetric group.
- What about a subset of the permutations? If it satisfies these properties it is called a permutation group.

- The set of automorphisms on any (V, R) (for a graph) satisfies all the properties.
- Which subsets of permutations satisfy can be determined as automorphisms of $G = (V, E)$?

What is common about all these?

Definition of a group

- What is common about all these definitions?

Definition of a group

- What is common about all these definitions?
- There is a set

Definition of a group

- What is common about all these definitions?
- There is a set
- There is a function... does it really matter?

Definition of a group

- What is common about all these definitions?
- There is a set
- There is a function... does it really matter?
- There is a way to compose objects!

Definition of a group

- What is common about all these definitions?
- There is a set
- There is a function... does it really matter?
- There is a way to compose objects!
- Can you think of such an example over numbers, say over integers?

Definition of a group

- What is common about all these definitions?
- There is a set
- There is a function... does it really matter?
- There is a way to compose objects!
- Can you think of such an example over numbers, say over integers?

Definition

A(n) (abstract) group is a set S along with an operator $*$ such that the following conditions are satisfied:

- Closure: $\forall a, b \in S$, $a * b \in S$.
- Associativity: $\forall a, b, c \in S$, $a * (b * c) = (a * b) * c$.
- Identity: $\exists e \in S$ s.t., $\forall a \in S, a * e = e * a = a$.
- Inverse: $\forall a \in S, \exists a' \in S$ s.t., $a * a' = a' * a = e$.

Examples of (abstract) groups

- Every permutation group is an abstract group.
- Every automorphism group is an abstract group.
- $(\mathbb{Z}, +)$ is a group.
- What about the following?
  1. $(\mathbb{Z}, \times)$.
  2. $(\mathbb{Q}, \times)$
  3. $(\mathbb{Q} \setminus 0, \times)$
  4. $(\mathbb{Z}_n, +_n)$
  5. $(\mathbb{Z}_n, \times_n)$
  6. $(\mathbb{Z}_n \setminus 0, \times_n)$.