Syllabus (MC322: 이산구조)

Department	Math & CS	**Credits**	3	**Instructor**	Sang-Hyun Yoon	**Class Room**	5708
Subject	MC322: Discrete Mathematics	**Class hrs/wk**	3	**Lab (e-mail)**		**Attendee**	
				5707			

1 Course Description

Course Objectives

On completion of this course, you'll hopefully be able to:

- Think in the language of mathematics (i.e. set/relation/logic)
  - Throughout this course, you will be trained to be able to think in terms of set/relation/logic fairly freely and comfortably.
- Synthesize (heavy) mathematical proofs;
- Model/analyze real-world problems and design algorithmic solutions to the problems along with mathematical proofs;
  - using discrete structures and combinatorial methods
- Think computationally/algorithmically;
  - appreciate the importance of algorithms in CS and beyond;
  - understand/appreciate limits of computation.

Contents

- Logic, Proofs, Sets, Relations, Algebraic structures (groups, rings, fields, lattices, etc.)
- Graph: Basic notions, Isomorphism, Coloring, Planarity, Connectivity, Independence
- Theory of computation: Turing machines, Undecidability, Incompleteness, Intractability
- Modular arithmetic, Cryptography
- Combinatorial analysis
  - Lattice paths, Cayley's formula, Pölya/Burnside methods, Chains & Antichains
- Combinatorial designs
  - Finite Fields, Finite geometries, Latin squares, block designs
- Combinatorial optimizations
  - Graph algorithms: shortest paths, minimum spanning trees, maximum flows
  - Matroids, Algebraic path problems
- Game theory
  - Combinatorial games: Nim, Sparague-Grundy functions, surreal numbers
  - Classical games: Nash equilibrium, solution concepts, mechanism design

2 Text & References

Text: None (slides and handouts)

References:

- "*Discrete and Combinatorial Mathematics*", R. Grimaldi
- "*Extremal Combinatorics*", S. Jukna
- "*Handbook of Discrete and Combinatorial Mathematics*", K. Rosen *et al.*
- "*Mathematical Logic*", H. Schwichtenberg
- "*Introduction to Set Theory*", K. Hrbacek and T. Jech
- "*On Numbers and Games*", J. Conway
- "*A Course in Game Theory*", M. Osborne and A. Rubinstein
- "*Graph Theory*", R. Diestel
- "*The Probabilistic Method*", N. Alon and J. Spencer
- "*Introduction to Theory of Computation*", M. Sipser
- "*Introduction to Modern Cryptography*", J. Katz and Y. Lindell
- "*Computers and Intractability: A Guide to the Theory of NP-Completeness*", M. Garey *et al.*
- "*Algorithm Design*", J. Kleinberg and E. Tardos
- "*Introduction to Algorithms*", T. Cormen, C. Leiserson, and R. Rivest

Course online:

- http://vod.ksa.hs.kr ⇒ Log in ⇒ MC322: Discrete Math

3 Grading

Activities	**Percentages**
Problem Sets	25%
Midterm Exam	15%
Final Exam	50%
Attendance/Quiz	10%

- Absolute evaluation
- 14 problem sets
- Short quiz for each class
- Two in-depth quizzes that substitute midterm exam (open-book/note)
- Final exam (open-book/note, unlimited time)
- Late-work policy: -30%/day

4 Lecture Schedule (Tabular)

Lec #	Topics	Assignments	Categories
1	Sets/Logic (basic notions)		Sets/Logic
2	Subgroups, Permutation Groups		Algebraic Structures
3	Group Actions/Homomorphisms	PS #1 due	
4	Groups & Rubik's Cube		
5	Finite Fields	PS #2 due	
6	Finite Geometries		
7	Order/Equivalence Relations	PS #3 due	Relations
8	Operations/Relations on Relations		
9	Graphs (basic notions)	PS #4 due	Graphs
10**	Graphs problems in CS		
11	Trees		
12	Counting	PS #5 due	Combinatorial Analysis
13	Finite Probability Space		
14	Cayley's Formula		
15-16	Chains/Antichains	PS #6 due	
17	Lattices (Stable Matching)		Algebraic Str.
18**	Turing Machines & Algorithms		Theory of Computation
19**	Universality & Undecidability	PS #7 due	
20	Incompleteness Theorems		
21	*Wrap-up for the midterm*	PS #8 due	
22*	Shortest Paths (Dijkstra)		Graph Algorithms (Combinatorial Optimization)
23	Shortest Paths (Floyd-Warshall)		
24	Algebraic Path Problems (Semiring)	PS #9 due	
25*	Minimum Spanning Trees		
26	Matroids		
27*	Flow Networks	PS #10 due	
28*	Polynomial-Time Reductions		Intractability
29*	NP-Completeness		
30	Combinatorial Games	PS #11 due	Game Theory
31	Nash Equilibrium		
32	Mechanism Design		
33	Latin Squares	PS #12 due	Combinatorial Design
34	Block Designs		
35**	Divisibility		Cryptography
36**	Modular Arithmetic	PS #13 due	
37**	Cryptology (informal overview)		
38**	Public-Key Cryptosystems		
39	*Wrap-up for the final exam*	PS #14 due	

*: overlap with MC422 **: overlap with MC221

5 Calendar

Mon		Tue		Wed		Thu		Fri	
2/22		2/23		2/24	*입학식*	2/25	**L1**	2/26	**L2**
2/29	**L3**	3/1	*holiday*	3/2		3/3	**L4**	3/4	**L5**
3/7	**L6**	3/8		3/9		3/10	**L7**	3/11	**L8**
3/14	**L9**	3/15		3/16		3/17	**L10**	3/18	**L11**
3/21	**L12**	3/22		3/23		3/24	**L13**	3/25	**L14**
3/28	**L15**	3/29		3/30		3/31	**L16**	4/1	**L17**
4/4	**L18**	4/5		4/6		4/7	**L19**	4/8	**L21**
4/11	*Midt.*	4/12	*Midt.*	4/13	*Midt.*	4/14	*Midt.*	4/15	*Midt.*
4/18	**L20**	4/19		4/20		4/21	**L22**	4/22	**L23**
4/25	**L24**	4/26		4/27		4/28	**L25**	4/29	**L26**
5/2	**L27**	5/3		5/4		5/5	*holiday*	5/6	**L28**
5/9	**L29**	5/10		5/11		5/12	**L30**	5/13	**L31**
5/16	**L32**	5/17		5/18	*holiday*	5/19	*holiday*	5/20	*holiday*
5/23	*SAF*	5/24	*SAF*	5/25		5/26	**L33**	5/27	**L34**
5/30	**L35**	5/31		6/1		6/2	**L36**	6/3	**L37**
6/6	*holiday*	6/7		6/8		6/9	**L38**	6/10	**L39**
6/13	**L40**	6/14		6/15		6/16	*Final*	6/17	*Final*
6/20	*Final*	6/21	*Final*	6/22	*Final*				

6 Lecture Outline

1. Sets/Logic (Set/Logic)
    - Propositional/predicate logic
    - Logical systems, soundness/completeness/consistency
    - Cardinalities of infinite sets, Russell's paradox
    - ZFC axioms
2. Groups & Rubik's cube #1 (Algebraic structures)
    - Subgroups, generators
    - The Symmetric group, disjoint cycle decomposition
    - Group representation for Rubik's cube
3. Groups & Rubik's cube #2 (Algebraic structures)
    - Group homomorphisms, kernels
    - The sign homomorphism, The alternating group,
    - Group actions, orbits
4. Groups & Rubik's cube #3 (Algebraic structures)
    - Necessary condition for valid configurations

- Sufficient condition (by using conjugators and generators)
- Number of valid configurations
- A lower bound for the worst-case number of moves

5. Finite fields (Algebraic structures)
   - Prime fields, polynomial rings
   - Irreducible polynomials, division of polynomials
   - The Galois field, uniqueness (up to isomorphism)

6. Finite geometries (Combinatorial design)
   - Axioms of Euclidean geometry
   - Affine planes, construction from the finite field
   - Projective planes

7. Relations #1 (Relations)
   - Operations on relations
   - Properties of binary relations
   - Order relations

8. Relations #2 (Relations)
   - Equivalence relations and partitions
   - Partition refinement, relations on relations

9. Graphs #1 (Graphs)
   - Basic notions, adjacency
   - Connectivity, articulation points
   - Eulerian/Hamiltonian paths/cycles
   - Planarity testing, Kuratowski's theorem
   - Graph isomorphism, subgraph isomorphism

10. Graphs #2 (Graphs)
    - Shortest paths, MSTs
    - Max-flow/min-cut, bipartite matching
    - Graph coloring, 4-coloring theorem
    - Independent sets, vertex covers, edge covers

11. Trees (Graphs)
    - Necessary and sufficient conditions for a graph to be a tree
    - Rooted trees, forest, binary trees
    - Decision trees, game trees, backward induction
    - Isomorphism

12. Counting (Combinatorial analysis)
    - Basic techniques (bijections, cartesian products, partitions, binary relations, inclusion-exclusion principle)
    - Recurrence relations, generating functions
    - Multi-dimensional Catalan numbers, Chung-Feller theorem

13. Discrete probability (Combinatorial analysis)
    - Frequentiest/Bayesian probability
    - Finite probability space
    - Bayesian decision problems
    - Probabilistic methods (counting sieve, linearity of expectation, derandomization)

14. Cayley's formula for the number of spanning trees (Combinatorial analysis)
    - Proof by bijection
    - Proof by recurrence relations
    - Proof by double counting
    - Proof by linear algebra

15. Chains/antichains #1 (Combinatorial analysis)
    - Hasse diagrams for posets
    - Decomposition of posets into chains/antichains
    - Dilworth's theorem (a specialization to Hall's condition for perfect matching)

16. Chains/antichains #2 (Combinatorial analysis)
    - Symmetric chains
    - Sperner system, LYM inequality
    - Bollobás's theorem, strong systems of distinct representatives

17. Lattices (Algebraic structures)
    - Lower/upper bounds in posets, meet/join operations
    - Distributive lattices, complete lattices
    - Complemented lattices (boolean algebra)
    - Applications in stable matching

18. Turing machines (Algorithms)
    - Turing machines
    - Formal notions of algorithmic problems and algorithms
    - Church-Turing thesis

19. Computability (Algorithms)
    - Universality, the universal Turing machine
    - Undecidability of the halting problem

- Undecidable problems in CS & math
- Proving the undecidability by reduction
- Rice's theorem

20. Incompleteness Theorems (Algorithms)
    - Logical systems
    - FOL, ZFC axioms, PA axioms
    - Soundness/Completeness/Consistency
    - Gödel's incompleteness theorems
21. *Wrap-up for the midterm*
22. Shortest paths: Dijkstra's greedy algorithm (Graphs)
    - Properties of shortest paths
    - Proof patterns with loop invariants (proofs with weaker/stronger induction hypothesis, by contradiction)
    - Applications (communication networks, arbitrage)
    - Negative-weight edges/cycles, longest path problems
23. Shortest paths: Floyd-Warshall's algorithm (Graphs)
    - Dynamic programming vs. recursion
    - Inductive formulation of shortest paths
    - Behavior with negative-weight edges/cycles
    - Minimum mean-cycle problem
24. Algebraic path problems (Graphs)
    - Idempotent semirings (dioids)
    - Inductive definition of set of paths
    - Semiring-based dynamic-programming formulation for algebraic path problems
25. Minimum spanning trees (Graphs)
    - Cuts, crossing edges, light edges, cut/cycle properties
    - The generic MST algorithm, specialization to Kruskal/Prim's algorithms
    - Applications (communication networks, TSP, Steiner trees)
26. Matroids (Combinatorial optimization)
    - Hereditary sets, k-exchange property
    - Graphic matroids
    - The generic greedy algorithm on weighted matroids
    - k-approximation
27. Flow network (Graphs)

- Max-flow min-cut theorem
- Ford-Fulkerson method, capacity scaling
- Bipartite matching, Hall's condition for perfect bipartite matching
- Applications

28. Polynomial-time reductions (Intractability)
    - Decision problems
    - Polynomial-time reductions
    - Standard reduction techniques (simple equivalence, restriction, local replacement, component design)
    - Reduction examples (3-SAT to INDEPENDENT SETS, 3-SAT to HAMILTONIAN CYCLES, 3-SAT to 3-DIMENSIONAL MATCHING, 3-SAT to GRAPH COLORING)

29. NP-completeness (Intractability)
    - Certifier-based definition of the class NP
    - Cook-Levin theorem
    - How to cope with intractability
    - Important complexity classes beyond NP (co-NP, PSPACE, ZPP, BPP, RP)

30. Combinatorial games #1 (Game theory)
    - Inductive definition of winning/losing positions
    - Impartial combinatorial games, Nim game
    - Sprague-Grundy theorem
    - Partizan games
    - Surreal numbers

31. Non-cooperative strategic form games (Game theory)
    - Dominant strategy equilibrium
    - Pure strategy Nash equilibrium
    - Mixed strategy Nash equilibrium

32. Mechanism design (Game theory)
    - Implementation of solution concepts (e.g. dominante strategies, Bayesian-Nash equilibrium)
    - The revelation principle, truthful implementation
    - Vickrey-Groves-Clarke (VGC) mechanism
    - Algorithmic issues in mechanism design

33. Latin squares (Combinatorial design)
    - Incomplete Latin squares
    - Orthogonal Latin squares
    - Construction by finite fields and extension from prime orders

- Applications (design of experiments)

34. Block designs (Combinatorial design)
    - Regularity, existence
    - Symmetric block design by using finite fields
    - Projective planes

35. Modular arithmetic (Cryptography)
    - Divisibility
    - Additive/multiplicative group modulo n
    - Modular linear equations, Chinese remainder theorem
    - Modular exponentiation, discrete logarithm

36. Cryptology (informal overview) (Cryptography)
    - Trapdoor one-way functions
    - Private-key cryptosystems, sharing private keys
    - Public-key cryptosystems

37. The RSA cryptosystem (Cryptography)
    - The RSA cryptosystem, security issues, digital signature
    - Primality testing (the prime density theorem, the Miller-Rabin randomized testing, the AKS algorithm)
    - RSA attacks, heuristics for prime factorization

38. Other cryptosystems & protocols (Cryptography)
    - Merkle-Hellman cryptosystem (intractability of the subset-sum problem)
    - ElGamal cryptosystem (discrete logs, elliptic curves)
    - Secret sharing, multi-party secure computations, zero-knowledge proofs

39. *Wrap-up for the midterm*