课程详述

COURSE SPECIFICATION

以下课程信息可能根据实际授课需要或在课程检讨之后产生变动。如对课程有任何疑问，请联系授课教师。

The course information as follows may be subject to change, either during the session because of unforeseen circumstances, or following review of the course at the end of the session. Queries about the course should be directed to the course instructor.

1.	**课程名称 Course Title**	**离散数学（H） Discrete Mathematics (H)**
2.	**授课院系 Originating Department**	计算机科学与工程系 Department of Computer Science and Engineering
3.	**课程编号 Course Code**	CS215
4.	**课程学分 Credit Value**	3
5.	**课程类别 Course Type**	专业基础课 Major Foundational Courses
6.	**授课学期 Semester**	秋季 Fall
7.	**授课语言 Teaching Language**	中英双语 English & Chinese
8.	**授课教师、所属学系、联系方式（如属团队授课，请列明其他授课教师） Instructor(s), Affiliation& Contact （For team teaching, please list all instructors）**	王琦，副教授， 计算机科学与工程系， wangqi@sustech.edu.cn Qi Wang, Associate Professor, Department of Computer Science and Engineering, wangqi@sustech.edu.cn
9.	**实验员/助教、所属学系、联系方式 Tutor/TA(s), Contact**	待公布 To be announced
10.	**选课人数限额(可不填) Maximum Enrolment （Optional）**	50

11.	授课方式 Delivery Method	讲授 Lectures	习题/辅导/讨论 Tutorials	实验/实习 Lab/Practical	其它(请具体注明) Other（Please specify）	总学时 Total
	学时数 Credit Hours	48				48

12.	先修课程、其它学习要求 Pre-requisites or Other Academic Requirements	MA102B 高等数学（下）A Calculus II A M107A 线性代数 I-A Linear Algebra I-A
13.	后续课程、其它学习规划 Courses for which this course is a pre-requisite	CS403 密码学与网络安全 Cryptography and Network Security
14.	其它要求修读本课程的学系 Cross-listing Dept.	无 Not applicable for other departments beside CSE.

教学大纲及教学日历 SYLLABUS

15. 教学目标 Course Objectives

本课程旨在理解和应用在计算机科学与工程中广泛存在的一系列抽象的离散结构。具体地说，本课程将介绍逻辑、集合与函数、数学证明、计算复杂度、数论及其应用、密码学、群环域代数结构及应用、数学归纳法、计数、递归、关系、图论及算法等内容，特别是这些内容在计算机中的实际应用。

The objective of this course is to understand and use (abstract) discrete structures that are backbones of computer sciences. In particular, this course is meant to introduce logic, sets and functions, mathematical proofs, complexity, number theory, cryptography, algebraic structures and applications, induction, counting, recurrences, relations, graph theory and related algorithms, with an emphasis on applications in computer science.

16. 预达学习成果 Learning Outcomes

本课程预期达到以下学习效果：

- 能够较好地阅读、理解、完成数学证明
- 理解离散数学中各部分问题的形式化表述，包括计数、数论、密码学、逻辑和证明、递归、图论等
- 学习一系列的离散数学工具并学会应用这些工具和方法解决计算机科学中的实际问题

On completion of this course, the students are expected to:

- be able to read, understand, and construct mathematical arguments and proofs
- understand the formulation of common problems in several areas of discrete mathematics, including counting, number theory, cryptography, logic and proof, recursions, graph theory, etc.
- learn a number of discrete mathematical tools and apply discrete mathematical tools to solve certain problems in computer science

17. 课程内容及教学日历 （如授课语言以英文为主，则课程内容介绍可以用英文；如团队教学或模块教学，教学日历须注明主讲人）
Course Contents (in Parts/Chapters/Sections/Weeks. Please notify name of instructor for course section(s), if this is a team teaching or module course.)

第一课：离散数学概论、命题逻辑

离散数学介绍、典型问题

命题逻辑、逻辑连接符、真值表

第二课：逻辑等价性、谓语逻辑

命题逻辑的应用

逻辑等价性及证明

命题逻辑的限制

谓语逻辑及量词

第三课：逻辑推导、数学证明思想

逻辑推导规则及应用

五种数学证明思路及举例证明

第四课：集合与函数

集合及运算、逻辑表示

定义函数、单射、满射函数

第五课：复合函数、序列、可数集

复合函数、函数逆定义

序列、序列求和、公式推导

可数集定义、证明及举例

第六课：计算复杂度 I

大 O 符号、复杂度计算举例

NP 理论介绍、决定和优化问题

第七课：计算复杂度 II、初等数论 I

NP 完全问题

整除、模运算、b 进制表示及相关算法

第八课：初等数论 II

素数、最大公约数

欧几里得算法、Bezout 等式

线性同余方程、模 n 逆及求解

第九课：初等数论应用

中国剩余定理、向后置换法

线性同余法生成伪随机数

费马小定理、欧拉定理

本原根定义

第十课：群环域抽象代数结构及应用

群、环、域定义及举例

有限域介绍、性质

有限域在随机序列、纠错编码的应用及相关举例

第十一课：密码学

密码学历史

对称密码学介绍、公钥密码学、RSA 加密机制

离散对数问题介绍、El Gamal 加密机制

第十二课：数学归纳法、递归 I

数学归纳法介绍及证明

数学归纳法弱准则、强准则

汉诺塔举例

递归式求解

第十三课：递归 II

递归式求解

主定理

第十四课：计数 I

排列组合计数、加法乘法规则

容斥原理及证明

鸽巢原理

一一对应原理

第十五课：计数 II

二项式系数及性质

Pascal 恒等式

组合证明

第十六课：高级计数方法

欧几里得算法复杂度分析

求解线性递归式

生成函数

第十七课：关系 I

二元关系

关系的性质及计数

关系复合

第十八课：关系 II

传递关系性质及证明

关系闭包

关系数据库

第十九课：关系 III

连通关系与传递闭包的关系

Roy-Warshall 算法

等价关系、等价类

偏序、Hasse 图

第二十课：图论 I

图论基本概念

无向图、有向图、二分图等

匹配、Hall 定理及证明

第二十一课：图论 II

图表示、邻接矩阵、关联矩阵

图同构

路径、连通性、欧拉图

第二十二课：图论 III

Hamilton 图

最短路径问题、Dijkstra 算法

平面图、欧拉公式

图染色问题

第二十三课：树 I

树基本概念

平衡树、相关数型数据结构介绍及算法

先序、中序、后序遍历

第二十四课：树 II、复习课

最小生成树及算法

深度、广度优先搜索

复习课

Overview of Discrete Math, Propositional Logic

Introduction to Discrete Math, typical problems

Propositional logic, logical connectives, truth tables

Logical Equivalence, Predicate Logic

Application of propositional logic

Logical equivalence and proof

Limitations of propositional logic

Predicate logic, quantifiers

Logical Inference, Proof Methods

Rules of logical inferences and applications

Five methods of proof, proof exercises

Set and Functions

Set, set operations, and representations using logic

Definition of functions, one-to-one functions, onto functions

Composite Functions, Sequences, Countable Sets

Composite function, inverse function
Sequences, sum of sequences, closed-form formula
Countable sets, proofs and examples

Computational Complexity I
Big-O notation, examples of complexity
NP theory
Decision problem, optimization problem

Computational Complexity II, Number Theory I
NP-Completeness
Divisibility, modular operation, base-b representation, related algorithms

Number Theory II
Primes, greatest common divisor
Euclidean algorithm, Bezout identity
Linear congruential equation, inverse modulo n

Applications of Number Theory
Chinese remainder theory, back substitution
Pseudorandom numbers using linear congruential method
Fermat's little theorem, Euler's theorem
Primitive root

Abstract Algebra and applications
Definitions of group, ring and field
Introduction to finite fields
Applications in pseudorandom sequences, error-correcting codes

Cryptography
History of cryptography
Symmetric encryption, public-key cryptography, RSA scheme
Discrete logarithm problem, El Gamal encryption scheme

Mathematical Induction, Recurrence I
Introduction to induction, typical proofs
Weak principle, strong principle of mathematical induction
Hanoi tower and recurrence
Solving recurrences with initial conditions

Recurrence II
Solving recurrences, more examples

The master theorem

Counting I

Permutations, combinatorial numbers, the sum/product rule

Inclusion-Exclusion principle and its proof

Pigeonhole principle

Bijection principle

Counting II

Binomial coefficient and properties

Pascal identity

Combinatorial proofs

Advanced Counting Techniques

Complexity of Euclidean algorithm

Solving linear recurrence relations with initial conditions

Generating functions

Relation I

Binary relation

Properties of relation, and counting

Composite relations

Relation II

Transitive relations, properties and proofs

Transitive closure

Relational database

Relation III

Connectivity relation and transitive closure

Roy-Warshall algorithm

Equivalence relations, equivalence class

Partial ordering, Hasse diagram

Graph Theory I

Basic concepts of graph theory

Undirected graphs, directed graphs, Bipartite graphs

Matching, Hall's marriage theorem, proof

Graph Theory II

Representations of graphs, adjacency matrix, incidence matrix

Isomorphism of graphs

Path, connectivity, Euler graph

Graph Theory III

Hamilton graph

Shortest path, Dijkstra algorithm

Planar graphs, Euler formula

Graph coloring

Tree I

Basic concepts of tree

Balanced tree and counting

More related data structures and algorithms

Preorder, inorder, postorder traversal

Tree II, Review Lecture

Minimum spanning tree and algorithms

Depth-first search and breadth-first search

review

18. 教材及其它参考资料 Textbook and Supplementary Readings

Textbook：Kenneth Rosen, Discrete Mathematics and Its Applications, 7th Edition, Mc Graw Hill Education, 2012.

Reference books: Ronald Graham, Donald Knuth, and Oren Patashnik, Concrete Mathematics: A Foundation for Computer Science, 2nd Edition, Addison-Wesley Professional, 1994.

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein, Introduction to Algorithms, 3rd Edition, MIT Press, 2009.

课程评估 ASSESSMENT

19.

评估形式 Type of Assessment	评估时间 Time	占考试总成绩百分比 % of final score	违纪处罚 Penalty	备注 Notes
出勤 Attendance				
课堂表现 Class Performance				
小测验 Quiz		10%		2-3 次 2-3 times
课程项目 Projects		5% optional		额外加分 optional
平时作业 Assignments		20%		5-7 次 5-7 times
期中考试 Mid-Term Test		30%		覆盖本课程前半部分 Convers the first part of the course
期末考试 Final Exam		40%		覆盖本课程全部内容 Covers the whole course

期末报告 **Final Presentation**				
其它（可根据需要改写以上评估方式） **Others (The above may be modified as necessary)**				

20. 记分方式 **GRADING SYSTEM**

☑ A. 十三级等级制 **Letter Grading**
☐ B. 二级记分制（通过/不通过） **Pass/Fail Grading**

课程审批 REVIEW AND APPROVAL

21. **本课程设置已经过以下责任人/委员会审议通过**
This Course has been approved by the following person or committee of authority