Math Puzzles And Algorithm Design

This course includes five chapters. Each chapter, being provided for 2-3 weeks, starts with a couple of math puzzles to draw interests of students. Then follows studies on how and why the basic ideas in these puzzles are important in design and analysis of contemporary algorithms.

1. Power of Randomization
Randomization is one of the key techniques in designing contemporary algorithms. However, it is only useful when used in a proper way. For instance it provides a surprising power when the same random number is shared by all parties (2.1), in some cases, we can exploit variance of a random variable that is not too small (2.2), and randomization is also powerful for proving mathematical properties that have nothing to do with probability (2.3). Randomized algorithms are often simple in their structures, but claiming their performances rigorously needs much work (1.4).

1.1 Locker Puzzle
1.2 Lamp board puzzle
1.3 Probabilistic methods
1.4 Two randomized algorithms; quick sort and random-walk 3SAT solver

2. Competition against God; Online algorithms
A specific problem is given as its input and a required output, for instance, sorting is to take a sequence of integers as its input and to output the sorted sequence. Thus we usually assume that the whole input is ready when the computation starts. Unfortunately this is not the case in several circumstances. Most typically, future information such as stock prices are not available, but we have to decide our action, buying or selling stocks, at each moment. We use a competitive ratio to evaluate such actions, online algorithms, which compares the gain of the algorithm to that of an optimal offline algorithm that can use the whole input.

2.1 Introductory puzzles: Stock investment, 7-Eleven, Ski-rental
2.2 Competitive analysis
2.3 Linear list search; upper and lower bounds (maybe skipped)
2.4 k-server; upper and lower bounds, randomization
2.5 Currency exchange; threat-based method and forecasts

3. Avoiding information leakage
If there is communication, some sort of information leakage is unavoidable and its prevention is one of the most important missions in our today's society. In this chapter, we study how we can use techniques, based on computer science, to achieve this goal. What plays an important role is complexity of computation, especially

computational hardness of some problems including prime factorization. We will study this topic also in Chapter 5.

3.1 Introductory puzzle: Voting with minimum information leak
3.2 Rock-Paper-Scissors via phone
3.3 Zero-knowledge proof

4. Fairness and Truthfulness
Human beings are inherently selfish, trying to maximize our own benefits, which can cause several disadvantages to other people and the whole society. This is an obvious motivation for developing mechanisms, based on computer science, (4.1) that are fair to all those selfish people, (4.2) that can discourage selfish activities and (4.3) that minimize the price we need to pay for such harmful selfishness.

4.1 Cake cutting and a related puzzle in CACM on asset heritage
4.2 Digital goods auction
4.3 Selfish routing and price of anarchy

5. More contemporary topics
After the turn of the century, several new topics in algorithms complexity theory have emerged. In this Chapter, we will look at some of them that are a bit surprising such as constant-time computation (5.1) and are closely related to our daily life (5.2).

5.1 Property testing: Constant-time computation
5.2 Differential privacy
5.3 PageRank manipulation
5.4 Theoretical foundation of Bit Coin