CS 215: Discrete Math (H)
2023 Fall Semester Project Description
Due: 23:59, Jan. 21st, 2024

The goal of this project is for you to have a better understanding of interesting topics in discrete math and its applications in various related areas. You are required to give a self-contained report, together with possible supplementary materials (demo, codes, etc.). The project is *optional*, and counts **5% additional** overall marks.

You are assumed to work *individually.* The project report is due on **Jan. 21st, 2024**. Each student may submit your project **directly to the homepage on Blackboard**. Please indicate **clearly** the references in your report. All your submissions will be evaluated individually based on your own project quality (work load, scope, clarity and organization of your report, etc.).

The suggested list of topics includes but not limited to the following:

- Boolean satisfiability problem. The *Boolean satisfiability problem* (SAT) is the problem of determining if there exists an interpretation that satisfies a given Boolean formula. For example, the formula $a \wedge \neg b$ is *satisfiable* because one can find the values $a = T$ and $b = F$, which assignment makes the formula TRUE. In comparison, $a \wedge \neg a$ is *unsatisfiable.* SAT is the *first* problem that was proven to be *NP-complete.* You may complete a survey report on SAT, for example, including basic definitions, conjunctive/disjunctive normal forms, Cook-Levin theorem, extensions of SAT, algorithms for solving SAT and their implementations, etc.

- Pseudorandom number generators. There are different methods of pseudorandom number generators, and they are widely used in applications, especially in cryptographic applications. You may survey these methods, discuss their "randomness" and summarize their corresponding mathematical foundations. In addition, you may survey the APIs/methods provided by different programming languages, and give implementations of them in interesting applications. You are also encouraged to survey applications of pseudorandom number generators in cryptographic standards, for example, *public key cryptography standards* (PKCS).

- RSA used in real world. RSA is so widely used today. However, what we learned about RSA in class is the “plain” RSA, and is cryptographically weak in real world. You may survey standards of RSA and how RSA algorithms are used in real applications, including also discussion on possible attacks. Furthermore, you may have a understanding of how the security requirements in real world are modeled in theory.

- Linear recurrence relations. It is very clear that solving linear recurrence relations is directly related to methods in linear algebra. You may give a more formal report on solving linear recurrence relations by relating it more concretely to what you have learned in linear algebra. Moreover, you may find the *Berlekamp-Massey algorithm* interesting to understand more about linear recurrence relations. Solving linear recurrence relations can be extended to finite fields besides the real numbers.

- Advanced topics in graph theory. Due to limit of time, many interesting advanced topics in graph theory cannot be covered in our course. However, you are encouraged to explore more on these advanced topics in graph theory, especially their applications in many areas, e.g., network flow, random graphs, and many others.