JOHNS HOPKINS
WHITING SCHOOL
*of* ENGINEERING

# Computer Science 601.730
# PSEUDORANDOMNESS and COMBINATORIAL CONSTRUCTIONS
# Fall, 2017 (3 credits, EQ)

## Instructor

Professor Xin Li, `lixints@cs.jhu.edu`, `www.cs.jhu.edu/~lixints`
Office: Malone Hall 215, 410-516-5847
Office hours: Wednesdays 2:00 pm–3:00 pm or by appointment

## Meetings

Tuesday and Thursday, 1:30–2:45 pm, Bloomberg 176

## Online Resources

Any related online material will be posted at the course website http://www.cs.jhu.edu/˜lixints/class/fall17.html.

## Course Information

- **Course description:** Randomness is very useful in almost all areas of computer science, such as algorithms, distributed computing and cryptography. However, computers generally do not have access to truly uniform random bits. To deal with this, we rely on various pseudorandom objects to reduce either the quantity or the quality of the random bits needed.

  In this course, we will develop provably good pseudorandom objects for a variety of tasks. We will frequently require explicit combinatorial constructions. That is, we will want to efficiently and deterministically construct such objects. Along the way, we will also explore the close connections of such objects to many other areas in computer science and mathematics, such as graph theory, coding theory, complexity theory and arithmetic combinatorics.
- **Prerequisites**

  Discrete math, probability theory, some familiarity with algebra.
- **Selective Elective**

## Course Goals

Specific Outcomes for this course are that:

- Students will learn to establish a formal foundation of the theory of computation.
- Students will learn to analyze and solve problems formally and mathematically.

This course will address the following Criterion 3 Student Outcomes:

- An ability to apply knowledge of computing and mathematics appropriate to the discipline (a)
- An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution (b)

## Course Topics

- Applications of randomness in computation, the probabilistic method (**1 week**).
- (Almost) k-wise independence, coding theory and small biased space (**2 weeks**).
- Expander graphs and random walks on expanders (**1 week**).

- Pseudorandom generators from hard functions, average case hardness, hardcore predicates and list-decoding (**2 weeks**).
- Left over hash lemma, extractors, pseudorandom generators for space bounded computation (**2 weeks**).
- Trevisans extractor, Kakeya sets and mergers (**2 weeks**).
- Seedless extractors (**1 week**).

**Course Expectations & Grading**

There will be 3-4 homework problem sets and a final project. Grading will be based on the following rule:

- Homework: 65%.
- Final project: 35%.

**Assignments & Readings**

Assignments and further readings will be posted on the course website http://www.cs.jhu.edu/~lixints/class/fall17.html

**Piazza:** piazza.com/jhu/fall2017/en601730

**Ethics**

The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful, abiding by the *Computer Science Academic Integrity Policy*:

> Cheating is wrong. Cheating hurts our community by undermining academic integrity, creating mistrust, and fostering unfair competition. The university will punish cheaters with failure on an assignment, failure in a course, permanent transcript notation, suspension, and/or expulsion. Offenses may be reported to medical, law or other professional or graduate schools when a cheater applies.
>
> Violations can include cheating on exams, plagiarism, reuse of assignments without permission, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition. Ignorance of these rules is not an excuse.
>
> Academic honesty is required in all work you submit to be graded. Except where the instructor specifies group work, you must solve all homework and programming assignments without the help of others. For example, you must not look at anyone else's solutions (including program code) to your homework problems. However, you may discuss assignment specifications (not solutions) with others to be sure you understand what is required by the assignment.
>
> If your instructor permits using fragments of source code from outside sources, such as your textbook or on-line resources, you must properly cite the source. Not citing it constitutes plagiarism. Similarly, your group projects must list everyone who participated.
>
> Falsifying program output or results is prohibited.
>
> Your instructor is free to override parts of this policy for particular assignments. To protect yourself: (1) Ask the instructor if you are not sure what is permissible. (2) Seek help from the instructor, TA or CAs, as you are always encouraged to do, rather than from other students. (3) Cite any questionable sources of help you may have received.
>
> On every exam, you will sign the following pledge: "I agree to complete this exam without unauthorized assistance from any person, materials or device. [Signed and dated]". Your course instructors will let you know where to find copies of old exams, if they are available.

[In addition, the specific ethics guidelines for this course are:

(1) *Collaboration policy:* While you should first think about homework problems on your own, I encourage you to discuss homework problems with your classmates. However, you must write up your own solutions. Students found sharing the same paragraph in their homework will receive 0 point for the homework, and risk further punishment such as automatic failure and report to the University. Furthermore, you must acknowledge any collaboration by writing the names of your collaborators on the front page of the assignment. You don't lose points by having collaborators.

(2) *Citation policy:* Try to solve the problems without reading any published literature or websites, besides the class text. If, however, you do use a solution or part of a solution that you found in the literature or on the web, you must cite it. Furthermore, you must write up the solution in your own words. You will get at most half credit for solutions found in the literature or on the web. Using

solutions from other resources without citation is considered plagiarism and will result in 0 point and potential further punishment as in (1).

(3) *Late Policy:* Homework are due at the beginning of the class. No late homework will be accepted.

Report any violations you witness to the instructor.

You can find more information about university misconduct policies on the web at these sites:

- Undergraduates: `e-catalog.jhu.edu/undergrad-students/student-life-policies/`
- Graduate students: `e-catalog.jhu.edu/grad-students/graduate-specific-policies/`

**Students with Disabilities**

Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516–4720, `studentdisabilityservices@jhu.edu`.