University of Illinois, Urbana Champaign
CS 598DK Special Topics in Cryptography

Author: Ima Student
Date: August 28, 2019

PROJECT
1

Instructions for Preparing Project Report

Using the provided `\makeheader` command, customize the above header with your name, date, and project title. Your project report should start with a description of goals, a high-level description of techniques, and how they fit in the broader context of the course.

1.1 Organization

The report should be presented in a sequence of sections. For example, you may choose to present background or prior work in one section, building blocks in the next section, the main results in another section, and any generalizations or conclusions in a final section. Do *not* use any subdivisions within sections (subsections, subsubsections, etc.). Use normal capitalization in section headings rather than initial caps.

1.2 Some do's

- Always preface a formal statement (theorem, lemma, proposition) with a discussion of its purpose and a brief and intuitive outline of the proof. Then clearly and formally write the actual proof.
- We all know from experience that a picture is worth a thousand words, so be generous with figures. See Figure 1.1 for an example usage of the figure environment.
- Write in complete sentences. Mathematical writing is not fundamentally different from any other form of expository prose. Take pride in your work.
- As with any writing, make sure to spell check your scribe notes.
- Be sure to include all bibliographic references, like so [1]. You will find all the needed references at the end of the corresponding chapter in the textbook. The bibliography must be incorporated using BibTex. When finished, please send me the following files by email: your LaTeX source file (`.tex`), your bibliography file (`.bib`) if you used one, any figures (ideally in `.pdf` format), and the resulting typeset document (`.pdf`). I prefer to receive a single ZIP archive rather than several individual attachments.

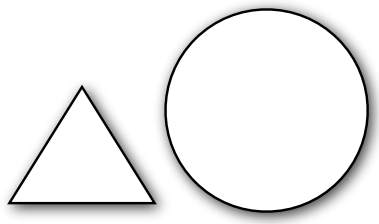

FIGURE 1.1: A triangle and a circle.

1.3 Mathematical environments

For your convenience, the style file comes with the following mathematical environments predefined: theorem, lemma, corollary, proposition, fact, claim, definition, example, assumption, remark, conjecture, open problem, problem. The environments are illustrated below. Please limit yourself to these environments.

THEOREM 1.1. *Statement here*

LEMMA 1.2. *Statement here*

COROLLARY 1.3. *Statement here*

PROPOSITION 1.4. *Statement here*

FACT 1.5. *Statement here*

CLAIM 1.6. *Statement here*

DEFINITION 1.7. Statement here

EXAMPLE 1.8. Statement here

ASSUMPTION 1.9. Statement here

REMARK 1.10. Statement here

CONJECTURE 1.11. Statement here

OPEN PROBLEM 1.12. Statement here

PROBLEM 1.13. Statement here

Note that LaTeX automatically numbers these environments within the lecture number (1 in this case). The same applies to the numbering of pages (this page being page 1-2), figures (Figure 1.1 above), and equations:

$$a = a_1 + a_2 + \cdots + a_n. \tag{1.1}$$

For proofs, use the provided `proof` environment, illustrated below.

Proof. Proof goes here. □

References

[1] E. Kushilevitz and N. Nisan. *Communication complexity.* Cambridge University Press, 2nd edition, 2006.