160B Project Title

Name 1, Name 2 ...

May 30, 2025

Contents

1 Introduction

In one page describe the contents of the project providing an outline of each of the sections of the report.

The report should follow the outline of Lecture 8 on Markov Chain Monte Carlo (MCMC) and message encryption/decryption. You can follow the provided section headings or modify based on your emphasis.

Your should pick an emphasis for your project (declaring it in the introduction) from one of the following three categories.

1. Applications – For this you should explain other applications and/or expand upon aspects of message decryption that would be required for real world applications (e.g. handling punctuation or special characters.)

2. Coding – For this emphasis you should address aspects related to the implementation of MCMC algorithms (e.g., run time, memory usage, parallelization etc). Document all improvements made to the current code.

3. Theory – For this option you are expected to include proofs (not necessarily original). For example, those from our lectures on Markov chains.

In the report you must cite at least three references.

- One of them must be Connor (2003)
- Another must be Ross (2019) (see Section 4.9).
- Any other reference of your choice added to `160B_project.aux`

Regardless of which emphasis you chose (applications, theory, or coding) your report should propose a modification to the algorithm section of Lecture 8. This modification can can be made to the proposal probability

$$\mathrm{q}(x, y) \tag{1}$$

or the acceptance probability $a(x, y)$ (see general the formula (2.2) in Connor (2003)). Recall that (1) proposes a move from a permutation x to a permutation y which is accepted with probability $a(x, y)$. The provided `README.pdf` document shows where to find these probabilities are found in the code.

2 Message encryption/decryption

Provide a brief outline of what is accomplished in this section. For your chosen emphasis please address the following.

2.1 Permutations on alphabets

Define alphabets and permutations to show how they can be used to encrypt text messages. Provide examples along the lines of (but different from) Lecture 8.

2.2 The likelihood of text

Define the likelihood function that reports how likely a given text is to belong to the english language. Discuss how the construction of this likelihood would be done in practice including the "training" part of the MCMC algorith that in our cases uses the novel "War and Peace" (see `README.pdf` in the code).

3 Markov Chain Monte Carlo

This section should describe the MCMC algorithm and your proposed modification. You can focus the content based on your emphasis but the following subsections should be present.

3.1 How it works

This section should address how MCMC decodes the encrypted message, making an explicit connection to the fact that finite, irreducible nd aperiodic Markov chains converge to their stationary distributions.

3.2 Proposed modification

Propose a modification as described below (1) and describe the expected impact of this modification. The latter can be an educated guess.

4 Results and conclusions

Document the impact of your modification on a decoding of an encrypted message of your choice. It is okay if the results differ from what you expected as long as you try to make sense of them.

A Code

You can use the verbatim environment to include `code`.

```
print("Hello")
```

B Supplements (optional)

References

Connor, S. (2003), 'Simulation and solving substitution codes', *Master's thesis, Department of Statistics, University of Warwick* .

Ross, S. M. (2019), *Introduction to Probability Models*, Elsevier. 12 ed.