Exponential Sums in Coding Theory
and Cryptology

Igor E. Shparlinski
Macquarie University

igor@comp.mq.edu.au

Lecture Notes of Tutorial Lectures given at the
Institute for Mathematical Sciences of the NUS

Singapore, 23–26 July, 2001

The author would greatly appreciate any comments,
corrections and critical remarks
Introduction

In these lecture notes we will try to exhibit, in a very informal way, some useful and sometimes surprising relations between exponential sums, which is a celebrated tool on analytical number theory, and several important problems of such applied areas as coding theory and cryptology.
One can certainly ask two natural questions:

- Why Exponential Sums?
  And the answer is:
  
  - Because they are beautiful and I like them;
  - Because exponential sums allow us to show the existence of objects with some special properties.

- Why Coding Theory and Cryptology?
  
  - Because they are beautiful and I like them as well;
  - Because to design/analyze some codes and cryptographic schemes we need to find objects with some special properties:
    
    * "good" for designs;
    * "bad" for attacks.

The main goal of these lectures is to show that exponential sums are very useful, yet user friendly objects, provided you know how to approach them. I will also provide a necessary background for everybody who would like to learn about this powerful tool and to be able to use it in her and his own work. I do not pretend to give a systematic introduction to the subject but rather I intend help to get started in making exponential sums an active working tool, at least in the situation where their application does not require any sophisticated technique or advanced analytical methods. I hope my lectures should help to develop some feeling of the kinds of questions where exponential sums can be useful and if you see that the actual application is beyond your level of expertise you can always seek an advise from one of the numerous experts in number theory (who probably otherwise would never know about your problem).

It is well know that for many years number theory was the main area of applications of exponential sums. Such applications include (but are not limited to)
• Uniform distribution (H. Weyl);

• Additive problems such the Goldbach and Waring problems (G. H. Hardy, J. E. Littlewood, R. Vaughan, I. M. Vinogradov);

• Riemann zeta function and distribution of prime numbers (J. Littlewood, N. M. Korobov, Yu. V. Linnik, E. C. Titchmarsh, I. M. Vinogradov).

However it has turned out that exponential sums provide a valuable tool for a variety of problems of theoretical computer science, coding theory and cryptography, see [65, 66].

I will try to explain:

• What we call exponential sums.

• How we estimate exponential sums (and why we need this at all).

• What is current state of affairs.

• What kind of questions can be answered with exponential sums.

• How various cryptographic and coding theory problems lead to questions about exponential sums.

Unfortunately there is no systematic textbook on exponential sums. However one can find a variety of results and applications of exponential sums in [33, 45, 65, 75].

Acknowledgment. The author would like to thank Harald Niederreiter for careful reading of the manuscript and numerous helpful suggestions.