Math 663 - Fall 2001
Crosslisted as **EE 663**

Topics in Applied Mathematics:

Coding Theory

Instructor: Joachim Rosenthal **Time:** MWF 3:00–3:50

Course Description:

Coding theory deals with the storage and transmission of information, and the ability to recover the information as completely as possible even if some of the data is lost. A good example is the genetic code stored in a DNA molecule or the ISBN numbers used by book publishers. Modern coding theory started in 1948 with the work of Shannon [7], who divided it into a stochastic part and an algebraic part. In this course we will concern ourselves mainly with the latter part. In the algebraic sense, a block code can be viewed as an algebraic subset of an affine space over a finite field, hence techniques of algebraic geometry can be fruitfully applied to the study of codes.

Assuming familiarity with some basic notions of algebra like e.g. the construction of the Galois field $\mathbb{F} := GF(q)$ we will provide a self contained introduction to algebraic coding theory. Our main reference will be the standard text book by MacWilliams and Sloane [3].

We will provide an introduction to Hamming codes and a treatment of cyclic codes, BCH codes and Alternant codes. After a review of the theory of algebraic curves defined over a finite field we will introduce Goppa codes, an important class of codes obtained from algebraic curves and more general varieties which are defined over a finite field.

In a second part of the course we will provide an introduction to several important research topics such as convolutional codes, Turbo codes and more general Codes on Graphs. Some of these topics will relate to current research questions and we will treat these topics as time does allow it.

References

[1] V. D. Goppa. *Geometry and Codes.* Kluwer Academic Publisher, 1988.

[2] S. Lin and D. J. Costello Jr. *Error Control Coding: Fundamentals and Applications.* Prentice-Hall, Englewood Cliffs, NJ, 1983.

[3] F. J. MacWilliams and N. J.A. Sloane. *The Theory of Error-Correcting Codes.* North Holland, Amsterdam, 1977.

[4] B. Marcus and J. Rosenthal, editors. *Codes, Systems and Graphical Models.* IMA Vol. 123. Springer-Verlag, New York, 2001.

[5] Ph. Piret. *Convolutional Codes, an Algebraic Approach.* MIT Press, Cambridge, MA, 1988.

[6] S. Roman. *Coding and Information Theory.* Graduate Texts in Mathematics. Springer Verlag, New York - Berlin, 1992.

[7] C.E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423 and 623–656, 1948.

[8] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, 1993.