In a modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. The communication is almost always in a digital form, i.e., the information is represented as a sequence of discrete symbols. Examples of digital communication systems are wire-based and wireless transmission lines, network connections, hard disks for computers, HDTV, CD and DVD players.

Any communication is to some extent affected by noise. In order to detect or correct the errors that occur, the information is represented as a sequence of code words in an error-correcting code. The reliability of a communication system depends on physical conditions, but also on the error-correcting code and the decoding algorithm being used. Coding theory deals with methods to construct and analyze error-correcting codes and to decode them in an efficient manner. The quality of digital communication, in particular mobile communication, is totally dependent on efficient error correction.

Description of the scientific activity

The main emphasis will be to continue the study of problems initiated during the last few years. This focus on a better understanding on the structure of codes (mainly linear) for error correction or error detection.

In particular, we give a more detailed description of some problem areas which we want to explore in this project. We emphasis that this list is not exhaustive.

Correction beyond half the minimum distance

Consider a binary linear code of length n and minimum distance d for error-correction. Many different decoding methods has been studied, most of them correct at most (d-1)/2 errors. However, many more errors are in most cases correctable (at least in principle) using maximum likelihood decoding (MLD) (even if the complexity is too large in most cases for MLD to be feasible). A study of MLD gives information about what is possible to do (in principle) for any decoding method. Therefore a better understanding of the limitations of MLD is of both theoretical and practical interest. Recently, we have started a study of several aspects of MLD: minimal uncorrectable errors, error-correcting capability, and probability of correct decoding. We propose to continue this study.

Permutation codes

Ordinary power lines, built for transport of electrical power, can also be used for transmission of data at the same time. However, the level and types of noise are different from other transmission media. Some common types of noise in power lines can be overcome using codes based on a type of frequency hopping, see [4]. The construction of these codes requires permutation codes, that is codes where the codewords are permutations. Let P(n,d) be the maximal size of a permutation code of length n and minimal Hamming distance d. Except for a few small values of the parameters (see for example [3]), the best upper bound known on P(n,d) is n!/(d-1)!. A trivial lower bound is for P(n,d) is n. Improved lower bounds depend on explicit constructions of permutation codes. We propose to study improved constructions.

Codes and sequences

The research group at The Selmer Center has a long experience on the construction and analysis of families of sequences with good correlation properties that have found many and important applications. In this project we will focus on coordinate sequences over Galois rings, cross correlation of m-sequences, and Merit Factor of binary sequences.

The cross correlation of m-sequences is a heavily studied problem since it reveals many important problems of m-sequences. For instance the famous familie of Gold sequences used in the Global Positioning System(GPS) and in many other applications is based on this problem. We will continue our present research on the cross correlation of m-sequences where we are currently developing new and promising techniques in collaboration with Professor Hans Dobbertin from University of Bochum.

Merit Factor. A problem in sequence design which is considered to be very hard as well as extremely important for applications is to construct sequences with good aperiodic correlation properties. In 1977 Golay introduced a criterion of goodness for low periodic autocorrelation of binary sequences as an alternative measure to the minimal peak sidelobes, called the aperiodic Merit Factor. There are only sporadic examples of sequences with a merit factor more than 6.0. Recently, Matthew Parker and a master student Raymond Kristiansen were for the first time able to construct arbitarily long sequences with a Merit Factor larger than 6.3.

Graph based coding theory

During the last decade, much of the research focus in coding theory has shifted towards turbo codes and LDPC codes. These codes have random-like properties, are decoded by suboptimal but efficient iterative decoding algorithms, and provide performance close to Shannon's theoretical limits. Both classes of codes can be conveniently described by graphs rather than, as in the classical coding theoretic setting, by algebraic constructions: The turbo codes rely on component codes (block or convolutional) whose trellises are of manageable complexity, whereas LDPC codes are directly described by a sparse graph. Therefore, for convenience we here refer to these codes as graph based codes. Although the recent research efforts have produced much insight into the virtues of these classes of codes, there are still a number of unsettled questions. Among these remaining problems are the following: How do we optimize performance at short to medium block lengths? How do the graph based codes behave on nonstandard channels? How do we optimize systems for graph based coded modulation?