On the weight adjacency matrix of convolutional codes

Schneider, Hans-Gert
1 Introduction

Since its birth Coding Theory has been a fast developing subject in the intersection of mathematics, engineering and computer science. Problems and their solutions in this field typically arise from all three disciplines. As a consequence, many theorems may have an impact on only one or two of the disciplines. In general, there is a division between applications-driven research, which is connected to the engineering community and computer scientist, and the theoretical aspects of coding theory, which are more popular with mathematicians. One result, that is equally important and admitted deeper insight for both groups is the MacWilliams Identity for block codes, which was already proven as early as 1961. Ever since, it has been an important tool in studying codes and one of their most important properties: the weights of their code words.

From a mathematical point of view a code word is nothing but a sequence of information bits, which is encoded from a shorter sequence of message bits and the code is then formed by the sets of these code words. The information bits come from an alphabet, which is a priori free to chose. By virtue of the difference in length of the message and the code word, extra information is added to the codeword such that the transmission of the codeword via a noisy, that is an error-susceptible, channel becomes more reliable. The idea is simply that the added information may be used to detect and, if necessary, to correct a limited number of errors that occurred on the transmission of the code word. Of course, in the digital world the most common alphabet is \{0, 1\}, which is given the structure of the finite field \(\mathbb{F}_2\) and codes are therefore subsets of some vector space \(\mathbb{F}_2^n\) with a prescribed block length \(n\). For the error detection a metric is imposed on that vector space creating a notion of distance of codewords. This metric is in general most powerful, if the code itself has the structure of a vector space. The class of these codes is referred to as linear block codes and has from the very beginning been at the center of attention of both mathematicians and engineers. One of the challenges in coding theory has been to find large codes where each two distinct codewords of the code are separated by a high distance. Obviously, the complexity of determining the minimal distance of a code increases with its dimension. The MacWilliams identity now is a tool that relates the distance or weight distribution of all codewords of a given high dimensional code with that of a low dimensional code and vice versa. Its use for applications is hence apparent. The impact on the mathematical side is more subtle, but equally wide-spread.

The second fundamental theorem of MacWilliams is the MacWilliams Equivalence or Extension Theorem, which clarifies when two codes are equally good. Common sense tells that rescaling and permuting the coordinates of each codeword of a given code leads to a code, which has similar distance properties as the original code. Due to the MacWilliams Equivalence Theorem this extrinsic notion of code equivalence happens to coincide with the intrinsic notion of having a linear isometry between two codes. The relevance for applications of this mathematically beautiful result is obvious. It gives an important indication when two codes should be identified.
because they have identical error-correcting properties.

The two theorems of MacWilliams are exceptional in the sense that they are equally well-known in the mathematical and engineering community. The mathematical part of coding theory soon developed a life of its own and to a large extent uncoupled from their motivation in applications. New fields of applications for coding theory like deep space communication, mobile phones and most important the ubiquitous use of personal computers, led to modifications of the original setting on the engineering side, which only hesitantly found their way to mathematicians, partly, because the resulting mathematics is not elegant. One of the modifications is the insight that information bits are usually not sent in blocks, but as a continuous stream of blocks at different time instances. This may be achieved by choosing a linear block code and sending a codeword (one block) at each time instance. Thereby, however, one sends blocks that are not interconnected. Each block contains no information on the previous and the following block. The idea of interconnecting the blocks of the different time instances leads to convolutional codes, which are no longer linear block codes in the classical sense. Among these codes there are codes that have impressive error-correcting capabilities and they naturally come with an efficient decoding algorithm. Therefore they have been implemented by engineers in many applications fields for more than three decades. Despite their distribution the mathematical theory of convolutional codes has long been and still is underdeveloped. Many of the known facts are due to engineers with exceptional mathematical capabilities.

Due to their nature block codes may be seen as a subclass of convolutional codes. Hence it is natural to see whether the results known for block codes may be generalised to convolutional codes. Both theorems of MacWilliams are natural candidates to start with, but until recently no generalisations to convolutional codes had been known. The mathematical tools in coding theory typically come from the field of algebra. Convolutional codes, however, share the structure of linear systems, which have extensively studied in systems theory. This likewise young discipline opens a new perspective on convolutional codes and provides a powerful tool to study them, which has, for instance, been demonstrated in [31].

In this thesis I will employ these methods to generalise the classical MacWilliams Identity for linear block codes to convolutional codes. In order to do so I will use a generalisation of the distance distribution of a block code to convolutional codes, which has not yet been extensively studied, the weight adjacency matrix of a convolutional code. It contains information not only on the minimal distance of the code, but also on more refined distance parameters. One of its disadvantages is, that it is on the first sight not an invariant of the convolutional code. Whereas this problem has recently been resolved [8], it remains a problem that there is no known way to derive the weight adjacency matrix of a code from the code directly. Only by representing the code in a suitable way may one obtain the weight adjacency matrix using systems theoretic tools. This problem is reflected in the proof of the MacWilliams identity. Apart from the original proof employed by MacWilliams it was very soon discovered that the MacWilliams identity is from a mathematical point of view most elegantly proven using a discrete Fourier transform. My attempts
to copy this principle and by this prove the generalisation of the MacWilliams identity for convolutional codes have been fruitless due to the very nature of the weight adjacency matrix. However, in this thesis a proof is be given, which verifies the identity with the help of technical means to describe the weight adjacency matrix. Having proved the MacWilliams identity, I survey the possibilities of using it to do some preliminary steps to develop a theory of self-dual convolutional codes.

Finally I briefly demonstrate the problems connected with the generalisation of the MacWilliams Equivalence Theorem to convolutional codes. It appears that the greatest challenge here is to find out when two convolutional codes are really equally good. In other words, how many algebraic and distance parameters two convolutional codes need to share to call them equivalent. Although no final answer is given, I obtain a result that gives a partial solution for the class of convolutional codes which is most important for applications.