Diss. ETH No. 8730

A Linear Complexity Approach to Cyclic Codes

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZUERICH

for the degree of
Doctor of Technical Sciences

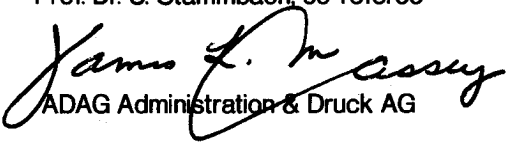
presented by

THOMAS SCHAUB

dipl. El. Ing. ETH
born October 29, 1952
citizen of Muttenz BL

accepted on the recommendation of

Prof. Dr. J. L. Massey, referee
Prof. Dr. U. Stammbach, co-referee



ADAG Administration & Druck AG
Zürich 1988

Abstract

Codes are widely used for error-correction or -detection and in cryptography. For error-correction or -detection a set of sequences with large Hamming distances is required, whereas in cryptography (stream ciphers) sequences with large linear complexities are needed. Blahut's theorem allows a unified treatment of both constraints by relating the linear complexity of a periodic sequence to the Hamming weight of the Discrete Fourier Transform (DFT) of its period.

The matrix formulation of the DFT is introduced. The linear complexity of a sequence is defined and its main properties are discussed. The linear complexity of periodic sequences is examined in detail and an extensive list of its properties is formulated. Then the Hamming weight of the DFT of a finite sequence is connected to the linear complexity of a periodic sequence by Blahut's theorem.

Cyclic codes are particularly suited for the DFT formulation. It is shown that a bound on the minimum distance of a cyclic code can be obtained by bounding the rank of a cyclic matrix. An algorithm is introduced that performs rank bounding of a matrix. As an example, the binary Golay code is analyzed and it is shown that its minimum distance is guaranteed entirely by the zeroes of its generator polynomial and that it does not depend on the fact that the code digits are restricted to the binary field. In a further step, the concept of zero-patterns is introduced. To illustrate the power of this approach, the validity of the classical bounds on the minimum distance of cyclic codes is proved and some of them are then extended.

The DFT approach can also be used for decoding purposes, namely to decode beyond the BCH bound. It is shown how to decode up to the Hartmann and Tzeng bound. Some hints are given on how codes can be transformed such that they satisfy the BCH bound. Finally, it is shown how the well-known formula of the weight enumerator for Reed Solomon codes can be derived using the DFT approach.

Zusammenfassung

Codes werden zur Fehlerkorrektur und -detektion sowie in der Kryptographie eingesetzt. Für die Fehlerkorrektur und -detektion benötigt man eine Menge von Sequenzen die sich gegenseitig durch eine grosse Hammingdistanz unterscheiden, während in der Kryptographie (Stream Ciphers) Sequenzen mit grosser linearer Komplexität gefordert werden. Das Theorem von Blahut erlaubt eine gemeinsame Behandlung beider Einschränkungen, indem es eine Beziehung zwischen der linearen Komplexität einer periodischen Sequenz und dem Hamminggewicht der diskreten Fouriertransformierten (DFT) seiner Periode angibt.

Die DFT wird als Multiplikation eines Vektors mit einer Matrix eingeführt. Die lineare Komplexität von Sequenzen wird definiert und ihre wichtigsten Eigenschaften werden besprochen. Für periodische Sequenzen wird die lineare Komplexität ausführlich behandelt und es werden dazu verschiedene Lemmas hergeleitet. Schliesslich wird mit Hilfe des Theorems von Blahut der Zusammenhang zwischen dem Hamminggewicht der DFT einer endlichen Sequenz und der linearen Komplexität einer periodischen Sequenz aufgezeigt.

Zyklische Codes eignen sich besonders für eine Behandlung mit der DFT Methode. Es kann eine Grenze für die minimale Hammingdistanz eines zyklischen Codes angegeben werden, indem man eine Grenze für den minimalen Rang einer entsprechenden zyklischen Matrix findet. Es wird ein Algorithmus angegeben, der eine solche Grenze für den Rang einer Matrix bestimmt. Als Beispiel wird der binäre Golay Code analysiert. Es zeigt sich, dass die minimale Hammingdistanz dieses Codes bloss durch die Nullstellen seines Generatorpolynoms bestimmt wird und nicht davon abhängt, dass die Komponenten der Codeworte dem binären Körper angehören. In einem weiteren Schritt wird das Konzept der "Nullstellen-Muster" eingeführt. Die anschliessende einfache Herleitung und die Erweiterung der klassischen Grenzen für die minimale Hammingdistanz zyklischer Codes rechtfertigen die neue Betrachtungsweise.

Die DFT Methode kann auch benützt werden, um empfangene Codeworte zu decodieren; u.a. auch dann, wenn man weiter als zur BCH Grenze decodieren will. Es wird gezeigt, wie es möglich ist, mit dieser Methode bis zur Grenze von Hartmann und Tzeng zu decodieren. Einige Hinweise werden auch gegeben, wie Codes transformiert werden können, so dass sie die BCH Grenze erfüllen.

Schliesslich wird gezeigt, wie die bekannte Gewichtsverteilung des Reed Solomon Codes mit Hilfe der DFT hergeleitet werden kann.