AN ALGEBRAIC APPROACH TO MDS AND DUAL GROUP CODES OVER FINITE ABELIAN GROUPS

by

ADNAN A. ZAIN

Submitted
in fulfilment of the requirements
of degree of
DOCTOR OF PHILOSOPHY

Electrical Engineering Department
INDIAN INSTITUTE OF TECHNOLOGY, DELHI

April, 1996

Dedicated to
my wife Suad
and
Children Arwa, Huda and Mohammed.

CERTIFICATE

This is to certify that the thesis entitled **"An Algebraic Approach to MDS and Dual Group codes over Finite Abelian Groups"** being submitted by **Adnan Abdulla Zain** to the Department of Electrical Engineering, Indian Institute of Technology, Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the bonafide research work carried out by him under my supervision and guidance. The results contained in this thesis have not been submitted to any other university or institute for the award of any degree or diploma.

29/10/96.

(B. Sundar Rajan)
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology, Delhi
New Delhi 110 016
INDIA

ACKNOWLEDGEMENTS

I take this opportunity to express my deep sense of gratitude towards my research supervisor Dr. B. Sundar Rajan for the invaluable guidance, advice and inspirations I received from him at every stage of this work, I benefited a lot from this constructive criticism, and thought provoking discussion with him.

Also, I would like to thank the faculty members and other staff of the E.E. Department, IITD, for their teaching and help during my stay in IITD.Special thanks also to Prof. H.M. Gupta, Prof. S. Prasad, S.S. Jamuar and G. Visweswaran.

I am grateful to ADEN University for allowing me do this research work and also to the Indian Council of Cultural Relations (ICCR) for granting me scholarship and financial support during my studies in India.

I also thank all my colleagues from Aden University who are doing their research in IITD for their help and support.

I am very much indebted to my dear family members in Yemen, especially my elder brother Mohammed for their encouragements, help and support.

Finally, I am proud of my wife Suad, daughters Arwa and Huda and son Mohammed, who had to sacrifice their personal priorities to cope up with my schedule.

Adnan A. Zain

ABSTRACT

A group code defined over a group G is a subset of G^n which forms a group under componentwise group operation. Group codes constitute an important ingredient in the construction of Geometrically Uniform codes, which include several important classes of known good codes as subclasses. In this thesis an algebraic approach, similar to the existing one for studying linear codes over finite fields, is developed for group codes over finite abelian groups, with emphasis on MDS codes, dual codes over arbitrary finite abelian groups and cyclic codes over elementary abelian groups.

Maximum Distance Separable (MDS) codes defined over abelian groups, which include as special cases MDS codes over finite fields, and cyclic groups, are characterized. The characterization is in terms of a matrix over the endomorphism ring of the abelian group, called associated matrix of the code, which uniquely defines the code. The necessary and sufficient conditions for the associated matrix to represent a MDS group code over abelian group is derived. The specific endomorphisms which, when appear as entries of the associated matrix, that lead to linear codes over finite fields are identified. The well known characterization of linear MDS codes over finite fields is shown to be a special case of the characterization obtained for MDS group codes over elementary abelian groups. A nonexistence result that shows that $(k+s,k)$ MDS group codes over elementary abelian group of order p^m do not exist, for $s,k \geq 2$, if $\max\{s,k\} \geq p^m$, is proved. When specialized to linear codes over finite fields this leads to the known non-existence results for linear codes over finite fields. Also, it is shown that not all group codes over elementary abelian groups are linear codes over finite fields, whereas every linear code over an integer residue ring is a group code over appropriate cyclic group and vice verse.

Specializing to the case of group codes over cyclic groups it is proved that over cyclic groups with M elements, where $M = p_1^{d_1} p_2^{d_2} \ldots p_m^{d_m}$, (k+s,k) MDS codes, for all $s,k \geq 2$, do not exist if $\max\{s,k\} \geq \min\{p_1, p_2, \ldots, p_m\}$.

The dual code of a systematic group code over an abelian group is characterized in terms of the endomorphisms of the abelian group. It is shown that the endomorphisms of the dual code for a given code are related to the defining endomorphisms of the code. For the special case of group codes over cyclic groups the identification of dual code turns out to be much simpler. For cyclic groups it is shown that the dual of an MDS group code is also MDS. The class of self-dual group codes over abelian groups are also characterized.

Discrete Fourier transform techniques to study the class of cyclic codes and related codes over finite fields are well known. This transform approach is extended to study cyclic codes over elementary abelian groups for the case when the length of the code equal to size of the group minus one. This class of codes include the conventional Reed-Solomon codes as special cases. The best codes, obtained by computer search, in terms of maximum minimum Euclidean distance, for length 3 over C_2^2 and length 7 over C_2^3, for certain code sizes, are tabulated. Some of these equal in minimum squared Euclidean distance the best Isaksson-Zetterberg codes.

CONTENTS