CODE SEQUENCES FOR SPREAD SPECTRUM MULTIPLE ACCESS AND CRYPTOGRAPHIC APPLICATIONS

BY

P. V. A. NARASIMHAM

Department of Electrical Engineering

THESIS SUBMITTED
IN FULFILMENT OF THE REQUIREMENTS
OF THE DEGREE OF

DOCTOR OF PHILOSOPHY

to the

INDIAN INSTITUTE OF TECHNOLOGY, DELHI

New Delhi - 110 016, India

May, 1991

CERTIFICATE

This is to certify that the thesis entitled "**Code Sequences for Spread Spectrum Multiple Access and Cryptographic Applications**", being submitted by P.V.A.Narasimham to the Department of Electrical Engineering, Indian Institute of Technology, New Delhi, for the award of degree of Doctor of Philosophy, is a bonafide research work carried out by him under our 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.

Surendra Prasad
Professor,
Department of Electrical Engineering,
Indian Institute of Technology,
New Delhi 110 016.

Vinod Chandra,
Professor,
Department of Electrical Engineering,
Indian Institute of Technology,
New Delhi 110 016.

Acknowledgements

It has, indeed, been a great privilege for me to work under Professor Surendra Prasad towards my Ph.D. dissertation. No amount of words can express my sense of gratitude to him for his constant encouragement and supervision during the course of this research programme.

I am also highly grateful to Shri. Y.S.Rao, General Manager (satellite), Centre for Development of Telematics, Bangalore, who took a keen interest in the progress of my research work and helped me in many ways to enable me to complete this dissertation work successfully. Special thanks are also due to the Chairman, Telecom Commission, Government of India, for granting me permission to pursue this research programme as an external candidate,

I would also take this opportunity to express my gratitude to Mrityunjoy whose constant inspiration and cooperation would always remain fresh in my memory.

Finally, I am immensely thankful to Janaki, my wife for her constant encouragement, cooperation and sacrifices through-out the course of this disseration work.

P.V.A.Narasimham.

Abstract

Spread spectrum multiple access (SSMA) methods are generally used in satellite communication systems to combat jamming as well as to protect sensitive information from eavesdropping etc. The presently used SSMA systems can be broadly classified into two categories, viz., the direct sequence systems and the frequency hopping systems. Both these require the use of code sequences with certain kinds of correlation and complexity properties. Code division multiplexing is the important mechanism of multiplexing in these systems. Thus the spreading sequences or codes are required to exhibit low auto-correlation and cross-correlation sidelobes to minimize cross-interference. The families of Gold and Gold-like sequences, Kasami sequences and several others exhibit these properties and are commonly used. Further, in order to make evesdropping difficult, it is desirable that the sequences should have a *large equivalent linear span*. Finally, to accommodate a large number of users, it is required that the cardinality or the size of the set containing the desirable kind of code words be large. Very few of the presently known codes satisfy all these requirements simultaneously. Similarly, there are very few known classes of frequency hopping patterns which combine the requirements of the so-called optimal Hamming correlation properties with high linear span.

An attempt has been made in this thesis to introduce many new classes of code sequences for the spread spectrum multiple access systems with a cryptographic flavor. More specifically, we have attempted here to derive techniques which can yield all the three desired features mentioned above, in the designed code sequence families. It is demonstrated that bit interleaving techniques which can be defined around certain known families of code sequences can be used effectively to generate additional classes of sequences which exhibit many of the desired properties.

To start with, a new family of large sequence sets, called here the *Narasimham-Prasad sequences* have been introduced. These are obtained by cyclically combining different phases of an m-sequence with certain related elementary sequences, generated by an irreducible polynomial. The sequence sets of this class are shown to have peak values of the CCF and out of phase ACF which are of the same order (being in fact, somewhat lower) as those of the famous Gold and Gold-like sequence sets. While the linear span of these sequence sets is not high, these are seen to exhibit an interleaved

structure which is exploited subsequently to generate additional families of sequences with both good correlation as well as linear span properties.

The use of bit-interleaving for synthesis or construction of sequences has received passing treatment in the literature. This technique, however, is potentially very powerful, and in this work we have attempted to demonstrate this fact. The use of this technique in the present work has been primarily motivated by the following two observations: (a) certain well known sequence classes have an interleaved structure in terms of smaller m-sequences and (b) the cross-correlation properties of such interleaved sequence sets are only dependent on the number of certain null subsequences that arise in the modulo-two sum of the member sequences. Further, these two properties are independent of the actual m-sequence used in the interleaved representation. These general findings have made it possible for us to introduce *three* classes of interleaved sequence sets, viz., the so-called *Kasami-like sequence sets*, the *Niho-like sequence sets* and the *Narasimham-Prasad like sequence sets*, which are derived, as the name suggests, from the parent sequences of the corresponding types. The new sequence families are shown to share the correlation properties of the corresponding parent families. The linear complexities of all the three classes of sequence sets, however, are seen to be very high as compared to those of the parent sequence classes. An important additional advantage offered by this construction technique is that many such sets of sequences can be obtained for each set of the parent class.

Later, we generalize this construction procedure into an even more powerful concept of *level-k interleaving*. With the help of this generalized concept it is possible to get phenomenal increase in the density of optimal sequence sets, along with significant enhancements in the values of their linear span.

The extension of interleaving techniques for the generation of optimal frequency hopping patterns for the frequency hopped spread spectrum systems is next investigated. It is shown that in combination with the concept of σ_k-transforms, the process of interleaving can now be used to generate additional optimal families of frequency hopping patterns starting from m-sequences and m-like sequences. Once again, it is possible to obtain several sequence sets starting from each parent set of a known family of such patterns.

Finally, we discuss a few miscellaneous sequence sets and their properties. The discussion on the interleaved structure of m-sequences and m-like sequences, which form the basis of much of the work on the thesis, is concluded with some thoughts on further possible manipulations in the interleaved structure. It is shown, for example that inversion of the null subsequences in certain subclass of m-like sequences can yield a considerable improvement in the linear span of these at a marginal cost in terms of their ACF properties (the ACF sidelobes values of "-1" are replaced with sidelobe values of "-1" and "3"). Similar properties are shown to be available for similar modifications on the level-k m-like sequences.

Table of Contents