ETH zürich

ETH Library

On Euclidean-space group codes

Doctoral Thesis

Author(s):
Loeliger, Hans-Andrea

Publication date:
1992

Permanent link:
https://doi.org/https://doi.org/10.3929/ethz-a-000640087

Rights / license:
In Copyright - Non-Commercial Use Permitted

This page was generated automatically upon download from the ETH Zurich Research Collection.
For more information, please consult the Terms of use.

Diss. ETH No. 9720

On Euclidean-Space Group Codes

A dissertation submitted to the

SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZÜRICH

for the degree of
Doctor of Technical Sciences

presented by

HANS-ANDREA LÖLIGER
dipl. El. Ing. ETH
born May 26, 1961
citizen of Pratteln BL

accepted on the recommendation of

Prof. Dr. J. L. Massey, referee
Prof. Dr. I. Ingemarsson, co-referee

1992

Abstract

Binary linear codes are well known to be 'matched' to binary signaling on a Gaussian channel. Recently, linear codes over Z_M (the ring of integers modulo M) have been presented which are similarly matched to M-ary phase modulation. Motivated by these new codes, the general problem of matching signal sets to generalized linear algebraic codes is addressed. A definition is given for the notion of matching. It is shown that any signal set in N-dimensional Euclidean space that is matched to an abstract group is essentially what Slepian has called a 'group code for the Gaussian channel'. If the group is commutative, this further implies, by a result of Ingemarsson, that any such signal set is equivalent to coded phase modulation with linear codes over Z_M.

It is well known that, for high signal-to-noise ratio, phase modulation does not effectively exploit the capacity of the bandlimited Gaussian channel. The above result, however, implies that all signal sets that are matched to commutative groups are subject to these same limits on performance. This motivates the investigation of signal sets matched to noncommutative groups, and of 'linear' codes over such groups. A general construction for large noncommutative signal sets is presented that is based on linear codes and their automorphism group.

Convolutional codes over groups, as recently introduced by Forney and Trott, are an attractive alternative to linear block codes over groups. A careful definition of such codes is proposed together with the basic system theory. A major problem of convolutional codes over arbitrary groups is that there is no obvious equivalent to the familiar linear shift-register encoders of convolutional codes over fields. A solution to this problem is presented in the form of a canonical feedforward encoder structure that contains nonlinear, i.e., nonhomomorphic, mappings.

Zusammenfassung

Lineare Binärcodes passen auf natürliche Weise mit binärer Modulation zusammen. Vor kurzem wurden nun auch lineare Codes über dem Ring Z_M der ganzen Zahlen modulo M vorgestellt, die in gleicher Weise mit M-wertiger Phasenumtastmodulation zusammenpassen. Der Versuch, dieses Zusammenpassen zu verallgemeinern, führt zunächst zur mathematischen Definition einer Signalkonstellation, die an eine Gruppe angepasst ist. Es wird sodann gezeigt, dass solche Signalkonstellationen im Wesentlichen identisch sind mit 'Gruppencodes für den Gausskanal', einem von Slepian geprägten Begriff. Aus einem Ergebnis von Ingemarsson folgt daher, dass Signalkonstellationen, die an eine abelsche Gruppe angepasst sind, einer Kombination von M-wertiger Phasenumtastmodulation mit einem linearen Code über Z_M äquivalent sind.

Es ist eine wohlbekannte Tatsache, dass Phasenmodulation die Kapazität eines bandbegrenzten Gauss'schen Kanals mit grossem Rauschabstand nur schlecht ausnützt. Das erwähnte Ergebnis bedeutet aber, dass alle Signalkonstellationen, die an eine abelsche Gruppe angepasst sind, der gleichen Beschränkung unterworfen sind. Dies regt die Erforschung von Signalkonstellationen an, die an nicht-abelsche Gruppen angepasst sind, und zur Suche nach 'linearen' Codes über solche Gruppen. Ein Ergebnis in dieser Richtung ist ein Verfahren zur Konstruktion grosser nicht-abelscher Gruppen, welches von linearen Codes und ihrer Automorphismengruppe ausgeht.

In diesem Zusammenhang liegt es nahe, den Begriff des Faltungscodes auf Gruppen zu erweitern, wie dies Forney und Trott vor kurzem vorgeschlagen haben. Der zweite Teil dieser Arbeit befasst sich daher mit solchen Faltungscodes über Gruppen. Aufbauend auf einer sorgfältig begründeten Definition solcher Codes werden die Grundzüge einer entsprechenden Systemtheorie über Gruppen hergeleitet. Ferner wird ein zentrales Problem solcher Codes angegangen, nämlich das Fehlen einer offensichtlichen Entsprechung für die wohlbekannten linearen Schieberegister-Encoder, und eine Lösung in Form einer kanonischen Encoderstruktur mit nicht-linearen, d.h. nicht-homomorphen Abbildungen angegeben.