Linear Algebra and its Applications 490 (2016) 124–144

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Linear tree codes and the problem of explicit constructions

Pavel Pudlák [1]

ARTICLE INFO

Article history:
Received 14 December 2013
Accepted 27 October 2015
Available online 12 November 2015
Submitted by R. Brualdi

MSC:
94B60
15B99

Keywords:
Tree code
Error correcting code
Triangular totally nonsingular matrix

ABSTRACT

We reduce the problem of constructing asymptotically good tree codes to the construction of triangular totally nonsingular matrices over fields with polynomially many elements. We show a connection of this problem to Birkhoff interpolation in finite fields.

1. Introduction

Tree codes, in the sense we are going to use in this paper, were introduced by L.J. Schulman in 1993. He showed that asymptotically good tree codes can be used in efficient interactive communication protocols and proved by a probabilistic argument that such tree codes exist [9,10]. He posed as an open problem to give an explicit effectively computable construction of them. Efficiently constructible tree codes would be very useful in designing robust interactive protocols. The field has attracted a lot of attention in recent years, however this central problem still remains open. A possible solution

E-mail address: pudlak@math.cas.cz.

[1] The author is supported by the grants P202/12/G061 of GACR and RVO: 67985840.

http://dx.doi.org/10.1016/j.laa.2015.10.030
0024-3795/

may be the construction of Moore and Schulman [5] found recently. Their construction provides asymptotically good tree codes if a certain number-theoretical conjecture, introduced in their paper, is true. The conjecture is inspired by some well-known results about exponential sums and is supported by numerical evidence.

In this paper we propose a different approach to this problem. We study generator and parity check matrices of linear codes and reduce the problem to constructing triangular totally nonsingular matrices over fields of polynomial size. A lower triangular matrix M is called triangular totally nonsingular if every square submatrix of M whose diagonal is entirely in the lower triangle is nonsingular. Explicit examples of such matrices are known over the field of real numbers, and these include matrices with integral elements. One can also show that triangular totally nonsingular matrices exist over finite fields of exponential size. The question whether they exist over finite fields of polynomial size (or at least subexponential size) is open. Since totally nonsingular matrices (i.e., matrices whose *all* square submatrices are nonsingular) do exist over fields of linear size, we conjecture that there exist triangular totally nonsingular matrices over fields of polynomial size.

In this way we may be reducing the problem of constructing tree codes to a more difficult problem. But since the concept of triangular totally nonsingular matrices is very natural, the problem of constructing such matrices over small fields is of independent interest. We also hope that due to this connection we will be able to draw attention of the linear algebra community to this important open problem in coding theory.

Here is a brief overview of the paper. In Section 1 we define linear codes and prove some basic facts about them. Some facts in this section are well-known, or well-known in some form. In particular, the existence of asymptotically good linear tree codes was first proved by Schulman. In Section 2 we observe that one can concatenate a tree code with a constant size alphabet and input length $\log n$ with a tree code with an alphabet of polynomial size and input length n in order to obtain a tree code with a constant size alphabet and input length $O(n \log n)$. Since the "short" tree code can be found by brute force search in polynomial time, it suffices to construct in polynomial time an asymptotically good tree code with an alphabet of polynomial size in order to get a polynomial time construction of asymptotically good tree codes. This is also a well-known fact and is included for the sake of completeness.

In the main part of the paper we focus on linear tree codes of rate 1/2. In Section 4 we give a characterization of parity check matrices of linear tree codes with a given minimum distance. In Section 5 we introduce MDS linear tree codes. We show that an MDS linear tree code of rate 1/2 is determined by a triangular totally nonsingular matrix. Since the minimum distance of rate 1/2 MDS tree codes is greater than 1/2, in order to solve the construction problem, it suffices to construct triangular totally nonsingular matrices over fields of polynomial size. We discuss some approaches to the problem of constructing such matrices in Section 6. In the last section we show a connection between MDS linear tree codes and the Birkhoff interpolation problem.