Finite Fields and Their Applications 25 (2014) 94–105

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Spread decoding in extension fields

Felice Manganiello [a,1], Anna-Lena Trautmann [b,*,2]

[a] Department of Mathematical Sciences, Clemson University, United States
[b] Institute of Mathematics, University of Zurich, Switzerland

ARTICLE INFO

Article history:
Received 21 February 2013
Received in revised form 5 July 2013
Accepted 12 August 2013
Available online 18 September 2013
Communicated by Shojiro Sakata

MSC:
11T71

Keywords:
Network coding
Subspace codes
Grassmannian
Projective space
Spreads

ABSTRACT

A spread code is a set of vector spaces of a fixed dimension over a finite field $\mathbb{F}_q$ with certain properties used for random network coding. It can be constructed in different ways which lead to different decoding algorithms. In this work we consider one such representation of spread codes and present a minimum distance decoding algorithm which is efficient when the code words, the received space and the error space have small dimension.

1. Introduction

In network coding, one is interested in efficient communication between different sources and receivers in a network which is representable through a directed acyclic graph. In multicast, one is looking at the communication between a sender and several receivers, where each receiver should receive the message sent by the sender. In [9,11] it is proven that one achieves the communication rate simply by allowing nodes of the network to forward random linear combinations of its information vectors. If the underlying topology of the network is unknown we speak about *random linear network coding*. Since linear spaces are invariant under linear combinations, they are what is needed as code

* Corresponding author.
E-mail addresses: manganm@clemson.edu (F. Manganiello), anna-lena.trautmann@math.uzh.ch (A.-L. Trautmann).

[1] The author is partially supported by Swiss National Science Foundation Grant nos. 126948 and 138738.
[2] The author is partially supported by Swiss National Science Foundation Grant nos. 126948 and 138080, and Forschungskredit of the University of Zurich, Grant no. 57104103.

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.08.002

words [8]. It is helpful for decoding to constrain oneself to subspaces of a fixed dimension, in which case we talk about *constant dimension codes*.

One class of constant dimension codes is the one of *spread codes*. These codes have maximal minimum distance and are optimal in the sense that they achieve the Singleton-like bound on the cardinality of network codes. They can be constructed with the help of companion matrices of irreducible polynomials, as explained in [13].

In this work we translate the construction of [13] to an extension field setting and evolve a minimum distance decoding algorithm for spread codes in this setting. The complexity of this new algorithm depends on different parameters than the algorithms of [5,8,14], which are also applicable to spread codes. Hence the new algorithm has an improved performance for network realizations where the code words and the received spaces have small dimension.

The paper is structured as follows: In Section 2 we give some preliminaries on random network coding and constant dimension codes. The main results of this work are found in Section 3, where we first show how to translate the spread code construction of [13] into a different setting and then explain how decoding can be done in this setting. We study the complexity of the decoding algorithm and give comparison to other known decoding algorithms in Section 4. Moreover, we study the probability that the algorithm terminates after fewer steps than the worst case scenario. We conclude this work in Section 5.

2. Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. We denote the set of all subspaces of $\mathbb{F}_q^n$ by $PG(n,q)$ and the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, called the Grassmannian, by $\mathcal{G}_q(k,n)$. The general linear group GL_n is the set of all invertible $n \times n$-matrices with entries in $\mathbb{F}_q$. Moreover, the set of all $k \times n$-matrices over $\mathbb{F}_q$ is denoted by $Mat_{k\times n}$.

Let $U \in Mat_{k\times n}$ be a matrix of rank k and

$$\mathcal{U} = \mathrm{rs}(U) := \text{row space}(U) \in \mathcal{G}_q(k,n).$$

We usually consider the matrix U to be in reduced row echelon form.

A *subspace code* is simply a subset of $PG(n,q)$ and a *constant dimension code* is a subset of the Grassmannian $\mathcal{G}_q(k,n)$.

The *subspace distance*, given by

$$d_S(\mathcal{U},\mathcal{V}) = \dim(\mathcal{U}+\mathcal{V}) - \dim(\mathcal{U}\cap\mathcal{V})$$

for $\mathcal{U},\mathcal{V}$ two subspaces of $\mathbb{F}_q^n$, is a metric function on $PG(n,q)$. It induces a metric on $\mathcal{G}_q(k,n)$ by

$$d_S(\mathcal{U},\mathcal{V}) = 2k - 2\dim(\mathcal{U}\cap\mathcal{V})$$

for any $\mathcal{U},\mathcal{V} \in \mathcal{G}_q(k,n)$. The minimum distance of a subspace code $\mathcal{C} \subseteq PG(n,q)$ is defined as

$$d(\mathcal{C}) := \min\left\{ d_S(\mathcal{U},\mathcal{V}) \,\middle|\, \mathcal{U},\mathcal{V}\in\mathcal{C},\ \mathcal{U}\neq\mathcal{V} \right\}.$$

The subspace distance is a suitable distance for coding over the operator channel [8], where errors and erasures can be corrected. An error corresponds to an inserted erroneous vector, i.e. an increase in dimension, whereas an erasure is a decrease in dimension of the code word. The error-and-erasure correction capability of a code $\mathcal{C} \subseteq PG(n,q)$ with minimum distance $d(\mathcal{C})$ is

$$t := \left\lfloor \frac{d(\mathcal{C})-1}{2} \right\rfloor.$$

Some constructions for constant dimension codes can be found e.g. in [3,7,8,14,15].