Finite Fields and Their Applications 52 (2018) 174–199

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Induced weights on quotient modules and an application to error correction in coherent networks

Eimear Byrne

School of Mathematics and Statistics, University College Dublin, Ireland

A R T I C L E   I N F O

Article history:
Received 5 October 2016
Received in revised form 9 January 2018
Accepted 11 April 2018
Available online 27 April 2018
Communicated by W. Cary Huffman

MSC:
94B05
94B25
94B60
94B65
94B99
12E20

Keywords:
Network code
Network error-correction
Coherent networks
Plotkin bound
Elias bound
Finite Frobenius ring
Homogeneous weight

A B S T R A C T

We consider distance functions on a quotient module M/K induced by distance functions on a module M. We define error-correction for codes in M/K with respect to induced distance functions. For the case that the metric is induced by a homogeneous weight, we derive analogues of the Plotkin and Elias–Bassalygo bounds and give their asymptotic versions. These results have applications to coherent network error-correction in the presence of adversarial errors. We outline this connection, extending the linear network coding scheme introduced by Yang et al.

E-mail address: ebyrne@ucd.ie.

https://doi.org/10.1016/j.ffa.2018.04.006

1. Introduction

Coding in data communication networks has been shown to offer many advantages in terms of data rate, error correction and security. Many coding models have been considered for a variety of networks. Error-correction in *coherent* network coding has been considered in [16,19,23–25,27]. For non-coherent networks, where the network topology is unknown, subspace codes have been shown to offer good solutions for error correction and have been widely studied. This is also often referred to as *random* network coding, albeit a different notion of random network coding as introduced by Ho et al. in [12].

We consider the set-up for coherent network coding described in [23–25]. In coherent network coding the network topology is known and the *encoding vectors* are often chosen deterministically, according to connectivity of the network. In [14], the authors describe a polynomial-time deterministic algorithm to generate a linear code for error-free networks, which is extended in [25] for networks with errors.

The network is described as a directed acyclic graph with a single source node and several sink nodes, or receivers. The source transmits some m data packets, one for each edge with which it is incident, all m of which are to be delivered to each sink. This is referred to as *multicast*. Successful delivery of all data packets to a sink requires at least m edge disjoint paths from the source to the sink. In a linear network coding scheme, at each node in the network linear combinations of packets on its incoming edges are transmitted along its outgoing edges. Transfer of data from source to sink nodes may be described by a *transfer matrix*, which can be assumed to be invertible if its coefficients are chosen from a large enough ring or field. Full details of this approach for a finite field alphabet may be read in [16]. A transfer matrix F is constructed as $F = (I - K)^{-1}$, where an entry of K is non-zero only if the corresponding entry of the adjacency matrix of the line graph of the network is non-zero, that is, if K 'fits' this adjacency matrix. Each column of F corresponds to an edge in the network; a particular sink only 'sees' the columns of F corresponding to the edges incident with it. The projection of F onto these columns yields a matrix whose row space is a linear code and the sink can retrieve all m packets if the particular m-subset of its rows (corresponding to the source packets) are linearly independent.

Error correction in the coherent network coding model is an important and challenging problem. A single (Hamming) error introduced in a link can propagate through the network infecting many other links. However, inherent redundancy in the network means that some error patterns are invisible to a given sink node, specifically, those error patterns corresponding to elements orthogonal to its code. Aside from these irrelevant errors, the code of a sink node may have some error correction capability.

In an effort to quantify these properties of a linear network code, in [25] the authors present refinements of the sphere-packing, Singleton and Gilbert–Varshamov bounds for an arbitrary linear error-correcting network code over a finite field. The error-model considered is for *adversarial errors*, that is, where it is assumed that an adversary has access to some number of edges in the network. The bounds in [25] and the references