Information Processing Letters 115 (2015) 507–511

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Randomized and deterministic algorithms for network coding problems in wireless networks

Zoltán Király [a,c], Erika R. Kovács [b]

[a] Department of Computer Science, Eötvös Loránd University, Budapest, Hungary
[b] Department of Operations Research, Eötvös Loránd University, Budapest, Hungary
[c] MTA-ELTE Egerváry Research Group, Hungary

ARTICLE INFO

Article history:
Received 13 February 2014
Received in revised form 23 October 2014
Accepted 25 November 2014
Available online 28 November 2014
Communicated by M. Chrobak

Keywords:
Network coding
Randomized algorithms
Gaussian relay networks

ABSTRACT

Network coding is a method for information transmission in a network, based on the idea of enabling internal nodes to forward a function of the incoming messages, typically a linear combination. In this paper we discuss generalizations of the network coding problem with additional constraints on the coding functions called network code completion problem, NCCP. We give both randomized and deterministic algorithms for maximum throughput-achieving network code construction for the NCCP in the multicast case. We also introduce the related problem of fixable pairs, investigating when a certain subset of coding coefficients in the linear combination functions can be fixed to arbitrary non-zero values such that the network code can always be completed to achieve maximum throughput. We give a sufficient condition for a set of coding coefficients to be fixable. For both problems we present applications in different wireless and heterogeneous network models.

1. Introduction

Network coding is a fairly new area on the boundary of information and graph theory, initiated by the seminal paper of Ahlswede et al. [1]. In contrast to a classical source-terminal encoding-decoding information transmission scheme, intermediate nodes of the network are enabled as well to perform coding. Properly chosen coding functions may increase throughput, security and reliability of a network [2]. Most algorithms apply linear network codes, when intermediate nodes forward a linear combination of the incoming messages. The coefficients in these linear combinations are called coding coefficients. In this paper, we investigate various linear network coding problems with partially predetermined coding coefficients. The first version of this problem, called deterministic network coding, was introduced by Harvey, Karger and Murota [3]. They reduced both the unicast and multicast cases to matrix completion. In order to avoid confusion of 'deterministic algorithm' and 'deterministic network coding problem' we call the latter the network code completion problem (NCCP) throughout the paper. In [4], Fragouli and Ebrahimi showed that the NCCP has an application for a Gaussian relay network model introduced by Avestimehr, Diggavi and Tse in [5]. For this special case, several unicast [6–8], and multicast [4] algorithms were given. These approaches rely on the layered structure of the model, which is a strong restriction compared to the NCCP. Former randomized algorithms for the NCCP such as [9] have a lower bound on the required field size which depends on the size of the network and the number of terminals. We eliminate the first factor and present randomized algorithms for both the unicast and multicast cases over any field of size greater than the number of terminals. Our approach relies on the idea of a simple deterministic algorithm for the NCCP,

E-mail addresses: kiraly@cs.elte.hu (Z. Király), koverika@cs.elte.hu (E.R. Kovács).

http://dx.doi.org/10.1016/j.ipl.2014.11.012

constructing a solution for the multicast problem from solutions of the unicast special case.

We also define a related new problem, called 'fixable pairs problem'. We give a sufficient condition for a subset of coding coefficients that can be fixed *arbitrarily* to nonzero values, such that the remaining coefficients can be chosen properly to attain a feasible network code. We present applications of this model, and give necessary and sufficient conditions for the solvability of network coding problems in heterogeneous networks.

The rest of the paper is organized as follows. In Section 2 definitions of network coding and its investigated special cases are given. In Section 3 we present deterministic and randomized algorithms for the NCCP. In Section 4 we discuss the problem of fixable pairs and present some applications in heterogeneous networks.

2. Problem formulation

Definition 1. Let $\mathbb{F}_q$ be a finite field of size q and let $\mathbb{F}_q^k$ denote the k-dimensional vector space over $\mathbb{F}_q$ and let $\mathbf{e}_i$ denote the ith unit vector in $\mathbb{F}_q^k$, $1 \le i \le k$. For a set W of vectors in $\mathbb{F}_q^k$, $\langle W \rangle$ denotes the linear subspace spanned by W. Let $\mathbf{M} = (M_1, M_2, \dots, M_k)$, $M_i \in \mathbb{F}_q$, $1 \le i \le k$ be an ordered set of k messages.

Let $D = (V, A)$ be an acyclic directed graph with node and arc set V and A, respectively, with a single source node s, from which the messages are sent, and a set of nodes $T \subseteq V - s$ called **terminals** where the messages are sent to. Without loss of generality we may assume that s has k leaving arcs $a_1, \dots, a_k$. A **linear network code** of k messages on D over $\mathbb{F}_q$ is a mapping $\mathbf{c} : A \to \mathbb{F}_q^k$ satisfying $\mathbf{c}(a_i) = \mathbf{e}_i$ which fulfills the **linear combination property**:

$$\mathbf{c}(uv) = \sum_{wu \in A} \alpha(wu, uv)\mathbf{c}(wu)$$

where $\alpha(wu, uv) \in \mathbb{F}_q$. Coefficients $\alpha(wu, uv)$ are the **local coefficients** of the network code and function $\mathbf{c}$ denotes the **global coefficients**. That is, on arc a message $\mathbf{c}(a) \cdot \mathbf{M}$ is sent. We will use the notation $\langle \mathbf{c}, u \rangle = \langle \{\mathbf{c}(wu) \mid wu \in A\} \rangle$. For a linear network code $\mathbf{c}$, a node v **can decode** (or receives) message M_i, if $\mathbf{e}_i \in \langle \mathbf{c}, v \rangle$. A network code is **feasible** if every node t in T can decode every message M_i, $1 \le i \le k$. The **network coding problem** given by parameters D, s, T, k, q is to construct a feasible network code of k messages in D over $\mathbb{F}_q$. Note that global coefficients can be determined from local coefficients, hence feasibility of the latter can be defined accordingly. If $|T| = 1$, the problem is called a **unicast** problem, while the general case is called **multicast**. The latter can be regarded as a network code construction which is simultaneously feasible for $|T|$ unicast problems.

Definition 2. Let $L \subseteq A \times A$ be the set of consecutive pairs of arcs: $L = \{(wu, uv) \mid w, u, v \in V,\ wu, uv \in A\}$. For the sake of shortness members of L are called **pairs**. The local coefficients of a network code form a mapping on the pairs: $\alpha : L \to \mathbb{F}_q$. For a subset of pairs $M \subseteq L$, a mapping $\alpha_0 : M \to \mathbb{F}_q$ is **extendable**, if there exist local coefficients α of a feasible network code such that $\alpha = \alpha_0$ on M. Given a network coding problem with a subset of pairs $M \subseteq L$ with a mapping $\alpha_0 : M \to \mathbb{F}_q$, the **network code completion problem** is to decide whether α_0 is extendable.

Definition 3. We say that $M \subseteq L$ is **fixable** if **any** nonzero-valued mapping $\alpha_0 : M \to \mathbb{F}_q - \{0\}$ is extendable. The **fixable pairs problem** is to decide whether a given set M is fixable or not. For a pair $\ell = (wu, uv) \in L$, wu and uv are the **first** and **second** arcs of the pair, respectively, and u is the **central node** of the pair. Two pairs ℓ_1 and ℓ_2 are **consecutive** if the second arc of ℓ_1 is the first arc of ℓ_2. A path contains a pair, if it contains both of its arcs. For a subset of pairs $M \subseteq L$, a node is M**-influenced** if it is the central node of a pair in M. A set of paths is M**-independent** if they are pairwise arc-disjoint and any M-influenced node is contained by at most one of them.

We use two well-known technical statements several times in this paper. Their proof can be found for example in [10].

Claim 4. *Let vectors $\mathbf{v}_1, \dots, \mathbf{v}_k \in \mathbb{F}_q^k$ form a basis of $\mathbb{F}_q^k$ and let $\mathbf{v} \in \mathbb{F}_q^k$. Then*

- *there is at most one value $\alpha \in \mathbb{F}_q$* not *satisfying that the set $\{\mathbf{v}_1' = \mathbf{v}_1 + \alpha\mathbf{v}\} \cup \{\mathbf{v}_i\}_{i=2}^k$ is also a basis,*
- *there is at most one value $\beta \in \mathbb{F}_q$* not *satisfying that the set $\{\mathbf{v}_1' = \beta\mathbf{v}_1 + \mathbf{v}\} \cup \{\mathbf{v}_i\}_{i=2}^k$ is also a basis.*

3. Network coding completion problem

The multicast NCCP is equivalent to determining the simultaneous max rank completion of the transfer matrices, and if the field size is greater than the number of matrices given, then the matrices have a simultaneous max rank completion as proved in [9,3]. This result can be reformulated as follows.

Theorem 5. *(See [3].) If $q > |T|$, a mapping is extendable over $\mathbb{F}_q$ if and only if for every $t \in T$ it is extendable for the one-element terminal set $\{t\}$. Such an extension can be found in polynomial time.*

We give another, simple proof for this theorem. We use the polynomial time algorithm of [3] for the unicast case as a subroutine.

Proof of Theorem 5. For a terminal $t \in T$, let α_t denote the extension of α_0 which is feasible for t and let $\mathbf{c}_t : A \to \mathbb{F}_q^k$ denote the corresponding global coefficients. We start by defining $\alpha(\ell) = \alpha_0(\ell)$ for each $\ell \in M$. Let $\ell_1, \dots, \ell_p$ be an arbitrary order of the pairs in $L \setminus M$. We will determine a value $\alpha(\ell_i)$ for each ℓ_i in this order maintaining that the following mappings α_t^i are feasible for every t.

$$\alpha_t^i(\ell) = \begin{cases} \alpha(\ell) & \text{if } \ell \in M \cup \{\ell_1, \dots, \ell_i\}, \\ \alpha_t(\ell) & \text{otherwise.} \end{cases}$$

To show the existence of an appropriate $\alpha(\ell_i)$ we prove some lemmas.