Variable-rate Linear Network Coding

FONG, Lik Hang Silas

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of
Master of Philosophy
in
Information Engineering

August 2007

Abstract of thesis entitled:
Variable-Rate Linear Network Coding
Submitted by FONG, Lik Hang Silas
for the degree of Master of Philosophy
at The Chinese University of Hong Kong in August 2007

Yeung and Zhang [3] and Ahlswede et al. [1] established that if coding is applied at the nodes in a network, rather than routing alone, the network capacity can be increased. Li et al. [6] proved that linear network coding is sufficient to achieve the maximum capacity in a single-source finite acyclic network. In this thesis, we study variable-rate linear network coding and propose a scheme for efficient implementation. Two efficient algorithms are proposed for implementing variable-rate linear network coding in different situations. In addition, a simple scheme that determines the maximum broadcast rate of a linear network code is presented.

Yeung and Zhang [3] 和 Ahlswede et al. [1] 證實在網絡節點(node)進行編碼，比起純粹路由(routing)更能提昇網絡傳輸極限。Li et al. [6] 證明在單一源頭、沒有循環、有限的網絡裡，線性網絡編碼(linear network code)能將傳輸速率提昇至網絡傳輸極限。這篇論文在探討可變速率線性網絡編碼(variable-rate linear network coding)的同時，也建議了兩個高效率的演算法(algorithm)，可在不同的情況下在網絡裡實行可變速率線性網絡編碼。此外，這篇論文也建議了另外一個簡單的演算法去計算任何一個線性網絡編碼最大的廣播傳輸速率(broadcast rate)。

Acknowledgement

I wish to express my gratitude to my supervisor, Prof. Raymond Yeung, for his precious advice on my thesis and his guidance during my Master of Philosophy in Information Engineering degree. My knowledge of network coding as well as analysis skill have improved during the master degree.

I would like to express my gratitude to my parents for their support for my education throughout many years. I would also like to thank my colleagues for answering me plenty of questions during the degree.

Last but not least, I would like to thank the almighty God, the source of all intelligence, for His guidance throughout my life.

Contents

Chapter 1

Introduction

Summary

Introduction to network coding is given.

Yeung and Zhang [3] and Ahlswede et al. [1] established that if coding is applied at the nodes in a network, rather than routing alone, the network capacity can be increased. The advantage of network coding over routing is explained by means of a simple example. We will use a finite directed graph to represent a point-to-point communication network. A node in the network corresponds to a vertex in the graph, while a communication channel in the network corresponds to an edge in the graph. We will not distinguish a node from a vertex, nor will we distinguish a channel from an edge. In the graph, a node is represented by a circle, with the exception that the unique source node, denoted by S, is represented by a square. Each edge carries one information symbol taken from some finite alphabet that can be transmitted over the channel per unit time. For simplicity, we assume every transmission on a channel and every internal processing of any node incur no delay. In this chapter, we assume that the information symbol is binary. When there is only one edge from node A to node B, we denote the edge by (A, B).

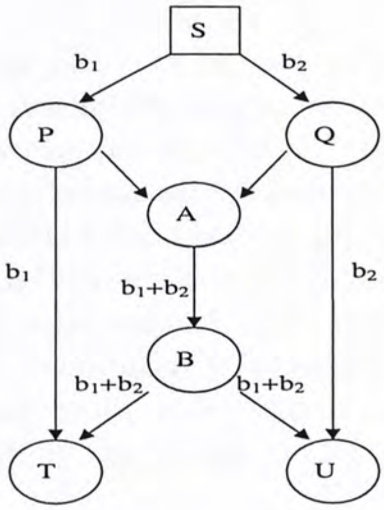

Figure 1.1: Butterfly Network

Example 1 *(Butterfly Network)[1][4] The well-known Butterfly Network is shown in Fig. 1.1. In this network, two bits b_1 and b_2 are generated at the source node S, and they are to be multicast to two sink nodes T and U. It can be easily proved that no routing scheme enables T and U to decode the two bits per unit time. If network coding is allowed, Fig. 1.1 shows a scheme which multicasts both b_1 and b_2 to nodes T and U, where '+' denotes modulo 2 addition. In this scheme, node A receives b_1 and b_2 and sends the encoded symbol $b_1 + b_2$ on channel (A, B). At node T, b_1 is received and b_2 can be recovered by adding b_1 and $b_1 + b_2$, because*

$$b_2 = b_1 + (b_1 + b_2).$$

Similarly, U can recover b_1 and b_2.

Li et al. [6] proved that linear network coding is sufficient to achieve the maximum capacity in a single-source finite acyclic network. Consequently, linear network coding for single-source finite acyclic networks has been a subject of much research interest. We refer the reader to [4] for a tutorial on the subject. In this work, they classify linear network codes for single-source finite acyclic networks into four types: (*a*) generic; (*b*) linear dispersion; (*c*) linear broadcast; (*d*) linear multicast. These four types of linear network code possess properties of decreasing strength. Although there has been much investigation into various properties of linear network codes with a fixed rate, little research has been undertaken to investigate into the possible relationships among codes with different rates. In this thesis, we focus on analyzing the linkage among linear broadcasts of different rates.

This thesis is organized as follows. Chapter 2 presents various kinds of linear network code, including linear broadcast. Chapter 3 presents the concept of variable-rate linear network coding and provides efficient algorithms for efficient implementations of variable-rate linear network coding. Chapter 4 concludes this thesis.

□ **End of chapter.**

Chapter 2

Linear Network Code

Summary

Various kinds of linear network code are presented.

2.1 Linear Network Code without Link Failures

A *network* is represented by a finite directed graph $G = (E, V)$ consisting of node set V and edge set E. *Nodes* are denoted by upper case letters (X, Y, etc). *Edges* are denoted by lower case letters (e, i, etc) on which a symbol from a finite field F, called the base field, can be transmitted. For simplicity, we assume every transmission on a channel and every internal processing of any node incur no delay. The *source* node is denoted by S which generates a message every unit time. The maximum flow from the source S to a non-source node T is denoted by *maxflow(T)*. The set of incoming edges and outgoing edges of node U are denoted by *In(U)* and *Out(U)* respectively. Let a pair of edges (d, e) be called an *adjacent pair* when there exists a node T with $d \in In(T)$ and $e \in Out(T)$.

In a linear network code, all the information symbols are regarded as elements of a base field F. These symbols include the symbols that comprise the information source as well as the symbols transmitted on the channels. For example, F is taken to be the field $GF(2)$ when the information unit is the bit. Furthermore, encoding and decoding are based on linear algebra defined on the base field, so that efficient algorithms for encoding and decoding as well as for code construction can be obtained. The global description of a linear network code described in [4] is used in this thesis.

Definition 1 *Let F be a finite field and ω be a positive integer. An ω-dimensional F-valued linear network code on an acyclic communication network consists of a scalar $k_{d,e}$ for every adjacent pair (d, e) in the network as well as an ω-dimensional column vector f_e for every edge e in the network such that:*

(i) $f_e = \sum_{d\in In(T)} k_{d,e} f_d$*, where* $e \in Out(T)$*;*

(ii) The vectors f_e for the ω imaginary channel $e \in In(S)$ form the natural basis of the vector space F^ω.

The vector f_e is called the global encoding kernel for edge e. The local encoding kernel at the node T refers to the $|In(T)| \times |Out(T)|$ matrix $K_T = [k_{d,e}]_{d\in In(T), e\in Out(T)}$.

Let the source generate a message $\vec{x}$ in the form of an ω-dimensional row vector. A node T receives the symbols $\vec{x} \cdot f_d$, $d \in In(T)$, from which it calculates the symbol $\vec{x} \cdot f_e$ for sending onto each edge $e \in Out(T)$ via the linear formula

$$\vec{x} \cdot f_e = \vec{x} \cdot \sum_{d\in In(T)} k_{d,e} f_d = \sum_{d\in In(T)} k_{d,e}(\vec{x} \cdot f_d),$$

where the first equality follows from (i).

Given the local encoding kernels at all the nodes in an acyclic network, the global encoding kernels can be calculated recursively in any upstream-to-downstream order by (i), while (ii) provides the boundary conditions. An ω-dimensional F-valued linear network code can be viewed as an F-valued linear network code that enables the source to transmit a message consisting of ω data units.

2.1.1 Linear Multicast and Linear Broadcast

Linear multicast and linear broadcast are described in [4] and their definitions are stated as follows:

Definition 2 *Let vectors f_e denote the global encoding kernels in an ω-dimensional F-valued linear network code on a single-source finite acyclic network. Let*

$$V_T = span\{f_d : d \in In(T)\}.$$

Then, the linear network code qualifies as a linear multicast and a linear broadcast respectively if the following statements hold:

(i) $dim(V_T) = \omega$ *for every non-source node* T *with* $maxflow(T) \geq \omega$;

(ii) $dim(V_T) = \min\{\omega, maxflow(T)\}$ *for every non-source node* T.

Clearly, $(ii) \Rightarrow (i)$. Thus, every linear broadcast is a linear multicast. Let p be the number of non-source node T with $maxflow(T) \geq \omega$ in an acyclic network. Using the algorithm proposed in [5], we can construct an ω-dimensional linear multicast on the network if the size of the base field is larger than p. A slight modification of this algorithm proves the following theorem.

Theorem 1 *Given a single-source finite acyclic network with n non-source nodes and a finite field F, an ω-dimensional F-valued linear broadcast can be constructed if $|F| > n$.*

Proof: It is similar to the proof in [5] and therefore omitted. □

Generally, a larger base field is required for constructing a linear broadcast than a linear multicast in the same network because the algorithms for constructing a linear broadcast need to consider more nodes compared with the algorithms for constructing a linear multicast.

2.2 Linear Network Code with Link Failures

In the discussion so far, a linear network code has been defined on a network with a fixed topology, where all the channels are assumed to be available at all times. In real life, a communication network often suffers from link failures or traffic congestions from time to time. In other words, the effective configuration of a communication network may vary from time to time. Link failures need to be handled efficiently because otherwise a large amount of data can be lost, especially when the data rate is high. Consider the use of, for instance, an ω-dimensional multicast on an acyclic network for multicasting a sequence of messages generated at the source node. When no channel failure occurs, a non-source node T with $maxflow(T)$ at least equal to ω would be able to decode the sequence of messages. In case of link failures, if $maxflow(T)$ in the resulting network is at least ω, the sequence of messages in principle can still be received at that node. However, the deployment of a network code for the new network topology is involved, which not only is cumbersome but also may cause a significant loss of data during the switchover. In order to develop an efficient scheme for handling link failures, a kind of linear network code called static network code described in [4] is studied in this thesis, which can provide the network with maximum robustness in case of channel failures. The configuration formally defined in [4] and the global description of static network code in [4] are stated as follows:

Definition 3 *A configuration ε of a network is a mapping from the set of channels in the network to the set $\{0,1\}$. Channels in $\varepsilon^{-1}(0)$ are idle channels with respect to this configuration, and the subnetwork resulting from the deletion of idle channels will be called the ε-subnetwork. The maximum flow from the source S to a non-source node T over the ε-subnetwork is denoted as $maxflow_\varepsilon(T)$.*

Definition 4 *Let F be a finite field and ω be a positive integer. Let $k_{d,e}$ be the local encoding kernel for every adjacent pair (d,e) in an ω-dimensional F-valued linear network code on an acyclic communication network. The ε-global encoding kernel for the channel e, denoted by $f_{e,\varepsilon}$, is the ω-dimensional column vector calculated recursively in an upstream-to-downstream order by:*

(*i*) $f_{e,\varepsilon} = \varepsilon(e) \sum_{d \in In(T)} k_{d,e} f_{d,\varepsilon}$, *where $e \in Out(T)$.*

(*ii*) *The ε-global encoding kernel for the ω imaginary channels are independent of ε and form the natural basis of the vector space F^{ω}.*

In the above definition, the local encoding kernels $k_{d,e}$ remain unchanged with ε. Let the source generate a message $\vec{x}$ in the form of an ω-dimensional row vector. A node T receives the symbols $\vec{x} \cdot f_{d,\varepsilon}$, $d \in In(T)$, from which it calculates the symbol $\vec{x} \cdot f_{e,\varepsilon}$ for sending onto each edge $e \in Out(T)$ via the linear formula

$$\vec{x} \cdot f_{e,\varepsilon} = \varepsilon(e) \sum_{d \in In(T)} k_{d,e}(\vec{x} \cdot f_{d,\varepsilon}).$$

In particular, a channel e with $\varepsilon(e) = 0$ has $f_{e,\varepsilon} = \vec{0}$ according to (*i*) and transmits the symbol $\vec{x} \cdot f_{e,\varepsilon} = 0$. In a real network, whenever a symbol is not received on an input channel due to channel failures, the symbol is regarded as being 0.

2.2.1 Static Linear Multicast and Static Linear Broadcast

Static linear multicast and static linear broadcast are described in [4] and their definitions are stated as follows:

Definition 5 *Following the notation of Definition* 4 *and letting*

$$V_{T,\varepsilon} = span\{f_{d,\varepsilon} : d \in In(T)\},$$

an ω-dimensional F-valued linear network code on a single-source finite acyclic network qualifies as a static linear multicast and a static linear broadcast respectively if the following statements hold:

(i) $dim(V_{T,\varepsilon}) = \omega$ *for every configuration* ε *and every non-source node* T *with* $maxflow_\varepsilon(T) \geq \omega$*;*

(ii) $dim(V_{T,\varepsilon}) = \min\{\omega, maxflow_\varepsilon(T)\}$ *for every configuration* ε *and every non-source node* T*.*

While the configuration ε varies, the local encoding kernels remain unchanged. Therefore, the advantage of using a static linear broadcast in case of link failures is that the local operation at any node in the network is affected only at the minimal level. Each receiving node in the network, however, needs to know the configuration ε before decoding the source message correctly.

Let p be the number of non-source node T with $maxflow(T) \geq \omega$ and m be the number of configurations in an acyclic network. Using the algorithm proposed in [2], we can construct an ω-dimensional static linear multicast on the network if the size of the base field is larger than mp. A slight modification of this algorithm proves the following theorem.

Theorem 2 *Given a single-source finite acyclic network with* n *non-source nodes,* m *configurations and a finite field* F*, an* ω*-dimensional* F*-valued static linear broadcast can be constructed if* $|F| > mn$*.*

Proof: It is similar to the proof of constructing a static linear multicast in [2] and therefore omitted. □

□ **End of chapter.**

Chapter 3

Variable-Rate Linear Network Coding

Summary

The concept of variable-rate linear network coding is presented and algorithms for efficient implementations of variable-rate linear network coding are provided.

3.1 Variable-Rate Linear Network Coding without Link Failures

3.1.1 Problem Formulation

In a single-source finite acyclic network, suppose the source wants to transmit messages at one of q possible rates within a session. Let $\bar{q}$ be the highest among the q rates. To avoid triviality, assume $\bar{q} \leq maxflow(T)$ for at least one non-source node T. We are now required to design a linear network coding system which enables every receiver T to decode the message if $maxflow(T)$ is greater than the transmission rate in that session. The most effective existing solution is to use the algorithm proposed in [5] to obtain q linear multicasts of different dimensions for the same network. Consequently, every node is required to store q different copies of the local encoding kernels in order to apply the suitable local encoding kernel for that session. This increases the complexity of the system considerably if the system is implemented in hardware. Besides, changing the local encoding kernels at the nodes consumes resources in the network.

As an attempt to alleviate the shortcomings in the existing solution, a new scheme based on linear broadcast is proposed for more efficient implementation of variable-rate linear network coding.

3.1.2 Algorithm and Analysis

Throughout this thesis, all the networks concerned are single-source finite acyclic networks and we let F^{ω} denote the vector space of all ω-dimensional column vectors.

Lemma 1 *An ω-dimensional F-valued linear network code is given on an acyclic network where $\omega \geq 2$. Let f_e be the global encoding kernel for all edge $e \in E$. Let $I_{\omega-1}$ denote the $(\omega - 1) \times (\omega - 1)$ identity matrix and let $\vec{b} \in F^{\omega-1}$ be any arbitrary $(\omega - 1)$-dimensional column vector. Let*

$$f_e^{\omega-1} = \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_e \tag{3.1}$$

for all non-imaginary channel e. Then, $f_e^{\omega-1}, e \in E$ constitute the global encoding kernels of an $(\omega - 1)$-dimensional F-valued linear network code in the same base field F. In particular, the local encoding kernel of this $(\omega - 1)$-dimensional linear network code at every non-source node is the same as that of the original ω-dimensional linear network code.

Proof: Let $k_{d,e}$ be the local encoding kernel for every adjacent pair (d,e) of the given ω-dimensional F-valued linear network code. We will show that $f_e^{\omega-1}, e \in E$ constitute the global encoding kernels of an $(\omega-1)$-dimensional F-valued linear network code by demonstrating the existence of the corresponding local encoding kernel $k_{d,e}^{\omega-1}$ for every adjacent pair (d,e).

By convention, we assume that the global encoding kernel for the $\omega-1$ imaginary channels form the standard basis of $F^{\omega-1}$. For any channel $e \in Out(S)$, since $f_e^{\omega-1}$ as specified in (3.1) is in $F^{\omega-1}$, $k_{d,e}^{\omega-1}, d \in In(S)$ can always be chosen.

For all non-imaginary channel $e \notin Out(S)$, let $k_{d,e}^{\omega-1} = k_{d,e}$. We now verify the relation

$$f_e^{\omega-1} = \sum_{d \in In(T)} k_{d,e}^{\omega-1} f_d^{\omega-1} \tag{3.2}$$

by considering

$$f_e = \sum_{d \in In(T)} k_{d,e} f_d.$$

Multiplying both sides by $\begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix}$, we obtain

$$\begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_e = \sum_{d \in In(T)} k_{d,e} \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_d.$$

Then (3.2) immediately follows from (3.1), since $k_{d,e}^{\omega-1} = k_{d,e}$ for all non-imaginary channel $e \notin Out(S)$. This shows that $f_e^{\omega-1}, e \in E$ constitute the global encoding kernels of an $(\omega-1)$-dimensional F-valued linear network code with the local encoding kernels $k_{d,e}^{\omega-1}$. In particular, $k_{d,e}^{\omega-1} = k_{d,e}$ for every adjacent pair (d,e) for $e \notin Out(S)$. In other words, the local encoding kernel at every non-source node of the $(\omega-1)$-dimensional linear network code specified by $f_e^{\omega-1}, e \in E$ is the same as that of the original ω-dimensional linear network code. □

Definition 6 *Let an ω-dimensional F-valued linear broadcast on an acyclic network where $\omega \geq 2$ and $\vec{b} \in F^{\omega-1}$, an $(\omega-1)$-dimensional column vector, be given. Define*

$$f_e^{\omega-1} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] f_e$$

for all non-imaginary channel e, where f_e is the global encoding kernel for channel e. Then, $\vec{b}$ is called a reduction vector for the given linear broadcast if $f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast.

Lemma 2 *Let F be a finite field, and ω and m be integers such that $\omega \geq 2$ and $1 \leq m \leq \omega - 1$. Let $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m} \in F^{\omega}$ be m linearly independent vectors, and let*

$$\vec{d_i} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] \vec{c_i} \tag{3.3}$$

for $i = 1, 2, \ldots, m$, where

$$\vec{b} = \left[\begin{array}{cccc} b_1 & b_2 & \cdots & b_{\omega-1} \end{array} \right]^T$$

and $b_1, b_2, \ldots, b_{\omega-1}$ are indeterminates in F. Then, there exists a nonzero polynomial

$$p(b_1, b_2, \ldots, b_{\omega-1}) = a_0 + a_1 b_1 + a_2 b_2 + \ldots + a_{\omega-1} b_{\omega-1}$$

where a_j's are constants in F such that $\vec{d_1}, \vec{d_2}, \ldots, \vec{d_m}$ are linearly independent whenever

$$p(b_1, b_2, \ldots, b_{\omega-1}) \neq 0.$$

Proof: Construct the matrix

$$D_m = \left[\begin{array}{cccc} \vec{d_1} & \vec{d_2} & \cdots & \vec{d_m} \end{array} \right].$$

We will show that there exists an $m \times m$ submatrix A of D_m whose determinant is equal to a nonzero polynomial in $b_1, b_2, \ldots, b_{\omega-1}$. We will further show that $det(A)$ has the form

$$a_0 + a_1 b_1 + a_2 b_2 + \ldots + a_{\omega-1} b_{\omega-1}$$

where a_j's are constants in F. Then by letting

$$p(b_1, b_2, \ldots, b_{\omega-1}) = det(A),$$

since A is a submatrix of D_m, it follows that $\vec{d_1}, \vec{d_2}, \ldots, \vec{d_m}$ are linearly independent whenever $p(b_1, b_2, \ldots, b_{\omega-1})$ is evaluated to a nonzero value in F.

To facilitate our discussion, we write

$$\vec{c_i} = \begin{bmatrix} \vec{h_i} \\ k_i \end{bmatrix}, \tag{3.4}$$

where $\vec{h_i} \in F^{\omega-1}$ and $k_i \in F$ for $i = 1, 2, \ldots, m$. It is readily seen from (3.3) that

$$\vec{d_i} = \vec{h_i} + k_i\vec{b}$$

for $i = 1, 2, \ldots, m$, which implies

$$D_m = \left[\begin{array}{cccc} \vec{h_1} + k_1\vec{b} & \vec{h_2} + k_2\vec{b} & \cdots & \vec{h_m} + k_m\vec{b} \end{array}\right]. \tag{3.5}$$

We first show that there exists some $\vec{b} \in F^{\omega-1}$ such that $\vec{d_1}, \vec{d_2}, \ldots, \vec{d_m}$ are linearly independent. Assume the contrary, i.e., $\vec{d_1}, \vec{d_2}, \ldots, \vec{d_m}$ are linearly dependent for all $\vec{b}$. We will show that this leads to a contradiction.

$Case\,1 : |span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}| < \omega - 1$

Since $|span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}|$ is at most $\omega - 2$, a vector $\vec{z} \in F^{\omega-1}$ can always be found such that $\vec{z} \notin span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}$. Then, by our assumption, $\{\vec{d_i}\}$ are linearly dependent for all $\vec{b}$, in particular for $\vec{b}$ equals $\vec{z}$. In other words, $\{\vec{h_i} + k_i\vec{z}\}$ are linearly dependent, i.e.,

$$\begin{aligned} & t_1(\vec{h_1} + k_1\vec{z}) + t_2(\vec{h_2} + k_2\vec{z}) \\ + & \ \ldots + t_m(\vec{h_m} + k_m\vec{z}) = \vec{0} \end{aligned}$$

for some $t_1, t_2, \ldots t_m \in F$ where not all t_i's are equal to 0. Regrouping the terms, we have

$$\begin{aligned} & (t_1\vec{h_1} + t_2\vec{h_2} + \ldots + t_m\vec{h_m}) \\ + & (t_1k_1 + t_2k_2 + \ldots + t_mk_m)\vec{z} = \vec{0}. \end{aligned}$$

Since $\vec{z} \notin span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}$, this implies

$$\begin{cases} t_1k_1 + t_2k_2 + \ldots + t_mk_m = 0 \\ t_1\vec{h_1} + t_2\vec{h_2} + \ldots + t_m\vec{h_m} = \vec{0}. \end{cases}$$

Consequently,

$$t_1\vec{c_1} + t_2\vec{c_2} + \ldots t_m\vec{c_m} = \vec{0}$$

(cf.(3.4)), which contradicts the linear independence among $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m}$.

$Case\,2 : |span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}| = \omega - 1$

Since m is at most $\omega - 1$ and $|span\{\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}\}|$ equals $\omega - 1$, m equals $\omega - 1$ and $\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}$ are linearly independent. However, for $\vec{b}$ equals $\vec{0}$,

$$\vec{d_i} = \vec{h_i}$$

for $i = 1, 2, \ldots, m$. Then, $\{\vec{d_i}\}$ are linearly independent for $\vec{b}$ equals $\vec{0}$, which contradicts our assumption.

Combining the two cases, we have shown that $\vec{d_1}, \vec{d_2}, \ldots, \vec{d_m}$ are linearly independent for some $\vec{b}$. For this choice of $\vec{b}$, there exists a submatrix A of D_m such that $det(A)$ is evaluated to a nonzero value. Since $det(A)$ is a polynomial in the indeterminates $b_1, b_2, \ldots, b_{\omega-1}$, this implies that $det(A)$ is a nonzero polynomial in these indeterminates. Since D_m is $(\omega - 1) \times m$ and A is an $m \times m$ submatrix of D_m, we see from (3.5) that

$$A = \left[\begin{array}{cccc} \vec{r_1} + k_1\vec{b}' & \vec{r_2} + k_2\vec{b}' & \cdots & \vec{r_m} + k_m\vec{b}' \end{array} \right],$$

where $\vec{r_1}, \vec{r_2}, \ldots, \vec{r_m}, \vec{b}' \in F^m$ are the corresponding subvectors of $\vec{h_1}, \vec{h_2}, \ldots, \vec{h_m}$ and $\vec{b}$ respectively. If $k_1 = \ldots = k_m = 0$, then $det(A) = a_0$ where $a_0 \in F$. Otherwise, assume without loss of generality that $k_1 \neq 0$. Then, by means of column operations on A, we see that $det(A)$ can be expressed in the form

$$C \left| \left[\begin{array}{cccc} \vec{l_1} + \tau \vec{b}' & \vec{l_2} & \cdots & \vec{l_m} \end{array} \right] \right|$$

where $C, \tau \in F$ and $\vec{l_i} \in F^m$. It then follows that in $det(A)$, the power of each component of $\vec{b}$ is at most one. Therefore,

$$det(A) = a_0 + a_1 b_1 + a_2 b_2 + \ldots + a_{\omega-1} b_{\omega-1}$$

where a_j's are constants in F for $j = 0, 1, \ldots, \omega - 1$. Let

$$p(b_1, b_2, \ldots, b_{\omega-1}) = det(A)$$

and this completes the proof of the lemma. $\square$

Lemma 3 *Let n be the total number of non-source nodes in an acyclic network, and an ω-dimensional F-valued linear broadcast be given, where $\omega \geq 2$. Then a reduction vector can be found if $|F| > n$.*

Proof: Let f_e be the global encoding kernel of the given linear broadcast for all edge $e \in E$. Let

$$\vec{b} = \left[\begin{array}{cccc} b_1 & b_2 & \cdots & b_{\omega-1} \end{array} \right]^T$$

be an $(\omega - 1)$-dimensional column vector where all b_ξ's are indeterminates in F, and let

$$f_e^{\omega-1} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] f_e$$

for all non-imaginary channel e. The existence of a reduction vector is proved by showing that by suitably choosing $\vec{b}$,

$f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast.

For each non-source node T, let

$$m = \min\{\omega - 1, maxflow(T)\}.$$

Then, m linearly independent vectors f_e can always be chosen from the set of incoming edge $e \in In(T)$ since the given linear network code is a linear broadcast. Denote these m vectors by $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m}$ and let

$$\vec{c_i}^{\,\omega-1} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] \vec{c_i}$$

for $i = 1, 2, \ldots, m$, where $\vec{c_i}^{\,\omega-1}$ is an $(\omega-1)$-dimensional column vectors. Note that m as well as the vectors $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m}$ and $\vec{c_1}^{\,\omega-1}, \vec{c_2}^{\,\omega-1}, \ldots, \vec{c_m}^{\,\omega-1}$ depend on node T although this is not explicitly indicated in order to keep the notation simple. Let g_T be the nonzero polynomial $p(b_1, b_2, \ldots, b_{\omega-1})$ in Lemma 2, which exists because $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m}$ are linearly independent. Let N_T denote the solution space of

$$g_T(b_1, b_2, \ldots, b_{\omega-1}) = 0.$$

Since g_T is a nonzero polynomial in $\omega - 1$ variables, $|N_T| \leq |F|^{\omega-2}$. We now consider

$$\left| F^{\omega-1} \cap \left(\bigcup_T N_T \right) \right|$$

in order to find a reduction vector

$$\vec{v} = \left[\begin{array}{cccc} v_1 & v_2 & \cdots & v_{\omega-1} \end{array} \right]^T.$$

By the union bound,

$$\left| F^{\omega-1} \cap \left(\bigcup_T N_T \right) \right| \leq \sum_T \left| \left(F^{\omega-1} \cap N_T \right) \right|.$$

Since $|N_T| \leq |F|^{\omega-2}$ and $n < |F|$, this implies

$$\begin{aligned}\sum_T |(F^{\omega-1} \cap N_T)| &\leq \sum_T |F|^{\omega-2} \\ &= n|F|^{\omega-2} \\ &< |F|^{\omega-1}.\end{aligned}$$

Therefore,

$$\left| F^{\omega-1} \cap (\bigcup_T N_T) \right| < |F^{\omega-1}|$$

and we can find $\vec{v} \in F^{\omega-1}$ such that $\vec{v} \notin \bigcup_T N_T$. In other words, $\vec{v}$ can be obtained such that

$$g_T(v_1, v_2, \ldots, v_{\omega-1}) \neq 0$$

for each non-source node T, which implies $\vec{c}_1^{\,\omega-1}, \vec{c}_2^{\,\omega-1}, \ldots, \vec{c}_m^{\,\omega-1}$ are linearly independent for each non-source node T when $\vec{b} = \vec{v}$ by Lemma 2. Consequently, $f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear network code that

$$\begin{aligned}dim(V_T) &= m \\ &= \min\{\omega - 1, maxflow(T)\}\end{aligned}$$

for each non-source node T when $\vec{b} = \vec{v}$. Therefore, $f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast for $\vec{b} = \vec{v}$. It then follows from Definition 6 that $\vec{v}$ is a reduction vector for the given linear broadcast. □

Lemma 3 provides an algorithm to find a reduction vector and an application of Lemma 3 is illustrated by the following simple example.

Example 2 *An acyclic network with 7 non-source nodes and a 3-dimensional $GF(11)$ linear broadcast on the network are shown in Fig. 3.1. The local encoding kernels at the non-source nodes of the linear broadcast are shown in Fig. 3.2. Since*

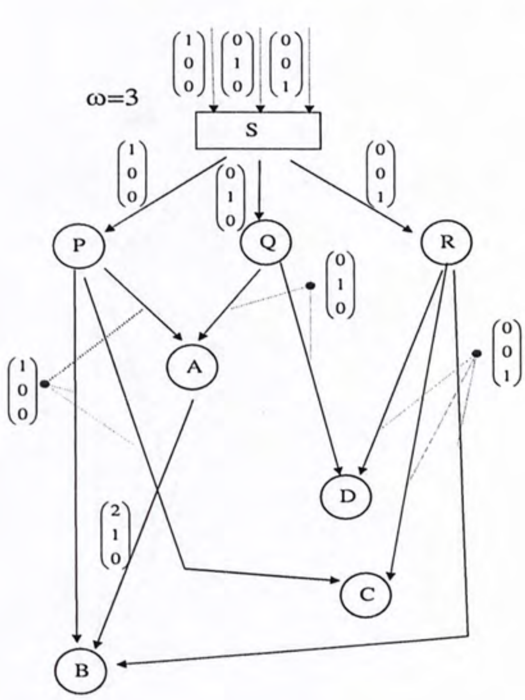

Figure 3.1: A 3-dimensional $GF(11)$ linear broadcast

K_P	K_Q	K_R	K_A
$[1\ 1\ 1]$	$[1\ 1]$	$[1\ 1\ 1]$	$\begin{bmatrix} 2 \\ 1 \end{bmatrix}$

Figure 3.2: The local encoding kernels at the non-source nodes

$|GF(11)| > 7$, a reduction vector can be found by Lemma 3 and $\begin{bmatrix} 1 & 2 \end{bmatrix}^T$ is found to be a reduction vector. The corresponding 2-dimensional $GF(11)$ linear broadcast constructed by the reduction vector is shown in Fig. 3.3. It can be easily observed that the two linear broadcasts have the same local encoding kernels at all the non-source nodes.

Theorem 3 *Let n be the total number of non-source nodes in an acyclic network. An ω-dimensional F-valued linear broadcast is*

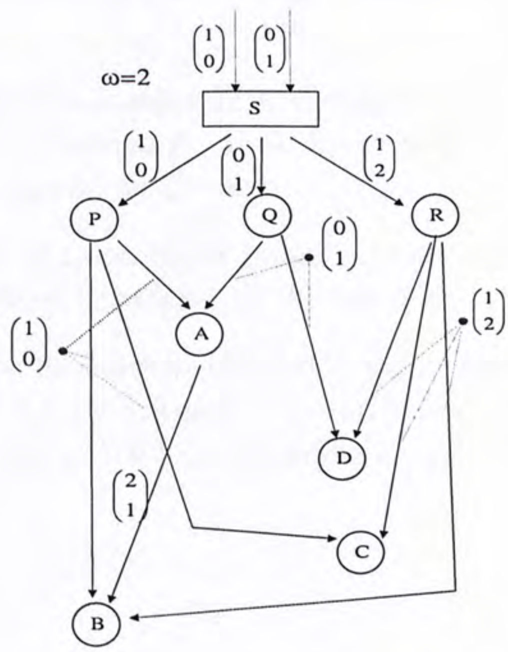

Figure 3.3: A 2-dimensional $GF(11)$ linear broadcast

given on the network where $\omega \geq 2$ *and* $|F| > n$. *Then, for every* $h = 1, 2, \ldots, \omega - 1$, *an* h*-dimensional* F*-valued linear broadcast can be constructed such that these linear broadcasts have the same local encoding kernels at all the non-source nodes.*

Proof: Using Lemma 3, a reduction vector for the given linear broadcast can be found and an $(\omega - 1)$-dimensional linear broadcast is obtained. By Lemma 1, the local encoding kernel of this $(\omega - 1)$-dimensional linear broadcast at every non-source node is the same as that of the original ω-dimensional linear broadcast. By repeating this procedure, each time reducing the dimension of the linear broadcast by one, the desired set of linear broadcasts can be obtained. □

The proof of Theorem 3 renders an efficient implementation of linear broadcasts of different dimensions on the same network.

A proposed solution to the problem in Section 3.1.1 consists of two steps.

Step 1 : Let n be the number of non-source node in the network and a $\bar{q}$-dimensional F-valued linear broadcast where $|F| > n$ is constructed by Theorem 1.

Step 2 : Lower-dimension linear broadcasts are obtained from the $\bar{q}$-dimensional broadcast by Theorem 3.

This solution provides an efficient implementation of the problem in Section 3.1.1 since each non-source node is only required to store one copy of the local encoding kernel.

3.2 Variable-Rate Linear Network Coding with Link Failures

3.2.1 Problem Formulation

In a single-source finite acyclic network with $2^{|E|}$ possible configurations, suppose the source wants to transmit messages to receivers $T_1, T_2, \ldots, T_j$. For each configuration ε, let

$$c_\varepsilon = \min\{maxflow_\varepsilon(T_i) \,|\, i = 1, 2, \ldots, j\}.$$

In any time period with a certain configuration ε, the source transmits messages at rate $= c_\varepsilon$ so that all the receivers T_i can always decode the message. Let ε_Ω denote the configuration with no link failure, i.e., $\varepsilon_\Omega(e) = 1$ for all non-imaginary channel $e \in E$. If we want to minimize the complexity of the local operation at all the nodes, an existing solution is to use the algorithm proposed in [2] to construct a static linear multicast for each rate $= 1, 2, \ldots, c_{\varepsilon_\Omega}$. Consequently, every node is required to store c_{ε_Ω} different copies of the local encoding kernels in order to apply the suitable local encoding kernel for the configuration ε at that time.

As an attempt to alleviate the shortcomings in the existing solution, a new scheme based on static linear broadcast is proposed for more efficient implementation of variable-rate linear network coding.

3.2.2 Algorithm and Analysis

Similar to the case of linear broadcast, we have the following definition, lemmas and theorem for static linear broadcast using the same scheme.

Lemma 4 *(counterpart of Lemma* 1*) An ω-dimensional F-valued linear network code is given on an acyclic network. Let $f_{e,\varepsilon}$ be* *the ε-global encoding kernel for all edge $e \in E$ and every configuration ε. Let $I_{\omega-1}$ denote the $(\omega-1) \times (\omega-1)$ identity matrix and let $\vec{b} \in F^{\omega-1}$ be any arbitrary $(\omega-1)$-dimensional column vector. Let*

$$f_{e,\varepsilon}^{\omega-1} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] f_{e,\varepsilon} \tag{3.6}$$

for all non-imaginary channel e and every configuration ε. Then, $f_{e,\varepsilon}^{\omega-1}, e \in E$ constitute the ε-global encoding kernels of an $(\omega-1)$-dimensional F-valued linear network code in the same base field F. In particular, the local encoding kernel of this $(\omega-1)$-dimensional linear network code at every non-source node is the same as that of the original ω-dimensional linear network code.

Proof: It is similar to the proof in Lemma 1 and therefore omitted. □

Definition 7 *(counterpart of Definition 6) Let an ω-dimensional F-valued static linear broadcast on an acyclic network where $\omega \geq 2$, and $\vec{b} \in F^{\omega-1}$, an $(\omega-1)$-dimensional column vector, be given. Define*

$$f_{e,\varepsilon}^{\omega-1} = \left[\begin{array}{cc} I_{\omega-1} & \vec{b} \end{array} \right] f_{e,\varepsilon}$$

for all non-imaginary channel e and every configuration ε, where $f_{e,\varepsilon}$ is the global encoding kernel for channel e under configuration ε. Then, $\vec{b}$ is called a static reduction vector for the given static linear broadcast if $f_{e,\varepsilon}^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast for every configuration ε.

Lemma 5 *(counterpart of Lemma 3) Let n be the total number of non-source nodes in an acyclic network and m be the total number of configurations ε in the network. For any ω-dimensional F-valued static linear broadcast where $\omega \geq 2$, a static reduction vector can be found if $|F| > mn$.*

Proof: Let $f_{e,\varepsilon}$ be the global encoding kernel of the given static linear broadcast for all edge $e \in E$ and every possible configuration ε. Let

$$\vec{b} = \begin{bmatrix} b_1 & b_2 & \cdots & b_{\omega-1} \end{bmatrix}^T$$

be an $(\omega - 1)$-dimensional column vector where all b_ξ's are indeterminates in F, and let

$$f_{e,\varepsilon}^{\omega-1} = \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_{e,\varepsilon}$$

for all non-imaginary channel e and every configuration ε. The existence of a static reduction vector is proved by showing that by suitably choosing $\vec{b}$, $f_{e,\varepsilon}^{\omega-1}$, $e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast for every configuration ε.

For each configuration ε, the network code on the ε-subnetwork is a linear broadcast. Therefore, we let a nonzero polynomial $g_{T,\varepsilon}(b_1, b_2, \ldots, b_{\omega-1})$ be g_T in the proof of Lemma 3 for each non-source node T under each ε. Let $N_{T,\varepsilon}$ denote the solution space of

$$g_{T,\varepsilon}(b_1, b_2, \ldots, b_{\omega-1}) = 0.$$

Since $g_{T,\varepsilon}$ is a nonzero polynomial in $\omega - 1$ variables, $|N_{T,\varepsilon}| \leq |F|^{\omega-2}$. We now consider

$$\left| F^{\omega-1} \cap \left(\bigcup_{\varepsilon} \left(\bigcup_{T} N_{T,\varepsilon} \right) \right) \right|$$

in order to find a static reduction vector

$$\vec{v} = \begin{bmatrix} v_1 & v_2 & \cdots & v_{\omega-1} \end{bmatrix}^T.$$

By the union bound,

$$\left| F^{\omega-1} \cap \left(\bigcup_{\varepsilon} \left(\bigcup_{T} N_{T,\varepsilon} \right) \right) \right| \leq \sum_{\varepsilon} \left(\sum_{T} \left| \left(F^{\omega-1} \cap N_{T,\varepsilon} \right) \right| \right).$$

Since $|N_T| \leq |F|^{\omega-2}$ and $mn < |F|$, this implies

$$\begin{aligned}\sum_{\varepsilon}(\sum_{T}|(F^{\omega-1}\cap N_{T,\varepsilon})|) &\leq \sum_{\varepsilon}(\sum_{T}|F|^{\omega-2}) \\ &= mn\,|F|^{\omega-2} \\ &< |F|^{\omega-1}.\end{aligned}$$

Therefore,

$$\left| F^{\omega-1}\cap(\bigcup_{\varepsilon}(\bigcup_{T} N_{T,\varepsilon}))\right| < |F^{\omega-1}|$$

and we can find $\vec{v} \in F^{\omega-1}$ such that $\vec{v} \notin \bigcup_{\varepsilon}(\bigcup_T N_{T,\varepsilon})$. In other words, $\vec{v}$ can be obtained such that

$$g_{T,\varepsilon}(v_1, v_2, \ldots, v_{\omega-1}) \neq 0$$

for each non-source node T under every configuration ε. By the similar arguments as the proof in Lemma 3, $f^{\omega-1}_{e,\varepsilon}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear broadcast for $\vec{b} = \vec{v}$ under every configuration ε. It then follows from Definition 7 that $\vec{v}$ is a static reduction vector.

Theorem 4 *(counterpart of Theorem 3) Let n be the total number of non-source nodes in an acyclic network and m be the total number of configurations. An ω-dimensional F-valued static linear broadcast is given on the network where $\omega \geq 2$ and $|F| > mn$. Then, for every $h = 1, 2, \ldots, \omega - 1$, an h-dimensional F-valued static linear broadcast can be constructed such that these static linear broadcasts have the same local encoding kernels at all the non-source nodes.*

Proof: Using Lemma 5, a static reduction vector for the given static linear broadcast can be found and an $(\omega-1)$-dimensional static linear broadcast is obtained. By Lemma 4, the local encoding kernel of this $(\omega - 1)$-dimensional static linear broadcast at every non-source node is the same as that of the original ω-dimensional static linear broadcast. By repeating this procedure, each time reducing the dimension of the static linear broadcast by one, the desired set of static linear broadcasts can be obtained. □

The proof of Theorem 4 renders an efficient implementation of static linear broadcasts of different dimensions on the same network. The problem in Section 3.2.1 can be efficiently solved in two steps.

Step 1 : Let n be the number of non-source nodes in the network and a c_{ε_Ω}-dimensional F-valued static linear broadcast where $|F| > 2^{|E|}n$ is constructed by Theorem 2.

Step 2 : Lower-dimension static linear broadcasts are obtained from the c_{ε_Ω}-dimensional static linear broadcast by Theorem 4.

The static linear broadcasts constructed have the same local encoding kernels at all the non-source nodes. Therefore, each non-source node is only required to store one copy of the local encoding kernel, which implies that only a small storage space at non-source nodes is needed and no switching of the local encoding kernel at non-source nodes is required. In addition, the source S only needs to store about c_{ε_Ω} different static reduction vectors, each vector corresponding to one rate, for transmitting messages in any possible configuration.

In the proof of Theorem 4, it is required that

$$|F| > 2^{|E|}n.$$

However, if $|F|$ satisfies only

$$n < |F| \leq 2^{|E|}n,$$

an alternative solution to the problem is proposed as follows.

Step 1 : A c_{ε_Ω}-dimensional F-valued static linear broadcast where $n < |F| \leq 2^{|E|}n$ is constructed.

Step 2 : Since the network code for each configuration ε is an F-valued linear broadcast where $|F| > n$, we can obtain all lower-dimension linear broadcasts by Theorem 3 for each ε.

Since all linear broadcasts constructed have the same local encoding kernels at every non-source node, every non-source node is still only required to store one copy of the local encoding kernel. This alternative solution, however, increases the complexity of encoding messages at the source S, because unlike the previous solution, the source may need to use different local encoding kernels for the same transmission rate. Consequently, the source S needs to store about $2^{|E|}n$ different reduction vectors, each of them corresponding to one (rate, configuration) pair, for transmitting messages in any possible configuration.

3.3 The Maximum Broadcast Rate of Linear Network Code

In the rest of this chapter, a simple scheme that determines the maximum rate at which a given linear network code can qualify as a linear broadcast is proposed.

Definition 8 *Let ω and k be integers such that $\omega \geq 2$ and $1 \leq k < \omega$. Suppose an ω-dimensional F-valued linear network code where*

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T is given on an acyclic network. Let $\vec{b} \in F^{\omega-1}$ be an $(\omega-1)$-dimensional column vector and let

$$f_e^{\omega-1} = \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_e$$

for all non-imaginary channel e. Then, $\vec{b}$ is called a k-reduction vector for the given linear network code if $f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear network code where

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T.

Lemma 6 *Let n be the total number of non-source nodes in an acyclic network, ω and k be integers such that $\omega \geq 2$ and $1 \leq k < \omega$. For any ω-dimensional F-valued linear network code where*

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T, a k-reduction vector exists if $|F| > n$.

Proof: Let f_e be the global encoding kernel of an ω-dimensional F-valued linear network code for all edge $e \in E$ where

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T. Let

$$\vec{b} = \begin{bmatrix} b_1 & b_2 & \cdots & b_{\omega-1} \end{bmatrix}^T$$

be an $(\omega-1)$-dimensional column vector where all b_ξ's are indeterminates in F, and let

$$f_e^{\omega-1} = \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} f_e$$

for all non-imaginary channel e. The existence of a k-reduction vector is proved by showing that by suitably choosing $\vec{b}$, $f_e^{\omega-1}, e \in E$ specify an $(\omega-1)$-dimensional F-valued linear network code where

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T.

For each non-source node T, let

$$m = \min\{k, maxflow(T)\}.$$

Then, m linearly independent vectors f_e can always be chosen from the set of incoming edge $e \in In(T)$ since

$$dim(V_T) \geq \min\{k, maxflow(T)\}.$$

Denote these m vectors by $\vec{c_1}, \vec{c_2}, \ldots, \vec{c_m}$, and let

$$\vec{c_i}^{\,\omega-1} = \begin{bmatrix} I_{\omega-1} & \vec{b} \end{bmatrix} \vec{c_i}$$

for $i = 1, 2, \ldots, m$. Let g_T be the nonzero polynomial $p(b_1, b_2, \ldots, b_{\omega-1})$ in Lemma 2, which exists because $\vec{c}_1, \vec{c}_2, \ldots, \vec{c}_m$ are linearly independent. Let N_T denote the solution space of

$$g_T(b_1, b_2, \ldots, b_{\omega-1}) = 0.$$

Since g_T is a nonzero polynomial in $\omega - 1$ variables, $|N_T| \leq |F|^{\omega-2}$. We now consider

$$\left| F^{\omega-1} \cap (\bigcup_T N_T) \right|$$

in order to find a k-reduction vector

$$\vec{v} = \begin{bmatrix} v_1 & v_2 & \cdots & v_{\omega-1} \end{bmatrix}^T.$$

By the union bound,

$$\left| F^{\omega-1} \cap (\bigcup_T N_T) \right| \leq \sum_T \left|(F^{\omega-1} \cap N_T)\right|.$$

Since $|N_T| \leq |F|^{\omega-2}$ and $n < |F|$, this implies

$$\begin{aligned} \sum_T \left|(F^{\omega-1} \cap N_T)\right| &\leq \sum_T |\, F\, |^{\omega-2} \\ &= n\, |\, F\, |^{\omega-2} \\ &< |\, F\, |^{\omega-1}. \end{aligned}$$

Therefore,

$$\left| F^{\omega-1} \cap (\bigcup_T N_T) \right| < | F^{\omega-1} |$$

and we can find $\vec{v} \in F^{\omega-1}$ such that $\vec{v} \notin \bigcup_T N_T$. In other words, $\vec{v}$ can be obtained such that

$$g_T(v_1, v_2, \ldots, v_{\omega-1}) \neq 0$$

for each non-source node T, which implies $\vec{c}_1^{\,\omega-1}, \vec{c}_2^{\,\omega-1}, \ldots, \vec{c}_m^{\,\omega-1}$ are linearly independent for each non-source node T when $\vec{b} = \vec{v}$ by Lemma 2. Consequently, $f_e^{\omega-1}, e \in E$ specify an $(\omega - 1)$-dimensional F-valued linear network code that

$$\begin{aligned} dim(V_T) &\geq m \\ &= \min\{k, maxflow(T)\} \end{aligned}$$

for each non-source node T when $\vec{b} = \vec{v}$. It then follows from Definition 8 that

$$\begin{bmatrix} v_1 & v_2 & \cdots & v_{\omega-1} \end{bmatrix}^T$$

is a k-reduction vector for the given linear network code. □

Lemma 7 *Suppose a finite field F and the local encoding kernel at every non-source node are given in an acyclic network. Let $I_{|Out(S)|}$ denote the $|Out(S)| \times |Out(S)|$ identity matrix. An $|Out(S)|$-dimensional F-valued linear network code is constructed by setting the local encoding kernel at the source S*

$$K_S = I_{|Out(S)|}.$$

For any non-source node T, let $\vec{x}$ be an $|Out(S)|$-dimensional row vector representing the message outgoing from S and $\vec{y}_T$ be an $|In(T)|$-dimensional row vector representing the received symbols of T. Then, there exists a unique $|Out(S)| \times |In(T)|$ matrix F_T such that

$$\vec{y}_T = \vec{x} \cdot F_T$$

for all $\vec{x}$ and

$$dim(V_T) = rank(F_T).$$

Proof: Let $\vec{x}'$ be an $|Out(S)|$-dimensional row vector representing the message incoming to S in the $|Out(S)|$-dimensional F-valued linear network code. Let F'_T be an $|Out(S)| \times |In(T)|$ matrix that

$$\vec{y}_T = \vec{x}' \cdot F'_T$$

for all $\vec{x}'$. Since K_S is equal to $I_{|Out(S)|}$, $\vec{x}$ is equal to $\vec{x}'$ and F_T is equal to F'_T. By [2],

$$F'_T = A(I - K)^{-1}B^T$$

where I is the $|E| \times |E|$ identity matrix, K is a unique $|E| \times |E|$ matrix depending on the local encoding kernels at all the non-source nodes and B is a unique $|In(T)| \times |E|$ matrix depending on T. Since the dimension of the constructed code is $|Out(S)|$ and

$$K_S = I_{|Out(S)|},$$

the dimension of A is $|Out(S)| \times |E|$ and A is a constant. Therefore, F'_T is a unique $|Out(S)| \times |In(T)|$ matrix, which implies F_T is also a unique $|Out(S)| \times |In(T)|$ matrix. Due to the fact that

$$dim(V_T) = rank(F'_T),$$

we have

$$dim(V_T) = rank(F_T). \ \square$$

Theorem 5 *Suppose a finite field F and the local encoding kernel at every non-source node are given in an acyclic network with $|Out(S)| \geq 1$. Let n be the number of non-source nodes in the network. An $|Out(S)|$-dimensional F-valued linear network code is then constructed by setting the local encoding kernel at the source S*

$$K_S = I_{|Out(S)|}.$$

Let k be the maximum non-negative integer such that

$$dim(V_T) \geq min\{k, maxflow(T)\}$$

for all non-source node T. If $|F| > n$, an h-dimensional F-valued linear broadcast can be constructed for every positive integer h less than or equal to k using the given local encoding kernels at all the non-source nodes.

Conversely, a υ-dimensional F-valued linear broadcast can never be constructed using the given local encoding kernels where $k < \upsilon \leq |Out(S)|$.

Proof: We will first show that there exists a k-dimensional F-valued linear broadcast on the network using the given local encoding kernels. It then follows that given the condition $|F| > n$, an h-dimensional F-valued linear broadcast can be constructed by Theorem 3 for every positive integer h less than or equal to k using the given local encoding kernels. Under the condition $|Out(S)| = 1$ or $k = 0$, it is trivial that a k-dimensional F-valued linear broadcast exists on the network using the given local encoding kernels. Therefore, we consider the case for $k \geq 1$ and $|Out(S)| \geq 2$. If $k = |Out(S)|$, the $|Out(S)|$-dimensional F-valued linear network code is the desired k-dimensional F-valued linear broadcast. If $k < |Out(S)|$, a k-reduction vector for the $|Out(S)|$-dimensional F-valued linear network code can be found by Lemma 6 and an $(|Out(S)| - 1)$-dimensional F-valued linear network code where

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T is obtained. This procedure can be repeated until we obtain a k-dimensional F-valued linear network code where

$$dim(V_T) \geq \min\{k, maxflow(T)\}$$

for all non-source node T. Since

$$dim(V_T) \leq \min\{k, maxflow(T)\}$$

for all non-source node T in a k-dimensional F-valued linear network code,

$$dim(V_T) = \min\{k, maxflow(T)\}$$

for all non-source node T, which implies this network code is a k-dimensional F-valued linear broadcast.

Next, we will prove the converse part of the theorem. For a fixed positive integer υ where $k < \upsilon \leq |Out(S)|$, there exists a non-source node T where

$$dim(V_T) < \min\{\upsilon, maxflow(T)\} \tag{3.7}$$

in the $|Out(S)|$-dimensional F-valued linear network code. Let F_T be the unique $|Out(S)| \times |In(T)|$ matrix in Lemma 7. Using Lemma 7,

$$dim(V_T) = rank(F_T),$$

which implies

$$rank(F_T) < \min\{\upsilon, maxflow(T)\}$$

by (3.7). Consider any local encoding kernel at the source K'_S and the corresponding υ-dimensional F-valued linear network code having the given local encoding kernel at every non-source node. Since the υ-dimensional linear network code and the $|Out(S)|$-dimensional linear network code have the same local encoding kernel at every non-source node, they have the same F_T in Lemma 7. In addition, the columns of $K'_S F_T$ consist of $f_e, e \in In(T)$, which implies

$$dim(V_T) = rank(K'_S F_T).$$

Consequently, in the υ-dimensional F-valued linear network code,

$$\begin{aligned} dim(V_T) &= rank(K'_S F_T) \\ &\leq rank(F_T) \\ &< \min\{\upsilon, maxflow(T)\}. \end{aligned}$$

Therefore, a υ-dimensional F-valued linear broadcast can never be constructed using the given local encoding kernels. □

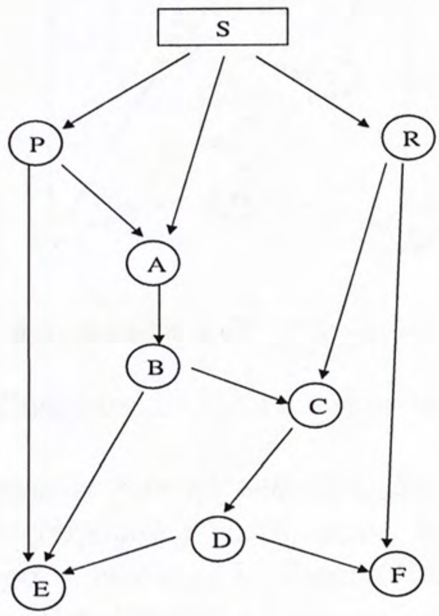

Figure 3.4: A single-source finite acyclic network

K_P	K_R	K_A	K_B	K_C	K_D
$[1\ 1]$	$[1\ 1]$	$\begin{bmatrix}1\\1\end{bmatrix}$	$[1\ 1]$	$\begin{bmatrix}1\\0\end{bmatrix}$	$[1\ 1]$

Figure 3.5: The local encoding kernels at the non-source nodes

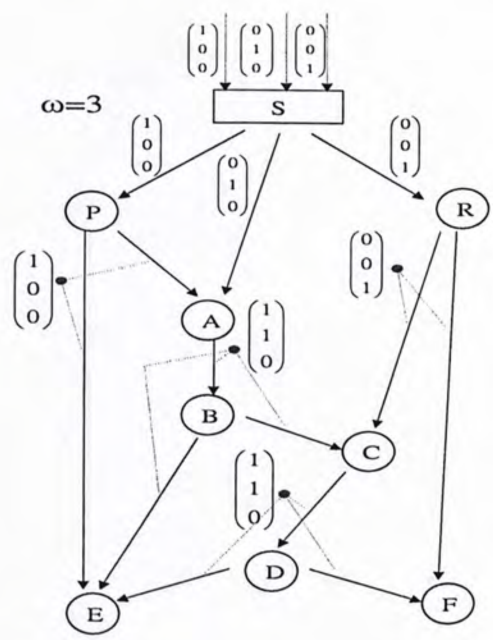

Figure 3.6: A 3-dimensional $GF(11)$ linear network code

Theorem 5 is illustrated by the following example.

Example 3 *An acyclic network with* $|Out(S)| = 3$ *is shown in Fig.* 3.4 *and the corresponding local encoding kernels at the non-source nodes are given in Fig.* 3.5. *Since* $|Out(S)| = 3$ *and the number of non-source nodes is* 8, *a* 3*-dimensional linear network code with* $K_S = I_3$ *is constructed and* F *is chosen to be* $GF(11)$. *The constructed* 3*-dimensional* $GF(11)$ *linear network code is shown in Fig.* 3.6. *From this network code,* k *in Theorem* 5 *is equal to* 2. *Therefore, an* h*-dimensional linear broadcast can be derived from the* 3*-dimensional linear network code by Theorem* 5 *for* $h = 1, 2$. *The derived* 2*-dimensional linear broadcast is shown in Fig.* 3.7.

Given the local encoding kernels at all the non-source nodes in a network, a set of linear network codes L can be derived.

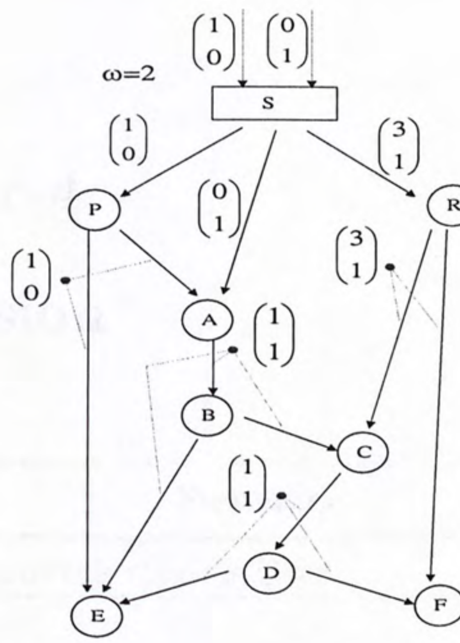

Figure 3.7: A 2-dimensional $GF(11)$ linear broadcast

Theorem 5 suggests a quick way to find the maximum rate k such that for at least one $l \in L$, l qualifies as a k-dimensional linear broadcast on the network. In addition, Theorem 5 can be extended to find the maximum rate k' such that for at least one $l' \in L$, l' qualifies as a k'-dimensional static linear broadcast on the network.

□ **End of chapter.**

Chapter 4

Conclusion

Summary

Conclusion of this thesis is given.

A scheme that enables efficient implementation of variable-rate linear network coding in a single-source finite acyclic network is developed. In our scheme, the same local encoding kernel at every non-source node can be used for different transmission rates. In addition, two efficient algorithms are proposed for implementing variable-rate linear network coding in different situations. Compared with existing solutions, our scheme is simpler and requires less storage space. Last but not least, a simple scheme that determines the maximum rate at which a given linear network code can qualify as a linear broadcast is presented.

Further research includes the complexity analysis of our algorithms that enable efficient implementation of variable-rate linear network coding. The performance analysis of randomly designed codes for variable-rate linear network coding is also interesting for future research. Since little research has been undertaken to investigate into the possible relationships among codes with different rates, efficient network code construction algorithms may evolve by exploring variable-rate linear network coding.

□ **End of chapter.**

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung. "Network information flow". *IEEE Transactions on Information Theory*, vol. 46:pp. 1204–1216, 2000.

[2] R. Koetter, M. Medard. "An Algebraic Approach to Network Coding". *Transactions on Networking*, Oct. 2003.

[3] R. W. Yeung and Z. Zhang. "Distributed source coding for satellite communications". *IEEE Trans. Inform. Theory*, IT-45:1111–1120, 1999.

[4] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang. "Network Coding Theory". *Foundations and Trends in Communications and Information Theory*, 2006.

[5] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen. "Polynomial time algorithms for multicast network code construction". *IEEE Transactions on Information Theory*, IT 51(1973–1982), Mar. 2005.

[6] S.-Y. R. Li, R. W. Yeung, and N. Cai. "Linear network coding". *IEEE Transactions on Information Theory*, Feb. 2003.