Robustness of Random Network Coding to Interfering Sources

Adrian Tauste Campo and Alex Grant
Institute for Telecommunications Research
University of South Australia
tausteng@hotmail.com alex.grant@unisa.edu.au

Abstract— **Random network codes are considered for multicast scenarios where not all of the sources are required by the sinks. These unwanted sources could model interfering or even adversarial sources. The objective of the paper is to determine the effect of the interfering sources on the probability of successful decoding. A lower bound on the success probability is determined. The bound is the product of the probability that the random network code is feasible without interference, multiplied by a robustness factor. The robustness factor uniquely depends on the in-degree of the sink and the size of the finite field. Analysis of the robustness factor shows that the effect of interference can be completely mitigated through a small increase in the field size.**

I. Introduction

It has been recently established that network layer coding can replace routing in a network. Network codes can increase the information transmission rate, particularly for multicast [1]. It is also known that linear network codes [2] can achieve max-flow upper bounds on the throughput in a single source multicast network. Not only does network coding offer higher throughput, it does so with fundamentally less complexity. Determination of optimal network codes can be performed in polynomial time, whereas determination of optimal multicast routes is NP complete. See [3] for an introduction to network coding.

Of particular interest in this paper are random network codes [4]–[6]. Random networks codes are linear network codes in which the encoding coefficients are chosen randomly from a finite field. The sink nodes can decode correctly if and only if the overall transfer matrix from the sources to each sink is invertible. It has been shown that the probability of successful decoding can be made as close to one as desired, by increasing the field size.

This paper considers the effect of interference in networks employing random network codes. There are several motivations for this investigation. Firstly, the existing network coding results only refer to robustness with regard to random link failures, but have not yet considered the effect of noise. Second, application of network coding to wireless scenarios necessarily results in interference. Moreover, it seems reasonable and useful to determine the degree to which the entire system is sensitive to the existence of undesired additional sources. Finally, it is important that network codes are robust to attack by malicious sources. For example, it is no good if the introduction of a single spurious source causes the entire network code to fail.

The main objective of this paper is to give a lower bound on the success probability of a random network code with interference. We first present a decoding strategy for network codes with extra noise sources, and from it derive the corresponding success probability in a randomized setting. We use the main result in [5] and introduce a new multiplicative factor which bounds the ability of the random network code in a particular network to accommodate extra noise sources.

We demonstrate that the new bound depends only on the total number of incoming sink edges in the network and the size of the finite field. Analysis reveals that super-linear dependence between the size of the field and the number of sink incoming edges leads to a factor which is approximately 1, thus recovering the interference-free success probability.

The paper is organized as it follows: Section II presents our model and introduces some algebraic notation. Section III enunciates some preliminary results which justify our decoding strategy. Section IV gives proofs of the main results and the last section concludes the paper with a summary of the results.

II. Model

We adopt the the model proposed in [4], [5]. The network is represented as a directed acyclic graph $G = (V, E)$ in which discrete random processes over a finite field $\mathbb{F}_q$ of size q are transmitted from $K \geq 1$ source nodes to $d \geq 1$ receivers through $\nu = |E|$ edges. Each sink has L incoming edges. Decoding is performed based on the field elements received on these incoming edges.

Each edge $l \in E$ can be defined as an incoming link of a node v if $v = \mathrm{head}(l)$ or as an outgoing link of v if $v = \mathrm{head}(l)$. We denote the total number of incoming edges of a node v as $|\overleftarrow{v}|$ and the total number of outgoing edges as $|\overrightarrow{v}|$. The time unit is chosen such that the capacity of each link is one bit per unit time and edges with larger capacity are modeled as parallel edges.

We assume that we are using linear coding which have been shown to be sufficient for the multicast problem [7] on acyclic delay networks.

As defined in [3], a *scalar linear code* for a network G with unit capacity edges is an assignment of linear encoding functions f_v to each node $v \in V$. Every linear encoding function maps from the vector space $\mathbb{F}_q^{|\overleftarrow{v}|}$ to $\mathbb{F}_q^{|\overrightarrow{v}|}$.

The message $m(e) \in \mathbb{F}_q$ on each outgoing edge is a linear combination of the messages $\{m(e'), e' \in \overleftarrow{v}\}$ on the incident

A. Grant is supported by the ARC under grant DP0557310.

edges.

$$m(e) = \sum_{e' \in \overleftarrow{v}} f(e, e')m(e')$$

where each $f(e, e') \in \mathbb{F}_q$.

The messages in the network are represented as column vectors and the linear encoding function for each node v as $|\overleftarrow{v}| \times |\overrightarrow{v}|$ matrices. It is also necessary to assume that the edges in the directed graph are ancestrally ordered.

We describe the overall encoding function as a $|E| \times |E|$ matrix F where F_{ij} is the coefficient applied to the symbol incoming on edge $j \in E$ for contribution to outgoing edge $i \in E$.

Similarly, define the *source matrix* A as the $|E| \times K$ matrix which maps messages onto outgoing source edges and the *sink matrix* B^l as the $|\overleftarrow{t_l}| \times |E|$ matrix which maps incoming sink edges onto the sinks $t_l \in V, l = 1, 2, \ldots, d$.

Define

$$B = \begin{bmatrix} B^1 \\ \vdots \\ B^d \end{bmatrix}, \quad L = \sum_{l=1}^{d} \left|\overleftarrow{t_l}\right|$$

Then the matrices A, F, B represent a *linear network code* and the messages incoming to each sink is given by

$$y = Mx$$

where $M = B(I - F)^{-1}A$ and $x \in \mathbb{F}^k$ is the information source vector [7].

Every sink can decode all sources if and only if each submatrix $M^l = B^l(I-F)^{-1}A$ has rank K . In case $K = L$ the condition turns out to be:

$$\det(B^l(I - F)^{-1}A) \neq 0.$$

We now formalize the concept of interference in a network code. A set of *information sources* in a noisy random network code is a vector $x \in \mathbb{F}_q^K$ where K is the number of desired users in the network. A set of *noise sources* in a noisy random network code is a vector $z \in \mathbb{F}_q^S$ where S is the number of interferers (i.e. unwanted, nuisance, or unintended message sources) in the network. The *complete message* in a noisy random network code is a vector $m = (x^T z^T)^T \in \mathbb{F}_q^{K+S}$ which is the concatenation of information and noise sources.

A linear network code with interference is represented by a $L \times (K + S)$ transfer matrix $\tilde{M} = [X|Z]$. The corresponding sink observations are

$$y = \tilde{M}^l m = X^l x + Z^l z, \ \ \forall l : 1 \leq l \leq d$$

where X^l is a $|\overleftarrow{t_l}| \times K$ sub-matrix consisting of the column vectors which multiply the information sources and Z^l is the $|\overleftarrow{t_l}| \times S$ sub-matrix which multiply the noise sources. The decoding problem is to determine x from y.

If the number of interferers is zero, $X^l = M^l$ and the decoding problem consists of solving the linear system $y = X^l x$ in each sink. In order to avoid the system $y = X^l x$ being under-determined we assume $|\overleftarrow{t_l}| \geq K + S$ which implies $\mathbb{F}_q^K \oplus \mathbb{F}_q^S \subseteq \mathbb{F}_q^{|\overleftarrow{t_l}|}$

III. A Decoding Strategy

We start with a basic result which will lead us to a sufficient condition for a successful decoding. Let $\tilde{M} = [X|Z]$ be a $L \times (K + S)$ transfer matrix of a linear random network code with interferences. If every sink can decode all sources X has rank K

Proposition 1: Let $y = X^l x + Z^l z$ be the output message in each sink where $x \in \mathbb{F}_q^K$ and $z \in \mathbb{F}_q^S$ are the information sources and the noise sources respectively. We can decode the message successfully in each sink if we have a $\tilde{K} \times L$ matrix $Q = \left[Q^1 \ldots Q^d\right]$ where $\tilde{K} = \dim(\langle \operatorname{span} Z \rangle^{\perp})$ and $\forall l : 1 \leq l \leq d$:

$$Q^l Z^l = 0 \tag{1}$$

$$\operatorname{rank}(Q^l X^l) = K \tag{2}$$

Proof: Given the hypothesis, $Q^l y = Q^l X^l x$ in each sink. Since $\operatorname{rank}(Q^l X^l) = K \ \forall l : 1 \leq l \leq d$ we can solve the linear system and obtain the information source vector in each sink. ∎

Proposition 2: Let $\tilde{M} = [X|Z]$ be the $L \times (K + S)$ transfer matrix of a linear network code with interference over $\mathbb{F}^q$, where $q > 2$. Let X^l have maximum rank K and $|\overleftarrow{t_l}| \geq K + S \ \forall l : 1 \leq l \leq d$. A matrix Q satisfying (1) and (2) of Proposition 1 exists if and only if $\langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle = 0$ $\forall l : 1 \leq l \leq d$.

Proof: Let $\langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle \neq 0$ for a $l : 1 \leq l \leq d$. Then there exists $v \in F^{|\overleftarrow{t_l}|}$ such that $v \in \langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle$. If $v \in \langle \operatorname{span} Z^l \rangle$ then $\langle \operatorname{span} Z^l \rangle^{\perp} \subseteq \langle v \rangle^{\perp}$ and consequently $\langle \operatorname{span} Q^l \rangle \subseteq \langle v \rangle^{\perp}$.

In each sink the product $Q^l X^l$ can be considered as a projection of the Q^l row vector basis into the X^l column vector basis. Now since $v \in \langle \operatorname{span} X^l \rangle$ and $Q^l v = 0$, for all $u \in \langle \operatorname{span} Q^l \rangle$, there is a null column vector or at least two dependent columns vectors in the matrix $Q^l X$. Hence, $\operatorname{rank}(Q^l X^l) \neq K$ contradicting our hypothesis.

Conversely, if $\langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle = 0 \ \forall l : 1 \leq l \leq d$ we can define each Q^l row vectors as a basis of $\langle \operatorname{span} Z^l \rangle^{\perp}$ with none of its vectors being equal to any vector in $\operatorname{span} X^l$.

Since $q > 2$ we have at least one different choice for every vector we introduce in each Q^l and we are able to avoid 0 products as a consequence of self-orthogonal vectors in $\mathbb{F}_q^{|\overleftarrow{t_l}|}$. Then $\langle \operatorname{span} X^l \rangle \subset \langle \operatorname{span} Q^l \rangle$ and $\operatorname{rank}(Q^l X^l) = K$ $\forall l : 1 \leq l \leq d$. ∎

IV. Robustness of Random Network Codes

From now on assume that every coefficient of the linear network code is random, chosen independently with a discrete-uniform probability function on $\mathbb{F}_q$. Our main result is stated as follows.

Theorem 1: Let $M = [X|Z]$ be the transfer matrix of a random network code over a field $\mathbb{F}_q$ in a network with L incoming sink edges, d receivers, ν edges with randomly chosen coefficients, K information sources and S interferers.

The probability that all the receivers can decode the source processes using the decoding strategy of Proposition 1 is at least

$$(1-2/q)^L(1-d/q)^v$$

for $q > d$.
In order to be able to prove Theorem 1 we first establish the following lemmas.

Lemma 1: The number of m-dimensional subspaces of $\mathbb{F}_q^L$ is given by the Gaussian coefficient

$$\begin{bmatrix} L \\ m \end{bmatrix}_q = \frac{\prod_{i=0}^{m-1}\left(q^L - q^i\right)}{\prod_{j=0}^{m-1}\left(q^m - q^j\right)}$$

Proof: The numerator is the number of bases of all m-dimensional subspaces, while the denominator is the number of bases of any given subspace. ■

Lemma 2: The probability over a discrete-uniform mass function that a K-dimensional subspace and a S-dimensional subspace have null intersection is

$$R(q, L, K, S) = \frac{\prod_{i=0}^{K-1}\left(q^L - (q^S - 1) - q^i\right)\prod_{j=0}^{S-1}\left(q^L - (q^K - 1) - q^j\right)}{\prod_{k=0}^{K-1}\left(q^L - q^k\right)\prod_{l=0}^{S-1}\left(q^L - q^l\right)}$$

Proof: Let $\mathcal{K}$ resp. $\mathcal{S}$ be the set of all K-dimensional resp. S-dimensional subspaces in $\mathbb{F}_q^L$ and consider the space of probability given by $(\omega, \mathcal{P}(\omega), \Pr)$ where

$$\omega = \{(k, s) \mid k \in \mathcal{K}, s \in \mathcal{S}\}$$

and Pr is the uniform assignment of probability over a discrete set. In the space $(\omega, \mathcal{P}(\omega), \Pr)$ we are interested in computing the probability of the event

$$W = \{(k, s) | k \in \mathcal{K}, s \in \mathcal{S}, k \cap s = 0\}$$

Hence

$$\begin{aligned}\Pr(W) = \frac{|W|}{|\mathcal{K}||\mathcal{S}|} &= \sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\Pr(W \cap \{(k, s)\}) \\ &= \sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\Pr(W \cap k)\Pr(W \cap s)\}) \\ &= \sum_{k\in\mathcal{K}}\sum_{s\in\mathcal{S}}\Pr(W|k)\Pr(k)\Pr(W|s)\Pr(s)\end{aligned}$$

We calculate $\Pr(W|k)$ counting the number of S-dimensional subspaces which do not have common vectors with any of the $q^K - 1$ non-null vectors of k. Since the probability function is uniform the number of these subspaces is divided by the total number of S-dimensional subspaces.

$$Pr(W|k) = \frac{\prod_{j=0}^{S-1}\left(q^L - (q^K - 1) - q^j\right)}{\begin{bmatrix} L \\ S \end{bmatrix}_q}$$

Similarly, we calculate

$$Pr(W|s) = \frac{\prod_{j=0}^{K-1}\left(q^L - (q^S - 1) - q^j\right)}{\begin{bmatrix} L \\ K \end{bmatrix}_q}$$

The result follows from $\Pr(k) = 1/|\mathcal{K}|$ and $\Pr(s) = 1/|\mathcal{S}|$. ■

We shall refer to the function $R(q, L, K, S)$ where $q > 2$, $L = K + S > 2$, $K, S \geq 0$ as the *robustness factor* of a random network code over the finite field $\mathbb{F}_q$.

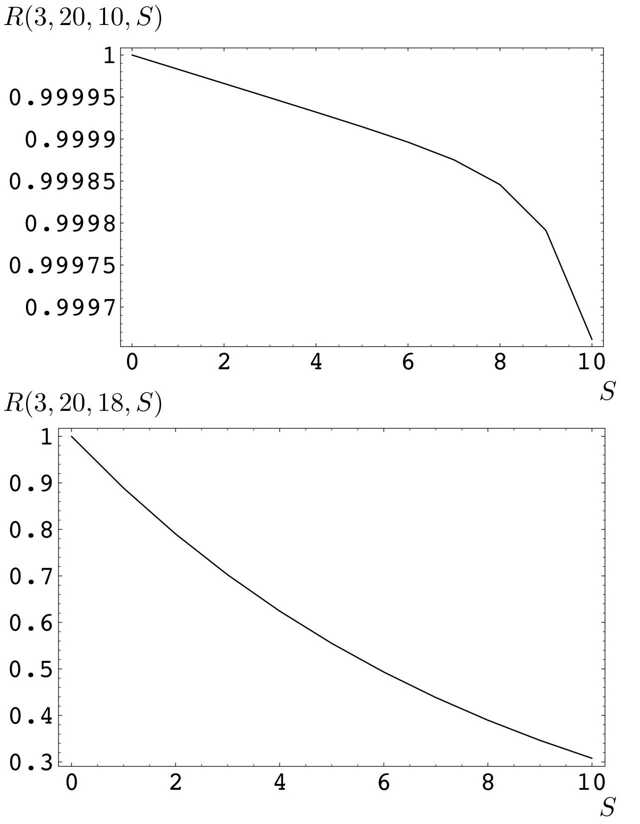
From the form of the function R we can derive some interesting and useful properties:

1) **Symmetry** $R(q, L, K, S) = R(q, L, S, K)$
2) **Robustness** If $K \neq 0$, $R(q, L, K, 0) = 1$
3) **Complexity Tradeoff** For fixed L, K, S

$$\lim_{q\to\infty} R(q, L, K, S) = 1$$

4) **Worst Case Bounds** $R(q, L, S, K) \geq R(q, L, L-1, 1)$, for all $L \geq 2$, $L = K + S$ and $q > 2$

The last property indicates that the decoding scheme presented in Proposition 1 shows a trade-off between the utilization of resources K/L and the robustness of the network code. Surprisingly, if we increase the ratio K/L for a fixed number of noise sources the robustness factor also decreases. However, as it seems reasonable, for a given utilization the robustness factor goes down with the increase of the number of interferers as shown in Figure 1 However, since the lower bound depends uniquely on q and L, for a sufficiently large finite fields the variables K and S and consequently the utilization is not a crucial factor in our decoding success.



1: Robustness factor for an utilization of 50 and 90% with $L = 20$ and $q = 3$.

Proof: [Theorem 1] Let $\tilde{M} = [X|Z]$ be a $L \times (K + S)$ transfer matrix of a random network code with interference. Success of the decoding scheme in Proposition 1 needs two requirements to be met: the feasibility and the robustness of the random network code. Since these two conditions are not independent we compute the overall success probability as follows.

Let the event $Q = \{\langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle = 0,\ \forall l : 1 \leq l \leq d\}$ in a space of probability $(\omega, \mathcal{P}(\omega), \Pr)$:

$$\begin{aligned}\Pr\{\text{success}\} &= \Pr(\{\text{Feasibility}\} \cap \{\text{Robustness}\})\\ &= \Pr(\prod_{l=1}^{d} \det(M^l) \neq 0 \cap Q)\\ &= \Pr(Q| \prod_{l=1}^{d} \det(M^l) \neq 0) \Pr(\prod_{l=1}^{d} \det(M^l) \neq 0)\\ &= \Pr(Q| \prod_{l=1}^{d} \det(M^l) \neq 0)\, (1 - d/q)^{\nu}.\end{aligned}$$

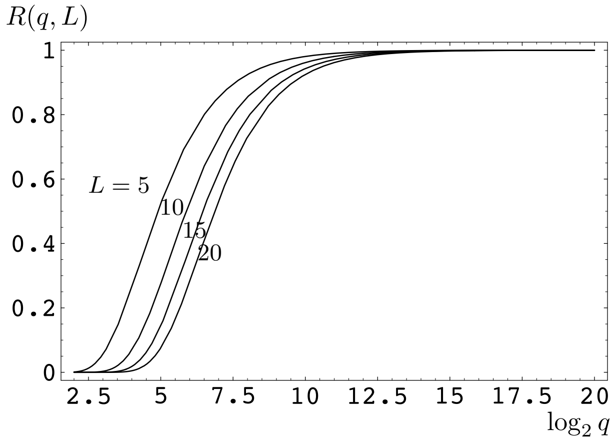
Given $\prod_{l=1}^{d} \det(M^l) \neq 0$, $\langle \operatorname{span} X^l \rangle$ has dimension K $\forall l : 1 \leq l \leq d$. Let $\langle \operatorname{span} Z^l \rangle$ have dimension $\tilde{S}$ where $\tilde{S} \leq S$. We can apply Lemma 2 to the subspaces $\langle \operatorname{span} X^l \rangle$ and $\langle \operatorname{span} Z^l \rangle$ in each of d sinks:

$$\begin{aligned}&\Pr(\{\langle \operatorname{span} X^l \rangle \cap \langle \operatorname{span} Z^l \rangle = 0 \ \mid \operatorname{rank}(X^l) = K, \forall l : 1 \leq l \leq d\})\\ &= \prod_{l=1}^{d} R(q, |\overleftarrow{t_l}|, K, S)\\ &\geq \prod_{l=1}^{d} R(q, |\overleftarrow{t_l}|, |\overleftarrow{t_l}| - 1, 1)\\ &\geq \left(\frac{q^{|\overleftarrow{t_l}|} - q^{|\overleftarrow{t_l}|-1} - q + 1}{q^{|\overleftarrow{t_l}|-1}}\right)^{L}\\ &\geq \left(\frac{q^{|\overleftarrow{t_l}|} - q^{|\overleftarrow{t_l}|-1} - q}{q^{|\overleftarrow{t_l}|}}\right)^{L}\\ &\geq (1 - 1/q - 1/q^{|\overleftarrow{t_l}|-1})^{L}\\ &\geq (1 - 2/q)^{L}.\end{aligned}$$

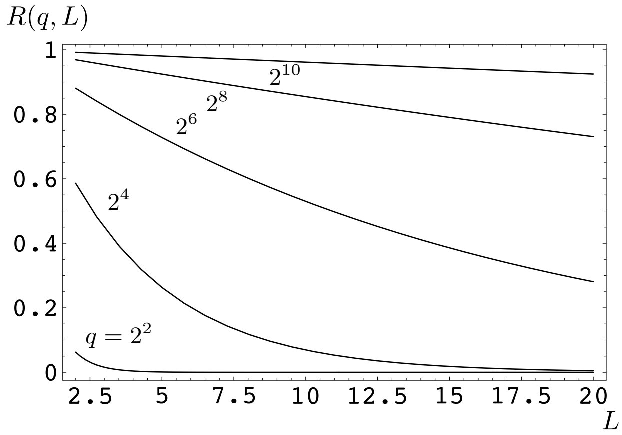
■

In essence, we use the bound found in [6] and we multiply it by a probability factor which shows the effect of interference. The function $R(q, L) = (1 - 2/q)^L$ is called the *robustness bound.*

It is important to point out that the robustness bound does not depend on the information sources or on the noise sources but on the total number of sinks. This derives from the fact that the bound represents the worst case in our decoding strategy in which in every sink the number of information sources is equal to $|\overleftarrow{t_l}| - 1$ and there is one extra undesirable source. In Figure 2 we show how the bound performs for different values of $q = 2^u$ and L.



2: Robustness bound for $2^2 \leq q \leq 2^{20}$ and $L = 5, 10, 15, 20$.



3: Robustness bound for $2 \leq L \leq 20$

As Figure 1 and Figure 2 show, $R(q, L)$ tends to zero as L gets larger and tends to 1 with the increase of q. It is reasonable to calculate in which degree we need to increase q (in relation with L) in order to have a robust factor that is not vulnerable to the increase of the number of incoming sink edges. Therefore, we have the following result:

Theorem 2: If $q \geq L^r$, $r > 0$ then

$$\lim_{L \to \infty} Rb(q, L) = 1 \iff r > 1$$

Proof: As q depends on L we use the function $q(L) = L^r$. We calculate the following limit

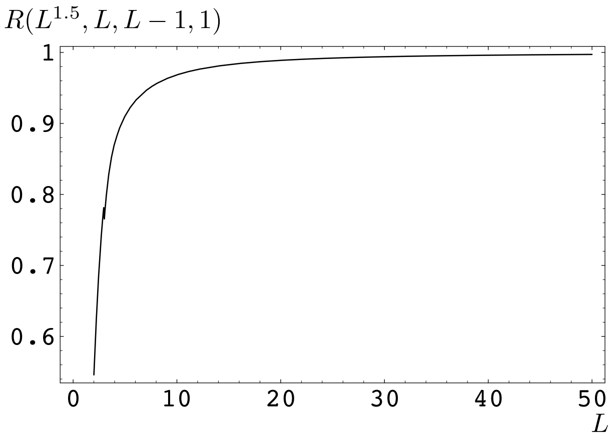
$$\begin{aligned}\lim_{L \to \infty} R(q(L), L) &\geq \lim_{L \to \infty} \left(1 - \frac{2}{q(L)}\right)^{2L}\\ &= \lim_{L \to \infty} e^{-L/L^r}\\ &= \begin{cases} 1 & r > 1 \\ 1/e & r = 1 \\ 0 & r < 1 \end{cases}\end{aligned}$$

■

Corollary 1: Given a random network code with d receivers and ν edges, let L be the total number of incoming sink edges for all receivers and $q(L) \geq L^r$ the size of a finite field. Then

$$\lim_{L \to \infty} \Pr_{success} = (1 - d/q)^{v} \iff r > 1$$

Our main results show that choosing the size of the field properly makes the decoding error probability tend to $1-(1-d/q)^v$ and the effect of the interference can be made negligible. Figure 3 shows this tendency for the choice $q(L) > L^{1.5}$



4: Robustness factor with $q(L) > L^{1.5}$

V. Conclusions

The main problem that we have studied in this paper is to compute how a random network code is robust to interference. We have presented an algebraic model that includes interference as extra noise sources and we have designed a strategy to successfully decode the information sources in the network.

Our decoding strategy has been translated to an algebraic condition that has leaded us to compute a multiplicative factor which indicates the robustness of the random network code.

We have given a more precise lower bound in the success probability of decoding with noise sources. Our research has demonstrated that the multiplicative factor due to interference is negligible for a finite fields of size equal or larger to any non unit power of the number of sink incoming edges.

References

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[2] S.-Y. R. Li, R. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[3] A. Grant, "Network information theory and coding," Institute for Telecommunications Research, University of South Australia, Tech. Rep., 2005.

[4] T. Ho, M. Médard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," in *41st Annual Allerton Conference on Communication, Control and Computing*, Monticello, USA, 2003.

[5] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *IEEE Int. Symp. Inform. Theory*, Yokohama, Japan, 2003.

[6] T. Ho, M. Médard, D. R. Karger, and M. Effros, "Toward a random operation of networks," *IEEE Trans. Inform. Theory*, 2004, submitted.

[7] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, Oct. 2003.