On Bounds for Network Codes

Eimear Byrne

### On Bounds for Network Codes

#### Eimear Byrne

Claude Shannon Institute and School of Mathematical Sciences University College Dublin Ireland

WCC Bergen 2013

# Network Coding for Error Correction

#### On Bounds for Network Codes

#### Eimear Byrne

- Yang, Yeung, Cai, Zhang introduced error correction in coherent networks, where the network topology is known to the receiver.
  - ideas from classical coding theory
- Kötter, Kschischang, Silva describe error correction where the network topology is not known to the receiver.

- subspace codes
- rank metric codes
- matrix channels

### The Alphabet

On Bounds for Network Codes

Eimear Byrne

*R* is a finite ring and *A* is a bimodule over *R* such that  $\mathcal{A}_R \cong Hom(R, \mathbb{C}^{\times})_R =: \hat{R}_R \text{ and } _R\mathcal{A} \cong _RHom(R, \mathbb{C}^{\times}) =: _R\hat{R}$ 

$$\blacksquare R = \mathcal{A} = \mathbb{F}_q$$

$$\blacksquare R = \mathcal{A} = \mathbb{F}_q^{n \times r}$$

$$\blacksquare R = \mathcal{A} = GR(p^n, m)$$

- R = A = a Frobenius ring
- R any finite ring  $\mathcal{A} = \hat{R}$

### The Network

On Bounds for Network Codes

Eimear Byrne

The network is a directed acyclic graph N with n unit edge capacities, a source node s and several sinks t ∈ T
The source transmits messages from a set of size M

$$\mathcal{M} = \{(x_0, 0) : x_0 \in \mathcal{M}_0 \subset \mathcal{A}^m, 0 \in \mathcal{A}^{n-m}\}.$$

• The transfer function is an *R*-automorphism

$$\mathcal{F}: \mathcal{A}^n \longrightarrow \mathcal{A}^n: z \mapsto (f_1(z), ..., f_n(z)).$$

If x is transmitted from s and edges of the network are corrupted by an error e ∈ A<sup>n</sup> then the network transmission is

$$y=\mathcal{F}(x+e).$$

・ロト ・ 日下 ・ 日下 ・ 日下 ・ 今日・

### Example - The Butterfly Network



### Transfer Function for the Butterfly Network

On Bounds for Network Codes

Eimear Byrne

The transfer function for the Butterfly Network is given by the matrix

$$F = I + T + T^{2} + T^{3} = (I - T)^{-1}$$

$$F = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

On Bounds for Network Codes

Eimear Byrne

The transfer function for sink t is the R-epimorphism

$$\mathcal{F}_t: \mathcal{A}^n \longrightarrow \mathcal{A}^{n_t}: z \mapsto (f_i(z))_{i \in E_t},$$

where *E<sub>t</sub>* is the set of *n<sub>t</sub>* edges incident with *t*.
Sink *t* receives

$$y = \mathcal{F}_t(x + e) \in \mathcal{A}^{n_t}.$$

The network code for t is the set

$$\mathcal{C}_t := \{\mathcal{F}_t(x) \in \mathcal{A}^{n_t} : x \in \mathcal{M}\} \subset \mathcal{A}^{n_t}$$

• Messages  $z, z' \in \mathcal{A}^n$  are identified if

$$z-z' \in \ker \mathcal{F}_t =: K_t$$

On Bounds for Network Codes

The transfer matrix for the Butterfly Network is given by

$$F = I + K + K^2 + K^3 = (I - K)^{-1}$$



On Bounds for Network Codes

The transfer matrix for the Butterfly Network is given by

$$F = I + K + K^2 + K^3 = (I - K)^{-1}$$



On Bounds for Network Codes

If the message  $x = [x_1, x_1, 0, 0, 0, 0, 0, 0, 0]$  is transmitted without error then receivers 1 and 2 get

	1	1 -		F 0	1	
	0	1		1	1	
	1	0		0	0	
	0	1		0	1	
$xF_1 = x$	0	1	$= [x_1, x_1 + x_2], xF_2 = x$	0	1	$= [x_2, x_1 + x_2].$
	0	0		1	0	
	0	1		0	1	
	0	1		0	0	
	0	0		0	1	

 $\mathcal{C}_1, \mathcal{C}_2 \subset GF(2)^2.$ 

### **Relevant Errors**

On Bounds for Network Codes

Eimear Byrne

• If x is sent and the error  $e \in K_t$  occurs then

$$\mathcal{F}_t(x+e) = \mathcal{F}_t(x) \in \mathcal{C}_t$$

is received, as if without error.

• The decoder is only interested in errors *e* such that

$$\mathcal{F}_t(e) \neq 0.$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへで

### A Distance Function

On Bounds for Network Codes

Given a distance function d on  $\mathcal{A}^n$ ,  $K_t$  induces one on  $\mathcal{A}^{n_t}$  by

$$d_t(u, v) := \min\{d(x, y) : (u, v) = (\mathcal{F}_t(x), \mathcal{F}_t(y))\},\$$
  
=  $d(x + K_t, y + K_t),$ 

where  $(u, v) = (\mathcal{F}_t(x), \mathcal{F}_t(y)).$ 

#### Example

For

$$x \in R^n, F_t \in R^{n \times n_t}, \mathcal{F}_t(x) = xF_t$$

the Hamming distance induces a weight,  $w_t(u) = d_t(u, 0)$ , which counts the minimum number of linearly independent rows of  $F_t$  required to obtain a representation of  $u = \mathcal{F}_t(x)$ .

# Weights Induced by $K_1$ for the Butterfly Network

On Bounds for Network Codes

Eimear Byrne

Recall that for the Butterfly Network we have

#### $K_1$ induces the following weights on $GF(2)^2$ .

С	00	01	10	11
$cF_1^{-1}$	$K_1$	$0100 + K_1$	$00100 + K_1$	$100 + K_1$
w(c)	0	1	1	1

### Error Correction

On Bounds for Network Codes

Eimear Byrne

■ Given the received word y<sub>t</sub>, the decoder at node t decides that c = F<sub>t</sub>(x) has been transmitted if

 $\mathrm{d}_t(y,c) < \mathrm{d}_t(y,c')$ 

for all  $c' \in C_t$ .

The decoder at node t can correct r errors if

$$\mathrm{d}_t(\mathcal{C}_t) \geq 2r+1.$$

That is, if  $d_t(\mathcal{C}_t) \ge 2r + 1$  then  $\mathcal{C}_t$  can correct any error pattern e satisfying  $w_t(\mathcal{F}_t(e)) \le r$ .

### Parameters of a Network Code

On Bounds for Network Codes

Eimear Byrne

#### Definition

Let  ${\cal N}$  be a network with a set of sink nodes  ${\cal T}.$  Let  ${\cal F}$  be a transfer function for  ${\cal N}.$ 

A network code  ${\mathcal C}$  for the network  ${\mathcal N}$  is a collection

$$\mathcal{C}:=\{\mathcal{C}_t:t\in\mathcal{T}\},\$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

where  $C_t = \{\mathcal{F}_t(x) : x \in \mathcal{M}\}$  is an  $(n_t, M, d_t)$  code.

# The Size of a Network Code

On Bounds for Network Codes

Eimear Byrne

#### Definition

$$A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\})$$

the maximum size of any  $(n, \{(n_t, \ell_t, M, d_t) : t \in \mathcal{T}\})$  network code. We denote by

$$A(n, n_t, \ell_t, d_t)$$

the maximum size of any  $(n_t, \ell_t, M, d_t)$  network code for sink t.

■  $\ell_t := |\text{supp } K_t|$ ■  $\text{supp } K_t := \{i \in \{1, ..., n\} : z_i \neq 0 \text{ some } z = (z_i)_{i=1}^n \in K_t\}$ 

# Some Known Upper Bounds

On Bounds for Network Codes

Theorem (Yang *et al*, 2011)

Let R = A = GF(q). Then

 $A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq$ 

$$\min\left\{\frac{q^{n_t}}{\sum_{i=1}^{n_t} \binom{n_t}{i}(q-1)^i} : t \in \mathcal{T}\right\} (sphere-packing bound) \\ \min\left\{q^{n_t-d_t+1} : t \in \mathcal{T}\right\} (refined Singleton bound)$$

# Some Known Upper Bounds

On Bounds for Network Codes

Theorem (Yang *et al*, 2011)

Let R = A = GF(q). Then

 $A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq$ 

$$\min\left\{\frac{q^{n_t}}{\sum_{i=1}^{n_t} \binom{n_t}{i}(q-1)^i} : t \in \mathcal{T}\right\} (sphere-packing bound) \\ \min\left\{q^{n_t-d_t+1} : t \in \mathcal{T}\right\} (refined Singleton bound)$$

- Plotkin bound?
- Elias bound?

#### The Classical Plotkin and Elias Bounds

On Bounds for Network Codes

The classical Plotkin and Elias bounds find upper and lower bounds on the sum of the distances between codewords of an (n, |C|, d) code for the homogeneous weight.

$$|C|(|C|-1)d \leq \sum_{x,y\in C} d(x,y) = \sum_{i=1}^{n} \sum_{x,y\in C} d(x_i,y_i)$$

#### The Classical Plotkin and Elias Bounds

On Bounds for Network Codes

The classical Plotkin and Elias bounds find upper and lower bounds on the sum of the distances between codewords of an (n, |C|, d) code for the homogeneous weight.

$$\begin{aligned} |C|(|C|-1)d &\leq \sum_{x,y \in C} d(x,y) &= \sum_{i=1}^{n} \sum_{x,y \in C} d(x_i,y_i) \\ &\leq \begin{cases} |C|^2 n\gamma & \text{Plotkin} \\ |C|^2 (2r - \frac{r^2}{\gamma n}) & \text{Elias} \\ r^2 - 2\gamma nr + \gamma nd > 0. \end{cases} \end{aligned}$$

"On Bounds for Codes Over Frobenius Rings Under Homogeneous Weights", Greferath & O'Sullivan, Discrete Mathematics, 2004.

# Pulling Back to the Network Code

On Bounds for Network Codes

Eimear Byrne

These arguments work because the homogeneous weight of a word can be expressed as the sum of the weights of its components.

This is not true of the distance function for the network.

For example, the Butterfly Network matrix  $F_1$  and the Hamming distance gives the induced weight:

С	00	01	10	11
$w(\mathbf{c})$	0	1	1	1

# The Homogeneous Weight

On Bounds for Network Codes

Eimear Byrne

#### Definition

A weight function w on a left R-module  $\mathcal{A}$  is called homogeneous if

H1 If Rx = Ry then w(x) = w(y) for all  $x, y \in A$ .

H2 There exists a real number  $\gamma$  such that

$$\sum_{y\in Rx} w(y) = \gamma |Rx| \ \forall \ 0 \neq x \in \mathcal{A}.$$

This weight always exists on  $\mathcal{A}$  and is unique of to choice of  $\gamma$ .

On Bounds for Network Codes

Eimear Byrne

• If  $R = \mathcal{A} = GF(q)$ , the Hamming weight is homogeneous with average weight  $\gamma = \frac{q-1}{q}$ .

On Bounds for Network Codes

Eimear Byrne

• If  $R = \mathcal{A} = GF(q)$ , the Hamming weight is homogeneous with average weight  $\gamma = \frac{q-1}{q}$ .

 If R = A = Z₄, the Hamming weight is not homogeneous, but the Lee weight is with average weight γ = 1.

On Bounds for Network Codes

Eimear Byrne

• If  $R = \mathcal{A} = GF(q)$ , the Hamming weight is homogeneous with average weight  $\gamma = \frac{q-1}{q}$ .

- If R = A = Z₄, the Hamming weight is not homogeneous, but the Lee weight is with average weight γ = 1.
- Let  $R = \mathcal{A} = GF(q)^{2 \times 2}$ . Then the weight

$$w(x) = \begin{cases} \frac{q^2 - q - 1}{q - 1} & \text{if } \operatorname{rank}(x) = 2, \\ q & \text{if } \operatorname{rank}(x) = 1, \\ 0 & \text{if } x = 0, \end{cases}$$

is homogeneous with average value  $\gamma = \frac{q^2-1}{q}$ .

On Bounds for Network Codes

Eimear Byrne

• If  $R = \mathcal{A} = GF(q)$ , the Hamming weight is homogeneous with average weight  $\gamma = \frac{q-1}{q}$ .

- If R = A = Z₄, the Hamming weight is not homogeneous, but the Lee weight is with average weight γ = 1.
- Let  $R = \mathcal{A} = GF(q)^{2 \times 2}$ . Then the weight

$$w(x) = \begin{cases} \frac{q^2 - q - 1}{q - 1} & \text{if } \operatorname{rank}(x) = 2, \\ q & \text{if } \operatorname{rank}(x) = 1, \\ 0 & \text{if } x = 0, \end{cases}$$

is homogeneous with average value  $\gamma = \frac{q^2-1}{q}$ . For the case q = 2, this is the Bachoc weight.

On Bounds for Network Codes

Eimear Byrne

• If  $R = \mathcal{A} = GF(q)$ , the Hamming weight is homogeneous with average weight  $\gamma = \frac{q-1}{q}$ .

- If R = A = Z₄, the Hamming weight is not homogeneous, but the Lee weight is with average weight γ = 1.
- Let  $R = \mathcal{A} = GF(q)^{2 \times 2}$ . Then the weight

$$w(x) = \begin{cases} \frac{q^2 - q - 1}{q - 1} & \text{if } \operatorname{rank}(x) = 2, \\ q & \text{if } \operatorname{rank}(x) = 1, \\ 0 & \text{if } x = 0, \end{cases}$$

is homogeneous with average value  $\gamma = \frac{q^2-1}{q}$ . For the case q = 2, this is the Bachoc weight.

•  $R = GF(q), \ \mathcal{A} = GF(q)^{2 \times 2}$  the Hamming weight is homogeneous for  $\gamma = \frac{q-1}{q}$ .

# A Plotkin Bound

On Bounds for Network Codes

#### Theorem

Let  $d = \min\{d_t : t \in \mathcal{T}\} > \gamma n$  and let  $\ell = \min\{\ell_t : t \in \mathcal{T}\}$ . Then

$$\begin{aligned} A(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) &\leq \min\left\{\frac{d_t - \gamma \ell_t}{d_t - \gamma n} : t \in \mathcal{T}\right\} \\ &\leq \frac{d - \gamma \ell}{d - \gamma n}, \end{aligned}$$

# A Plotkin Bound

On Bounds for Network Codes

#### Theorem

Let  $d = \min\{d_t : t \in \mathcal{T}\} > \gamma n$  and let  $\ell = \min\{\ell_t : t \in \mathcal{T}\}$ . Then

$$\begin{array}{ll} \mathcal{A}(n,\{(n_t,\ell_t,d_t):t\in\mathcal{T}\}) &\leq & \min\left\{\frac{d_t-\gamma\ell_t}{d_t-\gamma n}:t\in\mathcal{T}\right\}\\ &\leq & \frac{d-\gamma\ell}{d-\gamma n}, \end{array}$$

As  $\ell \longrightarrow 0$  this gives the classical Plotkin bound.

# An Elias Bound

On Bounds for Network Codes

Eimear Byrne

#### Theorem

Let  $d_t \leq \gamma n$  and let

$$\gamma \ell_t \leq \mathsf{r} \leq \gamma \mathsf{n} - \sqrt{\gamma (\gamma \mathsf{n} - \mathsf{d}_t)(\mathsf{n} - \gamma \ell_t)}$$

Then  $A(n, n_t, \ell_t, d_t) \leq$ 

$$\frac{\gamma(d_t - \gamma\ell_t)(n - \ell_t)|\mathcal{A}|^{n-\ell_t}}{[(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma\ell_t)]|B^{n-\ell_t}(r - \gamma\ell_t)|},$$
  
$$B^{n-\ell_t}(r - \gamma\ell_t) \text{ is the sphere of radius } r - \gamma\ell_t \text{ about } 0 \in \mathcal{A}^{n-\ell_t}.$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

# An Elias Bound

On Bounds for Network Codes

ar Byrne

#### Theorem

Let  $d_t \leq \gamma n$  and let

$$\gamma \ell_t \leq \mathsf{r} \leq \gamma \mathsf{n} - \sqrt{\gamma (\gamma \mathsf{n} - \mathsf{d}_t) (\mathsf{n} - \gamma \ell_t)}$$

Then  $A(n, n_t, \ell_t, d_t) \leq$ 

$$\frac{\gamma(d_t - \gamma\ell_t)(n - \ell_t)|\mathcal{A}|^{n - \ell_t}}{[(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma\ell_t)]|\mathcal{B}^{n - \ell_t}(r - \gamma\ell_t)|},$$

 $B^{n-\ell_t}(r-\gamma\ell_t)$  is the sphere of radius  $r-\gamma\ell_t$  about  $0 \in \mathcal{A}^{n-\ell_t}$ .

As  $\ell \longrightarrow 0$  this gives the classical Elias bound.

# The Homogeneity Property

On Bounds for Network Codes A key property of the homogeneous weight that gives these results is the following fact.

imear Byrne

#### Lemma

Let  $_{R}A_{R}$  be a Frobenius bimodule with homogenous weight function  $w : A \longrightarrow \mathbb{R}$ . Let C be an R-submodule of  $A^{n}$  and let  $x \in A^{n}$ . Then

$$\frac{1}{|C|}\sum_{c\in C}w(x+c)=\gamma|\mathrm{supp}\ C|+w(\pi_{\mathrm{supp}\ C}(x)).$$

# The Homogeneity Property

On Bounds for Network Codes

Eimear Byrne

A key property of the homogeneous weight that gives these results is the following fact.

#### Lemma

Let  $_{R}A_{R}$  be a Frobenius bimodule with homogenous weight function  $w : A \longrightarrow \mathbb{R}$ . Let C be an R-submodule of  $A^{n}$  and let  $x \in A^{n}$ . Then

$$\frac{1}{|C|}\sum_{c\in C}w(x+c)=\gamma|\mathrm{supp}\ C|+w(\pi_{\mathrm{supp}\ C}(x))$$

#### Corollary

$$w(x + C) \leq \gamma |\text{supp } C| + w(\pi_{\text{supp } C}(x)).$$



▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□ ● ● ●

We seek an upper bound on this quantity.

On Bounds for Network Codes

#### Definition

$$\alpha_t(\nu,\lambda,\delta) := \lim_{n\to\infty} \sup \frac{1}{n} \log_{|\mathcal{A}|} A(n,\nu n,\lambda n,\delta n).$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

We seek an upper bound on this quantity.

On Bounds for Network Codes

#### Theorem (Plotkin)

$$\alpha_t(\nu,\lambda,\delta)) \leq \begin{cases} 0 & \text{if } \delta > \gamma \\ 1 - \frac{\delta}{\gamma} & \text{if } \delta \le \gamma \end{cases}$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

On Bounds for Network Codes

#### Theorem (Plotkin)

$$\alpha_t(\nu,\lambda,\delta)) \leq \begin{cases} 0 & \text{if } \delta > \gamma \\ 1 - \frac{\delta}{\gamma} & \text{if } \delta \le \gamma \end{cases}$$

#### Theorem (Singleton)

Let  $0 < \delta < \nu < 1$ . Then

$$\alpha_t(\nu, \delta, \lambda) \leq \nu - \delta.$$

On Bounds for Network Codes

#### Theorem (Elias)

Let 
$$ho > 0$$
 and let  $u, \lambda, \delta \in (0, 1)$  satisfy  $\delta \leq \gamma$  and  $\gamma \lambda \leq \rho \leq \gamma - \sqrt{\gamma(\gamma - \delta)(1 - \lambda)}.$ 

Then

$$\alpha_t(\nu, \delta, \lambda) \leq 1 - \lambda - H\left(\gamma - \sqrt{\frac{\gamma(\gamma - \delta)(1 - \gamma\lambda)}{1 - \lambda}}\right)$$

where

$$H(\delta) := \lim_{N o \infty} \sup N^{-1} \log_{|\mathcal{A}|} |B^N(\delta N)|$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへぐ

On Bounds for Network Codes

#### Theorem (Elias)

Let 
$$ho > 0$$
 and let  $u, \lambda, \delta \in (0, 1)$  satisfy  $\delta \leq \gamma$  and  $\gamma \lambda \leq \rho \leq \gamma - \sqrt{\gamma(\gamma - \delta)(1 - \lambda)}.$ 

Then

$$\alpha_t(\nu, \delta, \lambda) \leq 1 - \lambda - H\left(\gamma - \sqrt{\frac{\gamma(\gamma - \delta)(1 - \gamma\lambda)}{1 - \lambda}}\right)$$

where

$$H(\delta) := \lim_{N o \infty} \sup N^{-1} \log_{|\mathcal{A}|} |B^N(\delta N)|$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

As  $\lambda \longrightarrow 0$ , this quantity  $\longrightarrow 1 - H(\rho)$ .





















On Bounds for Network Codes		
	Wakey, wakey	

On Bounds for Network Codes				
Eimear Byrne				
	Thanks!			
		<ul> <li>(四)</li> <li>(1)</li> <li>(1)</li></ul>	▶ Ē	৩৫৫

### References

On Bounds for Network Codes

Eimear Byrne

- M. Greferath and M. E. O'Sullivan, "On Bounds for Codes Over Frobenius Rings Under Homogeneous Weights", Discrete Mathematics, 289, pp. 11–24, 2004.
- R. Koetter, M. Medard, "An Algebraic Approach to Network Coding", *IEEE/ACM Transactions on Networking*, Vol. 11, Issue 5, Oct. 2003, pp. 782–795.
- S. Yang, C. K. Ngai, R. Yeung, "Refined Coding Bounds and Code Constructions for Coherent Network Error Correction", *IEEE Trans. Inform. Theory*, 57, (3) 2011. pp. 1576–1580.
- Z. Zhang, "Linear Network Error Correction Codes in Packet Networks", *IEEE Transactions on Information Theory*, Vol. 54, Issue 1, Jan. 2008, pp:209–218.