Upper Bounds for Network Error Correcting Codes

Eimear Byrne

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

Banff, August 6 2009

Outline

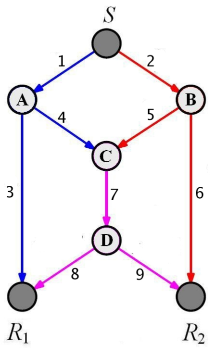
- Error Correction in Networks
- Some Known Upper Bounds
- The Classical Plotkin and Elias Bounds
- A Plotkin Bound
- An Elias Bound
- Asymptotic Bounds

Preliminaries

- The network is a directed acyclic graph $\mathcal{N}$ with unit edge capacities, a single source node s and several sinks $t \in \mathcal{T}$
- The **transfer matrix** is $F = (I - K)^{-1} \in GF(q)^{n \times n}$, where K and has zero coefficients whenever the adjacency matrix of the line graph of $\mathcal{N}$ does [Koetter, Medard 03].
- If $\mathbf{x}$ is transmitted from the source node s and edges of the network are corrupted by an error vector $\mathbf{e}$ then the network transmission is

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

Example - The Butterfly Network



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

The transfer matrix for the Butterfly Network is given by

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

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

The Transfer Matrix for each Receiver

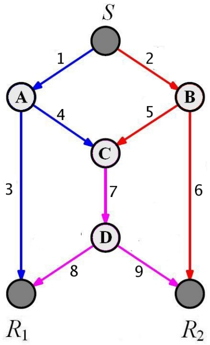
- F_t is the $n \times n_t$ submatrix of F whose columns correspond to the n_t edges connected to t.
- Node t receives
$$\mathbf{y} = (\mathbf{x} + \mathbf{e})F_t.$$
- The code $\mathcal{C}_t$ is a subset of $\{\mathbf{z}F_t : \mathbf{z} \in GF(q)^n\}$.
- Messages $\mathbf{z}, \mathbf{z}' \in GF(q)^n$ are identified if
$$\mathbf{z} - \mathbf{z}' \in \ker F_t =: K_t.$$

The Transfer Matrix for each Receiver

The transfer matrix for the Butterfly Network is given by

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

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

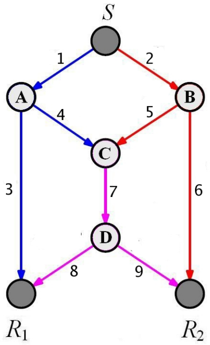


The Transfer Matrix for each Receiver

The transfer matrix for the Butterfly Network is given by

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

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



The Transfer Matrix for each Receiver

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

$$\mathbf{x}F_1 = \mathbf{x} \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} = [x_1, x_1 + x_2], \mathbf{x}F_2 = \mathbf{x} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} = [x_2, x_1 + x_2].$$

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

Relevant Errors

- Observe that if $\mathbf{x}$ is sent and the error $\mathbf{e} \in K_t$ occurs then $(\mathbf{x} + \mathbf{e})F_t = \mathbf{x}F_t$ is received, as if without error.
- Thus the decoder is only interested in errors $\mathbf{e}$ satisfying $\mathbf{e}F_t \neq \mathbf{0}$.

A Distance Function

- K_t induces a distance function on $GF(q)^{n_t}$ by

$$\mathrm{d}_t(\mathbf{u},\mathbf{v}) := \min\{\mathrm{d}(\mathbf{x},\mathbf{y}) : \mathbf{x}F_t = \mathbf{u}, \mathbf{y}F_t = \mathbf{v}\},$$

  where d is a distance function on $GF(q)^n$.
- Then $\mathrm{d}_t(\mathbf{u},\mathbf{v}) = 0$ if and only if $\mathbf{x}-\mathbf{y} \in K_t$ for some $\mathbf{x},\mathbf{y} \in GF(q)^n$ satisfying $\mathbf{x}F_t = \mathbf{u}, \mathbf{y}F_t = \mathbf{v}$.
- For the Hamming distance, $\mathrm{w}_t(\mathbf{u}) = \mathrm{d}_t(\mathbf{u},\mathbf{0})$ counts the minimum number of linearly independent rows of F_t required to obtain a representation of $\mathbf{u} = \mathbf{x}F_t$.

Weights Induced by K_1 for the Butterfly Network

Recall that for the Butterfly Network we have

$$F_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}^t.$$

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

$\mathbf{c}$	00	01	10	11
$\mathbf{c}F_1^{-1}$	K_1	$010\ldots0 + K_1$	$0010\ldots0 + K_1$	$10\ldots0 + K_1$
$\mathrm{w}(\mathbf{c})$	0	1	1	1

Error Correction

- Given the received word $\mathbf{y}_t$, the decoder at node t decides that $\mathbf{c} = \mathbf{x}F_t$ has been transmitted if

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

  for all $\mathbf{c}' \in \mathcal{C}_t$.

- The decoder at node t can correct e errors if

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

- That is, if $\mathrm{d}_t(\mathcal{C}_t) \geq 2e + 1$ then $\mathcal{C}_t$ can correct any error pattern $\mathbf{e}$ satisfying $\mathrm{w}_t(\mathbf{e}F_t) \leq e$.

Parameters of a Network Code

Definition

Let $\mathcal{N}$ be a network with a single source node s and set of sink nodes $\mathcal{T}$. Let F be a transfer matrix for $\mathcal{N}$.
A network code C is a collection

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

where $\mathcal{C}_t \subset \{\mathbf{x}F_t : \mathbf{x} \in GF(q)^n\} = GF(q)^{n_t}$ is an $(n_t, |\mathcal{C}_t|, d_t)$ code.

- $K_t := \ker F_t = \{\mathbf{x} \in GF(q)^n : \mathbf{x}F_t = \mathbf{o}\}$, $\ell_t := |\mathrm{supp}\, K_t|$.
- We say that C is an $(n, \{(n_t, \ell_t, |\mathcal{C}_t|, d_t) : t \in \mathcal{T}\})$ network code.

The Size of a Network Code

We call $c := \min\{|\mathcal{C}_t| : t \in \mathcal{T}\}$ the size of $\mathcal{C}$.

The number c denotes the minimum number of distinct messages that can be transmitted by s to any node t using the transfer matrix F.

Definition

We denote by

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

the maximum size of any $(n, \{(n_t, \ell_t, |\mathcal{C}_t|, d_t) : t \in \mathcal{T}\})$ network code.

Some Known Upper Bounds

Theorem (Yang, Yeung, NGai, 2007)

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

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

The Classical Plotkin and Elias Bounds

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.

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

The Classical Plotkin and Elias Bounds

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.

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

1	1	1	1	1	1	1
1	1	1	1	0	0	0
1	1	0	0	1	1	0
1	0	1	0	1	0	1
0	0	0	0	1	1	1
0	0	1	1	0	0	1
0	1	0	1	0	1	0
1	1	1	0	0	0	1
1	0	1	1	0	1	1
1	1	0	1	1	1	0
1	1	0	1	1	0	1
1	0	1	0	1	0	0
1	1	1	1	1	0	0
1	1	1	0	1	1	1
0	1	1	0	1	1	1

$$= \sum_{i=1}^{n} m_{\alpha}^{i}(|C| - m_{\alpha}^{i})$$

$$\leq \begin{cases} |C|^2 n\gamma & \text{Plotkin} \\ |C|^2(2r - \frac{r^2}{\gamma n}) & \text{Elias} \end{cases}$$

$$\gamma = \frac{q-1}{q},$$

$$r^2 - 2\gamma n r + \gamma n d > 0.$$

Pulling Back the Network Code

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

This is not true of our distance function!

For example, the Butterfly Network matrix F_1 gave

$\mathbf{c}$	00	01	10	11
$\mathrm{w}(\mathbf{c})$	0	1	1	1

.

Pulling Back the Network Code

$M_t := F_t^{-1}(\mathcal{C}_t)$							$\mathcal{C}_t$	weight
—	—	—	—	—	—	—	—	—
1	0	0	0	1	1	0	001	3
0	1	0	0	1	1	0		
1	0	1	1	1	1	0		
0	1	1	1	1	1	0		
—	—	—	—	—	—	—	—	—
0	1	1	0	0	0	0	010	2
1	0	1	0	0	0	0		
0	1	0	1	0	0	0		
1	0	0	1	0	0	0		
—	—	—	—	—	—	—	—	—
1	1	1	1	1	1	1	111	3
0	0	1	1	1	1	1		
1	1	0	0	1	1	1		
0	0	0	0	1	1	1		

The Trick

$$|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t \leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t,\mathbf{y}F_t)$$

The Trick

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t, \mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}', \mathbf{y}') : \mathbf{x}' - \mathbf{x}, \mathbf{y}' - \mathbf{y} \in K_t\}
\end{aligned}
$$

The Trick

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t,\mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x},\mathbf{y}'-\mathbf{y}\in K_t\} \\
&\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \mathrm{av}\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x},\mathbf{y}'-\mathbf{y}\in K_t\}
\end{aligned}
$$

The Trick

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t, \mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}', \mathbf{y}') : \mathbf{x}' - \mathbf{x}, \mathbf{y}' - \mathbf{y} \in K_t\} \\
&\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{av}\{\mathrm{d}_H(\mathbf{x}', \mathbf{y}') : \mathbf{x}' - \mathbf{x}, \mathbf{y}' - \mathbf{y} \in K_t\}
\end{aligned}
$$

Instead of computing the sum of the distances between the distinct cosets of K_t in M_t, we compute the sum of the average distances between elements of distinct cosets.

A Key Lemma

Lemma

Let $V < GF(q)^m$ *and let* $\mathbf{x} \in GF(q)^m$ *then*

$$\frac{1}{|V|} \sum_{\mathbf{v} \in V} \mathrm{w}(\mathbf{v} + \mathbf{x}) = \gamma |\mathrm{supp}\ V| + \mathrm{w}(\pi_V(\mathbf{x})),$$

where $\pi_V(\mathbf{x})$ *is obtained by puncturing* $\mathbf{x}$ *on* $\mathrm{supp}\ V$.

A Key Lemma

Lemma

Let $V < GF(q)^m$ *and let* $\mathbf{x} \in GF(q)^m$ *then*

$$\frac{1}{|V|}\sum_{\mathbf{v}\in V} \mathrm{w}(\mathbf{v}+\mathbf{x}) = \gamma|\mathrm{supp}\ V| + \mathrm{w}(\pi_V(\mathbf{x})),$$

where $\pi_V(\mathbf{x})$ *is obtained by puncturing* $\mathbf{x}$ *on* $\mathrm{supp}\ V$.

$$\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{array}$$

$$\gamma|\mathrm{supp}\ V| = \tfrac{1}{2} \times 4 \quad + \quad \mathrm{w}(110) = 2$$

A Plotkin Bound

Theorem

Let $\gamma = \frac{q-1}{q}$ *and let* $d > \gamma n$. *Then*

$$A_q(n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}) \leq \min \left\{ \frac{d_t - \gamma \ell_t}{d_t - \gamma n} : t \in \mathcal{T} \right\}.$$

Proof Sketch:

$$|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t \leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t, \mathbf{y}F_t)$$

Proof Sketch:

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t,\mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x}, \mathbf{y}'-\mathbf{y} \in K_t\}
\end{aligned}
$$

Proof Sketch:

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t,\mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x}, \mathbf{y}'-\mathbf{y} \in K_t\} \\
&\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t\in\mathcal{C}_t} \mathrm{av}\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x}, \mathbf{y}'-\mathbf{y} \in K_t\}
\end{aligned}
$$

Proof Sketch:

$$
\begin{aligned}
|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t &\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{d}_t(\mathbf{x}F_t,\mathbf{y}F_t) \\
&= \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \min\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x},\mathbf{y}'-\mathbf{y} \in K_t\} \\
&\leq \sum_{\mathbf{x}F_t,\mathbf{y}F_t \in \mathcal{C}_t} \mathrm{av}\{\mathrm{d}_H(\mathbf{x}',\mathbf{y}') : \mathbf{x}'-\mathbf{x},\mathbf{y}'-\mathbf{y} \in K_t\} \\
&= \cdots \\
&= \frac{1}{|K_t|^2}\left(\sum_{\mathbf{x},\mathbf{y}\in M_t} \mathrm{d}_H(\mathbf{x},\mathbf{y}) - |\mathcal{C}_t||K_t| \sum_{\mathbf{z}\in K_t} \mathrm{w}_H(\mathbf{z})\right)
\end{aligned}
$$

Proof Sketch:

$$= \frac{1}{|K_t|^2}\left(\underbrace{\sum_{\mathbf{x},\mathbf{y}\in M_t} \mathrm{d}_H(\mathbf{x},\mathbf{y})} - \underbrace{|\mathcal{C}_t||K_t|\sum_{\mathbf{z}\in K_t} \mathrm{w}_H(\mathbf{z})}\right)$$

Proof Sketch:

$$= \frac{1}{|K_t|^2}\left(\underbrace{\sum_{\mathbf{x},\mathbf{y}\in M_t} \mathrm{d}_H(\mathbf{x},\mathbf{y})}_{\text{Plotkin}} - \underbrace{|\mathcal{C}_t||K_t|\sum_{\mathbf{z}\in K_t} \mathrm{w}_H(\mathbf{z})}_{\text{Key Lemma}}\right)$$

$$=$$

Proof Sketch:

$$
\begin{aligned}
&= \frac{1}{|K_t|^2}\Bigg(\underbrace{\sum_{\mathbf{x},\mathbf{y}\in M_t} \mathrm{d}_H(\mathbf{x},\mathbf{y})}_{\text{Plotkin}} - \underbrace{|\mathcal{C}_t||K_t|\sum_{\mathbf{z}\in K_t} \mathrm{w}_H(\mathbf{z})}_{\text{Key Lemma}}\Bigg) \\
&= \\
&\leq \frac{1}{|K_t|^2}\left(|M_t|^2|\mathrm{supp}\ M_t|\gamma - |\mathcal{C}_t||K_t|^2|\mathrm{supp}\ K_t|\gamma\right)
\end{aligned}
$$

Proof Sketch:

$$
\begin{aligned}
&= \frac{1}{|K_t|^2}\Bigg(\underbrace{\sum_{\mathbf{x},\mathbf{y}\in M_t} \mathrm{d}_H(\mathbf{x},\mathbf{y})}_{\text{Plotkin}} - \underbrace{|\mathcal{C}_t||K_t| \sum_{\mathbf{z}\in K_t} \mathrm{w}_H(\mathbf{z})}_{\text{Key Lemma}}\Bigg) \\
&= \\
&\leq \frac{1}{|K_t|^2}\left(|M_t|^2|\mathrm{supp}\ M_t|\gamma - |\mathcal{C}_t||K_t|^2|\mathrm{supp}\ K_t|\gamma\right)
\end{aligned}
$$

So

$$|\mathcal{C}_t|(|\mathcal{C}_t|-1)d_t \leq |\mathcal{C}_t|^2|\mathrm{supp}\ M_t|\gamma - |\mathcal{C}_t||\mathrm{supp}\ K_t|\gamma.$$

Rearrange to get

$$|\mathcal{C}_t| \leq \frac{d_t - \gamma\ell_t}{d_t - \gamma n}.$$

An Elias Bound

Theorem

Let $d_t \leq \gamma n$. *Let* r *be a positive real number satisfying* $\gamma \ell_t \leq r \leq \gamma n - \sqrt{\gamma(\gamma n - d_t)(n - \ell_t)}$ *for each* $t \in \mathcal{T}$. *Then*

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

$$\min \left\{ \frac{(d_t - \gamma \ell_t)\gamma(n - \ell_t) q^{n-\ell_t}}{[(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma \ell_t)] |B^{n-\ell_t}(r - \gamma \ell_t)|} : t \in \mathcal{T} \right\},$$

where $B^{n-\ell_t}(r - \gamma \ell_t)$ *is the sphere of radius* $r - \gamma \ell_t$ *about* $\mathbf{0} \in GF(q)^{n-\ell_t}$.

A Well-Known Result

Lemma

Let $A, C \subset GF(q)^N$. *Then there exists* $\mathbf{x} \in GF(q)^N$ *such that*

$$|C| \leq \frac{|(\mathbf{x} + A) \cap C| q^N}{|A|}.$$

A Well-Known Result

Lemma

Let $A, C \subset GF(q)^N$. *Then there exists* $\mathbf{x} \in GF(q)^N$ *such that*

$$|C| \leq \frac{|(\mathbf{x} + A) \cap C| q^N}{|A|}.$$

Corollary

Set $A = B^{\mathrm{av}}(r), C = \mathcal{C}_t \subset GF(q)^{n_t}$. *Then*

$$|\mathcal{C}_t| \leq \frac{|B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t| q^{n_t}}{|B_t^{\mathrm{av}}(r)|}.$$

An Upper Bound

Corollary

Set $N = n_t, A = B^{\mathrm{av}}(r), C = \mathcal{C}_t \subset GF(q)^{n_t}$. *Then*

$$|\mathcal{C}_t| \leq \frac{|B^{\mathrm{av}}_t(r) \cap \mathcal{C}_t| q^{n_t}}{|B^{\mathrm{av}}_t(r)|}.$$

An Upper Bound

Corollary

Set $N = n_t, A = B^{\mathrm{av}}(r), C = \mathcal{C}_t \subset GF(q)^{n_t}$. *Then*

$$|\mathcal{C}_t| \leq \frac{|B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t| q^{n_t}}{|B_t^{\mathrm{av}}(r)|}.$$

- $B_t^{\mathrm{av}}(r) := \{\mathbf{z} \in GF(q)^{n_t} : \mathrm{av}\{\mathrm{w}_H(\mathbf{x}) : \mathbf{x}F_t = \mathbf{z}\} \leq r\}$.

An Upper Bound

Corollary

Set $N = n_t, A = B^{\mathrm{av}}(r), C = \mathcal{C}_t \subset GF(q)^{n_t}$. *Then*

$$|\mathcal{C}_t| \leq \frac{|B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t| q^{n_t}}{|B_t^{\mathrm{av}}(r)|}.$$

- $B_t^{\mathrm{av}}(r) := \{\mathbf{z} \in GF(q)^{n_t} : \mathrm{av}\{\mathrm{w}_H(\mathbf{x}) : \mathbf{x}F_t = \mathbf{z}\} \leq r\}$.
- $B_t^{\mathrm{av}}(r) = \{\mathbf{x}F_t \in GF(q)^{n_t} : \mathrm{w}_H(\pi_t(\mathbf{x})) \leq r - \ell_t\gamma\}$.

An Upper Bound

Corollary

Set $N = n_t, A = B^{\mathrm{av}}(r), C = \mathcal{C}_t \subset GF(q)^{n_t}$. *Then*

$$|\mathcal{C}_t| \leq \frac{|B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t| q^{n_t}}{|B_t^{\mathrm{av}}(r)|}.$$

- $B_t^{\mathrm{av}}(r) := \{\mathbf{z} \in GF(q)^{n_t} : \mathrm{av}\{\mathrm{w}_H(\mathbf{x}) : \mathbf{x}F_t = \mathbf{z}\} \leq r\}$.
- $B_t^{\mathrm{av}}(r) = \{\mathbf{x}F_t \in GF(q)^{n_t} : \mathrm{w}_H(\pi_t(\mathbf{x})) \leq r - \ell_t\gamma\}$.
- $|B_t^{\mathrm{av}}(r)| = |B^{n-\ell_t}(r - \gamma\ell_t)| q^{\ell_t - n + n_t}$.

$|B_t^{\text{av}}(r)| = |B^{n-\ell_t}(r - \gamma\ell_t)|q^{\ell_t - n + n_t}.$

$GF(q)^n := F_t^{-1}(GF(q)^{n_t})$							$GF(q)^{n_t}$	av. weight
—	—	—	—	—	—	—	—	—
0	0	0	0	|1	1	0	000	$4 = 2 + 2$
1	1	0	0	|1	1	0		
0	0	1	1	|1	1	0		
1	1	1	1	|1	1	0		
—	—	—	—	—	—	—	—	—
1	0	0	0	|1	1	0	001	$4 = 2 + 2$
0	1	0	0	|1	1	0		
1	0	1	1	|1	1	0		
0	1	1	1	|1	1	0		
—	—	—	—	—	—	—	—	—
0	0	1	0	|1	1	0	111	$4 = 2 + 2$
1	1	1	0	|1	1	0		
0	0	0	1	|1	1	0		
1	1	0	1	|1	1	0		
—	—	—	—	—	—	—	—	—
0	1	1	0	|1	1	0	111	$4 = 2 + 2$
1	0	1	0	|1	1	0		
0	1	0	1	|1	1	0		
1	0	0	1	|1	1	0		
—	—	—	—	—	—	—	—	—

An Upper Bound on $|B_t|$

Next we find an upper bound on $|B_t| := |B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t|$.

$$|B_t|(|B_t|-1)d_t \leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}_t(\mathbf{x}F_t - \mathbf{y}F_t)$$

An Upper Bound on $|B_t|$

Next we find an upper bound on $|B_t| := |B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t|$.

$$\begin{aligned} |B_t|(|B_t|-1)d_t &\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}_t(\mathbf{x}F_t - \mathbf{y}F_t) \\ &\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \underbrace{\mathrm{av}\{\mathrm{w}(\mathbf{z}) : \mathbf{z} \in (\mathbf{x}-\mathbf{y}) + K_t\}} \end{aligned}$$

An Upper Bound on $|B_t|$

Next we find an upper bound on $|B_t| := |B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t|$.

$$
\begin{aligned}
|B_t|(|B_t| - 1)d_t &\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}_t(\mathbf{x}F_t - \mathbf{y}F_t) \\
&\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \underbrace{\mathrm{av}\{\mathrm{w}(\mathbf{z}) : \mathbf{z} \in (\mathbf{x} - \mathbf{y}) + K_t\}}_{\text{Key Lemma}}
\end{aligned}
$$

An Upper Bound on $|B_t|$

Next we find an upper bound on $|B_t| := |B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t|$.

$$
\begin{aligned}
|B_t|(|B_t|-1)d_t &\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}_t(\mathbf{x}F_t - \mathbf{y}F_t) \\
&\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \underbrace{\mathrm{av}\{\mathrm{w}(\mathbf{z}) : \mathbf{z} \in (\mathbf{x}-\mathbf{y}) + K_t\}}_{\text{Key Lemma}} \\
&= \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} (\gamma |\mathrm{supp}\ K_t| + \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y})))
\end{aligned}
$$

An Upper Bound on $|B_t|$

Next we find an upper bound on $|B_t| := |B_t^{\mathrm{av}}(r) \cap \mathcal{C}_t|$.

$$\begin{aligned}
|B_t|(|B_t|-1)d_t &\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}_t(\mathbf{x}F_t - \mathbf{y}F_t) \\
&\leq \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \underbrace{\mathrm{av}\{\mathrm{w}(\mathbf{z}) : \mathbf{z} \in (\mathbf{x}-\mathbf{y}) + K_t\}}_{\text{Key Lemma}} \\
&= \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} (\gamma|\mathrm{supp}\ K_t| + \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y}))) \\
&= |B_t|(|B_t|-1)\ell_t\gamma + \sum_{\mathbf{x}F_t, \mathbf{y}F_t \in B_t} \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y})),
\end{aligned}$$

An Upper Bound on $|B_t|$

$$\leq \quad |B_t|(|B_t|-1)\ell_t\gamma + \underbrace{\sum_{\mathbf{x}F_t,\mathbf{y}F_t \in B_t} \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y}))}, $$

An Upper Bound on $|B_t|$

$$\leq \quad |B_t|(|B_t|-1)\ell_t\gamma + \underbrace{\sum_{\mathbf{x}F_t,\mathbf{y}F_t\in B_t} \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y}))}_{\text{Elias}},$$

An Upper Bound on $|B_t|$

$$\leq \quad |B_t|(|B_t|-1)\ell_t\gamma + \underbrace{\sum_{\mathbf{x}F_t,\mathbf{y}F_t \in B_t} \mathrm{w}(\pi_t(\mathbf{x}-\mathbf{y}))}_{\text{Elias}},$$

$$\leq \quad |B_t|(|B_t|-1)\ell_t\gamma + 2|B_t|^2(r-\ell_t\gamma) - \frac{|B_t|^2(r-\ell_t\gamma)}{\gamma(n-\ell_t)},$$

for $\gamma\ell_t \leq d \leq r \leq \gamma n$ and $(r-\gamma n)^2 - \gamma(\gamma n - d_t) > 0$.

As before, rearrange the inequality to obtain the required upper bound on $|B_t|$.

An Upper Bound on $|B_t|$

Theorem

Let $\gamma\ell_t \leq d \leq r \leq \gamma n$ *and let* $r^2 - 2\gamma nr + \gamma^2\ell_t n + \gamma d_t(n - \ell_t) \geq 0$. *Then*

$$|B_t| \leq \frac{\gamma(d_t - \gamma\ell_t)(n - \ell_t)}{(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma\ell_t)}.$$

An Elias-Like Bound

Theorem

Let $d_t \leq \gamma n$. Let r be a positive real number satisfying $\gamma \ell_t \leq r \leq \gamma n - \sqrt{\gamma(\gamma n - d_t)(n - \ell_t)}$ for each $t \in \mathcal{T}$. Then

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

$$\min \left\{ \frac{(d_t - \gamma \ell_t)\gamma(n - \ell_t)q^{n-\ell_t}}{[(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma \ell_t)]|B^{n-\ell_t}(r - \gamma \ell_t)|} : t \in \mathcal{T} \right\}.$$

where $B^{n-\ell_t}(r - \gamma \ell_t)$ is the sphere of radius $r - \gamma \ell_t$ about $\mathbf{0} \in GF(q)^{n-\ell_t}$.

Asymptotic Bounds

Definition

$$\alpha_q(\{(\nu_t, \lambda_t, \delta_t) : t \in \mathcal{T}\}) :=$$
$$\lim_{n\to\infty} \sup \frac{1}{n} \log_q \left(A_q(n, \{(\nu_t n, \lambda_t n, \delta_t n) : t \in \mathcal{T}\})\right).$$

We seek an upper bound on this quantity.

Asymptotic Bounds

- (Plotkin) Let $\delta_t > \gamma$ for each t. Then
$$\alpha_q(\{\nu_t, \delta_t, \lambda_t : t \in \mathcal{T}\}) = 0.$$
- (Singleton) Let $0 < \delta_t < 1$ for each t. Then
$$\alpha_q(\{\nu_t, \delta_t, \lambda_t : t \in \mathcal{T}\}) \leq \nu - \delta.$$

Asymptotic Bounds

Let $r > 0$. Given $n, \{(n_t, \ell_t, d_t) : t \in \mathcal{T}\}$ satisfying

- $d_t \leq \gamma n$,
- $\gamma \ell_t \leq r \leq \gamma n - \sqrt{\gamma(\gamma n - d_t)(n - \ell_t)}$

for each t, let $(v, \ell, d) =$

$$\mathrm{argmin} \left\{ \frac{(d_t - \gamma \ell_t)\gamma(n - \ell_t) q^{n-\ell_t}}{[(r - \gamma n)^2 - \gamma(\gamma n - d_t)(n - \gamma \ell_t)]|B^{n-\ell_t}(r - \gamma \ell_t)|} \right\}_{t \in \mathcal{T}}.$$

Asymptotic Bounds

Theorem

Let $\nu_t, \lambda_t, \delta_t \in (0,1)$ *such that* $\delta_t \leq \gamma$ *and*

$$\gamma\lambda_t \leq \rho \leq \gamma - \sqrt{\gamma(\gamma - \delta_t)(1-\lambda_t)}$$

for each t. *Let* $\xi = \dfrac{\rho - \gamma\lambda}{1-\lambda}$. *Let* $r = \rho n$, $d = \delta n$, $\ell = \lambda n$. *Then*

$$\alpha_q(\{\nu_t, \delta_t, \lambda_t : t \in \mathcal{T}\}) \quad \leq \quad (1-\lambda)(1 - H_q(\xi)).$$

Remark: As $\lambda \longrightarrow 0$, this quantity $\longrightarrow 1 - H_q(\rho)$.

Asymptotic Bounds

Corollary (Asymptotic Elias Bound)

$$\alpha_q(\{\nu_t, \delta_t, \lambda_t : t \in \mathcal{T}\}) \leq (1-\lambda)\left[1 - H_q\left(\gamma - \sqrt{\frac{\gamma(\gamma-\delta)}{1-\lambda}}\right)\right].$$

Concluding Remarks

- These results extend completely to the case where we replace $GF(q)$ by a finite Frobenius ring and the Hamming weight with the homogeneous weight.
  For example, for codes over $\mathbf{Z}_4$ for the Lee weight.
- In both bounds, the support size ℓ_t of the kernel K_t plays a role, whereas n_t does not, (unless we replace ℓ_t by $n - n_t \leq \ell_t$).

References

- 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, "Construction of Linear Network Codes that Achieve a Refined Singleton Bound", *IEEE International Symposium on Information Theory*, June 2007. pp. 1576–1580.
- S. Yang, R. Yeung, "Refined Coding Bounds for Network Error Correction", *IEEE Information Theory Workshop on Information Theory for Wireless Networks*, July 2007 pp. 1–5.
- Z. Zhang, "Linear Network Error Correction Codes in Packet Networks", *IEEE Transactions on Information Theory*, Vol. 54, Issue 1, Jan. 2008, pp:209–218.