Blockcodes with Errors-and-Erasures Decoding and Feedback

Barış Nakiboğlu Lizhong Zheng

Laboratory for Information and Decision Systems
Massachusetts Institute of Technology, Cambridge

June 3, 2008

Outline

Motivating Ideas and Questions

- It is helpful to know it when a decoding error is made.
- In all most all of the cases to decrease the undetected error probability, overall error probability has to increase.
- What is the (exponential) trade off?

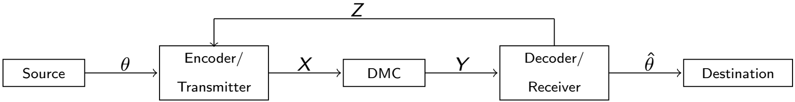
Motivating Ideas and Questions

- It is helpful to know it when a decoding error is made.
- In all most all of the cases to decrease the undetected error probability, overall error probability has to increase.
- What is the (exponential) trade off?
- Forney'68, [1] has investigated the problem for case, for the case without feedback.

Motivating Ideas and Questions

- It is helpful to know it when a decoding error is made.
- In all most all of the cases to decrease the undetected error probability, overall error probability has to increase.
- What is the (exponential) trade off?
- Forney'68, [1] has investigated the problem for case, for the case without feedback.
- Does feedback help in terms of asymptotic performance? How much does it help?

Problem Statement



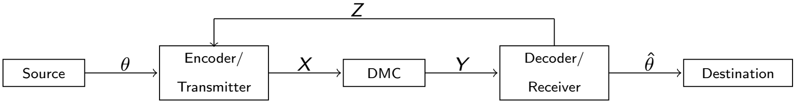
- A Message θ from message set $\mathcal{M} = \{1, 2, \ldots |\mathcal{M}|\}$ is given
- Encoder for a fixed length block code with feedback, for all $k \leq n$

$$X_k(\theta, Z^{k-1}) : \quad \mathcal{M} \times \mathcal{Z}^{k-1} \to \mathcal{X}$$

- Errors and erasures decoder for a fixed length block code

$$\hat{\theta}(Y^n) : \quad \mathcal{Y}^n \to \{\mathbf{x}, 1, 2, \ldots |\mathcal{M}|\}$$

Problem Statement



- A Message θ from message set $\mathcal{M} = \{1, 2, \dots |\mathcal{M}|\}$ is given
- Encoder for a fixed length block code with feedback, for all $k \leq n$

$$X_k(\theta, Z^{k-1}) : \quad \mathcal{M} \times \mathcal{Z}^{k-1} \rightarrow \mathcal{X}$$

- Errors and erasures decoder for a fixed length block code

$$\hat{\theta}(Y^n) : \quad \mathcal{Y}^n \rightarrow \{\mathbf{x}, 1, 2, \dots |\mathcal{M}|\}$$

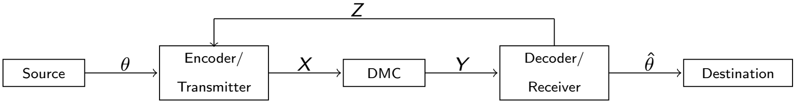
- Error and Erasure Probabilities

$$P_e = \left(\mathbf{P}\left[\hat{\theta} \neq \theta\right] - \mathbf{P}\left[\hat{\theta} = \mathbf{x}\right]\right) \qquad P_x = \mathbf{P}\left[\hat{\theta} = \mathbf{x}\right]$$

- Rate, Erasure Exponent and Error Exponent are given by

$$R = \frac{\ln |\mathcal{M}|}{n} \qquad E_x = -\frac{\ln P_x}{n} \qquad E_e = -\frac{\ln P_e}{n}$$

Problem Statement



- A Message θ from message set $\mathcal{M} = \{1, 2, \ldots |\mathcal{M}|\}$ is given
- Encoder for a fixed length block code with feedback, for all $k \leq n$

$$X_k(\theta, Z^{k-1}): \quad \mathcal{M} \times \mathcal{Z}^{k-1} \rightarrow \mathcal{X}$$

- Errors and erasures decoder for a fixed length block code

$$\hat{\theta}(Y^n): \quad \mathcal{Y}^n \rightarrow \{\mathbf{x}, 1, 2, \ldots |\mathcal{M}|\}$$

- Error and Erasure Probabilities

$$P_{\mathrm{e}} = \left(\mathbf{P}\left[\hat{\theta} \neq \theta\right] - \mathbf{P}\left[\hat{\theta} = \mathbf{x}\right]\right) \qquad P_{\mathrm{x}} = \mathbf{P}\left[\hat{\theta} = \mathbf{x}\right]$$

- Rate, Erasure Exponent and Error Exponent are given by

$$R = \frac{\ln |\mathcal{M}|}{n} \qquad E_{\mathrm{x}} = -\frac{\ln P_{\mathrm{x}}}{n} \qquad E_{\mathrm{e}} = -\frac{\ln P_{\mathrm{e}}}{n}$$

- $\mathcal{E}_{\mathrm{e}}(R, E_{\mathrm{x}}) = ?$

Related Work / Behaviour On The Extremes

- Error exponents of blockcodes with feedback (without erasures): $\mathcal{E}_{\mathbf{e}}(R)$

$$\mathcal{E}_{\mathbf{e}}(R,\infty) = \mathcal{E}_{\mathbf{e}}(R)$$
$$\mathcal{E}_{\mathbf{e}}(R,E_{\mathbf{x}}) = \mathcal{E}_{\mathbf{e}}(R) \qquad \forall E_{\mathbf{x}} \geq \mathcal{E}_{\mathbf{e}}(R)$$

Related Work / Behaviour On The Extremes

- Error exponents of blockcodes with feedback (without erasures): $\mathcal{E}_{\mathbf{e}}(R)$

$$\mathcal{E}_{\mathbf{e}}(R, \infty) = \mathcal{E}_{\mathbf{e}}(R)$$
$$\mathcal{E}_{\mathbf{e}}(R, E_{\mathbf{x}}) = \mathcal{E}_{\mathbf{e}}(R) \qquad \forall E_{\mathbf{x}} \geq \mathcal{E}_{\mathbf{e}}(R)$$

i.e. we are only interested in $E_{\mathbf{x}} \leq \mathcal{E}_{\mathbf{e}}(R)$.

Related Work / Behaviour On The Extremes

- Error exponents of blockcodes with feedback (without erasures): $\mathcal{E}_{\mathbf{e}}(R)$

$$\mathcal{E}_{\mathbf{e}}(R,\infty) = \mathcal{E}_{\mathbf{e}}(R)$$
$$\mathcal{E}_{\mathbf{e}}(R,E_{\mathbf{x}}) = \mathcal{E}_{\mathbf{e}}(R) \qquad \forall E_{\mathbf{x}} \geq \mathcal{E}_{\mathbf{e}}(R)$$

  i.e. we are only interested in $E_{\mathbf{x}} \leq \mathcal{E}_{\mathbf{e}}(R)$.

- Error exponent of variable length blockcodes with feedback: $\mathcal{E}_{\mathbf{e}V}(R)$

$$\mathcal{E}_{\mathbf{e}}(R,0) = \mathcal{E}_{\mathbf{e}V}(R) = \left(1 - \frac{R}{C}\right) D$$

Related Work / Behaviour On The Extremes

- Error exponents of blockcodes with feedback (without erasures): $\mathcal{E}_{\mathbf{e}}(R)$

$$\mathcal{E}_{\mathbf{e}}(R,\infty) = \mathcal{E}_{\mathbf{e}}(R)$$
$$\mathcal{E}_{\mathbf{e}}(R,E_{\mathbf{x}}) = \mathcal{E}_{\mathbf{e}}(R) \qquad \forall E_{\mathbf{x}} \geq \mathcal{E}_{\mathbf{e}}(R)$$

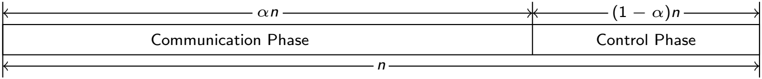
  i.e. we are only interested in $E_{\mathbf{x}} \leq \mathcal{E}_{\mathbf{e}}(R)$.

- Error exponent of variable length blockcodes with feedback: $\mathcal{E}_{\mathbf{e}V}(R)$

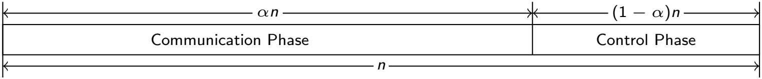
$$\mathcal{E}_{\mathbf{e}}(R,0) = \mathcal{E}_{\mathbf{e}V}(R) = \left(1 - \frac{R}{C}\right) D$$

- What is $\mathcal{E}_{\mathbf{e}}(R,E_{\mathbf{x}})$ for $0 < E_{\mathbf{x}} < \mathcal{E}_{\mathbf{e}}(R)$

A Parametrized Class of Error-Erasure Codes

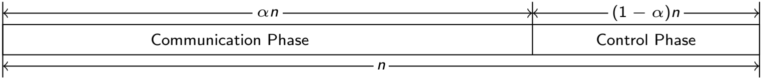


A Parametrized Class of Error-Erasure Codes



- Transmitter uses a fixed composition code of type P, rate $R' = \frac{R}{\alpha}$ length $n_1 = \alpha n$.
- Receiver makes a maximum mutual information decoding, $\tilde{\theta}$
- Transmitter accepts by sending $x_{\mathcal{A}}$ if $\tilde{\theta} = \theta$ or reject by sending $x_{\mathcal{R}}$ else.

A Parametrized Class of Error-Erasure Codes



- Transmitter uses a fixed composition code of type P, rate $R' = \frac{R}{\alpha}$ length $n_1 = \alpha n$.
- Receiver makes a maximum mutual information decoding, $\tilde{\theta}$
- Transmitter accepts by sending $x_{\mathcal{A}}$ if $\tilde{\theta} = \theta$ or reject by sending $x_{\mathcal{R}}$ else.
- Receiver uses a partial order, $\succ$, between (i, y^n) pairs to decide.

$$\hat{\theta} = \left\{ \begin{array}{ll} \tilde{\theta} & \text{iff}(\tilde{\theta}, y^n) \succ (i, y^n) \quad \forall i \neq \tilde{\theta} \\ \mathbf{x} & \text{else} \end{array} \right\} \tag{1}$$

Error and Erasure Probabilities

- An error or an erasure will happen if θ can not dominate all other messages?

$$P_{\mathbf{e}}(i) + P_{\mathbf{x}}(i) = \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (i, y^n) \not\succ (j, y^n)\} \middle| \theta = i\right]$$

Error and Erasure Probabilities

- An error or an erasure will happen if θ can not dominate all other messages?

$$P_{\mathrm{e}}(i) + P_{\mathrm{x}}(i) = \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (i, y^n) \nsucc (j, y^n)\} | \theta = i\right]$$

- An error will occur if a message other than θ dominates all message.

$$P_{\mathrm{e}}(i) = \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (k, y^n) \quad \forall k \neq j\} | \theta = i\right]$$

- Note that

$$\{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (k, y^n) \quad \forall k \neq j\} \subset \{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (i, y^n)\}$$

Error and Erasure Probabilities

- An error or an erasure will happen if θ can not dominate all other messages?

$$P_{\mathrm{e}}(i) + P_{\mathrm{x}}(i) = \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (i, y^n) \not\succ (j, y^n)\} | \theta = i\right]$$

- An error will occur if a message other than θ dominates all message.

$$P_{\mathrm{e}}(i) = \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (k, y^n) \quad \forall k \neq j\} | \theta = i\right]$$

- Note that

$$\{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (k, y^n) \quad \forall k \neq j\} \subset \{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (i, y^n)\}$$

- Thus

$$P_{\mathrm{e}}(i) \leq \mathbf{P}\left[\{y^n : \exists j \neq i \text{ s.t.} (j, y^n) \succ (i, y^n)\} | \theta = i\right]$$

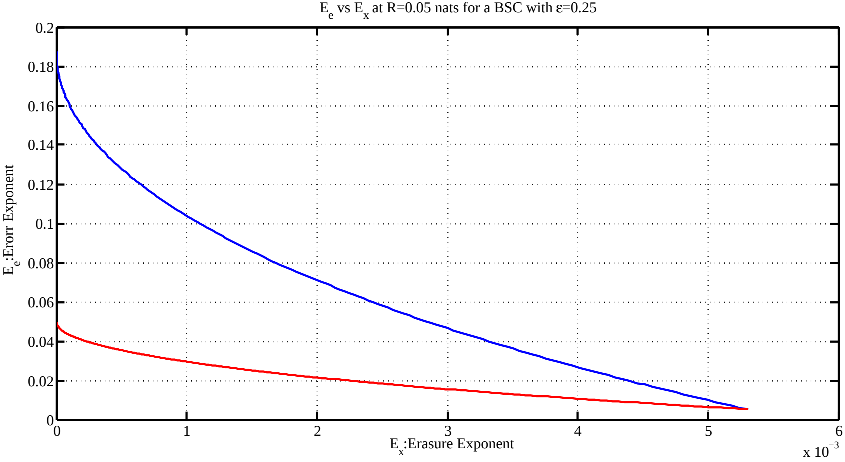
Optimization of $\succ$

- Use packing lemma to bound both of the probabilities.
- Choose the $\succ$ to minimize P_{e} while keeping P_{x} small enough, and obtain $E_{\mathrm{e}}(R, P, E_{\mathrm{x}}, \alpha, \varphi)$.
- Only $\alpha \geq \alpha^*(R, P, E_{\mathrm{x}})$ are allowed,[1] where $\alpha^*(R, P, E_{\mathrm{x}})$ is the unique solution of $E_{\mathrm{x}} = \alpha E_r\left(\frac{R}{\alpha}, P\right)$.
- $E_{\mathrm{e}}(R, P, E_{\mathrm{x}}, \alpha, \varphi)$ is a convex function of α.
- Thus

$$E_{\mathrm{e}}(R, P, E_{\mathrm{x}}) = \max_{\varphi} E_{\mathrm{e}}(R, P, E_{\mathrm{x}}, \alpha^*, \varphi) \tag{2}$$

[1] Else there are too many errors in the first phase.

Comparison with Non-feedback Case



Converse Idea

- In erasure free-case straight line bound to connect low rate upper bounds to high rate ones.
- Shannon, Gallager and Berlekamp, [2, Theorem 1]:

$$\tilde{\mathcal{P}}_{\mathbf{e}}(M, n, L) \geq \tilde{\mathcal{P}}_{\mathbf{e}}(M, n_1, L_1)\tilde{\mathcal{P}}_{\mathbf{e}}(L_1 + 1, n - n_1, L) \quad (3)$$

- Can we use same idea to connect the bounds we have for different points?
- $\tilde{\mathcal{P}}_{\mathbf{e}}(M, n, L) \rightarrow \mathcal{P}_{\mathbf{e}}(M, n, L, P_{\mathbf{x}})$

Converse

Theorem

For any n, M , L, P_x *and for any* $n_1 \leq n$, L_1, *minimum error probabilities of fixed length block codes with feedback is satisfy,*

$$\mathcal{P}_e(M, n, L, P_x) \geq \mathcal{P}_e(M, n_1, L_1, 0) \cdot \mathcal{P}_e\left(L_1 + 1, n - n_1, L, \frac{P_x}{\mathcal{P}_e(M, n_1, L_1, 0)}\right) \quad (4)$$

Straight Line Bound

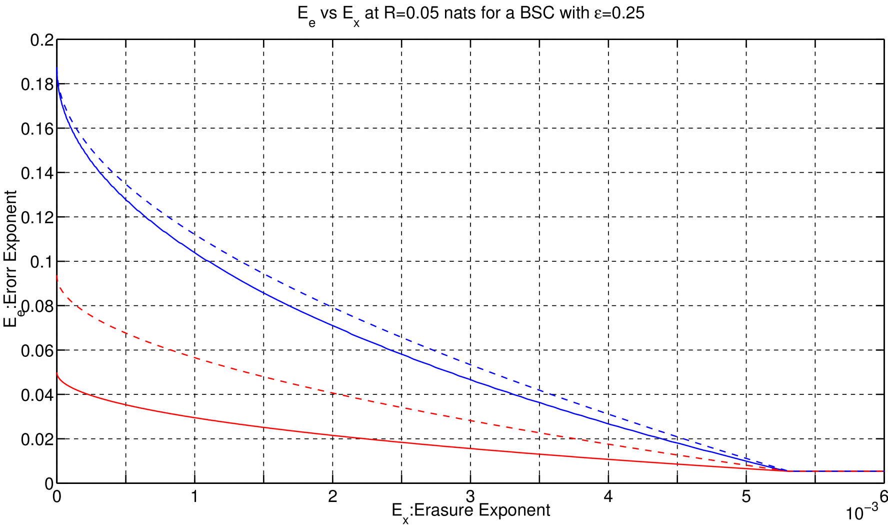
Theorem

For any rate $R \geq 0$, $E_{\mathsf{x}} \leq E_h(R)$, *for any* $\gamma \in \left(\frac{R}{C}, \gamma^*(R, E_{\mathsf{x}})\right)$

$$\mathcal{E}_{\mathsf{e}}\left(R, E_{\mathsf{x}}\right) \leq \gamma E_h\left(\frac{R}{\gamma}\right) + (1-\gamma)\mathcal{E}_{\mathsf{e}}\left(0, \frac{E_{\mathsf{x}} - \gamma E_h\left(\frac{R}{\gamma}\right)}{1-\gamma}\right)$$

where $\gamma^*(R, E_{\mathsf{x}})$ *is the unique solution of* $\gamma E_h\left(\frac{R}{\gamma}\right) = E_{\mathsf{x}}$ *if it exists,* 1 *else.*

Upper and Lower Bounds Together



Current/Future Work

- Better codes for low rates.
- Erasure exponents of zero-error codes.
- List decoding improvements on two phase coding schemes.
- Error exponent - erasure exponent trade off at zero rate.

Jr. G. Forney.
Exponential error bounds for erasure, list, and decision feedback schemes.
IEEE Transactions on Information Theory, Vol.14, Iss.2:206–220, 1968.

C.E. Shannon, R.G. Gallager, and E.R. Berlekamp.
Lower bounds to error probability for coding on discrete memoryless channels.
Information and Control, 10, No. 1:65–103, 1967.

Packing Lemma

- Any $\succ$ in terms of $(\mathbb{V}(1), \mathbb{V}(2) \ldots \mathbb{V}(|\mathcal{M}|))$ and α where

$$\mathbb{V}_{j,l}(i) = \frac{\#\text{ of } k \text{ such } y_k = l \text{ and } x_k(i) = j \text{ in } y^{n_1}}{\#\text{ of } k \text{ s.t. } x_k(i) = j \text{ in } y^{n_1}}$$

$$\alpha_{l|i,j} = \frac{\#\text{ of } k \text{ s.t. } \mathbf{x}_{ak} = i \text{ and } \mathbf{x}_{rk} = j \text{ and } y_{\alpha n+k} = l \text{ in } y^n_{n_1+1}}{\#\text{ of } k \text{ s.t. } \mathbf{x}_{ak} = i \text{ and } \mathbf{x}_{rk} = j \text{ in } y^n_{n_1+1}}$$

- But we will restrict ourselves to orders, for which $(i, y^n) \succ (j, y^n)$ can be determined solely by $\mathbb{V}(i)$, $\mathbb{V}(j)$ and α.

Lemma (Packing Lemma)

For every $R > 0$, $\delta > 0$ and every type P of the sequences $\mathcal{X}^n$ satisfying $H(P) > R$, there exist at least $e^{n(R-\delta)}$ distinct sequences $x^n(i) \in \mathcal{X}^n$ of type P such that for every pair of stochastic matrices $V : \mathcal{X} \to \mathcal{Y}$, $\hat{V} : \mathcal{X} \to \mathcal{Y}$ and for every i

$$|T_V(x^n(i)) \bigcap \cup_{j \neq i} T_{\hat{V}}(x^n(j))| \leq |T_V(x^n(i))| e^{-n|I(P,\hat{V})-R|^+}$$