Performance Enhancements for Algebraic Soft Decision Decoding of Reed-Solomon Codes

ISIT 2004

Mostafa El-Khamy, Robert J. McEliece, and Jonathan Harel

{mostafa, rjm, harel}@systems.caltech.edu

California Institute of Technology
Pasadena, CA 91125, USA
Introduction

Goal:

What is the ultimate performance of ASD of RS Codes?
Introduction

Goal:

What is the ultimate performance of ASD of RS Codes?

Find better Multiplicity Assignment algorithms
Introduction

Goal:

What is the ultimate performance of ASD of RS Codes?

Find better Multiplicity Assignment algorithms

Existing Multiplicity Assignment Algorithms for ASD:
Introduction

Goal:

What is the ultimate performance of ASD of RS Codes?

Find better Multiplicity Assignment algorithms

Existing Multiplicity Assignment Algorithms for ASD:

Kötter and Vardy Algorithm [KV03]
Gaussian Approximation [PV03]
Introduction

- $n$-dimensional vector over $F$: $\mathbf{u} = (u_1, \ldots, u_n)$
Introduction

- \( n \)-dimensional vector over \( F \): \( u = (u_1, \ldots, u_n) \)
- \( q \times n \) arrays: \( W = (w_i(\beta)) \), where \( i = 1, \ldots, n \) and \( \beta \in F \).
Introduction

- $n$-dimensional vector over $F$: $u = (u_1, \ldots, u_n)$
- $q \times n$ arrays: $W = (w_i(\beta))$, where $i = 1, \ldots, n$ and $\beta \in F$.
- Cost:

$$|W| \triangleq \frac{1}{2} \sum_{i=1}^{n} \sum_{\beta \in F} w_i(\beta) (w_i(\beta) + 1).$$
Introduction

- $n$-dimensional vector over $F$: $\mathbf{u} = (u_1, \ldots, u_n)$
- $q \times n$ arrays: $W = (w_i(\beta))$, where $i = 1, \ldots, n$ and $\beta \in F$.
- Cost:
  \[
  |W| \triangleq \frac{1}{2} \sum_{i=1}^{n} \sum_{\beta \in F} w_i(\beta) (w_i(\beta) + 1).
  \]
- Score:
  \[
  \langle \mathbf{u}, W \rangle \triangleq \sum_{i=1}^{n} w_i(u_i).
  \]
Introduction

- $n$-dimensional vector over $F$: $\mathbf{u} = (u_1, \ldots, u_n)$
- $q \times n$ arrays: $W = (w_i(\beta))$, where $i = 1, \ldots, n$ and $\beta \in F$.
- Cost:
  \[
  |W| \triangleq \frac{1}{2} \sum_{i=1}^{n} \sum_{\beta \in F} w_i(\beta) (w_i(\beta) + 1).
  \]
- Score:
  \[
  \langle \mathbf{u}, W \rangle \triangleq \sum_{i=1}^{n} w_i(u_i).
  \]
- $c \in \mathbb{C}$ will be an $(n, k, d)$ Reed-Solomon code over $F$. 

Introduction

- $n$-dimensional vector over $F$: $\mathbf{u} = (u_1, \ldots, u_n)$
- $q \times n$ arrays: $W = (w_i(\beta))$, where $i = 1, \ldots, n$ and $\beta \in F$.
- Cost:
  \[
  |W| \overset{\Delta}{=} \frac{1}{2} \sum_{i=1}^{n} \sum_{\beta \in F} w_i(\beta) \left( w_i(\beta) + 1 \right).
  \]
- Score:
  \[
  \langle \mathbf{u}, W \rangle \overset{\Delta}{=} \sum_{i=1}^{n} w_i(u_i).
  \]
- $c \in \mathbb{C}$ will be an $(n, k, d)$ Reed-Solomon code over $F$.
- Channel Output: APP matrix:
  \[
  \Pi = (\pi_i(\beta)) = (Pr \{ c_i = \beta | r_i \})
  \]
Algebraic Soft Decoding

\[ \Pi \Rightarrow \quad \text{Multiplicity Assignment Algorithm; } A \quad \Rightarrow \quad M \]

\[ c \rightarrow \Pi \xrightarrow{A} M \]

\[ m_i(\beta) \text{ is a non-negative integer.} \]
Algebraic Soft Decoding

\[ \Pi \Rightarrow \text{Multiplicity Assignment Algorithm; } A \Rightarrow M \]

- \( c \rightarrow \Pi \xrightarrow{A} M \)
- \( m_i(\beta) \) is a non-negative integer.
- \( c \) is on the GS list if

\[ \langle c, M \rangle > D_{k-1}(|M|) \equiv c \vdash M \]

- \( D_v(\gamma) \leq -\frac{v}{2} + \sqrt{2v\gamma} + \frac{v^{3/2}}{8\sqrt{2\gamma}}. \)
Algebraic Soft Decoding

\[ \Pr \{ E_A \} = \sum_{\Pi \in \text{APP}} \Pr \{ E_A | \Pi \} \Pr \{ \Pi \} ; \ E_A = \{ c \not\in M \} \]
Algebraic Soft Decoding

\[ \Pr \{ \mathcal{E}_A \} = \sum_{\Pi \in \text{APP}} \Pr \{ \mathcal{E}_A | \Pi \} \Pr \{ \Pi \}; \quad \mathcal{E}_A = \{ c \not\in M \} \]

Theorem:

\[ \Pr \{ \mathcal{E}_A | \Pi \} = \frac{1}{\sum_{c \in \mathcal{C}} P(c)} \sum_{c \in \mathcal{C}} \Delta [c \not\in M] P(c). \]
Algebraic Soft Decoding

\[ \Pr \{ \mathcal{E}_A \} = \sum_{\Pi \in \text{APP}} \Pr \{ \mathcal{E}_A | \Pi \} \Pr \{ \Pi \}; \quad \mathcal{E}_A = \{ c \not\in M \} \]

**Theorem:**

\[ \Pr \{ \mathcal{E}_A | \Pi \} = \frac{1}{\sum_{c \in \mathcal{C}} P(c)} \sum_{c \in \mathcal{C}} \Delta [c \not\in M] P(c). \]

Find A: Hard Problem!
Multiplicity Assignment Problem

KV Simplification: \( x \rightarrow \Pi \xrightarrow{A} M \)
Multiplicity Assignment Problem

- KV Simplification: \( x \rightarrow \Pi \xrightarrow{A} M \)
- Independence Assumption: \( P(x) = \prod_{i=1}^{n} \pi_i(x_i) \)

\[
P(\Pi, M) \triangleq \sum_{x \in F^n} \Delta [x \not\in M] P(x)
\]
**Multiplicity Assignment Problem**

- **KV Simplification:** \( x \rightarrow \Pi \rightarrow A \rightarrow M \)

- **Independence Assumption:** \( P(x) = \prod_{i=1}^{n} \pi_i(x_i) \)

\[
P(\Pi, M) \triangleq \sum_{x \in F^n} \Delta [x \not\in M] P(x)
\]

- **ASD Decoder:**

\[
P(\Pi, \gamma) = \min_{|M| \leq \gamma} P(\Pi, M)
\]

\[
M(\Pi, \gamma) = \arg_M \min_{|M| \leq \gamma} P(\Pi, M)
\]

\[
P(\Pi, \infty) \triangleq \lim_{\gamma \to \infty} P(\Pi, \gamma)
\]
Multiplicity Assignment Problem

- KV Simplification: \( x \rightarrow \Pi \xrightarrow{A} M \)

- Independence Assumption: \( P(x) = \prod_{i=1}^{n} \pi_i(x_i) \)

\[
\mathcal{P}(\Pi, M) \triangleq \sum_{x \in F^n} \Delta [x \not\in M] P(x)
\]

- ASD Decoder: Hard Problem!

\[
P(\Pi, \gamma) = \min_{|M| \leq \gamma} \mathcal{P}(\Pi, M)
\]

\[
M(\Pi, \gamma) = \arg_M \min_{|M| \leq \gamma} \mathcal{P}(\Pi, M)
\]

\[
P(\Pi, \infty) \triangleq \lim_{\gamma \to \infty} P(\Pi, \gamma)
\]
Relax Integer Constraint: $Q = (q_i(\beta))$ 'soft' matrix.
Soft Multiplicity Matrices

- Relax Integer Constraint: $Q = (q_i(\beta))$ 'soft' matrix.
- Relaxed problem:

$$\mathcal{P}(\Pi, Q) \triangleq \sum_{x \in F^n} \Delta [x \not\in Q] P(x)$$

$$P^*(\Pi, \gamma) \triangleq \min_{|Q| \leq \gamma} \mathcal{P}(\Pi, Q)$$

$$Q^*(\Pi, \gamma) \triangleq \arg \min_{|Q| \leq \gamma} \mathcal{P}(\Pi, Q)$$

$$P^*(\Pi, \infty) \triangleq \lim_{\gamma \to \infty} P^*(\Pi, \gamma).$$
Soft Multiplicity Matrices

Theorem: \( P^*(\Pi, \infty) = P(\Pi, \infty) \)
Theorem: $P^*(\Pi, \infty) = P(\Pi, \infty)$

$Q^* = ?$  Still a Hard Problem?
Soft Multiplicity Matrices

- Theorem: $P^*(\Pi, \infty) = P(\Pi, \infty)$

- $Q^*$ =? Still a Hard Problem?

- Minimize the Chernoff Bound on the Error Probability!
The Chernoff Bound-Finite Cost

- $S_i$ are independent r.v.;

$$\langle x, Q \rangle = S_Q = S_1 + \cdots + S_n.$$ 

- $$\phi_i(s, \pi_i, q_i) = \mathbb{E}_{S_i} \left\{ e^{sS_i} \right\} = \sum_{\beta \in F} \pi_i(\beta) e^{sq_i(\beta)}.$$ 

- $$\Phi(s, \Pi, Q) = \mathbb{E}_{S_Q} \left\{ e^{s \sum_{i=1}^{n} S_i} \right\} = \prod_{i=1}^{n} \phi_i(s, \pi_i, q_i).$$

- Chernoff Bound:

$$\Pr \{ S_Q \leq \delta \} \leq \min_{s \geq 0} \left\{ e^{s\delta} \Phi(-s, \Pi, Q) \right\}.$$
The Chernoff Bound-Finite Cost

Transformation [PV03]

\[ X_i(\beta) = q_i(\beta) + 1/2; \quad L^2 = 2\gamma + \frac{nq}{4}; \quad D' = D_v(\gamma) + \frac{n}{2}. \]
The Chernoff Bound-Finite Cost

Transformation [PV03]

\[ X_i(\beta) = q_i(\beta) + 1/2; \quad L^2 = 2\gamma + \frac{nq}{4}; \quad D' = D_v(\gamma) + \frac{n}{2}. \]

Transformed Problem:

\[ P^*(\Pi, \gamma) \leq \min_{\|X\|^2 = L^2} \min_{s \geq 0} \left\{ e^{sD'} \Phi(-s, \Pi, X) \right\}. \]

The (sub)optimum matrix

\[ \bar{X}^* = \arg_{\bar{X}} \min_{\|\bar{X}\|^2 = L^2} \min_{s \geq 0} \left\{ e^{sD'} \Phi(-s, \Pi, \bar{X}) \right\}. \]
Theorem: \( v = k - 1 \)

\[
P(\Pi, \infty) = \min_{\|R\|^2=1} \sum_{x \in F^n} \Delta \left[ \langle x, R \rangle \leq \sqrt{v} \right] P(x)
\]
Chernoff Bound-Infinite Cost

**Theorem:** \( \nu = k - 1 \)

\[
P(\Pi, \infty) = \min_{\|R\|^2=1} \sum_{x \in F^n} \Delta \left[ \langle x, R \rangle \leq \sqrt{\nu} \right] P(x)
\]

**Chernoff Bound:**

\[
P(\Pi, \infty) \leq \min_{\|R\|^2=1} \min_{s \geq 0} \left\{ \Phi(-s, \Pi, R) e^{s\sqrt{\nu}} \right\}
\]

**(Sub)Optimum Matrix:**

\[
R^\chi(\Pi) = \arg_{R} \min_{\|R\|^2=1} \min_{s \geq 0} \left\{ \Phi(-s, \Pi, R) e^{s\sqrt{\nu}} \right\}
\]
The Lagrangian

Constrained Optimization Problem:

\[
\min \left( sD' + \sum_{i=1}^{n} \ln \phi_i(-s, \pi_i, X_i) \right)
\]

subject to

\[
s \geq 0
\]

\[
\|X\|^2 = L^2 = 2\gamma + \frac{1}{4}nq.
\]
The Lagrangian

Constrained Optimization Problem:

\[
\min \left( sD' + \sum_{i=1}^{n} \ln \phi_i(-s, \pi_i, X_i) \right)
\]

subject to

\[
s \geq 0
\]

\[
\|X\|^2 = L^2 = 2\gamma + \frac{1}{4}nq.
\]

The Lagrangian:

\[
\mathcal{L}(s, X, \lambda) = sD' + \sum_{i=1}^{n} \ln \phi_i(-s, \pi_i, X_i) + \frac{\lambda}{2} \left( \|X\|^2 - L^2 \right).
\]
The Lagrangian

\[ \frac{\partial L}{\partial \lambda} \bigg|_{\lambda = \lambda^*} = 0 \quad \Rightarrow \quad \| X \|^2 = L^2 \]
The Lagrangian

\[ \frac{\partial L}{\partial \lambda} \bigg|_{\lambda=\lambda^*} = 0 \Rightarrow \|X\|^2 = L^2 \]

\[ D' - \sum_{i=1}^{n} \left( \frac{\sum_{\beta \in F} X_i(\beta) \pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \right) \bigg|_{s=s^*} = 0 \]
The Lagrangian

\[ \frac{\partial L}{\partial \lambda} \bigg|_{\lambda=\lambda^*} = 0 \quad \Rightarrow \quad \|X\|^2 = L^2 \]

\[ D' - \sum_{i=1}^{n} \left( \frac{\sum_{\beta \in F} X_i(\beta) \pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \right) \bigg|_{s=s^*} = 0 \]

\[ \frac{X_i(\beta)}{L^2} \sum_{i=1}^{n} \left( \frac{\sum_{\beta \in F} X_i(\beta) \pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \right) - \frac{\pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \bigg|_{X=X^*} = 0 \]
The Lagrangian

\[ \frac{\partial L}{\partial x} \bigg|_{\lambda = \lambda^*} = 0 \quad \Rightarrow \quad \|X\|^2 = L^2 \]

\[ D' - \sum_{i=1}^{n} \left( \frac{\sum_{\beta \in F} X_i(\beta) \pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \right) \bigg|_{s = s^*} = 0 \]

\[ \frac{X_i(\beta)}{L^2} \sum_{i=1}^{n} \left( \frac{\sum_{\beta \in F} X_i(\beta) \pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \right) - \frac{\pi_i(\beta) e^{-sX_i(\beta)}}{\phi_i(-s, \pi_i, X_i)} \bigg|_{X=X^*} = 0 \]

\[ \frac{D'}{L^2} X_i(\beta) - \frac{\pi_i(\beta) e^{-s^*X_i(\beta)}}{\sum_{\beta \in F} \pi_i(\beta) e^{-s^*X_i(\beta)}} \bigg|_{X=X^*, s=s^*} = 0 \]
Define

\[ \mathcal{L}_s(s) = \mathcal{L}^*(s, \mathbf{X}) \bigg|_{\mathbf{X} = \text{const}}, \quad \mathcal{L}_X(\mathbf{X}) = \mathcal{L}^*(s, \mathbf{X}) \bigg|_{s = s^*}. \]
Convexity

- Define

\[ \mathcal{L}_s(s) = \mathcal{L}^*(s, \mathbf{X}) \bigg|_{\mathbf{X}=\text{const}}, \quad \mathcal{L}_X(\mathbf{X}) = \mathcal{L}^*(s, \mathbf{X}) \bigg|_{s=s^*}. \]

- \( \mathcal{L}_s(s) \) is convex in \( s \)
Convexity

Define

\[ \mathcal{L}_s(s) = \mathcal{L}^*(s, X)|_{X=\text{const}}, \quad \mathcal{L}_X(X) = \mathcal{L}^*(s, X)|_{s=s^*}. \]

- \( \mathcal{L}_s(s) \) is convex in \( s \)
- \( \mathcal{L}_X(X) \) is convex in \( X \)
Iterative Algorithm

Initialize \( \mathbf{X}^0 = \frac{L^2}{D'} \Pi, \ s^0 = 0.1 \ast \frac{D'}{L^2} \) and \( j = 0 \).

Do

\( j := j + 1 \)

I. Solve for \( s^j \),

\[
\nabla_s (L^*(s, X^{j-1})) = \left. \frac{\partial L^*(s, X^{j-1})}{\partial s} \right|_{s=s^j} = 0
\]

II. Solve for \( X^j \),

\[
\nabla_X (L^*(s^j, X)) = \left\{ \frac{\partial L^*(s^j, X)}{\partial X^j_i(\beta)} \right\}, i = 1, \ldots, n, \ \beta \in F \left|_{X=X^j} \right. = 0
\]

While \( \left\| \frac{s^j - s^{j-1}}{s^{j-1}} \right\|_1 \leq \epsilon \).
Iterative Algorithm

For finite cost multiplicity matrix $M = (m_i(\beta))$:

$$m_i(\beta) = \text{Round} \left\{ \max \{0, X_i^*(\beta) - 0.5\} \right\}.$$
Iterative Algorithm

- For finite cost multiplicity matrix \( M = (m_i(\beta)) \):

\[
m_i(\beta) = \text{Round} \left\{ \max \{0, X_i^*(\beta) - 0.5\} \right\}.
\]

- Solve could be replace by a Newton type algorithm.
Iterative Algorithm

- For finite cost multiplicity matrix $M = (m_i(\beta))$: 

  $$m_i(\beta) = \text{Round} \left\{ \max \{0, X^*_i(\beta) - 0.5\} \right\}.$$ 

- **Solve** could be replace by a Newton type algorithm.

- To reduce computational complexity:

  Set $X_i(\beta) = 0$ if $m_i(\beta) < \text{threshold}$
Numerical Results & Conclusions

ASD of (15,11) RS code BPSK modulated over AWGN Channel

Codeword Error Rate vs. $E_b/N_0$ (dB) for different decoding techniques:
- HD–BM
- KV, $\gamma = \infty$
- Gauss, $\gamma = \infty$
- Chernoff, $\gamma = \infty$
- KV, $\gamma = 10^4$
- Chernoff, $\gamma = 10^4$
Numerical Results & Conclusions

ASD of (15,11) RS code over AWGN, Infinite Cost

- HD−BM
- KV
- Gauss
- Chernoff
- ML−sim
- ML−TSB

Codeword Error Rate vs. Eb/N₀
Numerical Results & Conclusions

ASD of (15,11) RS Code 16-PSK modulated over AWGN

- HD-BM
- KV, C=∞
- Gauss, C=∞
- Chernoff, C=∞
- KV, C=1e4
- Chernoff, C=1e4

Codeword Error Rate vs. Eb/N0

6 8 10 12 14 16 18

10^{-8} 10^{-7} 10^{-6} 10^{-5} 10^{-4} 10^{-3} 10^{-2} 10^{-1} 10^{0}
Numerical Results & Conclusions

SD of (31,25) RS code BPSK modulated over AWGN Channel

- HD-BM
- KV
- Gauss
- Chernoff
Numerical Results & Conclusions

SD of (31,25) RS code BPSK modulated over AWGN Channel

- HD–BM
- KV
- Gauss
- Chernoff
- ML–TSB

SNR (dB)

Codeword Error Rate

2 3 4 5 6 7 8 9

10^{-2} 10^{-1} 10^{0} 10^{1} 10^{2} 10^{3} 10^{4} 10^{5} 10^{6} 10^{7} 10^{8} 10^{9}
Future Work

- Finding less complex Algorithms with high efficiency.
- Minimize the true Error Probability directly.
- Precondition II to have information from other symbols and the channel.
- Iterative Algebraic Decoding.
Thank You!

http://mostafa.caltech.edu/Academia.html