List Decoding of Concatenated Codes: Improved Performance Estimates

Alexander Barg
Andrew McGregor
List Decoding of Concatenated Codes: Improved Performance Estimates

Alexander Barg

Andrew McGregor
Important Words
Important Words

- List Decoding
Important Words

- List Decoding
- Concatenated Codes
Important Words

• List Decoding
• Concatenated Codes

Inner: Arbitrary \( q \)-ary \([n,k,d]\) code \( A=\{x_1,x_2,\ldots\} \)
Important Words

- List Decoding
- Concatenated Codes

Inner: Arbitrary $q$-ary $[n,k,d]$ code $A=\{x_1,x_2,\ldots\}$

Outer: Reed-Solomon $q^k$-ary $[N, K=\kappa N, D]$ code $B$
Important Words

• List Decoding
• Concatenated Codes

Inner: Arbitrary $q$-ary $[n,k,d]$ code $A=\{x_1, x_2, \ldots\}$
Outer: Reed-Solomon $q^k$-ary $[N, K=\kappa N, D]$ code $B$

"Message" $\xrightarrow{B} jhfsoirheqck$
Important Words

- List Decoding
- Concatenated Codes

**Inner:** Arbitrary $q$-ary $[n,k,d]$ code $A=\{x_1,x_2,\ldots\}$

**Outer:** Reed-Solomon $q^k$-ary $[N, K=\kappa N, D]$ code $B$

```
B
```

"Message"

```
  jhfsoirheqck
  0 1 1 0 1 1 0 1 0 0 1 1
  1 1 0 1 0 1 0 1 1 1 0 1
  0 1 1 1 0 1 0 1 1 1 1 1
  1 0 1 0 1 0 1 0 0 1 1 1
  0 1 0 1 0 1 0 1 0 1 0 1
```

```
A
```

![Diagram](image-url)
Some Previous Work

• GMD Decoding (Forney, 1966)

• G-S Decoding (Guruswami, Sudan 2000)
Some Previous Work

- GMD Decoding (Forney, 1966)

\[ N \ln \frac{(1 - \kappa)\delta}{2} \]

- G-S Decoding (Guruswami, Sudan 2000)
Some Previous Work

- GMD Decoding (Forney, 1966)
  \[ Nn \frac{(1 - \kappa)\delta}{2} \]

- G-S Decoding (Guruswami, Sudan 2000)
  \[ Nn \left[ J(\delta, q) - \sqrt{\delta \kappa} \right] \]
Our Work
Our Work

- Combined GMD/G-S Decoding
Our Work

• Combined GMD/G-S Decoding
• Improve Estimates for Random Inner Codes
Decoding Radius of GMD Decoding
Decoding Radius of **GMD Decoding**

**G-S Decoding**

List Decoding Radius

Outer Code Rate $\kappa$
Decoding Radius of GMD Decoding
G-S Decoding
Our Result
Column Reliability
Column Reliability

• Receive word $x$ as in column $i$
Column Reliability

• Receive word $x$ as in column $i$
• Consider column *reliable* if $h_i = d(x, A)$ is small
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- GMD: Inner Decoder passes 1 inner codeword and $h_i$. 
Column Reliability

• Receive word $x$ as in column $i$
• Consider column \textit{reliable} if $h_i = d(x, A)$ is small
• \textbf{GMD}: Inner Decoder passes 1 inner codeword and $h_i$.
• \textbf{G-S}: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$. 
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The *weight* of an outer codeword $c = a_1a_2...a_N$ is
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The *weight* of an outer codeword $c = a_1 a_2 \ldots a_N$ is

$$w(c) = \sum_{1 \leq i \leq N} w_i(a_i)$$
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The **weight** of an outer codeword $c = a_1a_2...a_N$ is
  \[ w(c) = \sum_{1 \leq i \leq N} w_i(a_i) \]
- G-S decoding will output codeword $c$ if
Column Reliability

- Receive word $x$ as in column $i$
- Consider column \textit{reliable} if $h_i = d(x, A)$ is small
- \textbf{GMD}: Inner Decoder passes 1 inner codeword and $h_i$.
- \textbf{G-S}: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The \textit{weight} of an outer codeword $c = a_1a_2 \ldots a_N$ is

\[
w(c) = \sum_{1 \leq i \leq N} w_i(a_i)
\]

- G-S decoding will output codeword $c$ if

\[
w(c) \geq \sqrt{K \sum_{i,j} w_i(x_j)^2}
\]
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The *weight* of an outer codeword $c = a_1 a_2 \ldots a_N$ is

$$w(c) = \sum_{1 \leq i \leq N} w_i(a_i)$$

- G-S decoding will output codeword $c$ if

$$w(c) \geq \sqrt{K \sum_{i,j} w_i(x_j)^2}$$

where $w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^+$
Column Reliability

- Receive word $x$ as in column $i$
- Consider column *reliable* if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The *weight* of an outer codeword $c = a_1 a_2 \ldots a_N$ is
  \[ w(c) = \sum_{1 \leq i \leq N} w_i(a_i) \]
- G-S decoding will output codeword $c$ if
  \[ \text{where } w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^+ \]
Column Reliability

- Receive word $x$ as in column $i$
- Consider column reliable if $h_i = d(x, A)$ is small
- **GMD**: Inner Decoder passes 1 inner codeword and $h_i$.
- **G-S**: Inner Decoder passes weights $w_i(x_j)$ on each $x_j \in A$.
- The weight of an outer codeword $c = a_1 a_2 \ldots a_N$ is
  \[
  w(c) = \sum_{1 \leq i \leq N} w_i(a_i)
  \]
- G-S decoding will output codeword $c$ if
  \[
  \# \text{ errors} \leq Nn \left[ J(\delta, q) - \sqrt{\delta} \kappa \right]
  \]
  where
  \[
  w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^+ \]
Most Reliable Columns...
Most Reliable Columns...

- Consider the $N-D$ most reliable columns
Most Reliable Columns...

- Consider the $N-D$ most reliable columns

$$H = \sum_{\text{most reliable columns}} h_i$$
Most Reliable Columns...

• Consider the $N-D$ most reliable columns

\[ H = \sum_{\text{most reliable columns}} h_i \]

• [Dumer ’81] GMD decodes
Most Reliable Columns...

- Consider the $N-D$ most reliable columns
  \[ H = \sum_{\text{most reliable columns}} h_i \]

- [Dumer ’81] GMD decodes
  \[ N n \frac{\delta (1 - \kappa)}{2} + H \]
Most Reliable Columns...

• Consider the \( N-D \) most reliable columns

\[
H = \sum_{\text{most reliable columns}} h_i
\]

• [Dumer '81] GMD decodes

\[
N n \frac{\delta(1 - \kappa)}{2} + H
\]

• But what if \( H \) is small...
Weight-Settings in G-S

- G-S: Set weights such that many c have
Weight-Settings in G-S

- G-S: Set weights such that many $c$ have

$$w(c) \geq \sqrt{K \sum_{i,j} w_i(x_j)^2}$$
Weight-Settings in G-S

- G-S: Set weights such that many $c$ have
  \[ w(c) \geq \sqrt{K \sum_{i,j} w_i(x_j)^2} \]

- Previously $w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^{+}$

- New $w_i(x_j) = \left| \max\{J(q, \delta), d - h_i\} - d(x, x_j) \right|^{+}$
Weight-Settings in G-S

• G-S: Set weights such that many $c$ have

\[ w(c) \geq \sqrt{K \sum_{i,j} w_i(x_j)^2} \]

\text{Goes down!}

\text{Goes up!}

• Previously

\[ w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^+ \]

• New

\[ w_i(x_j) = \left| \max\{J(q, \delta), d - h_i\} - d(x, x_j) \right|^+ \]
Combing GMD and G-S
Combing GMD and G-S

- G-S decodes:
Combing GMD and G-S

- G-S decodes:

\[ Nn \left( J + \kappa(\delta - J) - H - \sqrt{\kappa \left( \left( 1 - \kappa + \frac{H/Nn}{\delta - J} \right) \delta + \left( \kappa - \frac{H/Nn}{\delta - J} \right) \delta^2 \right)} \right) \]
Combing GMD and G-S

• G-S decodes:

\[ Nn \left( J + \kappa(\delta - J) - H - \sqrt{\kappa \left( \left( 1 - \kappa + \frac{H/Nn}{\delta - J} \right) \delta + \left( \kappa - \frac{H/Nn}{\delta - J} \right) \delta^2 \right)} \right) \]

• GMD decodes:
Combing GMD and G-S

- G-S decodes:

\[
Nn \left( J + \kappa (\delta - J) - H - \sqrt{\kappa \left( \left( 1 - \kappa + \frac{H/Nn}{\delta - J} \right) \delta + \left( \kappa - \frac{H/Nn}{\delta - J} \right) \delta^2 \right)} \right)
\]

- GMD decodes:

\[
Nn \delta \frac{(1 - \kappa)}{2} + H
\]
Combing GMD and G-S

• G-S decodes:

\[ Nn \left( J + \kappa (\delta - J) - H - \sqrt{\kappa \left( \left( 1 - \kappa + \frac{H/Nn}{\delta - J} \right) \delta + \left( \kappa - \frac{H/Nn}{\delta - J} \right) \delta^2 \right)} \right) \]

• GMD decodes:

\[ Nn \frac{\delta (1 - \kappa)}{2} + H \]

• Combined G-S/GMD decodes:
Combing GMD and G-S

- G-S decodes:
  \[ Nn \left( J + \kappa(\delta - J) - H - \sqrt{\kappa \left( (1 - \kappa + \frac{H/Nn}{\delta - J}) \delta + \left( \kappa - \frac{H/Nn}{\delta - J} \right) \delta^2 \right)} \right) \]

- GMD decodes:
  \[ Nn \frac{\delta(1 - \kappa)}{2} + H \]

- Combined G-S/GMD decodes:

  \[ \text{#errors} \leq \begin{cases} 
  J - \sqrt{\delta \kappa} & T(\delta, \kappa) \geq \kappa(\delta - J) \\
  \frac{\delta(1 - \kappa)}{2} + T(\delta, \kappa) & 0 \leq T(\delta, \kappa) \leq \kappa(\delta - J) \\
  \frac{\delta(1 - \kappa)}{2} & T(\delta, \kappa) \leq 0, 
  \end{cases} \]

  where \( T(\kappa, \delta) = \frac{1}{2} \left( J + \kappa(\delta - J) - \sqrt{\delta \kappa} - (1 - \kappa) \delta/2 \right) \)
Random Inner Codes

• Analysis of G-S uses:
  \[ \sum_{j} w_i(x_j)^2 \leq \delta n^2 \text{ when } w_i(x_j) = \left| J(q, \delta) - d(x, x_j) \right|^+ \]

• Using knowledge of the coset distribution:
  \[ \sum_{j} w_i(x_j)^2 \leq \delta^2 n^2 E(\epsilon) \text{ when } w_i(x_j) = \left| d(1 - \epsilon) - d(x, x_j) \right|^+ \]

• With new weight setting, G-S corrects:
  \[ \delta N n \max_{\epsilon \leq 1/2} \left[ (1 - \epsilon) - \sqrt{\kappa E(\epsilon)} \right] \]
Using Coset Distribution

- Coset Distribution Result [Zyablov & Pinsker ’81]: For almost all \([n, rn]\) linear codes the number of codewords in a sphere of radius \(n(\delta-\varepsilon)\), is at most

\[
q^{(1-r)/e h_q'(\delta)}
\]
How big can \( \sum_j \left( \left| (1 - \epsilon) \delta n - d(x, x_j) \right|^+ \right)^2 \) be?
• Questions…

Thank you :-)
UGLY EXPRESSIONS!

(since you asked…)

\[ J(q, \delta) = \left(1 - \frac{1}{q}\right) \left(1 - \sqrt{1 - \frac{\delta}{1 - 1/q}}\right) \]

\[ E(\epsilon) = \left(1 - \epsilon\right)^2 + q \frac{2(1-r)}{h'_q(\delta)\delta} \left(1 - \frac{1}{e} - \frac{1}{2}\right)^2 + \frac{1-r}{h'_q(\delta)\delta} \ln q \int_{1/2}^{1-\epsilon} \left(1 - \frac{\epsilon}{1 - u}\right)^2 q^{\frac{1-r}{(1-u)h'_q(\delta)\delta}} du \]