List Decoding of Concatenated Codes: Improved Performance Estimates

Alexander Barg

Andrew McGregor

List Decoding of Concatenated Codes: Improved Performance Estimates

Alexander Barg
UNIVERSITY OF MARYLAND

Andrew McGregor
Penn
UNIVERSITY of PENNSYLVANIA

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

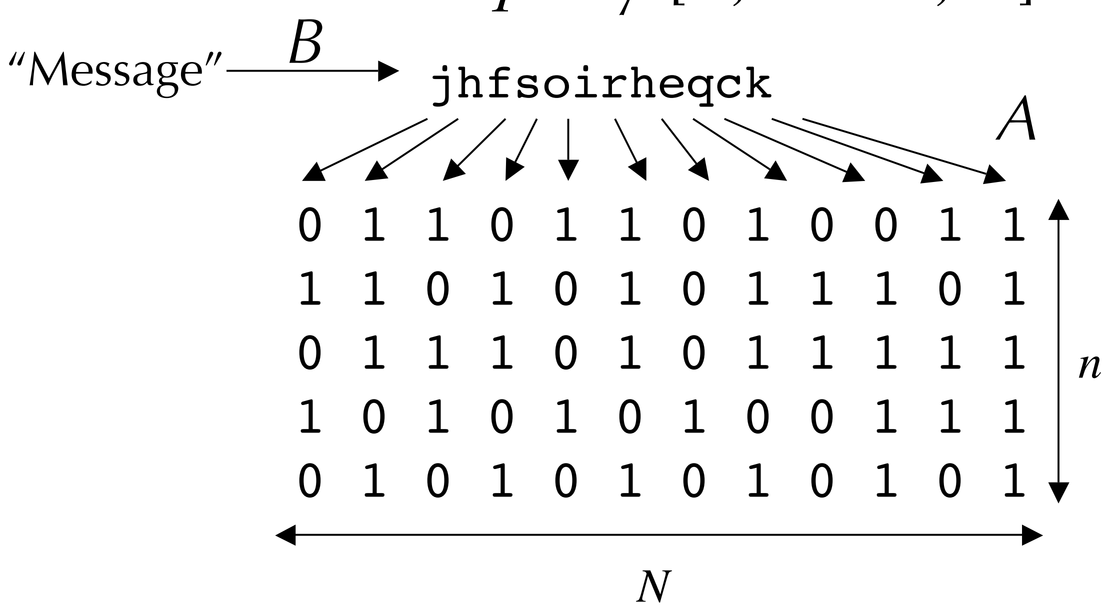
"Message" $\xrightarrow{B}$ `jhfsoirheqck`

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



Some Previous Work

- GMD Decoding (Forney, 1966)

- 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)

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

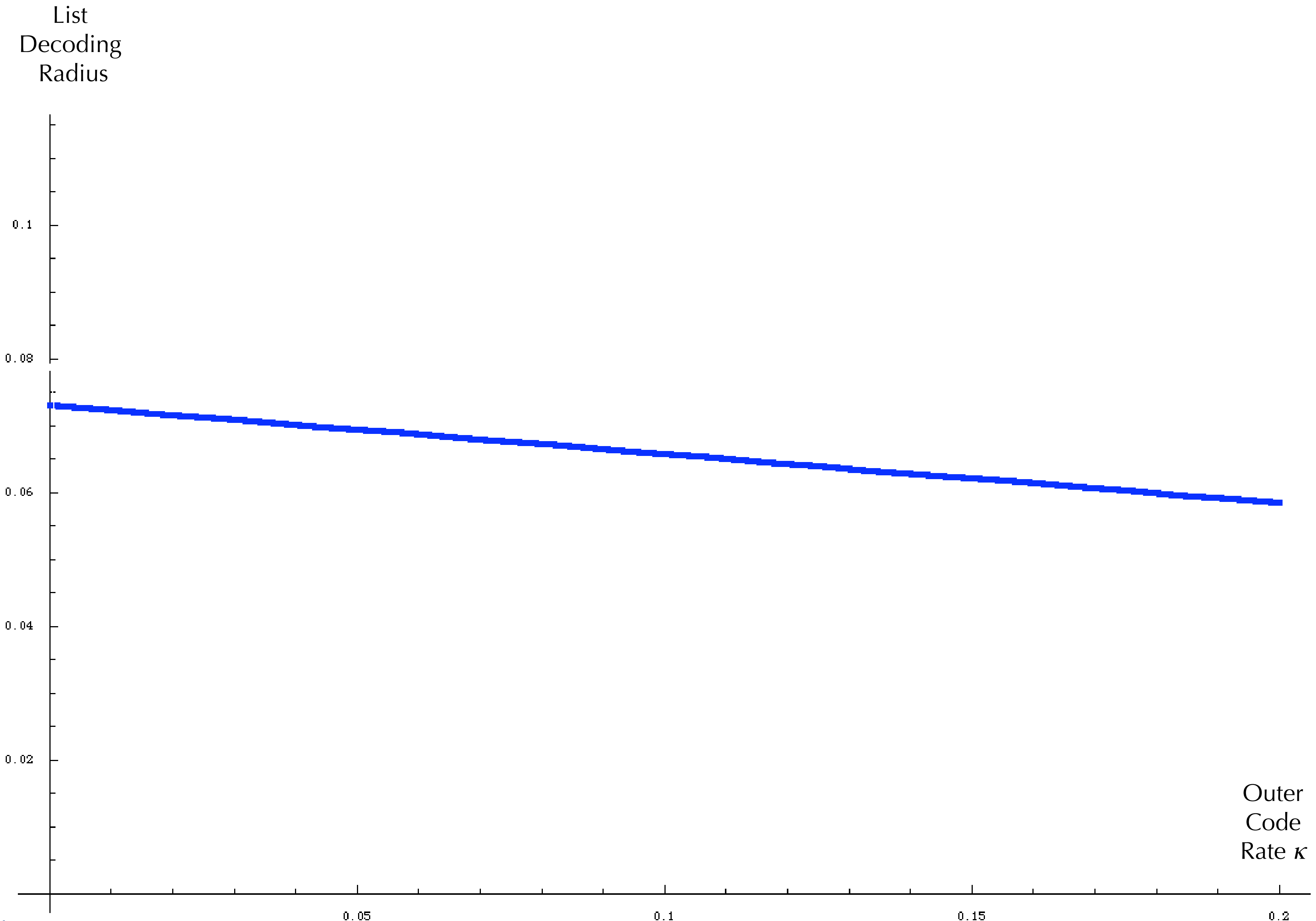
Our Work

- Combined GMD/G-S Decoding

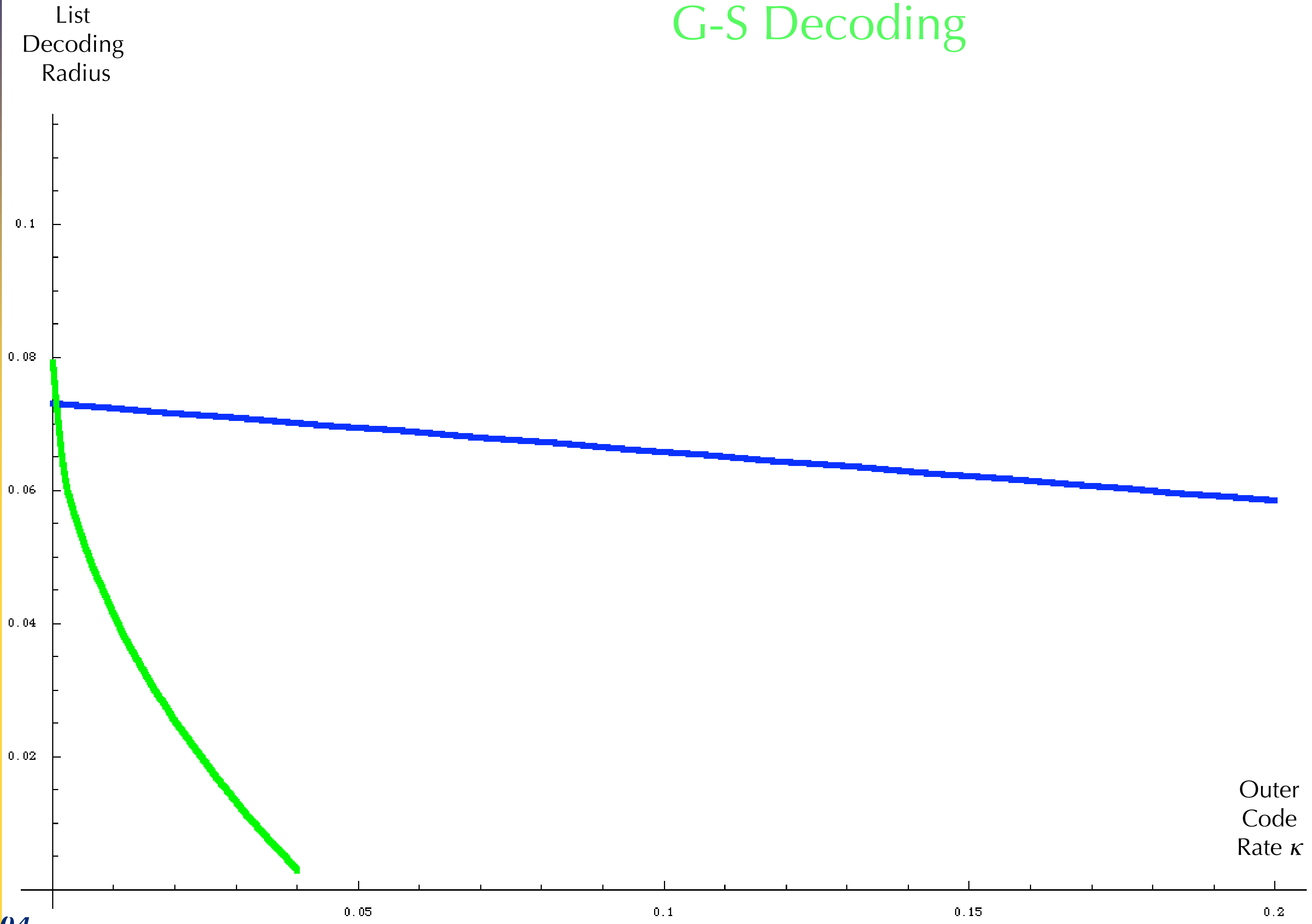
Our Work

- Combined GMD/G-S Decoding
- Improve Estimates for Random Inner Codes

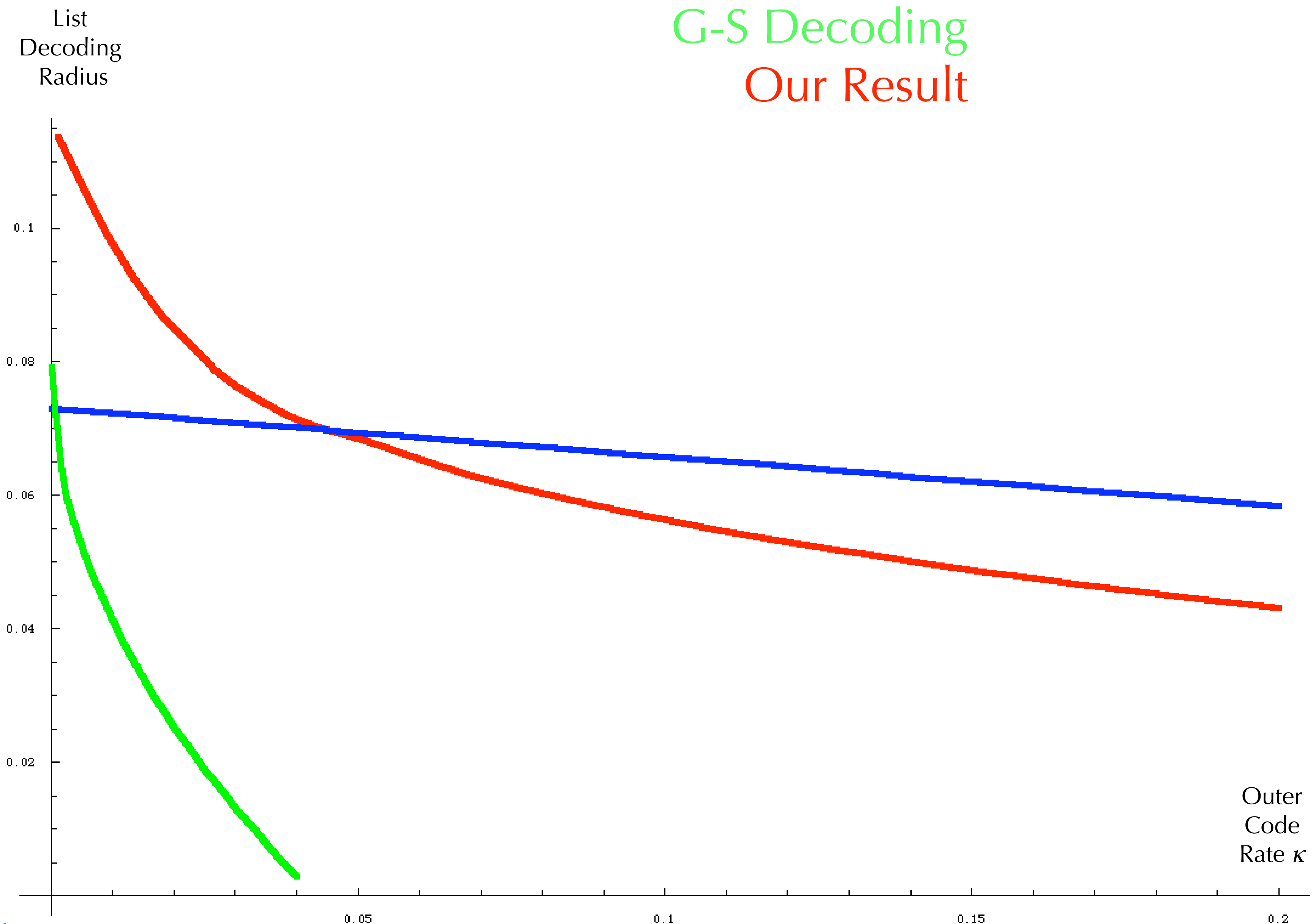
Decoding Radius of GMD Decoding



Decoding Radius of GMD Decoding
G-S Decoding



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 *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 $x_j \in A$.

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

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 $c=a_1a_2\ldots a_N$ 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 $c = a_1 a_2 \ldots a_N$ is

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

- G-S decoding will output codeword c if

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

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

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

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

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

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

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

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

- G-S decoding will output codeword c if

$$\#\text{ errors} \le Nn\left[J(\delta, q) - \sqrt{\delta\kappa}\right]$$

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

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

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

Most Reliable Columns…

- Consider the *N-D* most reliable columns

$$H = \sum_{\text{most reliable columns}} h_i$$

- [Dumer '81] GMD decodes

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

- 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

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

Goes up! Goes down!

- 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:

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

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:

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

- GMD decodes:

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

- Combined G-S/GMD decodes:

$$\#\text{errors} \;\le \begin{cases} J-\sqrt{\delta\kappa} & T(\delta,\kappa)\ge\kappa(\delta-J) \\ \frac{\delta(1-\kappa)}{2}+T(\delta,\kappa) & 0\le T(\delta,\kappa)\le\kappa(\delta-J) \\ \frac{\delta(1-\kappa)}{2} & T(\delta,\kappa)\le 0, \end{cases}$$

where $T(\kappa,\delta)=\dfrac{1}{2}(J+\kappa(\delta-J)-\sqrt{\delta\kappa}-(1-\kappa)\delta/2)$

Random Inner Codes

- Analysis of G-S uses:

$$\sum_j w_i(x_j)^2 \leq \delta n^2 \text{ when } w_i(x_j) = \Big| J(q,\delta) - d(x,x_j) \Big|^+$$

- Using knowledge of the coset distribution:

$$\sum_j w_i(x_j)^2 \leq \delta^2 n^2 E(\epsilon) \text{ when } w_i(x_j) = \Big| d(1-\epsilon) - d(x,x_j) \Big|^+$$

- With new weight setting, G-S corrects:

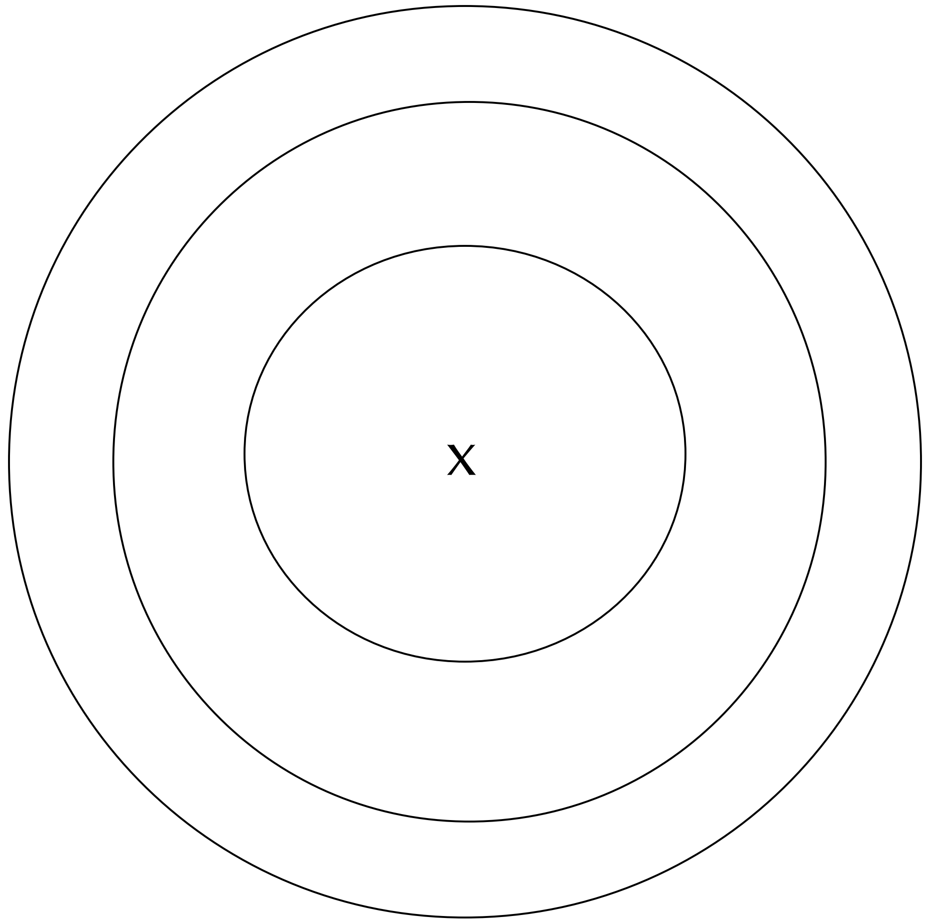
$$\delta N n \max_{\epsilon \leq 1/2} \left[\Big(1-\epsilon\Big) - \sqrt{\kappa E(\epsilon)} \right]$$

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

$$q^{(1-r)/\epsilon h_q'(\delta)}$$

How big can $\sum_j \left(\left| (1-\epsilon)\delta n - d(x, x_j) \right|^+ \right)^2$ be?



- Questions…

?

UGLY EXPRESSIONS!

(since you asked…)

$$J(q,\delta) = \Big(1 - \frac{1}{q}\Big)\Big(1 - \sqrt{1 - \frac{\delta}{1 - 1/q}}\Big)$$

$$E(\epsilon) = \Big(1-\epsilon\Big)^2 + q^{\frac{2(1-r)}{h_q'(\delta)\delta}}\Big(1-\frac{1}{c}-\frac{1}{2}\Big)^2 + \frac{1-r}{h_q'(\delta)\delta}\ln q \int_{1/2}^{1-\epsilon}\Big(1-\frac{\epsilon}{1-u}\Big)^2 q^{\frac{1-r}{(1-u)h_q'(\delta)\delta}}\,du$$