ANNOUNCEMENT: April 20 deadline for Wikipedia entry

Start playing with in-house wiki soon

May 7, 8; 1.4pm Bell 242 paper presentations

RECAP: Strongly explicit asymptotically good codes.

Q: Can we design poly time decoding algo for concatenated codes that correct $< \frac{d}{2}$ errors?
Correct $\frac{d}{2}$ errors

Capacity achieving BSCp codes

Today

first assume that a poly time algo E.
\( (RS)_C = \text{Suggest and go?} \)

- \( N = nN \) \( \text{poly}(N) \)

- \( \text{Suggest and go?} \)

- \( \text{"Reverse" the encoding process} \)
  - Define \( y = (y_1, \ldots, y_N) \in \mathbb{F}_q^N \)
  - \( \text{Decode inner code first} \)
    - \( y' \in \mathbb{F}_q^N \)
    - \( y'_2 = \text{MLD}_{\text{in}}(y_i) \forall i \)
  - \( \text{Decode outer code} \)
    - Run RS decoder on \( y' \) \( \text{poly}(N) \)

- \( O(nq^k) = O(nN) \)
  - \( \text{How many errors?} \)

- \( \text{poly}(nN) \)
Thm: Alg 1 can correct \(<\frac{dD}{4}\) errors.

Idea: \(<\frac{dD}{4}\) \Rightarrow sufficient condition is satisfied

Suff. condition: Step 2 works i.e.

\(\Delta(y', \text{Cont}(m)) < \frac{D}{2}\)

\(\exists \) disagree \(\frac{d}{2}\) as \(\text{MLD}(y_i) = \text{Cont}(m)\)

\(\exists \) agree \(\frac{d}{2}\) \(<\frac{d}{2}\) errors \(\Rightarrow\) \(<\frac{D}{2}\) positions

\(\Delta(y_i, \text{Cont}(m)) \geq \frac{d}{2}\)
Poly time unique decoder for RS codes

Correct $\frac{D}{2}$ errors

$\rightarrow$ Peterson 1960 $O(n^3)$

poly time being efficient was not yet established.

$\rightarrow$ Berlekamp-Massey $O(n^2)$

$\rightarrow$ $O(n \text{poly}(\log n))$ algo

$\rightarrow$ Berlekamp-Welch $O(n^3)$

$\rightarrow$ US patent

$\rightarrow$ Gemell-Sudan 92
\[ e < \frac{D}{2} = \frac{N-K+1}{2} \] (knowing \( E \Rightarrow \text{erasure/noise model} \))

\[ \text{rcvd word:} \ 
\begin{align*}
(y-P(x)) \cdot (x-x_i) &= 0 \\
\begin{array}{c}
\text{D} \\
\text{-D}
\end{array}
\end{align*}
\]

Claim: Knowing \( E \Rightarrow \text{a polytime algo or decoding erasures is easy for RS codes} \) \((< N-K \text{erasures})\)

\[ \text{E} \rightarrow \text{set of error locations:} \]

\[ (y-P(x)) \prod_{x \in E} (x-x_i) = 0 \ (\text{for rcvd word}) \]

can do polynomial interpolation \( \Leftrightarrow \) know \( K \) codeword symbols \( \Leftrightarrow \)
\[ Q(x, y) = (y - P(x)) E(x) \]
\[ = y \underbrace{E(x) - P(x) E(x)}_{\text{deg } \leq e} \]
\[ \left\{ \begin{array}{l}
\text{deg } \leq e + k - 1
\end{array} \right\} \]

Read word is

\((x_i, y_i)\)

\[ \Rightarrow \forall i, Q(x_i, y_i) = 0 \]

\[ \Rightarrow Q(x, y) \text{ explains } (x_i, y_i) \]

i.e. \(1 \leq i \leq N, Q(x_i, y_i) = 0 \)

\[ \Rightarrow Q(x, y) = y \underbrace{A(x)}_{\text{deg } = e} + \underbrace{B(x)}_{\text{deg } \leq e + k - 1} \]

**IDEA**: Compute \(Q(xy)\) and show that degree constraints

\[ \Rightarrow (*) \text{ is the "only" solution to } Q(x, y) \]