REMINDERS

- HW 3 due on Th (11:59pm)
- Miniproject report due next Tue (11:59pm)
  - If you submit your report by Th (& let me know),
    I'll grade it / give feedback by the weekend.
  - Else I’ll grade it after due date.
- Please fill in mid-term course evals
- HW 2 has been graded

RECAP:

- BSC\(p\): each bit independently gets flipped with prob \(p\)
- Shannon's capacity thm \(\Rightarrow \) Capacity \(C = 1 - H(p)\)
  - \(1\): \(R < C \Rightarrow \) exp small decoding prob
  - \(2\): \(R > C \Rightarrow \) at least one message has dec. error prob \(> \frac{1}{2}\)

- Our proof only shows if general code \(\exists\) that achieves capacity
  - Q: Can linear codes achieve BSC\(p\) capacity?
    - A: Yes (Ex 6.4)

TODAY (Proof reader: Yichen)

- Hamming: Follow up Qs to Shannon’s result.
- Hamming vs. Shannon
  - Qualitative
  - Quantitative
- List decoding

Two issues with Shannon’s result (even with linear codes):
  - Codes are not “explicit”
  - Decoding time is exponential

Def: (Linear) code \(C\) is explicit if \(\exists\) a poly time algo to compute a generator matrix.
Def: Linear code is strongly explicit if given \((i,j)\in [k]\times[n]\), can compute \(G_{i,j}\) in poly(log\(n\)) time.
Q1: Can we get a (strongly) explicit construction of codes with poly time decoding + encoding that achieves BSCp capacity?

Q2: Above but with \( R > 0, \ p > 0 \)? (Ex. 6.13)

**Hamming vs. Shannon (Qualitative)**

<table>
<thead>
<tr>
<th>Hamming</th>
<th>Shannon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focuses on codewords</td>
<td>Directly deals w/ encoding + decoding</td>
</tr>
<tr>
<td>Explicit Codes</td>
<td>Not necessarily explicit at all</td>
</tr>
<tr>
<td>( R ) vs ( S )</td>
<td>( R ) vs &quot;error parameter&quot;</td>
</tr>
<tr>
<td>Worst-case errors</td>
<td>Memoryless stochastic errors</td>
</tr>
</tbody>
</table>

**Obs:** Code can handle \( (p\epsilon) \) - face of worst-case errors

\[ \Rightarrow \text{reliable communication over BSCp}. \]

By Chernoff bound, \[ \text{Prob} > (p\epsilon)n \text{ errors is } e^{-3\epsilon^2/n}. \]

Converse (Ex.??) \[ \exp \text{small decoding error prob w/ C} \]

\[ \Rightarrow C \text{ is rel distance } \Omega(1). \]

**Quantitative Hamming vs. Shannon (Large p)**

**Hamming:** \[ \leq \frac{1}{2} \text{ face of errors}. \]

\[ \Rightarrow p_{\text{min}} \leq \frac{1-R}{2}. \]

**Shannon:** \[ q_{\text{SCp}} \text{ Capacity } 1 - H_q(p). \]

It can be shown: \[ 1 - p - E \leq 1 - H_q(\frac{\epsilon}{q}) \leq 1 - p \]

\[ q > 2 \Rightarrow \epsilon \]

\[ \Rightarrow p_{\text{min}} \geq 1 - R - E \text{ is possible} \]

Can correct up to twice as many errors in Shannon's setting.
Volume of all Hamming balls = $2^k \text{ Vol}_2 \left( \frac{\delta n}{2}, n \right) \leq 2^k \cdot 2^{k - H(\delta) \cdot n}$

$\Rightarrow$ Empty space ratio \( \geq 1 - \frac{2^k \cdot 2^{k - H(\delta) \cdot n}}{2^k} = 1 - 2^{k - H(\delta) \cdot n}$

By Hamming bound
\[
R \leq 1 - H\left(\frac{\delta}{2}\right) \Rightarrow R = 1 - H\left(\frac{\delta}{2}\right) - \frac{2^n}{n} (1 - H(\delta))
\]

We know if
\[
(1) \text{ Deal w/ worst case errors } \Rightarrow \text{Shannon's setup: relax this!}
\]
\[
(2) \text{ Always output the transmitted message/codeword } \Rightarrow \text{ unique decoding}
\]

Next! relax this!
List decoding (N. Elias & Wozencraft late 50s)

Def: \(0 \leq \rho \leq 1\), \(L \geq 1\), \(C \subseteq \mathbb{F}_q^n\) is \(\mathbb{F}(\rho, L)\) list decodable

\[
\left| \{ \mathbf{c} \in \mathbb{F}_q^n \mid d_{\mathbb{F}_q}(\mathbf{c}, \mathbf{y}) \leq \rho \mathbf{y} \} \right| \leq L
\]

\[
\Rightarrow \left| \{ \mathbf{c} \in \mathbb{F}_q^n \mid \sum_{i=1}^n c_i \leq L \} \right| \leq L.
\]

If \(C\) has \(\delta\)-distance \(s\), \(C\) is \((< \frac{s}{2}, 1)\) list decodable

\[\Rightarrow (\delta, L)\)-Ld. \(C\) \Rightarrow for any transmitted codeword \(m\), if we have \(\leq \rho\) fraction of errors \(\Rightarrow\) combinatorially, \(m\) is in a list of size \(\leq L\)

Want: \(L\) to be \(\text{poly}(n)\).

What to do with lists of size \(\geq 1\):

- Declare an error.
  - \(L\) random errors w/ Hamming balls of radius \(s - \varepsilon\)
  - have \(\leq 1\) codeword (Sec 7.5)

- If \(\exists\) side information \(\Rightarrow \mathcal{O}(\log L)\) bits of information suffice!

Q3: Can we correct \(> \frac{1}{2}\) errors w/ list size \(\text{poly}(n)\)

Q4: What is the max frac of errors w/ Ld. & \(L = \text{poly}(n)\)