SESSION 3: BINNING SCHEMES & QIM

- Binning Schemes
- Basic Quantization Index Modulation (QIM)
- Distortion-Compensated QIM
- Sparse QIM
- Lattice QIM
- Minimum Distance Decoders
- Practical QIM Codes
Binning Schemes

- Fundamental information-theoretic technique (Marton’79)
- Application: encoding data with side info at transmitter only
  \[\Rightarrow\] blind data hiding
Example 1: binary length-3 sequence $S$

• Embed information in $S$, obtain $X$

• Distortion constraint: $S$ and $X$ differ at most by 1 bit
  $\Rightarrow S \oplus X \in \{000, 001, 010, 110\}$
  $\Rightarrow$ can embed at most 2 bits

• Spread Spectrum doesn’t work!

• Consider instead the following binning scheme:

<table>
<thead>
<tr>
<th></th>
<th>$m = 00$</th>
<th>$m = 01$</th>
<th>$m = 10$</th>
<th>$m = 11$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x =$</td>
<td>000</td>
<td>001</td>
<td>010</td>
<td>011</td>
</tr>
<tr>
<td></td>
<td>111</td>
<td>110</td>
<td>101</td>
<td>100</td>
</tr>
</tbody>
</table>

• Find $X$ closest to $S$ in column $m$  
  [try $S = 010$]

• Error-free decoding
Example 2: LSB Coding

- Consider $\mathcal{S} = \{0, 1, \cdots, 2^b - 1\}$, partition into two bins:
  
  \[ \mathcal{S}_e = \{0, 2, \cdots, 2^b - 2\}, \quad \mathcal{S}_o = \{1, 3, \cdots, 2^b - 1\} \]

- Binary sequence $s = \{s_1, s_2, \cdots, s_n\}$

- Distortion constraint: $|x_i - s_i| \leq 1$ for all $i$

- Embed binary sequence $m = \{m_1, m_2, \cdots, m_n\}$

- LSB code can be written as $x_i = m_i + 2 \left\lfloor \frac{s_i}{2} \right\rfloor$

  \[ \Rightarrow \ \text{choose} \begin{cases} 
  x_i \in \mathcal{S}_e & : \text{if } m_i = 0 \\
  x_i \in \mathcal{S}_o & : \text{if } m_i = 1
\end{cases} \]

  \[ \Rightarrow \ \text{view } \mathcal{S}_e \text{ and } \mathcal{S}_o \text{ as two bins} \]
Quantization Index Modulation

- Introduced by Chen and Wornell (1999)
- Embed signal-dependent patterns using quantization techniques
- Example: Dithered scalar quantization (1 bit):
  - Let \( m \in \{0, 1\} \) (1-bit message), \( s \in \mathbb{R} \) (1 sample), no key \( k \)
  - Two quantizers \( Q_0(s) \) and \( Q_1(s) \).
  - Define \( x(s, 0) = Q_0(s) \) and \( x(s, 1) = Q_1(s) \)
  - Embedding Distortion \( \approx \frac{\Delta^2}{12} \)
Minimum-Distance Decoder

\[
\begin{align*}
\Lambda_0 &= -\frac{\Delta}{4} + \Delta \mathbb{Z} : \text{circles} \\
\Lambda_1 &= \frac{\Delta}{4} + \Delta \mathbb{Z} : \text{crosses}
\end{align*}
\]

- Two lattices:
- Attack: \( y = x + w \)
- Decoder finds closest quantizer point and obtains
  \[
  \hat{m} = \arg\min_{m\in\{0,1\}} \text{dist}(y, \Lambda_m)
  \]
- No decoding error if \( |w| < \Delta/4 \)
- Binning scheme with noise protection
Distortion-compensated QIM

\[
X = \begin{cases} 
Q_0(\alpha S') + (1 - \alpha)S & : m = 0 \\
Q_1(\alpha S') + (1 - \alpha)S & : m = 1 
\end{cases}
\]

\[
= \begin{cases} 
S + (Q_0(\alpha S') - \alpha S) & : m = 0 \\
S + (Q_1(\alpha S') - \alpha S) & : m = 1 
\end{cases}
\]

Prototype \(X_{sym}(s)\)  \(m = 0\)  \(m = 1\)
Sparse QIM (Project & Quantize)

- Choose random unit vector $p \in \mathbb{R}^L$

$$x = \begin{cases} 
    s + (Q_0(s^T p) - s^T p) p & : m = 0 \\
    s + (Q_1(s^T p) - s^T p) p & : m = 1 
\end{cases}$$

- Decoder: $\hat{m} = \text{argmin}_{m \in \{0, 1\}} \text{dist}(y^T p, \Lambda_m)$
- Distance between $\Lambda_0$ and $\Lambda_1$ is $d_{\text{min}} = \frac{\Delta}{2} = \sqrt{3LD_e}$
- Can also use distortion compensation
Lattice QIM

Example: embed 1 bit in cubic lattice: \( m \in \{0, 1\}, \ s \in \mathbb{R}^L \)

- Distance between \( \Lambda_0 \) and \( \Lambda_1 \) is \( d_{\min} = \frac{1}{2} \Delta \sqrt{L} = \sqrt{3LD_e} \)
- Decoder implements \( \hat{m} = \text{argmin}_{m \in \{0, 1\}} \text{dist}(y, \Lambda_m) \)
General Principles

- Minimum distance of lattice code is $d_{\text{min}} = O(\Delta \sqrt{L})$
- Rate of code is $R = 1/L$
- Robustness to noise increases with $\Delta \sqrt{L}/\sigma_w$
- Embedding distortion increases with $\Delta$
- $\Delta$ determines tradeoff between robustness and fidelity
- $\alpha$ determines tradeoff between quantization noise and attack noise at receiver (see later why)
General Construction of Lattice QIM Codes

- Use nested codes
- Define
  \[ \Lambda / \Lambda' = L\text{-dimensional lattice partition} \]
  \( (\Lambda = \text{fine lattice}, \Lambda' = \text{coarse lattice}) \)
  \[ Q : \mathbb{R}^L \to \Lambda' = \text{quantization function} \]
  \[ \mathcal{V} = \{x \in \mathbb{R}^N : Q(x) = 0\} = \text{Voronoi cell of } \Lambda' \]
  \[ \mathcal{C} = \text{quotient } \Lambda / \Lambda' \]
  \[ \Lambda_m = c_m + \Lambda' = \text{coarse lattice translated by } c_m \in \mathcal{C} \]
Example, Revisited

\[ \Lambda' = \Delta \mathbb{Z}^L \]
\[ \Lambda = D_L^+ = \Delta \mathbb{Z}^L \cup \left( \frac{\Delta}{2}, \cdots, \frac{\Delta}{2} \right) + \Delta \mathbb{Z}^L \]
\[ C = \{ (0, \cdots, 0), \left( \frac{\Delta}{2}, \cdots, \frac{\Delta}{2} \right) \} \]
\[ \mathcal{V} = \left[ -\frac{\Delta}{2}, \frac{\Delta}{2} \right]^L \Rightarrow D_e = \frac{\Delta^2}{12} \]
General Principles

- Assume large number of messages

- $Q$ should be a good vector quantizer with m.s. distortion $D_1$
  \[ \Rightarrow \quad \mathcal{V} \sim \text{“nearly spherical”} \]

- $\mathcal{C}$ should be a good channel code w.r.t. Gaussian noise
  \[ \Rightarrow \quad \text{codewords in } \mathcal{C} \text{ are “far apart”} \]

**Encoder:** outputs $x = (1 - \alpha)s + Q_m(\alpha s - c_m) + c_m$

**Decoder:** outputs $\hat{m} = \arg\min_{m \in \mathcal{M}} \text{dist}(\alpha y, \Lambda_m)$
 Practical Codes

• In practice, cannot afford arbitrary high-dim. lattices

• Use lattices with special structure:
  – product of low-dimensional lattices
  – trellis-coded scalar quantization
  – classical error correcting codes (Hamming, turbo, etc.)