

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 \mathbf{S}

- Embed information in \mathbf{S} , obtain \mathbf{X}
- Distortion constraint: \mathbf{S} and \mathbf{X} differ at most by 1 bit
 $\Rightarrow \mathbf{S} \oplus \mathbf{X} \in \{000, 001, 010, 110\}$
 \Rightarrow can embed at most 2 bits
- Consider the following binning scheme:

	$m = 00$	$m = 01$	$m = 10$	$m = 11$
$\mathbf{x} =$	000	001	010	011
	111	110	101	100

- Find \mathbf{X} closest to \mathbf{S} in column m [try $\mathbf{S} = 010$]
- Error-free decoding

Example 2: LSB Coding

- Consider $\mathcal{S} = \{0, 1, \dots, 2^b - 1\}$, partition into two bins:

$$\mathcal{S}_e = \{0, 2, \dots, 2^b - 2\}, \quad \mathcal{S}_o = \{1, 3, \dots, 2^b - 1\}$$

- Binary sequence $\mathbf{s} = \{s_1, s_2, \dots, s_n\}$
- Distortion constraint: $|x_i - s_i| \leq 1$ for all i
- Embed binary sequence $m = \{m_1, m_2, \dots, m_n\}$

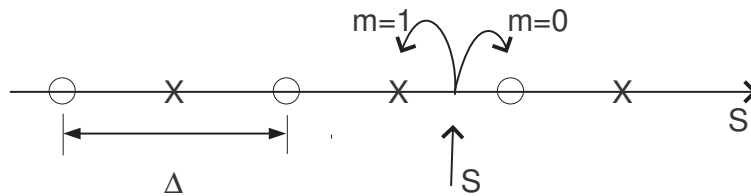
- LSB code can be written as $x_i = m_i + 2 \lfloor \frac{s_i}{2} \rfloor$

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

\Rightarrow view \mathcal{S}_e and \mathcal{S}_o as two bins

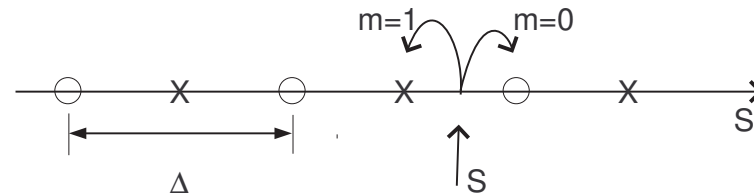
Quantization Index Modulation

- Introduced by Willems (1988) and 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

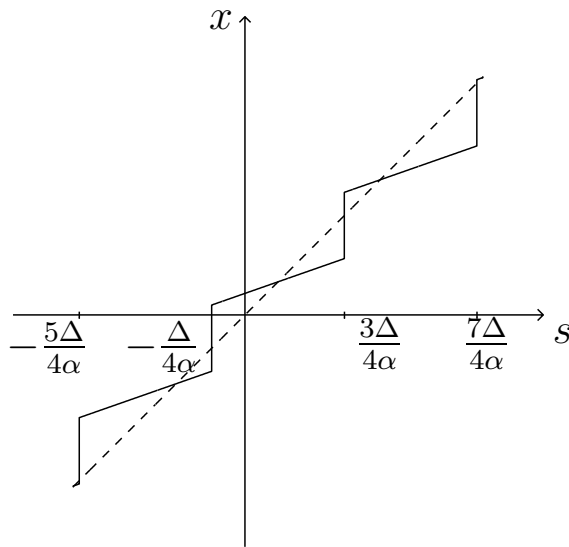


- Two lattices:
$$\begin{cases} \Lambda_0 = -\frac{\Delta}{4} + \Delta\mathbb{Z} & : \text{circles} \\ \Lambda_1 = \frac{\Delta}{4} + \Delta\mathbb{Z} & : \text{crosses} \end{cases}$$
- Attack: $y = x + w$
- Decoder finds closest quantizer point and obtains

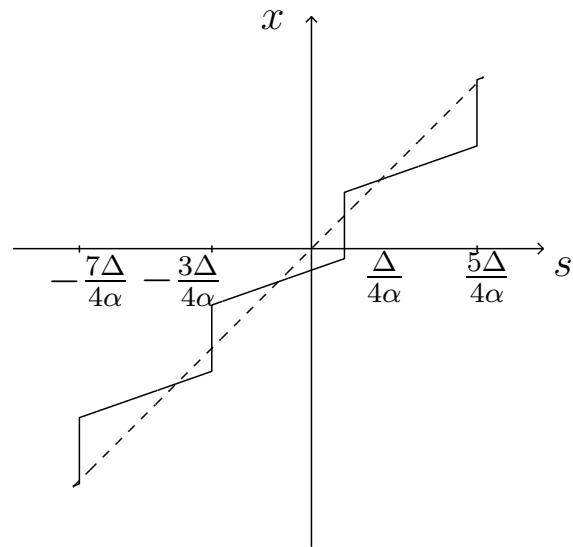
$$\hat{m} = \operatorname{argmin}_{m \in \{0,1\}} \operatorname{dist}(y, \Lambda_m)$$
- No decoding error if $|w| < \Delta/4$
- Binning scheme with noise protection

Distortion-compensated QIM

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



$m = 0$

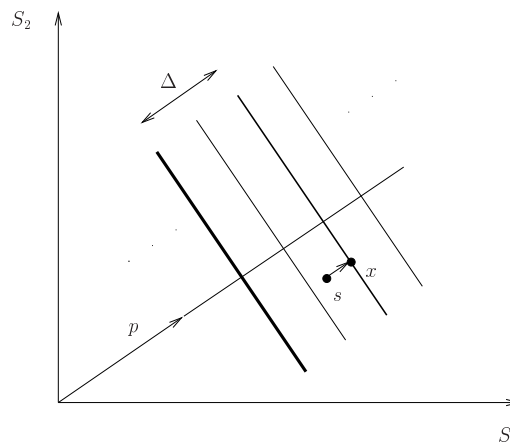


$m = 1$

Sparse QIM (Project & Quantize)

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

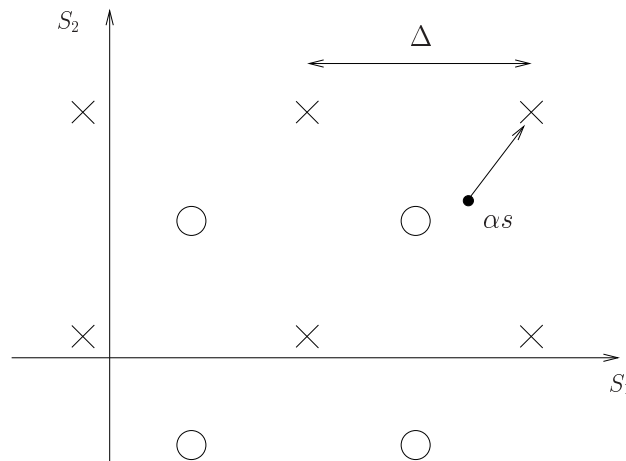
$$\mathbf{x} = \begin{cases} \mathbf{s} + (Q_0(\mathbf{s} \cdot \mathbf{p}) - \mathbf{s} \cdot \mathbf{p}) \mathbf{p} : m = 0 \\ \mathbf{s} + (Q_1(\mathbf{s} \cdot \mathbf{p}) - \mathbf{s} \cdot \mathbf{p}) \mathbf{p} : m = 1 \end{cases}$$



- Decoder: $\hat{m} = \operatorname{argmin}_{m \in \{0,1\}} \operatorname{dist}(\mathbf{y} \cdot \mathbf{p}, \Lambda_m)$
- Distance between Λ_0 and Λ_1 is $d_{\min} = \frac{\Delta}{2} = \sqrt{3LD_e}$

Lattice QIM

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



- Distance between Λ_0 and Λ_1 is $d_{\min} = \frac{1}{2}\Delta\sqrt{L} = \sqrt{3LD_e}$
- Decoder implements

$$\hat{m} = \operatorname{argmin}_{m \in \{0,1\}} \operatorname{dist}(\mathbf{y}, \Lambda_m)$$

General Principles

- Embedding r.m.s. distortion is proportional to Δ
- Rate of code is $R = 1/L$
- Minimum distance of lattice code is $d_{\min} = O(\Delta\sqrt{L})$
- Robustness to noise increases with d_{\min}/σ_w
- Δ determines tradeoff between robustness and fidelity
- α determines tradeoff between quantization noise and attack noise at receiver (see later why)

General Construction of Lattice QIM Codes

- Use *nested codes*

- Define

Λ/Λ' = L -dimensional *lattice partition*

($\Lambda =$ *fine* lattice, $\Lambda' =$ *coarse* lattice)

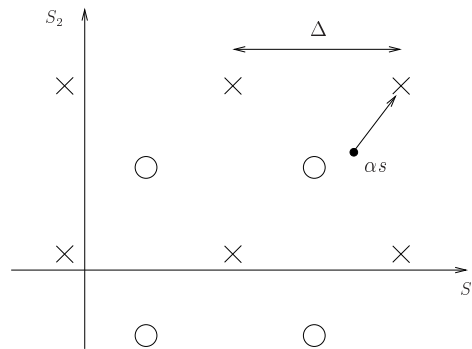
$Q : \mathbb{R}^L \rightarrow \Lambda'$ = quantization function

\mathcal{V} = $\{\mathbf{x} \in \mathbb{R}^L : Q(\mathbf{x}) = 0\}$ = Voronoi cell of Λ'

\mathcal{C} = quotient Λ/Λ'

$\Lambda_m = \mathbf{d}_m + \Lambda'$ = coarse lattice translated by $\mathbf{d}_m \in \mathcal{C}$

Example, Revisited



$$\Lambda' = \Delta \mathbb{Z}^L$$

$$\Lambda = D_L^+ = \Delta \mathbb{Z}^L \cup \left(\frac{\Delta}{2}, \dots, \frac{\Delta}{2} \right) + \Delta \mathbb{Z}^L$$

$$\mathcal{C} = \left\{ (0, \dots, 0), \left(\frac{\Delta}{2}, \dots, \frac{\Delta}{2} \right) \right\}$$

$$\mathcal{V} = \left[-\frac{\Delta}{2}, \frac{\Delta}{2} \right]^L \Rightarrow D_e = \frac{\Delta^2}{12}$$

General Principles

- Assume $R > 0$
- Q should be a *good vector quantizer* with m.s. distortion D_1
 $\Rightarrow \mathcal{V} \sim$ “nearly spherical”
- \mathcal{C} should be a *good channel code* w.r.t. Gaussian noise
 \Rightarrow codewords in \mathcal{C} are “far apart”

Encoder: outputs $\mathbf{x} = (1 - \alpha)\mathbf{s} + Q_m(\alpha\mathbf{s} - \mathbf{d}_m) + \mathbf{d}_m$

Decoder: outputs $\hat{m} = \operatorname{argmin}_{m \in \mathcal{M}} \operatorname{dist}(\alpha\mathbf{y}, \Lambda_m)$

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.)

