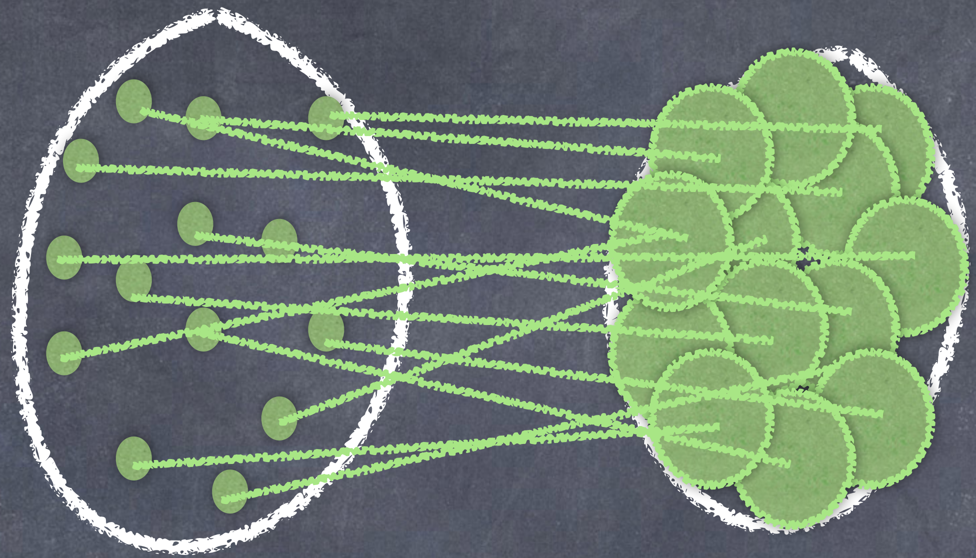
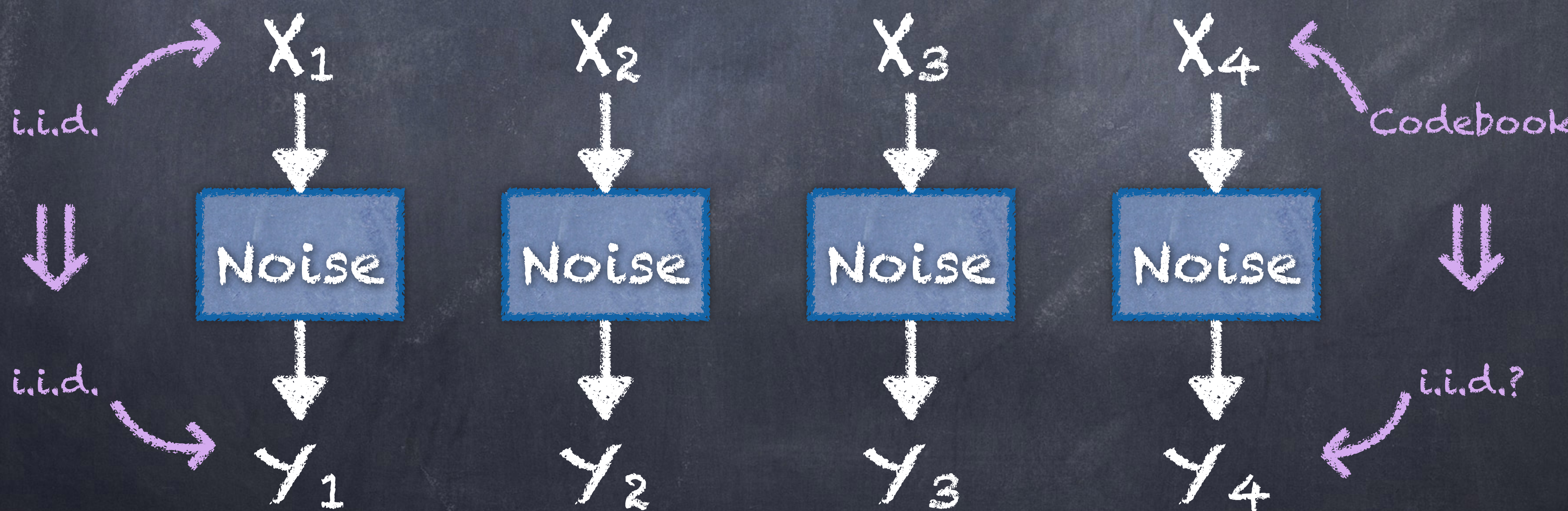


Soft-Covering Exponent

Paul Cuff and Semih Yagli

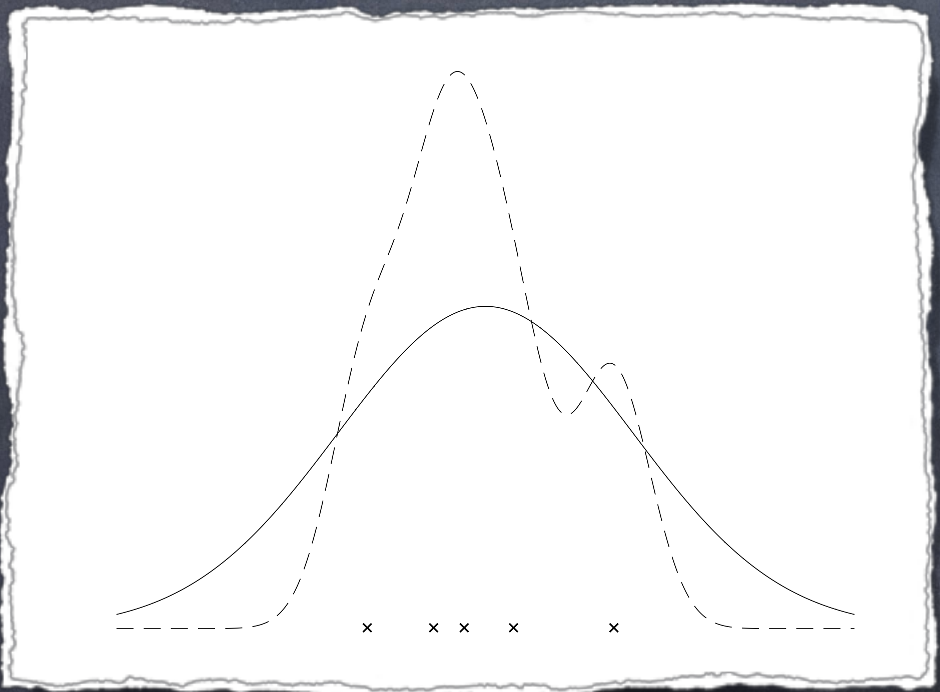
Soft Covering

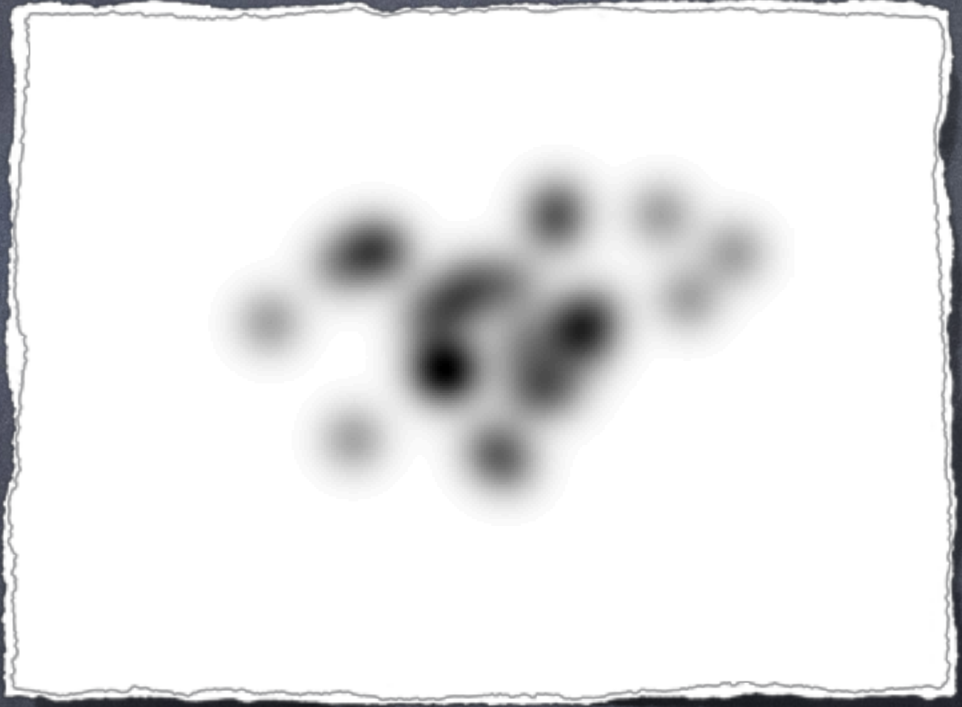
- Opposite of Reliable Decoding
- What happens when rate is too high?



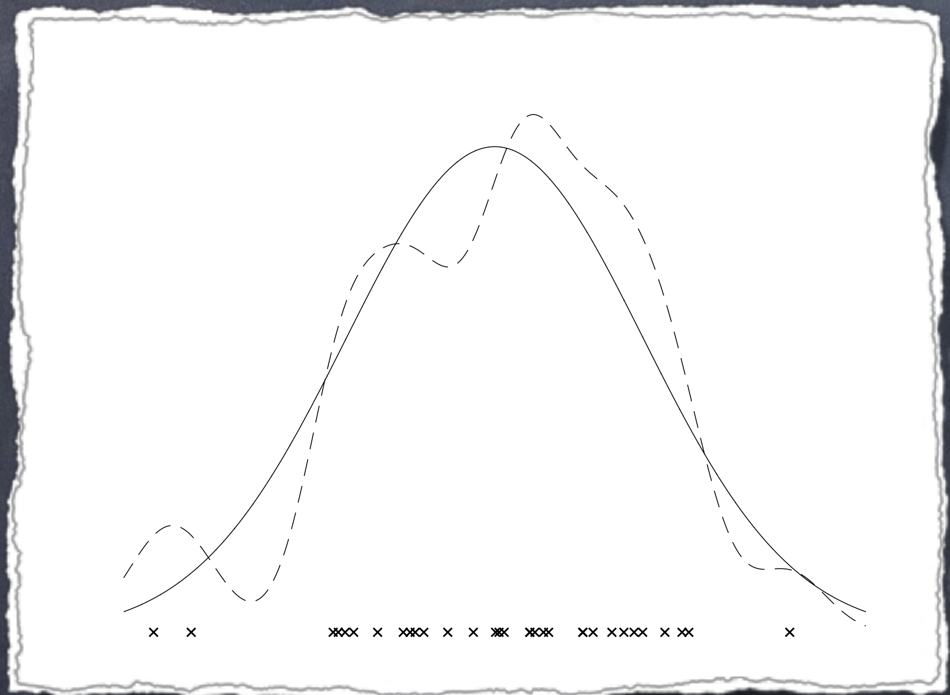
Output Distribution

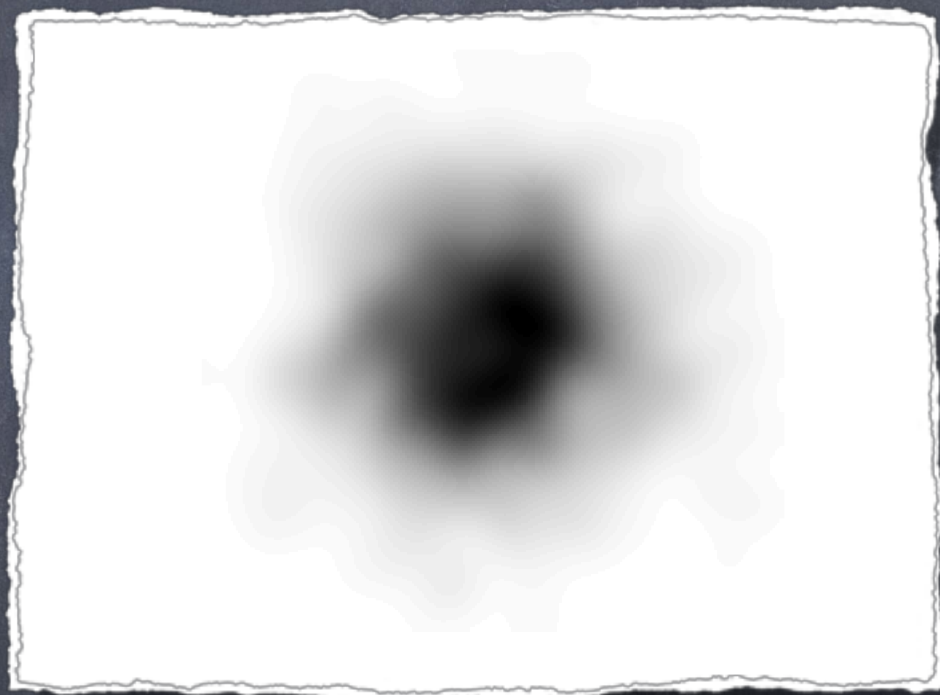
Gaussian Example





Gaussian Example





Soft Covering (origin)

- Theorem 6.3 of Wyner's Common Information Paper
- $R > I(X;Y)$ produces the phenomenon

Various Names

- Covering [Ahlswede, Winter, Wilde]
- Sampling Lemma [Winter]
- Resolvability [Han, Verdu]
- Cloud Mixing

Applications

- Security and Privacy
  - e.g. wiretap channel
- Encoder analysis
- Common Information

Main Result

For any $R > I(P_X, P_{Y|X})$,

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathbb{E}\left[\left\|P_{Y^n|\mathscr{C}_M^n} - P_{Y^n}\right\|_1\right]$$
$$= \min_{Q_{XY}} \left\{ D(Q_{XY}\|P_{XY}) + \frac{1}{2}[R - D(Q_{XY}\|P_X Q_Y)]_+ \right\}$$
$$= \max_{\lambda\in[1,2]} \left\{ \frac{\lambda-1}{\lambda}\left(R - I_\lambda(P_X, P_{Y|X})\right)\right\},$$

$$I_\lambda(P_X, P_{Y|X}) = \frac{\lambda}{\lambda-1}\log \mathbb{E}\left[\mathbb{E}^{\frac{1}{\lambda}}\left[\exp(\lambda\, \imath_{X;Y}(X;\widetilde{Y}))\middle|\widetilde{Y}\right]\right]$$
$$= \frac{\lambda}{\lambda-1}\log \sum_{y\in\mathcal{Y}}\left(\sum_{x\in\mathcal{X}} P_X(x) P^{\lambda}_{Y|X}(y|x)\right)^{\frac{1}{\lambda}}$$

Previous lower bounds

- Notable bounds by Hayashi, Han, Verdu, Cuff
- Best previous:

$$= \max_{\lambda \geq 0} \max_{\lambda' \leq 1} \left\{ \frac{\lambda}{2\lambda + 1 - \lambda'} \left(R - (1-\lambda') D_{1+\lambda}(P_{XY} \| P_X P_Y) - \lambda' \widetilde{D}_{1+\lambda'}(P_{XY} \| P_X P_Y) \right) \right\},$$

TV vs KL-divergence

- Inspired by [Parizi, Telatar, Merhav 17]
- Solved exponent for KL-divergence

$$\lim_{n\to\infty} -\frac{1}{n}\log \mathbb{E}\left[D\left(P_{Y^n|\mathscr{C}_M^n}\middle\|P_{Y^n}\right)\right]$$

Features of TV

- Accepted standard for cryptography
- Tractable multi-stage encoder analysis
- Stronger concentration result

New Features of TV Proof

- "Typical set" approach is not optimal
- Poisson codebook size used in converse
- (Taylor expansion not possible for absolute value)

Equivalence

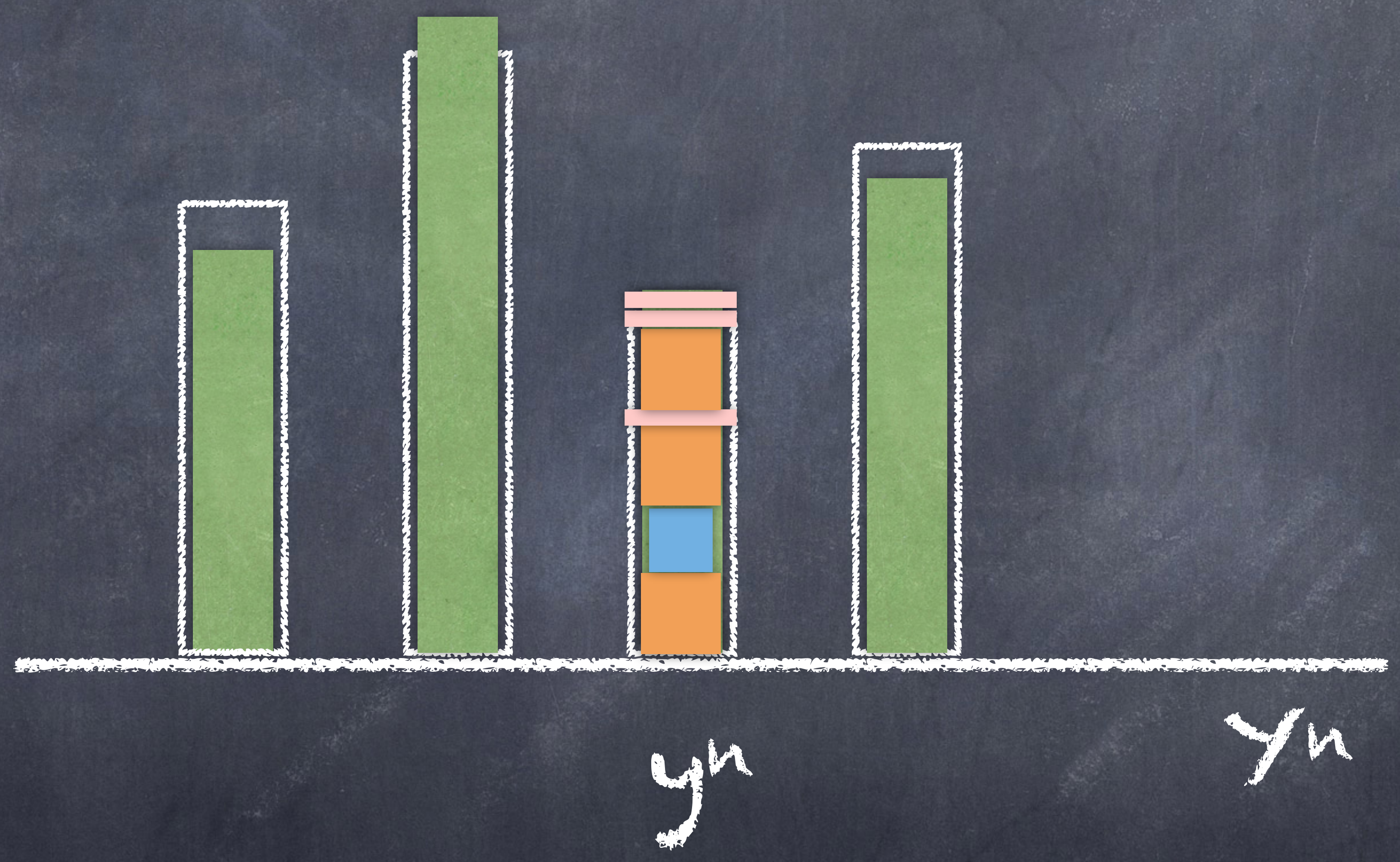
$$
\begin{aligned}
&\lim_{n\to\infty} -\frac{1}{n}\log \mathbb{E}\left[\left\|P_{Y^n|\mathscr{C}_M^n} - P_{Y^n}\right\|_1\right] \\
&\quad = \min_{Q_{XY}} \left\{ D(Q_{XY}\|P_{XY}) + \frac{1}{2}\left[R - D(Q_{XY}\|P_X Q_Y)\right]_+ \right\} \\
&\quad = \max_{\lambda\in[1,2]} \left\{ \frac{\lambda-1}{\lambda}\left(R - I_\lambda(P_X, P_{Y|X})\right) \right\},
\end{aligned}
$$

$$[R - D(Q_{XY}\|P_X Q_Y)]_+ = \max_{\lambda\in[0,1]} \lambda(R - D(Q_{XY}\|P_X Q_Y))$$

- Carefully swap min's and max's
- Massage

Proof of Error Upper Bound

Illustration of codebook approximation



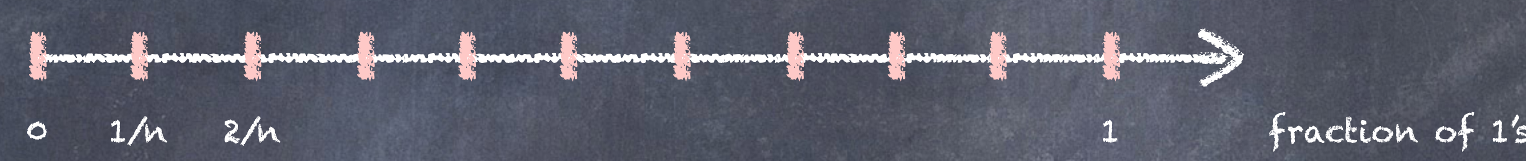
Conditional Type

y^n	0	0	0	0	1	0	0	0
x^n	0	1	0	1	1	1	0	1
	1	1	1	1	1	0	0	0

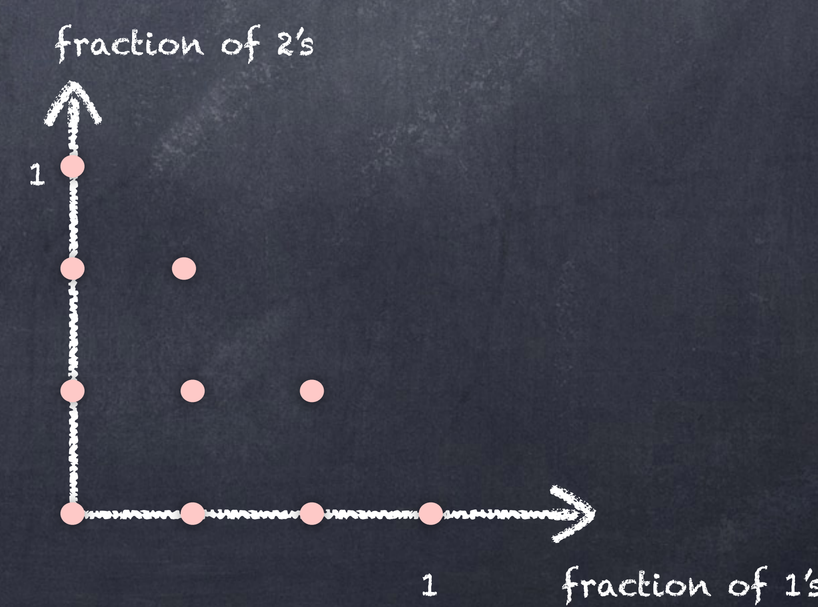
same conditional type

Polynomial Number of Types

Length-n binary types



Length-n ternary types



Key Quantities

$$L_{\mathscr{C}_M^n}(y^n) = \begin{cases} \dfrac{P_{Y^n|\mathscr{C}_M^n}(y^n)}{P_{Y^n}(y^n)} & \text{if } P_{Y^n}(y^n) > 0, \\ 1 & \text{otherwise.} \end{cases}$$

$$= \begin{cases} \dfrac{1}{M}\displaystyle\sum_{j=1}^{M} \dfrac{P_{Y^n|X^n}(y^n|X_j^n)}{P_{Y^n}(y^n)} & \text{if } P_{Y^n}(y^n) > 0, \\ 1 & \text{otherwise.} \end{cases}$$

$$L_{\mathscr{C}_M^n}(y^n) = \frac{1}{M} \sum_{Q_{\bar{X}|\bar{Y}} \in \mathcal{P}_n(\mathcal{X}|Q_{\bar{Y}})} N_{Q_{\bar{X}|\bar{Y}}}(y^n) l_{Q_{\bar{X}|\bar{Y}}}(y^n),$$

$$N_{Q_{\bar{X}|\bar{Y}}}(y^n) = \left|\left\{X^n \in \mathscr{C}_M^n : X^n \in \mathcal{T}^n_{Q_{\bar{X}|\bar{Y}}}(y^n)\right\}\right|$$
$$= \sum_{X^n \in \mathscr{C}_M^n} 1\left\{X^n \in \mathcal{T}^n_{Q_{\bar{X}|\bar{Y}}}(y^n)\right\}$$

$$Z_{Q_{\bar{X}|\bar{Y}}}(y^n) = \frac{1}{M} N_{Q_{\bar{X}|\bar{Y}}}(y^n) l_{Q_{\bar{X}|\bar{Y}}}(y^n),$$

Bound each type in one of two ways

$$
\begin{aligned}
&\mathbb{E}\left[\left\|P_{Y^n|\mathscr{C}_M^n} - P_{Y^n}\right\|_1\right] \\
&\quad = \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n)\mathbb{E}\left[\left|L_{\mathscr{C}_M^n}(y^n) - 1\right|\right] \\
&\quad = \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n)\mathbb{E}\left[\left|\sum_{Q_{\bar{X}|\bar{Y}} \in \mathcal{P}_n(\mathcal{X}|Q_{\bar{Y}})} Z_{Q_{\bar{X}|\bar{Y}}}(y^n) - \mathbb{E}[Z_{Q_{\bar{X}|\bar{Y}}}(y^n)]\right|\right] \\
&\quad \leq \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n) \sum_{Q_{\bar{X}|\bar{Y}} \in \mathcal{P}_n(\mathcal{X}|Q_{\bar{Y}})} \mathbb{E}\left[\left|Z_{Q_{\bar{X}|\bar{Y}}}(y^n) - \mathbb{E}[Z_{Q_{\bar{X}|\bar{Y}}}(y^n)]\right|\right]
\end{aligned}
$$

Proof of Error Lower Bound

Poisson Trick

- Let the number of codewords M be Poisson distributed
- Take care of this assumption at the end

Another Look

$$
\begin{aligned}
&\mathbb{E}\left[\left\|P_{Y^n|\mathscr{C}_M^n} - P_{Y^n}\right\|_1\right] \\
&\quad = \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n)\mathbb{E}\left[\left|L_{\mathscr{C}_M^n}(y^n) - 1\right|\right] \\
&\quad = \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n)\mathbb{E}\left[\left|\sum_{Q_{\bar{X}|\bar{Y}} \in \mathcal{P}_n(\mathcal{X}|Q_{\bar{Y}})} Z_{Q_{\bar{X}|\bar{Y}}}(y^n) - \mathbb{E}[Z_{Q_{\bar{X}|\bar{Y}}}(y^n)]\right|\right] \\
&\quad \leq \sum_{y^n \in \mathcal{Y}^n} P_{Y^n}(y^n) \sum_{Q_{\bar{X}|\bar{Y}} \in \mathcal{P}_n(\mathcal{X}|Q_{\bar{Y}})} \mathbb{E}\left[\left|Z_{Q_{\bar{X}|\bar{Y}}}(y^n) - \mathbb{E}[Z_{Q_{\bar{X}|\bar{Y}}}(y^n)]\right|\right]
\end{aligned}
$$

$$
Z_{Q_{\bar{X}|\bar{Y}}}(y^n) = \frac{1}{M} N_{Q_{\bar{X}|\bar{Y}}}(y^n) l_{Q_{\bar{X}|\bar{Y}}}(y^n),
$$

Need independence for different types

A Simple Lemma

- $\{X_i\}$ independent
- $E[X_i]=0$

$$\mathbb{E}\left|\sum_i X_i\right| \geq \max_i \mathbb{E}\left|X_i\right|$$

Initial Details

$$
\begin{aligned}
(1+\delta)\mathbb{E}&\left[\left|P_{Y^n|\mathscr{C}_M^n}(y^n) - P_{Y^n}(y^n)\right|\right] \\
&\geq \frac{1}{\mu_n}\mathbb{E}\left[\left|MP_{Y^n|\mathscr{C}_M^n}(y^n) - \mu_n P_{Y^n}(y^n)\right|\right] \\
&\qquad - \frac{P_{Y^n}(y^n)}{\sqrt{\mu_n}} - a^{\mu_n}_{\delta-\frac{1}{\mu_n}}.
\end{aligned}
$$

Poisson to Fixed Codebook