Lecture 5: Reliable Communications

Scribe: 蕭晨豪、何星燁 Lecture Date: 3/29, 2017 Lecturer: I-Hsiang Wang

Outline

- Energy efficiency reliable communication via Orthogonal Codes
- Rate efficient reliable communication via Linear Block Codes
- Basic Coding Theory

Recap Last time, we introduced repetition code which has vanishing error probability. At the price of:

1. Vanishing Rate (Rate $\to 0$ as $n \to \infty$)
2. Unbounded energy per bit ($E_b \to \infty$ as $n \to \infty$)

Obviously, we can do better because repetition code is too simple minded.

1 Energy Efficient Reliable Communication

1.1 Orthogonal Codes

Select n orthogonal vectors in $\mathbb{R}^n$ and use this n vectors $\{\underline{a}_1, \underline{a}_2 ... \underline{a}_n\}$ as the constellation set
When the noise is iid Gaussian, WLOG we can choose $\underline{a}_i = \underline{e}_i \sqrt{E_s}$ where $\underline{e}_i$ is the i^{th} standard basis (because rotation doesn't effect the performance of the code)

Rate: $R = \dfrac{\log_2 n}{n}$ (bits/symbol time) $\to 0$ as $n \to \infty$
Energy per bit: $E_b = \dfrac{E_s}{\log_2 n}$

1.2 Probability of error (SER)

Because we have the same error event for $i = 1 \sim n$,

$$
\begin{aligned}
P_e^{(n)} &= Pr\{\hat{i} \neq 1 \,|\, i = 1\} \text{ (i is the selected index of the pulse)} \\
&= Pr\{\bigcup_{j=2}^{n} \{\hat{i} = j\} \,|\, i = 1\} \\
&\leq \sum_{j=2}^{n} Pr\{\hat{i} = j \,|\, i = 1\} \text{ (union bond, can be improved)} \\
&= \sum_{j=2}^{n} \mathbb{P}_2\{1 \to j\} \text{ (binary detection that misclassify } \underline{a}_1 \text{ to } \underline{a}_j) \\
&= \sum_{j=2}^{n} Q(\frac{\left\|\underline{a}_i - \underline{a}_j\right\|}{2\sigma}) \\
&= (n-1) \cdot Q(\frac{\sqrt{2E_s}}{2\sigma}) \\
&= (n-1) \cdot Q(\sqrt{\frac{E_s}{2\sigma^2}})
\end{aligned}
$$

$$\leq (n-1)\exp(-\frac{1}{4}\cdot\frac{E_s}{\sigma^2})$$
$$\leq n\cdot\exp(-\frac{1}{4}\cdot\frac{E_s}{\sigma^2})$$
$$\leq \exp(\ln n-\frac{1}{4}\cdot\frac{E_s}{\sigma^2})$$

Now we hope to find the relationship between n and E_s to have R.C.
$\ln n < \frac{1}{4}\frac{E_s}{\sigma^2} = \frac{1}{4\sigma^2}E_b\cdot\log_2 n \Leftrightarrow \frac{E_b}{\sigma^2} > 4\frac{\ln n}{\log_2 n} = 4\ln 2$
$\therefore$ Energy per bit $E_b = \frac{E_s}{\log_2 n} > (4\ln 2)\sigma^2$
Question: Is $4\ln 2$ the best constant?
Answer: No, using a smarter argument (tighter bound than union bound), we can show that the constant is $2\ln 2$ for orthogonal code.
Using Shannon's channel coding theorem, we can find that the constant $2\ln 2$ is optimal for this problem.

1.3 Shannon's Capacity Formula

$C = \frac{1}{2}\log(1+\frac{P}{\sigma^2})$, $P:$ power
If $R < C$, then there exist a code with rate R s.t. $P_e^{(n)} \to 0$ as $n\to\infty$ (R.C. is possible)
If $R > C$, then for all coding schemes with rate R, $P_e^{(n)} \to 1$ as $n\to\infty$ (R.C. is impossible)
We can use this result to compute the optimal rate efficiency and energy efficiency:

- Optimal Rate: $C = \frac{1}{2}\log_2(1+\frac{P}{\sigma^2})$
- Optimal (minimum) energy per bit:

$$R < \frac{1}{2}\log_2(1+\frac{P}{\sigma^2}) \Rightarrow 1+\frac{P}{\sigma^2} > 2^{2R} \Rightarrow P > (2^{2R}-1)\sigma^2$$

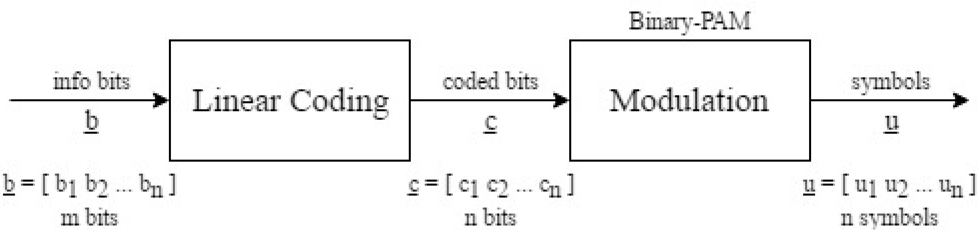
$$\text{energy per bit} = \frac{P(\text{energy per symbol time})}{R(\text{bits per symbol time})} = E_b(\text{energy per bit})$$

$$\Rightarrow E_b = \frac{P}{R} = \frac{1}{R}(2^{2R}-1)\cdot\sigma^2$$
$$\min E_b = \lim_{R\to 0}\frac{1}{R}(2^{2R}-1)\sigma^2 = 2\ln 2\cdot\sigma^2$$

2 Rate Efficient Reliable Communication

2.1 Linear Block Code

We use a simple architecture:



$\therefore$ Rate $R = \frac{m}{n}$
For encoding, we use Linear Block Code: $\underline{c} = \underline{b}\cdot G$, $G\in\{0,1\}^{m\times n}$, matrix with $\{0,1\}$ entries
(arithmetic in Binary Field $\mathbb{F}_2 = \{0,1\}$)
For decoding, we use maximum likelihood (ML) rule
$\underline{y} = \underline{u}+\underline{z}$, ML decoding: $\underline{y} \to \boxed{\text{ML}} \to \underline{z}$, likelihood function: $Pr\{\underline{y}\,|\,\underline{b}\}$
Below we show that "most" linear codes guarantees arbitrarily low pe with $R > 0$
The goal here is not constructing a explicit linear transformation G, we show the existence of G instead.

2.2 Probability of error analysis

How to pick G ? Total number of possible G is 2^{mn}
Step1: randomly choose G
$(G)_{ij} \overset{\text{iid.}}{\sim} Ber\big(\frac{1}{2}\big)$, $\forall (i,j) \in [m] \times [n]$
Step2: Compute the average-over-random-G performance
Consider a particular realization of $\mathbb{G}$, G, ε : error event
Probability of error when the codebook is G : $Pr\{\varepsilon \,|\, \mathbb{G} = G\}$
Let's compute the expected Prob. of error over random $\mathbb{G}$:

$$
\begin{aligned}
\mathbb{E}_{\mathbb{G}}[Pr\{\varepsilon \,|\, \mathbb{G}\}] &= \sum_{G \in \{0,1\}^{m\times n}} \big(\frac{1}{2}\big)^{mn} Pr\{\varepsilon \,|\, \mathbb{G} = G\} \\
&= \big(\frac{1}{2}\big)^{mn} \sum_{G \in \mathbb{F}_2^{m\times n}} \Big\{ \sum_{k=1}^{2^m} \frac{1}{2^m} Pr\{\varepsilon \,|\, \mathbb{G} = G,\, \underline{B} = \underline{b}_k\} \Big\} (\text{seperating the cases for different } \underline{b}_k)
\end{aligned}
$$

Noticed that

$$
\begin{aligned}
Pr\{\varepsilon \,|\, \mathbb{G} = G,\, \underline{B} = \underline{b}_k\} &= Pr\Big\{ \bigcup_{j \neq k} \{\hat{\underline{B}} = \underline{b}_j \,|\, \underline{B} = \underline{b}_k,\, \mathbb{G} = G\} \Big\} \\
&\leq \sum_{j\neq k} Pr\{\hat{\underline{B}} = \underline{b}_j \,|\ ,\underline{B} = \underline{b}_k,\, \mathbb{G} = G\} \text{ (union bond)} \\
&= \sum_{j\neq k} \mathbb{P}_2\{\underline{b}_k \to \underline{b}_j \,|\, \mathbb{G} = G\} \\
&= \sum_{j\neq k} Q\Big(\frac{\|\underline{u}_k - \underline{u}_j\|}{2\sigma}\Big) \\
&= \sum_{j\neq k} Q\Big(\frac{\sqrt{d(\underline{c}_k, \underline{c}_j)\cdot (2A)^2}}{2\sigma}\Big) (d(\underline{c}_k, \underline{c}_j) \text{ is the Hamming distance between } \underline{c}_k \text{ and } \underline{c}_j) \qquad (1) \\
&= \sum_{j\neq k} Q\Big(\frac{\sqrt{d(\underline{c}_k, \underline{c}_j)}}{\sigma} A\Big)
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\mathbb{E}_{\mathbb{G}}[Pr\{\varepsilon \,|\, \mathbb{G}\}] &\leq \big(\frac{1}{2}\big)^{mn} \big(\frac{1}{2}\big)^{m} \sum_{G \in \mathbb{F}_2^{m\times n}} \sum_{k=1}^{2^m} \sum_{j\neq k} Q\Big(\frac{A}{\sigma}\sqrt{d(\underline{c}_k, \underline{c}_j)}\Big) \text{ (implies } \mathbb{G} = G) \\
&= \big(\frac{1}{2}\big)^{m} \sum_{k=1}^{2^m} \sum_{j\neq k} \Big\{ \frac{1}{2^{mn}} \sum_{G \in \mathbb{F}_2^{m\times n}} Q\Big(\frac{A}{\sigma}\sqrt{d(\underline{c}_k, \underline{c}_j)}\Big) \Big\} \qquad (2) \\
&= \big(\frac{1}{2}\big)^{m} \sum_{k=1}^{2^m} \sum_{j\neq k} \Big\{ \sum_{d=1}^{n} f(d) Q\Big(\frac{A\sqrt{d}}{\sigma}\Big) \Big\} \qquad (3)
\end{aligned}
$$

$f(d)$ is the fraction of codebooks such that $d(\underline{c}_j, \underline{c}_k) = d$ $\big(\therefore f(d) = \binom{n}{d}\big(\frac{1}{2}\big)^n\big)$, so

$$
\begin{aligned}
\mathbb{E}_{\mathbb{G}}[Pr\{\varepsilon \,|\, \mathbb{G}\}] &= \big(\frac{1}{2}\big)^{m} \sum_{k=1}^{2^m} \sum_{j\neq k} \sum_{d=1}^{n} \big(\frac{1}{2}\big)^{n} \binom{n}{d} Q\Big(\frac{A\sqrt{d}}{\sigma}\Big) \\
&\leq \big(\frac{1}{2}\big)^{m} \sum_{k=1}^{2^m} \sum_{j\neq k} \Big(\big(\frac{1}{2}\big)^{n} \sum_{d=1}^{n} \binom{n}{d} e^{-\frac{1}{2}\frac{A^2}{\sigma^2}d} \Big) \\
&\leq \big(\frac{1}{2}\big)^{m} \big(\frac{1}{2}\big)^{n} \sum_{k=1}^{2^m} \sum_{j\neq k} \big(1 + e^{-\frac{1}{2}\frac{A^2}{\sigma^2}}\big)^n \qquad (4) \\
&\leq \big(\frac{1}{2}\big)^{m} \big(\frac{1}{2}\big)^{n} 2^m \cdot 2^m \big(1 + e^{-\frac{1}{2}\frac{A^2}{\sigma^2}}\big)^n
\end{aligned}
$$

$$= \left(\frac{1}{2}\right)^{n-m}\left(1+e^{-\frac{1}{2}\frac{A^2}{\sigma^2}}\right)^n$$
$$= 2^{n\left(\log_2(1+e^{-\frac{1}{2}\frac{A^2}{\sigma^2}})-1+R\right)}$$

A sufficient condition for $E_{\mathbb{G}}[Pr\{\varepsilon \,|\, \mathbb{G}=G\}] \to 0$ as $n \to \infty$ is :

$$R - 1 + \log_2(1+e^{-\frac{1}{2}\frac{A^2}{\sigma^2}}) < 0$$
$$\Leftrightarrow R < 1 - \log_2(1+e^{-\frac{1}{2}\frac{A^2}{\sigma^2}}) \text{ (assume } = R^*)$$
$$R^* > 0 \Rightarrow R^* \in (0,1)$$

(1) is because $\underline{u}_i$ is the modulated symbol (Binary-PAM here) of coded bits $\underline{c}_i$, so $\underline{u}_i \in \{A, -A\}$
(2) is by changing the order of summation
You can obtain (3) by separating the cases of different $d(\underline{c}_k, \underline{c}_j)$ in the curly brackets in (2)
(4) is due to the Binomial theorem, we add the $d=0$ term in it so it's an inequality

2.3 Conclusion

When we choose G randomly, we show that "on-average" $P_e \to 0$ as $n \to \infty$ as long as $R < R^*$
So when $R < R^*$, there must exist a particular G s.t. $P_e \to 0$ as $n \to \infty$
Now we find a coding scheme that satisfy:

1. Rate efficient: any $R < R^*$ is OK
2. Energy efficient: $E_b = \dfrac{A^2}{R^*}$ finite $\Rightarrow E_b \geq \lim\limits_{A\to 0} \dfrac{A^2}{1-\log_2\left(1+\exp(-\frac{1}{2}\frac{A^2}{\sigma^2})\right)} = (4\ln 2)\sigma^2$

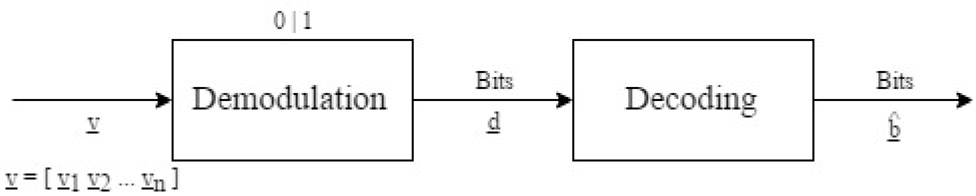
3 Hard Decision v.s. Soft Decision

So far, we see that linear block codes combined with very simple modulation(binary - PAM) is able to attain rate efficient and energy efficient reliable communication.
But issues are :

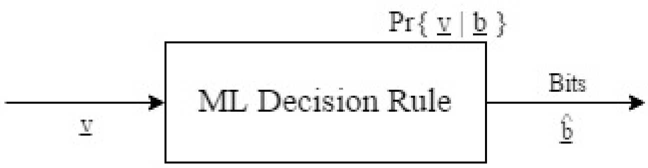
1. No explicit construction for G
2. Use ML rule for decoding is too costly in complexity($\Theta(e^n)$)

Actually, we need to have "structured" encoding and codebook so that low-complexity decoding is possible.

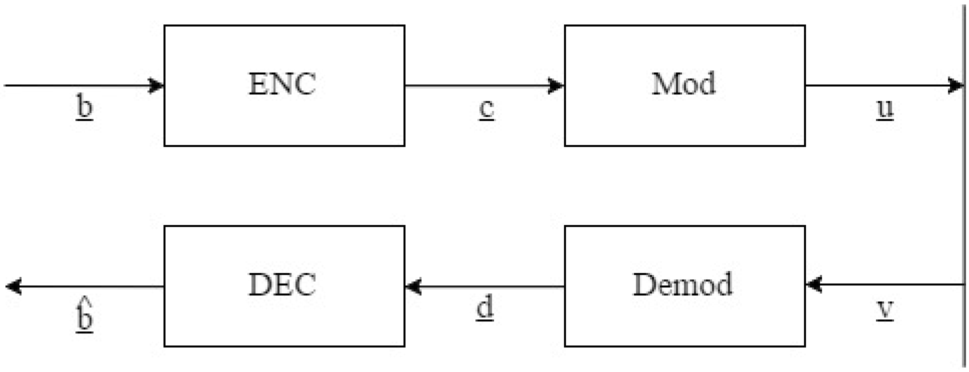
Can we do better if we first convert the received code symbols back to group of bits?
Hard Decision:



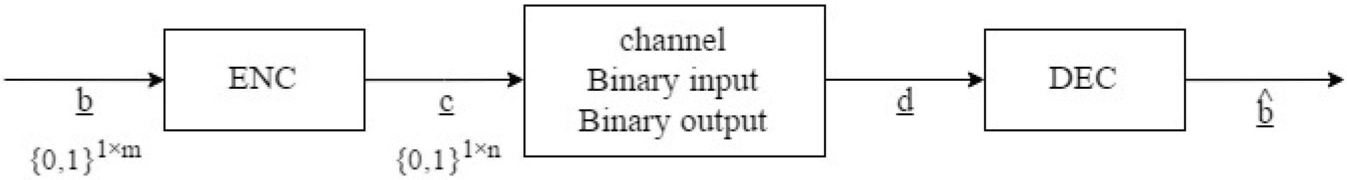
Soft Decision:



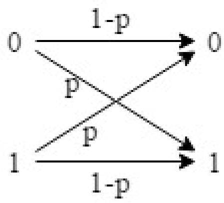
Recall the channel coding diagram:



Here is a equivalent channel:



In Lab 2, we have to characterize the end-to-end bit error rate p of this black box:



ML decoding under hard decision
Likelihood function:

$$Pr\{\underline{d}\,|\,\underline{c}\} = (1-p)^{n-d(\underline{c},\underline{d})} p^{d_H(\underline{c},\underline{d})} = (1-p)^n (\frac{p}{1-p})^{d_H(\underline{c},\underline{d})}$$

ML rule:

$$\underline{\hat{c}} = \arg\max_{\underline{c}\in C} (\frac{p}{1-p})^{d_H(\underline{c},\underline{d})} = \arg\min_{\underline{c}\in C} d_H(\underline{c},\underline{d})$$

Still, the decoding complexity is exponential.