COMPSCI 690T Coding Theory and Applications	April 24, 2017
Lecture 22	
Instructor: Arya Mazumdar	*Scribe: Names Redacted*

1 Review

We will take a brief look at what we have seen so far in the course:

There are broadly 2 types codes.

1. **Shannon Type**:
   - Deals with random errors in Binary Symmetric channel(BSC) or Binary Erasure Channel(BEC).
   - Weight distribution or distance distribution.
   - capacity of channels achieves vanishing error probability.
   - Polar Codes
2. **Hamming Type**:
   - Adverserial error or worst case error
   - strong connection with minimum distance of the code
   - List decodable codes. Random coding method to show the existance of such code
   - Bound on those codes
   - BCH codes , Hamming codes , Reed Muller codes (Binary codes achieving Plotkin bound), Reed Solomon codes (Singleton Bounds)

There are some codes that perform well in both cases like LDPC codes, Expander codes.

Applications of Coding Theory:

1. Sparse recovery:
   - Group Testing
   - Compressed Sensing
2. Security:
   - Secret Sharing
   - Wiretap Channel
3. Distributed Storage -locally repairable codes, Turan's theorem

2 Polar Codes

2.1 Introduction

We want to construct error correcting codes that achieve the capacity of the binary symmetric channel.
Let W be a binary-input discrete channel $W : \{0,1\} \to \mathcal{Y}$.
Consider code $C \in \{0,1\}^n$ with rate R and decoder $g : \mathcal{Y}^n \to C$.
Define the error probability as:

$$P_e^n = \frac{1}{|C|} \sum_{x \in C} P(g(y) \neq x)$$

Note that, we want as $n \to \infty$, $P_e^n \to 0$.

A sequence of codes C_n, $n \geq 1$ is said to attain the transmission rate $I(W)$ on the channel W if for any $\epsilon > 0$ there exists a sufficiently large n_0 such that for all $n \geq n_0$ both $R > I(W) - \epsilon$ and $P_e(C_n) \leq \epsilon$.
Define the capacity of a channel as:

$$\max_{P_e^n \to 0} \frac{\log |C|}{n}$$

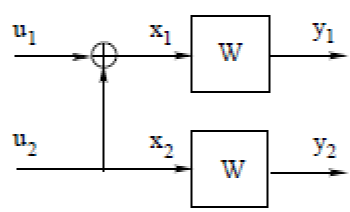
For a binary symmetric channel with parameter p, capacity of the channel is equal to $1 - h(p) \equiv I(p)$.

2.2 Polar Codes on BSC Channel

If u comes from $\text{Ber}(\frac{1}{2})$ distribution, then $I(U;Y) = 1 - h(p)$.
Consider transmitting binary digits u_1, u_2 in two uses of the channel W. The combined channel can be written as $W^2(y_1^2|u_1^2)$, where $y_1^2 = (y_1, y_2)$, $u_1^2 = (u_1, u_2)$. Of course,

$$W^2(y_1^2|u_1^2) = W(y_1|u_1)W(y_2|u_2)$$

and the capacity of the channel is $2I(p) = 2(1 - h(p))$.
Now consider the following channel,



$$\begin{aligned}
2I(p) &= I(Y_1, Y_2; U_1, U_2) \\
&= I(Y_1, Y_2; U_1) + I(Y_1, Y_2; U_2|U_1) \\
&= I(Y_1, Y_2; U_1) + H(U_2|U_1) - H(U_2|Y_1, Y_2, U_1) \\
&= I(Y_1, Y_2; U_1) + H(U_2) - H(U_2|Y_1, Y_2, U_1) \\
&= I(Y_1, Y_2; U_1) + I(Y_1, Y_2, U_1; U_2)
\end{aligned} \tag{1}$$

Note that:

$$I(Y_1, Y_2; U_1) \leq I(p)$$

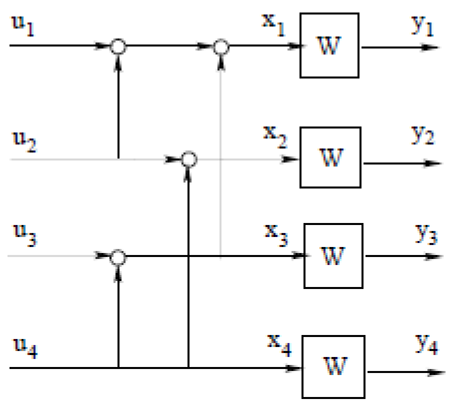
because,

$$\begin{aligned} I(Y_1, Y_2, U_1; U_2) &= H(U_2) - H(U_2|Y_1, Y_2, U_1) \\ &\geq H(U_2) - H(U_2|Y_2) \\ &= I(Y_2; U_2) \\ &= I(p) \end{aligned} \tag{2}$$

From (2), (3) we obtain,

$$I(Y_1, Y_2; U_1) \leq I(p) \leq I(Y_1, Y_2, U_1; U_2)$$

The following figure shows a channel with m = 4,



After m steps of the above recursion we obtain a collection of 2^m channels. We randomly pick one of these channels and denote its capacity by I_m. In this part we establish convergence properties of the random process I_m. The sequence of random variables I_m converges almost surely to a Bernoulli 0-1-valued random variable I_∞ such that:

$$I_\infty = \begin{cases} 1 & \text{w.p. } 1 - h(p) \\ 0 & \text{w.p. } h(p) \end{cases} \tag{3}$$

or equivalently,

$$\begin{gathered} Pr[I_\infty \geq 1 - \epsilon] = 1 - h(p) \\ Pr[I_\infty \leq \epsilon] = h(p) \end{gathered} \tag{4}$$

This theorem implies that in the "polarization limit," the channels for bits $u_1, \cdots, u_n$ become either *noiseless* (with probability $1 - h(p)$) or fully random (with probability $h(p)$). The polarization effect defines a subset $A \subset \{1, 2, \cdots, n\}$ of coordinates where the data is carried over the channel with no errors, and the number of these coordinates is $|A| = n(1 - h(p))$.

3 Finite Field Extension: BCH Codes

Take $[7, 4, 3]$ Hamming code which can correct 1 erasure. Parity check matrix is

$$\begin{matrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

To correct 2 errors we need to use finite field extension.

How to construct $\mathbb{F}_8$ form $\mathbb{F}_2$?
We need a 3^{rd} order irreducible polynomial $x^3 + x + 1$. If α is solution then $\alpha^3 + \alpha + 1 = 0$

Power Representation	0	1	α	α^2	α^3	α^4	α^5	α^6
Polynomial Representation	0	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$
Vector Representation	$[0, 0, 0]$	$[0, 0, 1]$	$[0, 1, 0]$	$[1, 0, 0]$	$[0, 1, 1]$	$[1, 1, 0]$	$[1, 1, 1]$	$[1, 0, 1]$

Parity check matrix (with arranging the column)

$$\begin{matrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \end{matrix}$$

This parity check matrix can correct 2 errors. If there are are 2 errors occurring in position i and j then from syndrome decoding

$$\begin{aligned} i + j &= s_1 && (5) \\ i^3 + j^3 &= s_2 && (6) \\ \Rightarrow (i + j)(i^2 + j^2 + ij) &= s_2 \\ s_1(s_1^2 + ij) &= s_2 \\ ij &= \frac{s_2}{s_1} - s_1^2 && (7) \end{aligned}$$

By solving for the above equations, we can correct 2 errors. This is a 2 error correcting BCH codes. For a t error-correcting the BCH code, the length is $2^m - 1$ the dimension is $2^m - 1 - mt$ and minimum distance $\geq 2t + 1$. The code can be similarly constructed by adding zeros.