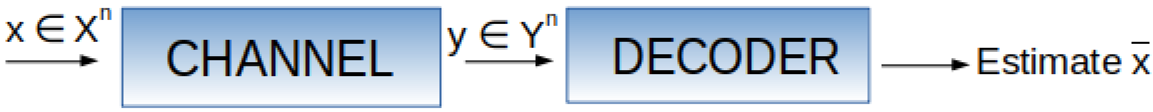
IIIT Hyderabad | **Scribed By: K Raghuchandra(20161305)**
Introduction to Coding Theory | **Lecture #2**
Instructor: Dr. Prasad Krishnan | **07.01.2020**

---

1 Decoder



Decoder converts transmitted vector on the channel to message vector.At the decode we assume that the *priory probability* $P\left(x\right)$ and *likelihood* $P\left(y|x\right)$ are known.

1.1 Probabilistic Relation between Input and Output of the Channel

We want to design a decoder to predict the message with the least average probability of error.

$$P_c \implies Probability\ of\ correctness\ \&\ P_e \implies Probability\ of\ error$$
$$P_e = 1 - P_c$$

We map all the output to all inputs of the channel its a one to one map.

$$f : \mathbb{Y}^n \to \mathbb{X}^n$$

1.1.1 MAP Rule

We deduce decoder for maximum P_c .

$$\begin{aligned} P_c = \Pr[x = f(y)] &= \sum_{x,y\ \in\ \mathbb{X}^n \times \mathbb{Y}^n} P(x, y) \\ &= \sum_{y\ \in\ \mathbb{Y}^n} P(y)P(f(y)|y) \\ \implies f(y) = \arg\max_{x \in \mathbb{X}^n} P(x|y) & \qquad \text{(as we have to maximize } P_c\text{)} \qquad (1) \end{aligned}$$

The operator 'arg max' returns $x \in \mathbb{X}^n$ where the function has maximum value.The probability $P(x|y)$ is called the *a posterior probability*. The rule Eqn.1 is called the *maximum a posterior probability*(MAP) rule.

1.1.2 ML Rule

Eqn.1 can be modified into

$$\arg\max_{x\in\mathbb{X}^n} P(x|y) = \arg\max_{x\in\mathbb{X}^n} P(x)P(y|x)$$

.If P(x) is uniform Then equation becomes

$$\arg\max_{x\in\mathbb{X}^n} P(x|y) = \arg\max_{x\in\mathbb{X}^n} P(y|x) \tag{2}$$

This rule Eqn.2 is called *maximum likelihood*(ML) rule.

2 Worst case Error Model

It's for those with Both input and output vector of channel belong to same discrete alphabet $\mathbb{X}$.

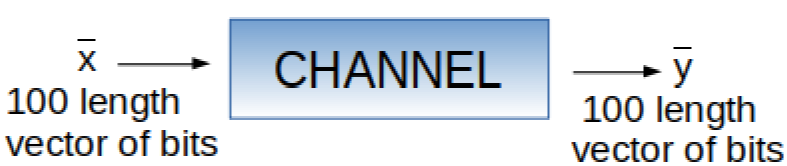
Definition 2.1. Hamming distance between two vectors $\overline{x}$, $\overline{y}$ $\in$ $\mathbb{X}^n$ is the number of coordinates these vectors differ.
Let $\overline{x} = (x_1, x_2, ..., x_n)$ & $\overline{y} = (y_1, y_2, ..., y_n)$ hamming distance($d_H(\overline{x}, \overline{y})$) is number places $\forall i \in [1, n]$ where $x_i \neq y_i$.

In this model we impose a condition that channel can't flip more than 't' coordinates of the input vector.

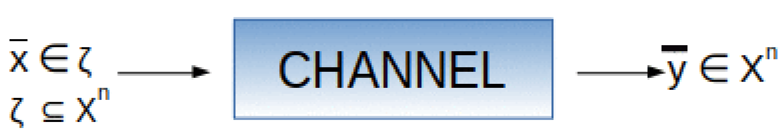
$$d_H(\overline{y}, \overline{x}) \leq t \tag{3}$$

$\overline{x}, \overline{y}$ are the input and output vectors of channel.We want to ensure that Decoder can estimate correct output given This condition 3.

Example 2.1. *Let $n = 100$,$\mathbb{X} = \{0,1\}$ and $t = 5$.*
So if we consider set of all possible 2^{100} 100-length sequences,We can't exactly find i/p sequence by



seeing the o/p sequence i.e We can't make unique decoding.So we choose a subset from 2^{100} sequence we choose such that decoding problem becomes unique decoding.This is part of 'Error control Codes'.



Definition 2.2. A **code** ζ is a subset of $\mathbb{X}^n$ with alphabet of the code is $\mathbb{X}$ and *length of the code* ζ is n.Elements of the code are called *code words.*

Example 2.2. *Let* $t = 1$ *, and* $\zeta = \{000, 011, 110, 101\}$ & $\mathbb{X} = \{0, 1\}$ *say* $y = 001$ *even now there is no unique decoding situation.*

3 Minimum Hamming Distance Decoder

Definition 3.1. Minimum Distance of a Code ζ is

$$d_{min} = \min_{c_1 \neq c_2 \ \forall c_1, c_2 \ \in \ \zeta} d_H(c_1, c_2)$$

.

Lemma 1. *A code* $\zeta \subseteq \mathbb{X}^n$ *can ensure error less correct decoding on a discrete channel with i/p,o/p alphabet* $\mathbb{X}$ *and worst case error up to* t *iff*

$$d_{min} \ \geq \ 2t + 1 \ \forall c_1, c_2 \in \zeta, \ \ c_1 \neq c_2$$

References

[1] class notes