1 How to build a finite field extension (in the context of Assignments)

1. Start with a finite field with prime number $q$ of elements. For example, in a 3-ary finite field, $F_3 = \{0, 1, 2\}$.

2. Find an irreducible polynomial of degree $t$ if you want a $t$th degree extension (to construct a field of size $q^t$). In $F_3$ an example is $p(x) = x^2 + 2x + 2$.

3. Let $\alpha$ be the root of $p(x)$. This implies that $x^2 + 2x + 2 = 0$, or equivalently, $\alpha^2 = -2\alpha - 2 = \alpha + 1$ in the above example.

4. $0$ and powers of $\alpha$ generates the field. For example, $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\}$ is $F_9$. So there is a polynomial representation corresponding to each exponential representation.

2 Fano’s inequality (continuing from last class)

Theorem Let $S$ be a random variable with finite sample space $|\Omega| = M$. Let $X$ be another random variable that is obtained from $S$ (such as $S$ transmitted through some channel). $\hat{S}$ is the estimator for $S$ that we derive from $X$ with a function $f$ such that $\hat{S} = f(X)$.

$S \rightarrow X \rightarrow \hat{S}$

Under this setup, the probability of error in estimating $S$ is lower bounded by:

$$P_e = P(\hat{S} \neq S) \leq \frac{H(S|\hat{S}) - 1}{\log(M - 1)}$$

3 Wiretap Channel

The wiretap channel is an information-theoretic model for communication in the presence of an eavesdropper. Suppose Alice wishes to communicate a message $S$ to Bob. However, Eve can eavesdrop on the channel between Alice and Bob, and Alice wishes to make sure that Eve cannot decode (or only partly decode) the message $S$. A discrete-memoryless wiretap channel is a broadcast channel with sender Alice, legitimate receiver Bob and eavesdropper Eve. Alice wishes to communicate at a rate $R$ to Bob while ensuring a given level equivocation for Eve.

$K$-bit $S$ $\xrightarrow{\text{encode}}$ $N$-bit $X$ $\xrightarrow{\text{decode}}$ $\hat{S}$

Alice \hspace{1cm} Eve sees $\mu$-bit $Z$ \hspace{1cm} Bob

Define:

$$P_e = P(S \neq \hat{S}) \quad \Delta = H(S|Z) \quad R = \text{Rate} = \frac{K}{N}$$

$$\alpha = \frac{\mu}{N} \quad \delta = \frac{\Delta}{N}$$
We are going to prove

\[ \Delta = \begin{cases} 
K & \text{when } \mu \leq N - K \\
KP_e + N - \mu & \text{when } \mu \geq N - K 
\end{cases} \]

i.e.

\[ \delta = \frac{\Delta}{K} \leq \begin{cases} 
1 & \text{when } \alpha \leq 1 - R \\
\frac{1}{P_e + \frac{1-\alpha}{P_e}} & \text{when } \mu \geq N - K 
\end{cases} \]

Proof:

\[ \Delta = H(S|Z) \]
\[ = H(S, Z) - H(Z) \]
\[ = H(S, X, Z) - H(X|S, Z) - H(Z) \]
\[ = H(S|X, Z) + H(X, Z) - H(Z) \]
\[ = H(S|X, Z, \hat{S}) + H(X|Z) \]

\[ \Delta \leq H(S|\hat{S}) + H(X|Z) \]
\[ = P_e \log(2^K - 1) + N - \mu \quad \text{(applied Fano’s inequality)} \]

\[ \frac{\Delta}{K} \leq P_e + \frac{N(1 - \frac{\mu}{K})}{P_e} = P_e + \frac{1-\alpha}{P_e}. \]

4 Data Compression

Suppose we have n bit sequence \( X \). \( X \in \{0, 1\}^n \).

We want to compress it into k bit sequence \( Y \)

\( Y \in \{0, 1\}^k \).

We want to recover the n bit sequence \( \hat{X} \) from the k bit sequence \( Y \) within allowed error

\[ X \rightarrow Y \rightarrow \hat{X} \]
We could have $2^k$ different $\hat{X}$. Let’s call that set which form a ensemble $\mathcal{M}$, $|\mathcal{M}| = 2^k$.

**Covering Code**: A code $\mathcal{M} \subseteq \{0, 1\}^n$ is called a covering code with covering radius $\delta n$ if $\forall x \in \{0, 1\}^n$, $\exists \hat{x} \in \mathcal{M}$ such that $d(x, \hat{x}) \leq \delta n$ where $d(\cdot, \cdot)$ is the Hamming distance.

Let us show a lower bound for the size of a covering code with covering radius $\delta n$. Let us define the rate of a covering code to be $R \equiv \lim_n \frac{\log |\mathcal{M}|}{n}$.

We must have

$$|\mathcal{M}| \sum_{i=0}^{\delta n} \binom{n}{i} \geq 2^n$$

which gives us,

$$R \geq 1 - h(\delta).$$