Final Exam

Information and Coding Theory

March 18, 2021 Clayton Seitz

Problem 0.1. *Chang's Lemma*

Solution. We first find the entropy of $\bar{X}$

$$H(\bar{X}) = H((X_1 \dots X_n) = \alpha \cdot 2^n \cdot H_2(p)$$

Next we show

$$\begin{aligned}
H(X_i) &= H_2(p) \\
&= H_2\left(\frac{1 + 2p - 1}{2}\right) \\
&= H_2\left(\frac{1 + \mathbb{E}[X_i]}{2}\right) \\
&\leq 1 - \frac{(\mathbb{E}[X_i])^2}{2\ln 2}
\end{aligned}$$

Now, we show that

$$\sum_{i \in [n]} H(X_i) \leq \sum_{x \in [n]} \left(1 - \frac{(\mathbb{E}[X_i])^2}{2\ln 2}\right)$$

when taking the maximum possible value for the LHS to be $n \log 2 + \log \alpha$, since we have a uniform distribution, we have

$$\begin{aligned}
\sum_{i \in [n]} \left((\mathbb{E}[X_i])^2\right) &\leq -2\ln 2 \cdot (n(\log 2 - 1) + \log \alpha) \\
&= -2\ln 2 \cdot \frac{\ln(\alpha)}{\ln 2} = 2 \cdot \ln \frac{1}{\alpha}
\end{aligned}$$

■

Problem 0.2. *q-ary Entropy and Counting Codes*

Solution. We would like to prove the following bounds on the size of Hamming ball of radius r centered at the origin

$$q^{H_q(\alpha)\cdot n - o(n))} \leq |B_q(\alpha \cdot n)| \leq q^{H_q(\alpha)\cdot n}$$

where we have

$$H_q(\alpha) = \alpha \cdot \log_q(q-1) - \alpha \cdot \log_q(\alpha) - (1-\alpha)\cdot \log_q(1-\alpha)$$

and therefore,

$$\begin{aligned} q^{H_q(\alpha)\cdot n} &= q^{\alpha n \cdot \log_q(q-1) - \alpha n \cdot \log_q(\alpha) - (1-\alpha) n \cdot \log_q(1-\alpha)} \\ &= (q-1)^r \cdot \alpha^{-r} \cdot (1-\alpha)^{r-n} \end{aligned}$$

First, we will show the upper bound by showing that $|B_q(\alpha \cdot n)|/q^{H_q(\alpha)\cdot n} \leq 1$

$$\begin{aligned} \frac{|B_q(r)|}{q^{H_q(r)}} &= \frac{\sum_{i=0}^{r} \binom{n}{i} (q-1)^i}{(q-1)^r \cdot \alpha^{-r} \cdot (1-\alpha)^{r-n}} \\ &= \sum_{i=0}^{r} \binom{n}{i} (q-1)^i (q-1)^{-r} \alpha^r (1-\alpha)^{n-r} \\ &= \sum_{i=0}^{r} \binom{n}{i} (q-1)^i (1-\alpha)^n \left(\frac{\alpha}{(q-1)(1-\alpha)} \right)^r \\ &\leq \sum_{i=0}^{r} \binom{n}{i} \alpha^i (1-\alpha)^{n-i} = 1 \end{aligned}$$

which can be seen from the condition $\alpha \leq 1 - \frac{1}{q}$. Also this last result is just the binomial distribution. The lower bound comes from the fact that

$$\begin{aligned} |B_q(r)| &\geq \binom{n}{r} (q-1)^r \\ &> \frac{(q-1)^r}{\alpha^r (1-\alpha)^{n-r}} \\ &\geq q^{H_q(\alpha)\cdot n - o(n))} \end{aligned}$$

Now we can show a q-ary Hamming bound

$$|C| \cdot |B_q(r)| \leq |\mathbb{F}_q^n|$$

We can find the maximum $|C|$ by using the lower bound on $|B_q(r)|$ that we derived above:

$$|C| \leq \frac{|\mathbb{F}_q^n|}{|B_q(r)|} = \frac{q^n}{q^{H_q(\alpha)\cdot n - o(n)}} = q^{n\cdot(1-H_q(\alpha))+o(n)}$$

■

Problem 0.3. *Correlated bad inputs*

Solution. We have that $\forall x$

$$\Pr_R[A(R,x) \neq f(x)] \leq \delta$$

Then it must be true that

$$\begin{aligned}\Pr_{R,X}[A(R,X) \neq f(x)] &= \sum_x P(x) \cdot \Pr_R[A(R,x) \neq f(x)] \\ &= \Pr_R[A(R,x) \neq f(x)] \leq \delta\end{aligned}$$

Now, we have

$$\begin{aligned}H(R|X,E) &= (1-p) \cdot H(R|X,E=0) + p \cdot H(R|X,E=1) \\ &\leq (1-p) \cdot H(R) + p \cdot H(R|X,E=1) \\ &= H(R) - p \cdot \log \frac{1}{\delta}\end{aligned}$$

Finally, we can rearrange this result to show that

$$\begin{aligned}p &= \Pr_{R,X}[A(R,X) \neq f(x)] \\ &\leq \frac{H(R) - H(R|X,E)}{\log \frac{1}{\delta}} \\ &= \frac{H(R) - (H(R|X) - H(E|R,X))}{\log \frac{1}{\delta}} \\ &\leq \frac{I(R;X) + 1}{\log \frac{1}{\delta}}\end{aligned}$$

$\blacksquare$

Problem 0.4. *Through two codes at once*

Solution.

If $C_1 \cap C_2$ is a linear code, then $x_1, x_2 \in C_1 \cap C_2$ requires that $x_1 + x_2 \in C_1 \cap C_2$

By the nature of the intersection, if $x_1, x_2 \in C_1$ then we also have $x_1, x_2 \in C_2$ and since C_1 and C_2 are linear, $x_1 + x_2 \in C_1$ and $x_1 + x_2 \in C_2$ which means $x_1 + x_2 \in C_1 \cap C_2$.

We define the parity check matrix H_1 for a code C_1 s.t.

$$C_1 = \{x \in C_1 | H_1 x = 0\}$$

Simultaneously, we define the parity check matrix H_2 for a code C_2 s.t.

$$C_2 = \{x \in C_2 | H_2 x = 0\}$$

If we now want to find a parity check matrix H for $C_1 \cap C_2$, we

$$C_1 \cap C_2 = \{x \in C_1 \cap C_2 | Hx = 0\}$$

which can be found easily if we consider $x_1 + x_2 \in C_1 \cap C_2$ which means $H_1(x_1 + x_2) = 0$ and $H_2(x_1 + x_2) = 0$ and a parity check matrix $H = H_1 + H_2$ gives

$$(H_1 + H_2)(x_1 + x_2) = 0$$

In other words, if $x \in \text{null}(H_1)$ and $x \in \text{null}(H_2)$ then $x \in \text{null}(H_1 + H_2)$.

Now we would like to prove that

$$\Delta(C_1 \cap C_2) = \max\{\Delta(C_1), \Delta(C_2)\}$$

To see this, consider the two codewords

$$x_1 = \underset{x \in C_1}{\text{argmin}}\{\text{wt}(x)\}$$

$$x_2 = \underset{x \in C_2}{\text{argmin}}\{\text{wt}(x)\}$$

where $\text{wt}(x_1) > \text{wt}(x_2)$. Now, notice that only $x_2 \in C_1 \cap C_2$ since if it $x_1 \in C_1 \cap C_2$, then $\Delta(C_1) = \Delta(C_2)$. Therefore, $\Delta(C_1 \cap C_2) = \max\{\Delta(C_1), \Delta(C_2)\}$.

We just showed that

$$\Delta(C_1 \cap C_2) = \max\{\Delta(C_1), \Delta(C_2)\}$$

and we know that for $C_1 \cap C_2$ to be linear, we can only use $n-r+1$ points in the domain. Since each of these codes can have $n-d$ nonzero values we have $\Delta(C) = (n-r+1)-(n-d) = d-r+1$. Thus $\Delta(C_1 \cap C_2) = d-r+1$ and

$$\dim(C_1 \cap C_2) = d - r + 1$$

■

Problem 0.5. *Confused professor*

Solution.

Recall that Sanov's theorem states that if

$$P^* := \text{Proj}_Q(\mathcal{L}_1) = \underset{P}{\text{argmin}}\ D(P \in \mathcal{L}_1 || Q)$$

then

$$\lim_{n\to\infty} \left(\frac{1}{n} \log \underset{\bar{x}\sim Q^n}{\mathbf{Pr}} [P_{\bar{x}} \in \mathcal{L}_0] \right) \to -D(P^*||Q)$$

Therefore, we can write $\beta - \alpha$ as

$$\beta - \alpha = \lim_{n\to\infty} \left[\frac{1}{n} \left(\log \left(\underset{\bar{x}\sim Q^n}{\mathbf{Pr}} [P_{\bar{x}} \in \mathcal{L}_0] \right) - \log \left(\underset{\bar{x}\sim Q^n}{\mathbf{Pr}} [P_{\bar{x}} \in \mathcal{L}_1] \right) \right) \right]$$

$$\to D(P_1^*||Q) - D(P_0^*||Q)$$

Now consider the Pythagoras theorem which holds with equality for both of these linear families $\mathcal{L}_1$ and $\mathcal{L}_2$

$$D(P_0||Q) = D(P_0||P_0^*) + D(P_0^*||Q)$$

$$D(P_1||Q) = D(P_1||P_1^*) + D(P_1^*||Q)$$

combining these equations and using that $P_1 \in \mathcal{L}_0$ since $\mathcal{L}_1 \subseteq \mathcal{L}_0$ gives

$$D(P_1^*||Q) - D(P_0^*||Q) = D(P_0||P_1^*) \leq \epsilon$$

$\blacksquare$