Final Exam

Information and Coding Theory

March 18, 2021

Clayton Seitz

Problem 0.1. *Chang's Lemma*

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

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

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

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

$\blacksquare$

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 $|B_q(\alpha \cdot n)|/q^{H_q(\alpha)\cdot n} \leq 1$

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

Since $\alpha \leq 1 - \frac{1}{q}$, we have

Now we can show a q-ary Hamming bound . Analogous to the binary case we must have

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

Using the upper bound we derived above, we have

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

$\blacksquare$

Problem 0.3.

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

Finally, these two Reed-Solomon codes are each defined over n positions in the domain and have degree at most d. However, $C_1 \cap C_2$ consists of at most $n - r + 1$ positions, and the number of times a polynomial will pass through zero is d, the number of nonzero values in these $n - r + 1$ positions region can only be $d - r + 1$. Thus we have

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

■

Problem 0.5. *Confused professor*

Solution.

We can use Sanov's theorem to show that

$$\begin{aligned}
\beta - \alpha &= \lim_{n\to\infty} \left[\frac{1}{n} \left(\log \left(\mathop{\mathbf{Pr}}_{\bar{x}\sim Q^n} [P_{\bar{x}} \in \mathcal{L}_0] \right) - \log \left(\mathop{\mathbf{Pr}}_{\bar{x}\sim Q^n} [P_{\bar{x}} \in \mathcal{L}_1] \right) \right) \right] \\
&= D(P_0^*||Q) - D(P_1^*||Q) \\
&= D(P_0^*||P_1^*) \\
&\leq \epsilon
\end{aligned}$$

■