QUESTION: EXTENSION OF MAXIMAL CODE LEMMA TO TWO RECEIVERS?

CHANDRA NAIR

Abstract. We seek a generalization of the Maximal code lemma[KM77] to the case of two receivers.

1. Maximal Code Lemma

Here is the Maximal code lemma from [KM77] (slight change to modern notation).

A discrete memoryless channel(DMC) is a model of a noisy channel for communication that accepts input x from a discrete set $\mathcal{X}$ and produces an output y, belonging to another discrete set $\mathcal{Y}$, according to a fixed probability transition matrix $V \equiv [V(y|x)]$. The term memoryless is used when the channel satisfies an additional property $p(y_i|x_1,...,x_i,y_1,...,y_{i-1}) = p(y_i|x_i)$, or in other words the "error events" have no memory (sometimes referred to as random errors).

Let $P = \{P(a) : a \in \mathcal{X}\}$ be a probability distribution on $\mathcal{X}$, and denote by Q the probability distribution on $\mathcal{Y}$ induced by P and the transition matrix V. Let ϵ_n be a sequence of positive numbers such that $\epsilon_n \to 0$ and $\epsilon_n\sqrt{n} \to \infty$. We define the set of all typical sequences of length n,

$$\Gamma_n(P) := \{x^n \in \mathcal{X}^n : |\pi(a|x^n) - P(a)| \leq \epsilon_n P(a), \forall a \in \mathcal{X}\},$$

where $\pi(a|x^n) = \frac{1}{n}\|\{i : x_i = a\}\|$ is the empirical fraction of the letter a in the sequence x^n. In other words, typical sequences are collections of sequences whose empirical fractions match the true probabilities.

Also define the typical output sequences corresponding to an (typical) input sequence $x^n \in \Gamma_n(P)$ according to

$$\Gamma_n(x^n,V) := \{y^n \in \mathcal{Y}^n : |\pi(ab|x^ny^n) - P(a)V(b|a)| \leq \epsilon_n P()V(b|a), \forall(a,b) \in \mathcal{X}\times\mathcal{Y}\}.$$

For $\mathcal{F} \subseteq \mathcal{X}^n$ and $0 < \eta < 1$, define

$$G_V(\mathcal{F},\eta) := \min\{Q^n(\mathcal{A}) : \mathcal{A} \subseteq \mathcal{Y}^n, V^n(\mathcal{A}|x^n) \geq \eta, \forall x^n \in \mathcal{F}\}.$$

In other words $G_V(\mathcal{F},\eta)$ is the image (or more precisely contains η-fraction of the image) of the set $\mathcal{F}$, when transmitted via the channel V, in the space $\mathcal{Y}^n$.

Now we are ready to state the theorem.

Theorem 1.1. *(Maximal Code Lemma) Given a triple of numbers $0 < \epsilon,\delta,\eta < 1$, there exists a number $n_0 = n_0(\epsilon,\delta,\eta)$ such that, for $n \geq n_0$, the following two statements hold:*

(1) Direct Part*: For any $\mathcal{F} \subseteq \Gamma_n(P)$ there exists a code $\{x_1^n,...,x_M^n;\mathcal{A}_1,...,\mathcal{A}_M\}$ for the channel V such that: (i) $x_i^n \in \mathcal{F},\forall i$; (ii) $\mathcal{A}_i \subseteq \Gamma(x_i^n,V),\forall i$; (iii) $V^n(\mathcal{A}_i|x_i^n) > 1-\epsilon,\forall i$; (iv) the sets $\mathcal{A}_i$ are disjoint; and (v)*

$$M \geq \exp[n(I(X;Y)-\delta)] \cdot G_V(\mathcal{F},\eta).$$

Date: September 17, 2008.

(2) Converse Part*: Let* $\{x_1^n, ..., x_M^n; \mathcal{A}_1, ..., \mathcal{A}_M\}$ *be a code for the channel* V *such that* $\mathcal{F} := \{x_1^n, ..., x_M^n\} \subseteq \Gamma_n(P)$,

$$V^n(\mathcal{A}_i|x_i^n) > 1 - \epsilon, \quad \forall i,$$

where the sets $\mathcal{A}_i$ *are disjoint. Then*

$$M \leq \exp[n(I(X;Y) + \delta)] \cdot G_V(\mathcal{F}, \eta).$$

Remark 1.2. *In other, given a subset* $\mathcal{F} \subset \mathcal{X}^n$ *there exists a codebook of size*

$$M \geq \exp[n(I(X;Y) - \delta)] \cdot G_V(\mathcal{F}, \eta)$$

and any codebook whose codewords are in $\mathcal{F}$ *must satisfy*

$$M \leq \exp[n(I(X;Y) + \delta)] \cdot G_V(\mathcal{F}, \eta).$$

1.1. **Extension to two receivers.** Suppose there are two channels $V_1(y_1|x)$ and $V_2(y_2|x)$, suppose you are given $\mathcal{F} \subseteq \Gamma_n(P)$ (a subset of the typical $\mathcal{X}^n$ sequences). Then $\{x_1^n, ..., x_M^n; \mathcal{A}_1, ..., \mathcal{A}_M; \mathcal{B}_1, ..., \mathcal{B}_M\}$ is a code for channels V_1, V_2 (equivalently receivers $\mathcal{Y}_1, \mathcal{Y}_2$) if (i) $x_i^n \in \mathcal{F}, \forall i$; (ii) $\mathcal{A}_i \subseteq \Gamma(x_i^n, V_1), \forall i$; (iii) $\mathcal{B}_i \subseteq \Gamma(x_i^n, V_2), \forall i$; (iv) $V^n(\mathcal{A}_i|x_i^n) > 1 - \epsilon, \forall i$; (v) $V^n(\mathcal{B}_i|x_i^n) > 1 - \epsilon, \forall i$; (vi) the sets $\mathcal{A}_i$ are disjoint; and (vi) the sets $\mathcal{B}_i$ are disjoint.

Question: What is the tight characterization, similar to Theorem 1.1, for the largest codebook consisting of codewords from a given subset $\mathcal{F} \in \Gamma_n(P)$.

Remark 1.3. *We can make the following simple observations*

- *Taking the minimum of the two channels in question, we obtain that*

$$\min\{\exp[n(I(X;Y_1) + \delta)] \cdot G_{V_1}(\mathcal{F}, \eta), \exp[n(I(X;Y_2) + \delta)] \cdot G_{V_2}(\mathcal{F}, \eta)\}$$

  is an upper bound to the size of the largest codebook.
- *Lap Chi Lau made a nice observation that a better way to write the upper bound would be the following,*

$$\min_{\mathcal{F}_1 \subseteq \mathcal{F}}\{\exp[n(I(X;Y_1) + \delta)] \cdot G_{V_1}(\mathcal{F}_1, \eta) + \exp[n(I(X;Y_2) + \delta)] \cdot G_{V_2}(\mathcal{F}_1^c, \eta)\}.$$

- *Using a random coding argument, we obtain that*

$$\min\{P^n(\mathcal{F}) \exp(n(I(X;Y_1) - \delta)), P^n(\mathcal{F}) \exp(n(I(X;Y_2) - \delta))\}$$

  is a lower bound to the size of the largest codebook.

Remark 1.4. *Assuming that we are restricting ourselves to a fixed probability distribution* $P(x)$ *is not a big restriction, as there are at most* $(n+1)^{\mathcal{X}}$ *empirical distributions of length* n *and therefore any exponential size codebook must have at least one empirical distribution with the "same" exponential size of codewords belonging to it.*

References

[KM77] J Körner and K Marton, *Images of a set via two channels and their role in mult-user communication*, IEEE Trans. Info. Theory **IT-23** (Nov, 1977), 751–761.