### 18.413: Error-Correcting Codes Lab

February 5, 2004
Lecture 2

Lecturer: Daniel A. Spielman

### 2.1 Channels

A channel is given by a set of input symbols $a_{1}, \ldots, a_{m}$, a set of output symbols $b_{1}, \ldots, b_{n}$, and a set of transition probabilities $p_{i, j}$, where

$$
p_{i, j}=\operatorname{Pr}\left[b_{j} \text { is received } \mid a_{i} \text { is sent }\right] .
$$

Given a general channel, we now examine how to determine the probability that a particular input was transmitted given that a particular output was received. That is, we examine how to interpret the output of the channel. Our derivation follows from many applications of the law of conditional probability. We let $x$ be the random variable corresponding to the input to the channel, and $y$ be the output. We assume that $x$ is chosen uniformly from $a_{1}, \ldots, a_{m}$.

$$
\begin{aligned}
\operatorname{Pr}\left[x=a_{i} \mid y=b_{j}\right] & =\frac{\operatorname{Pr}\left[x=a_{i} \text { and } y=b_{j}\right]}{\operatorname{Pr}\left[y=b_{j}\right]} \\
& =\frac{\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right] \operatorname{Pr}\left[x=a_{i}\right]}{\operatorname{Pr}\left[y=b_{j}\right]} \\
& =\frac{\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right] \operatorname{Pr}\left[x=a_{i}\right]}{\sum_{k} \operatorname{Pr}\left[y=b_{j} \text { and } x=a_{k}\right]} \\
& =\frac{\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right] \operatorname{Pr}\left[x=a_{i}\right]}{\sum_{k} \operatorname{Pr}\left[y=b_{j} \mid x=a_{k}\right] \operatorname{Pr}\left[x=a_{k}\right]} \\
& =\frac{\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right](1 / m)}{\sum_{k} \operatorname{Pr}\left[y=b_{j} \mid x=a_{k}\right](1 / m)} \\
& =\frac{\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right]}{\sum_{k} \operatorname{Pr}\left[y=b_{j} \mid x=a_{k}\right]} \\
& =\frac{p_{j, i}}{\sum_{k} p_{j, k}} .
\end{aligned}
$$

### 2.2 Capacity and Mutual Information

The capacity of a channel provides a sharp threshold: If one communicates over a channel using any code of rate greater than the capacity, then the probabiliy that one will have a communication error tends to 1 . On the other hand, there exist codes of every rate less than capacity that drive
the probability of communication error to zero. It is easy to compute the capacity of symmetric channels.

Definition 2.2.1. A channel is symmetric if

- For all $i_{1}$ and $i_{2}$, the vectors $\left(p_{i_{1}, 1}, \ldots, p_{i_{1}, n}\right)$ and $\left(p_{i_{2}, 1}, \ldots, p_{i_{2}, n}\right)$ are permutations of each other, and
- For all $j_{1}$ and $j_{2}$, the vectors $\left(p_{1, j_{1}}, \ldots, p_{m, j_{1}}\right)$ and $\left(p_{1, i_{2}}, \ldots, p_{m, j_{2}}\right)$ are permutations of each other.

Most of the channels we consider will be symmetric.
Let $x$ be the random variable uniformly chosen from $a_{1}, \ldots, a_{m}$ and let $y$ be the random variable giving the output of the channel on input $x$. Then, the capacity of the channel is the mutual information of $x$ and $y$, written $I(x ; y)$ and defined by

$$
I(x ; y) \stackrel{\text { def }}{=} \sum_{i, j} \operatorname{Pr}\left[x=a_{i} \text { and } y=b_{j}\right] \log _{2}\left(\frac{\operatorname{Pr}\left[x=a_{i} \text { and } y=b_{j}\right]}{\operatorname{Pr}\left[x=a_{i}\right] \operatorname{Pr}\left[y=b_{j}\right]}\right)
$$

If a channel has a simple description, the one can compute $I(x ; y)$ directly. Otherwise, one can estimate $I(x ; y)$ by experiment if one can compute the quantity $\operatorname{Pr}\left[y=b_{j} \mid x=a_{i}\right] / \operatorname{Pr}\left[y=b_{j}\right]$ : repeatedly choose $x$ at random, generate $y$, compute

$$
i(x ; y) \stackrel{\text { def }}{=} \log _{2}\left(\frac{\operatorname{Pr}\left[x=a_{i} \text { and } y=b_{j}\right]}{\operatorname{Pr}\left[x=a_{i}\right] \operatorname{Pr}\left[y=b_{j}\right]}\right)
$$

and take the average of all the $i(x ; y)$ values obtained.

### 2.3 What I should have said

We will extend the definition of a symmetric channel to the following:
Definition 2.3.1. A channel is symmetric if its output symbols can be partitioned into sets such that for each set $S$ in the partition,

- For all $i_{1}$ and $i_{2}$, the vectors $\left(p_{i_{1}, j}\right)_{j \in S}$ and $\left(p_{i_{2}, j}\right)_{j \in S}$ are permutations of each other, and
- For all $j_{1} \in S$ and $j_{2} \in S$, the vectors $\left(p_{1, j_{1}}, \ldots, p_{m, j_{1}}\right)$ and $\left(p_{1, i_{2}}, \ldots, p_{m, j_{2}}\right)$ are permutations of each other.
$x 2$

In particular, this defition includes the "nice" channels that I defined in class, which satisfy:

- The channel has two input symbols, $a_{1}$ and $a_{2}=1$, and


Figure 2.1: A "nice" channel.

- The output symbols come in pairs, $b_{j}$ and $b_{j^{\prime}}$ such that $p_{1, j}=p\left(2, j^{\prime}\right)$ and $p_{2, j}=p\left(1, j^{\prime}\right)$.

For example, the following channel is symmetric:
The channels we will encounter in Small Project 1 are all nice.
Note that for any output symbol $b_{j}$ of a nice channel, it is easy to compute $\operatorname{Pr}\left[y=b_{j}\right]$ :

$$
\begin{aligned}
\operatorname{Pr}\left[y=b_{j}\right] & =\operatorname{Pr}\left[x=0 \text { and } y=b_{j}\right]+\operatorname{Pr}\left[x=1 \text { and } y=b_{j}\right] \\
& =\operatorname{Pr}\left[y=b_{j} \mid x=0\right] \operatorname{Pr}[x=0]+\operatorname{Pr}\left[y=b_{j} \mid x=1\right] \operatorname{Pr}[x=1] .
\end{aligned}
$$

