

## I. BINARY BROADCAST CHANNEL

Definition 1 (Binary BC) We define the Binary Broadcast Channel depicted in Fig. 1. We set the following distributions

$$
\begin{align*}
Z_{1} & \sim B\left(p_{1}\right)  \tag{1}\\
Z_{2} & \sim B\left(p_{2}\right)  \tag{2}\\
\tilde{Z}_{2} & \sim B\left(\tilde{p_{2}}\right)  \tag{3}\\
Z_{1} & \perp Z_{2}  \tag{4}\\
Z_{2} & =Z_{1} \oplus \tilde{Z}_{2} \tag{5}
\end{align*}
$$

thus $p_{2}=p_{1} * \tilde{p_{2}}=p_{1}\left(1-p_{2}\right)+\left(1-p_{1}\right) p_{2}$. Additionally, we define

$$
\begin{align*}
& Y_{1}=X \oplus Z_{1}  \tag{6}\\
& Y_{2}=Y_{1} \oplus \tilde{Z}_{2}=X \oplus Z_{1} \oplus \tilde{Z}_{2}=X \oplus Z_{2} \tag{7}
\end{align*}
$$



Fig. 1. The Binary Broadcast Channel

The capacity region of the degraded broadcast channel is the set of all pair rates $\left(R_{1}, R_{2}\right)$ that satisfies

$$
\begin{align*}
& R_{1}<I\left(X ; Y_{1} \mid U\right) \\
& R_{2}<I\left(U ; Y_{2}\right) \tag{8}
\end{align*}
$$

for some joint distribution $p(u) p(x \mid u) p\left(y_{1}, y_{2} \mid x\right)$. We state the capacity of the Binary Broadcast Channel.

Lemma 1 (Capacity of the Binary BC) The capacity region of the Binary Broadcast Channel is the of all pairs $\left(R_{1}, R_{2}\right)$ that satisfies

$$
\begin{align*}
& R_{1}<h\left(\alpha * p_{1}\right)-h\left(p_{1}\right)  \tag{9}\\
& R_{2}<1-h\left(\alpha * p_{2}\right) . \tag{10}
\end{align*}
$$

Where $\alpha \in[0,1]$.

## Proof:

Achievability: Let us define two r.v $U \sim B\left(\frac{1}{2}\right), V \sim B(\alpha)$ and change $X=U \oplus V$. We now apply these new definitions to (8)

$$
\begin{align*}
R_{2} & =I\left(U, Y_{2}\right)  \tag{11}\\
& =H\left(Y_{2}\right)-H\left(Y_{2} \mid U\right)  \tag{12}\\
& =1-h\left(\alpha * p_{2}\right) \tag{13}
\end{align*}
$$

Furthermore,

$$
\begin{align*}
R_{1} & =I\left(X ; Y_{1} \mid U\right)  \tag{15}\\
& =I\left(U \oplus V ; U \oplus V \oplus Z_{1} \mid U\right)  \tag{16}\\
& =I\left(V ; V \oplus Z_{1}\right)  \tag{17}\\
& =h\left(V \oplus Z_{1}\right)-h\left(V \oplus Z_{1} \mid V\right)  \tag{18}\\
& =h\left(\alpha \oplus p_{1}\right)-h\left(p_{1}\right) \tag{19}
\end{align*}
$$

Thus we obtained the desired region and proved the achievability part. In order to prove the converse we introduce the following lemma.

Lemma 2 (Mrs. Gerber Lemma) Let $X$ and $U$ be two random variables where $X$ is binary. If $Y \sim B(P)$ is independent of $(X, U)$ then

$$
\begin{equation*}
h(X \oplus Y \mid U) \geq h\left(h^{-1}(h(X \mid U)) * p\right) \tag{20}
\end{equation*}
$$

where $a * b=\bar{a} b+b \bar{a}$ and $h$ is the binary entropy.
The similarity between the Mrs Gerber Lemma and the EPI is shown in the Appendix. We now return to the converse,

Converse:

$$
\begin{align*}
I\left(Y_{2} ; U\right) & =h\left(Y_{2}\right)-h\left(Y_{2} \mid U\right)  \tag{21}\\
& \leq 1-h\left(Y_{2} \mid U\right) \tag{22}
\end{align*}
$$

We bound $h\left(Y_{2} \mid U\right)$ from both sides

$$
\begin{equation*}
1=h\left(Y_{2} \mid U\right) \geq h\left(Y_{2} \mid X\right)=h\left(p_{2}\right) \tag{23}
\end{equation*}
$$

by the Markov chain $Y_{2}-X-U$. Therefore there exists an $\alpha$ s.t

$$
\begin{equation*}
h\left(Y_{2} \mid U\right)=h\left(\alpha \oplus p_{2}\right) \tag{24}
\end{equation*}
$$

thus

$$
\begin{equation*}
R_{2}<1-h\left(\alpha \oplus p_{2}\right) \tag{25}
\end{equation*}
$$

Now for $R_{1}$,

$$
\begin{align*}
I\left(X ; Y_{2} \mid U\right) & =h\left(Y_{1} \mid U\right)-h\left(Y_{1} \mid U, X\right)  \tag{26}\\
& =h\left(Y_{1} \mid U\right)-h\left(p_{1}\right) \tag{27}
\end{align*}
$$

By setting $X=Y_{1}, Y=Z_{2}$ in the Mrs. Gerber Lemma we obtain

$$
\begin{align*}
h\left(Y_{2} \mid U\right) & \geq h\left(h^{-1}\left(h\left(Y_{1} \mid U\right)\right) * \tilde{p_{2}}\right)  \tag{28}\\
h\left(\alpha * p_{2}\right) & \geq h\left(h^{-1}\left(h\left(Y_{1} \mid U\right)\right) * \tilde{p_{2}}\right)  \tag{29}\\
\alpha * p_{1} * \tilde{p_{2}} & \geq h^{-1}\left(h\left(Y_{1} \mid U\right)\right) * \tilde{p_{2}} \tag{30}
\end{align*}
$$

$$
\begin{align*}
\alpha * p_{1} & \geq h^{-1}\left(h\left(Y_{1} \mid U\right)\right)  \tag{31}\\
h\left(\alpha * p_{1}\right) & \left.\left.\geq h\left(Y_{1} \mid U\right)\right)\right) \tag{32}
\end{align*}
$$

therefore,

$$
\begin{equation*}
R_{1} \leq h\left(\alpha * p_{1}\right)-h\left(p_{1}\right) \tag{33}
\end{equation*}
$$

which concludes the proof.

## II. Appendix

A. A binary analogue to the EPI

We will introduce an analogue between the EPI and the Mrs. Gerber Lemma. The EPI states that for any independent $X \sim f(x)$ and $Z \sim f(z)$

$$
\begin{equation*}
2^{2 h(X+Y)} \geq 2^{2 h(X)}+2^{2 h(Y)} \tag{34}
\end{equation*}
$$

If we define $\eta(x)=\frac{1}{2} \log (2 \pi e x)$ then,

$$
\begin{equation*}
\eta^{-1}(h(X+Y)) \geq \eta^{-1}(h(X))+\eta^{-1}(h(Y)) \tag{35}
\end{equation*}
$$

Now let $X$ and $Y$ be independent r.v with finite alphabet and entropy $H(X)<1, H(Y)<$ 1 respectively. We define $\sigma(x)=h^{-1}(H(X))$ thus

$$
\begin{align*}
\sigma(X \oplus Y) & \geq \sigma(X) * \sigma(Y)  \tag{36}\\
h^{-1}(H(X \oplus Y)) & \geq h^{-1}(H(X)) * h^{-1}(H(Y)) \tag{37}
\end{align*}
$$

Notice the similarity of (35) and (37). Now we set $Y \sim B(p) \perp(X, U)$ thus we obtain

$$
\begin{align*}
h^{-1}(H(X \oplus Y \mid U)) & \geq h^{-1}(H(X \mid U)) * h^{-1}(H(Y \mid U))  \tag{38}\\
h^{-1}(H(X \oplus Y \mid U)) & \geq h^{-1}(H(X \mid U)) * p \tag{39}
\end{align*}
$$

taking $h(\cdot)$ on both sides (which is possible since $h$ is monotonically increasing), we obtain the Mrs. Gerber Lemma.

## References

[1] Abbas El Gamal and Young-Han Kim, "Network Information Theory", Lecture notes, Available online
[2] Thomas Cover and Joy Thomas, "Elements of Information Theory", 2nd ed., Wiley- Interscience, 2006.

