EE 121 - Introduction to Digital Communications
Homework 1 Solutions

January 30, 2008

1 (a)

$$
\begin{aligned}
E[V+W] &= \sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}}(v+w)\Pr(v,w)\\
&= \sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}} v\Pr(v,w) + \sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}} w\Pr(v,w)\\
&= \sum_{v\in\mathcal{V}} v\sum_{w\in\mathcal{W}}\Pr(v,w) + \sum_{v\in\mathcal{V}} w\sum_{w\in\mathcal{W}}\Pr(v,w)\\
&= \sum_{v\in\mathcal{V}} v\Pr(v) + \sum_{v\in\mathcal{V}} w\Pr(w)\\
&= E[V]+E[W]
\end{aligned}
$$

(b)

$$
\begin{aligned}
E[VW] &= \sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}} vw\Pr(v,w)\\
&= \sum_{v\in\mathcal{V}}\sum_{w\in\mathcal{W}} vw\Pr(v)\Pr(w)\\
&= \left(\sum_{v\in\mathcal{V}} v\Pr(v)\right)\left(\sum_{v\in\mathcal{V}} w\Pr(w)\right)\\
&= E[V]E[W].
\end{aligned}
$$

(c) Assume V is either 1 or -1 with probability 0.5 and also W=V. Then it is clear that

$$0 = E[V] = E[W] = E[V]E[W] \neq E[VW] = 1.$$

For the equality assume that V is uniform on $\{-1,0,1\}$ and W is zero when V is not zero and is one otherwise. It is clear that $\Pr(V=0, W=0) = 0 \neq \Pr(V=0)\Pr(W=0)$ therefore V and W are not independent. On the other hand $E[VW] = 0 = E[V]E[W]$.

(d)

$$\begin{aligned}
\sigma_{v+w}^2 &= E[(V+W)^2] - E^2[V+W] \\
&= E[V^2 + 2VW + W^2] - (E[V] + E[W])^2 \\
&= E[V^2] + 2E[V]E[W] + E[W^2] - E^2[V] - 2E[V]E[W] - E^2[W] \\
&= E[V^2] - E^2[V] + E[W^2] - E^2[W] \\
&= \sigma_v^2 + \sigma_w^2.
\end{aligned}$$

2 (a) Yes it is. Proof by induction on n. For $n = 2$ it is easy to verify that

$$P(Z=0) = P(Z=1) = \frac{1}{2}.$$

Also $\Pr(Z = 1, X_1 = 1) = \Pr(X_1 = 1, X_2 = 0) = \frac{1}{4} = \Pr(Z = 1)\Pr(X_1 = 1)$. It is also easy to verify that for all other three possible choices of Z and X_1 we have $\Pr(Z, X_1) = \frac{1}{4} = \Pr(Z)\Pr(X_1)$ therefore Z and X_1 are independent. Now assume that Z and X_1 are independent for n=k, we prove it for n=k+1: let

$$Z_k = X_1 \oplus \cdots \oplus X_k$$

and

$$Z_{k+1} = X_1 \oplus \cdots \oplus X_{k+1} = Z_k \oplus X_{k+1}$$

Now since Z_k and X_{k+1} are independent of X_1 therefore $Z_{k+1} = Z_k \oplus X_k$ is also independent of X_1.

(b) Yes because

$$\Pr(Z|X_1, \ldots, X_{n-1}) = \Pr(X_n = Z \oplus X_1 \oplus \cdots \oplus X_{n-1}|X_1, \ldots, X_{n-1}) = \Pr(Z) = \frac{1}{2}$$

therefore

$$\Pr(Z, X_1, \ldots, X_{n-1}) = \Pr(Z)\Pr(X_1, \ldots, X_{n-1}) = \Pr(Z)\Pr(X_1)\ldots\Pr(X_{n-1})$$

(c) No, because given $X_1, \ldots, X_n$ we completely know Z.

(d) Assume $n = 2$ and $\Pr(X_i = 1) = p \neq \frac{1}{2}$ and $\Pr(X_i = 0) = 1 - p$ for $i = 1, 2$. Then we have $\Pr(Z = 1) = 2p(1-p)$ and $\Pr(Z = 0) = p^2 + (1-p)^2$. Therefore

$$\Pr(Z = 1, X_1 = 1) = \Pr(X_2 = 0, X_1 = 1) = p(1-p) \neq 2p(1-p)p.$$

3 (a) Let X denote the input r.v. and Y the output r.v.. From Bayes law

$$\begin{aligned} p_1 &= \Pr(X=1|Y=1) \\ &= \frac{\Pr(Y=1|X=1)\Pr(X=1)}{\Pr(Y=1|X=0)\Pr(X=0)+\Pr(Y=1|X=1)\Pr(X=1)} \\ &= \frac{(1-\epsilon)(1-p)}{\epsilon p+(1-\epsilon)(1-p)} \end{aligned}$$

(b) For this part let Y_1 denote the first output r.v. and Y_2 the second.

$$\begin{aligned} p_2 &= \Pr(X=1|Y_1=1,Y_2=1) \\ &= \frac{\Pr(Y_2=1|X=1,Y_1=1)\Pr(X=1|Y_1=1)}{\Pr(Y_2=1|Y_1=1)} \\ &= \frac{\Pr(Y_2=1|X=1,Y_1=1)\Pr(X=1|Y_1=1)}{\Pr(Y_2=1|Y_1=1,X=1)P(X=1|Y_1=1)+P(Y_2=1|Y_1=1,X=0)P(X=0|Y_1=1)}. \end{aligned}$$

As Y_1 and Y_2 are conditionally independent given X we have

$$\begin{aligned} p_2 &= \frac{\Pr(Y_2=1|X=1)\Pr(X=1|Y_1=1)}{\Pr(Y_2=1|X=1)P(X=1|Y_1=1)+P(Y_2=1|X=0)P(X=0|Y_1=1)} \\ &= \frac{(1-\epsilon)p_1}{(1-\epsilon)p_1+\epsilon(1-p_1)}. \end{aligned}$$

(c) Using Bayes law we have

$$\begin{aligned} p_n &= \Pr(X=1|Y_1=1,\dots,Y_n=1) \\ &= \frac{\Pr(Y_1=1,\dots,Y_n=1|X=1)\Pr(X=1)}{\Pr(Y_1=1,\dots,Y_n=1|X=0)\Pr(X=0)+\Pr(Y_1=1,\dots,Y_n=1|X=1)\Pr(X=1)} \end{aligned}$$

As the $Y_1,\dots,Y_n$ are conditionally independent given X we have

$$\begin{aligned} p_n &= \frac{\prod_{i=1}^n \Pr(Y_i=1|X=1)\Pr(X=1)}{\prod_{i=1}^n \Pr(Y_i=1|X=0)\Pr(X=0)+\prod_{i=1}^n \Pr(Y_i=1|X=1)\Pr(X=1)} \\ &= \frac{(1-\epsilon)^n(1-p)}{\epsilon^n p+(1-\epsilon)^n(1-p)} \end{aligned}$$

This function is plotted in figure 1. By writing p_n like so

$$\begin{aligned} p_n &= \frac{1}{\frac{\epsilon^n p}{(1-\epsilon)^n(1-p)}+1} \\ &= \frac{1}{\frac{p}{(1/\epsilon-1)^n(1-p)}+1} \end{aligned}$$

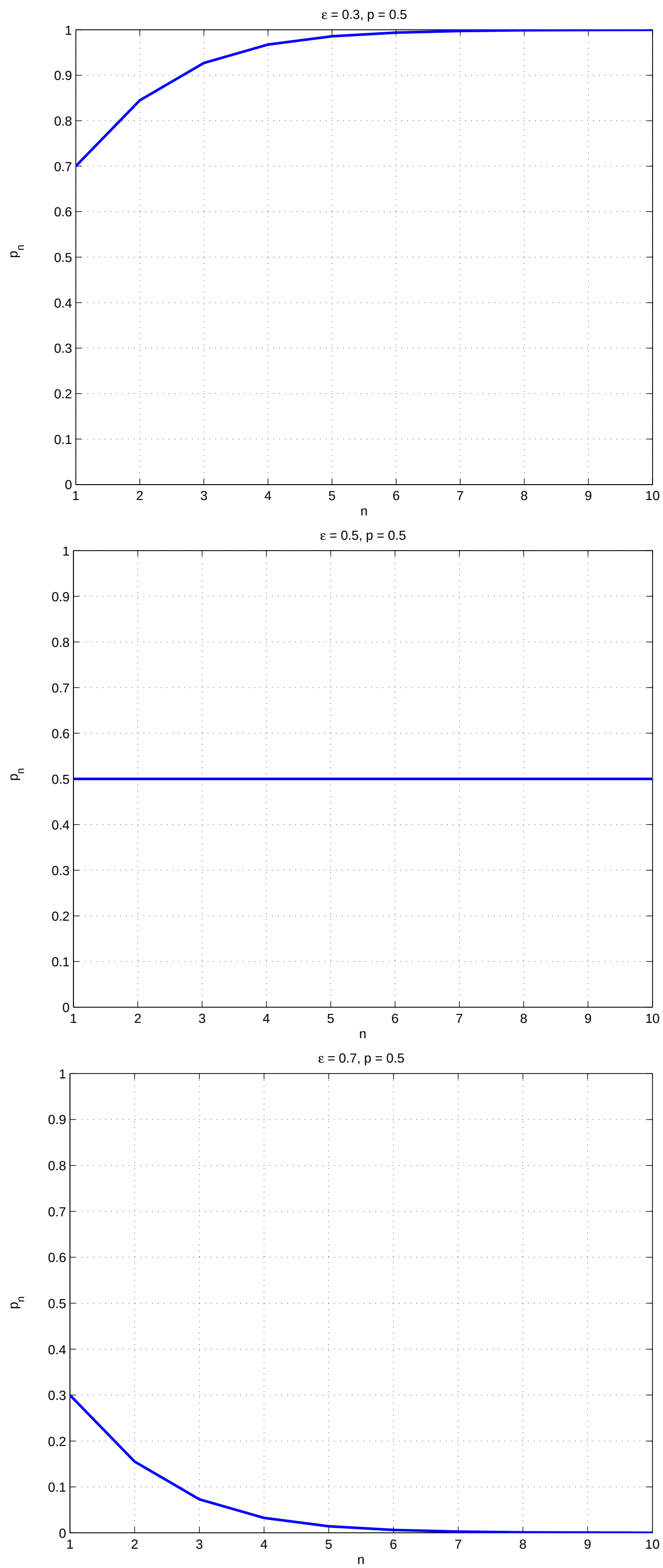

Figure 1: p_n versus n for sample values of ϵ and p.

we see that for $\epsilon < 0.5$, $p_n \to 1$ as $n \to \infty$ and for $\epsilon > 0.5$, $p_n \to 0$ as $n \to \infty$.

4 (a) Y_n is a binomial r.v. and thus has PMF

$$\begin{aligned}\Pr(Y_n = x) &= \Pr\left(\frac{1}{n}\sum_{t=1}^{n} X_t = x\right)\\ &= \Pr\left(\sum_{t=1}^{n} X_t = nx\right)\\ &= \binom{n}{nx} p^{nx}(1-p)^{n(1-x)}\end{aligned}$$

where nx is an integer. This function is plotted in figure 2 for several values of n. The plots show that as $n \to \infty$ the probability of deviating from the mean by more than a fixed amount diminishes as $n \to \infty$, i.e. they support the statement that for any $\epsilon > 0$, $\Pr\left(|Y_n - p| > \epsilon\right) \to 0$ as $n \to \infty$.

(b) Let $I_{\{X_i=n\}}$ be the indicator random variable for the event $\{X_i = n\}$, i.e.

$$I_{\{X_i=n\}} = \begin{cases} 0, & \text{if } X_i \neq n \\ 1, & \text{if } X_i = n. \end{cases}$$

Suppose we observe symbols $X_1, X_2, \ldots, X_N$. Estimate the pmf of X_i by counting the number of occurrences of each symbol, i.e.

$$\hat{P}(X_i = n) = \frac{1}{N}\sum_{i=1}^{N} I_{\{X_i=n\}}.$$

Note that the estimate $\hat{P}(X_i = n)$ is a random variable. From the law of large numbers we know that as $n \to \infty$

$$\begin{aligned}\hat{P}(X_i = n) &\to E\left[\frac{1}{N}\sum_{i=1}^{N} I_{\{X_i=n\}}\right]\\ &= \left[\frac{1}{N}\sum_{i=1}^{N} E[I_{\{X_i=n\}}]\right]\\ &= \left[\frac{1}{N}\sum_{i=1}^{N} \Pr(X_i = n)\right]\\ &= \Pr(X_i = n)\end{aligned}$$

in probability, and thus our estimated pmf converges to the true pmf.

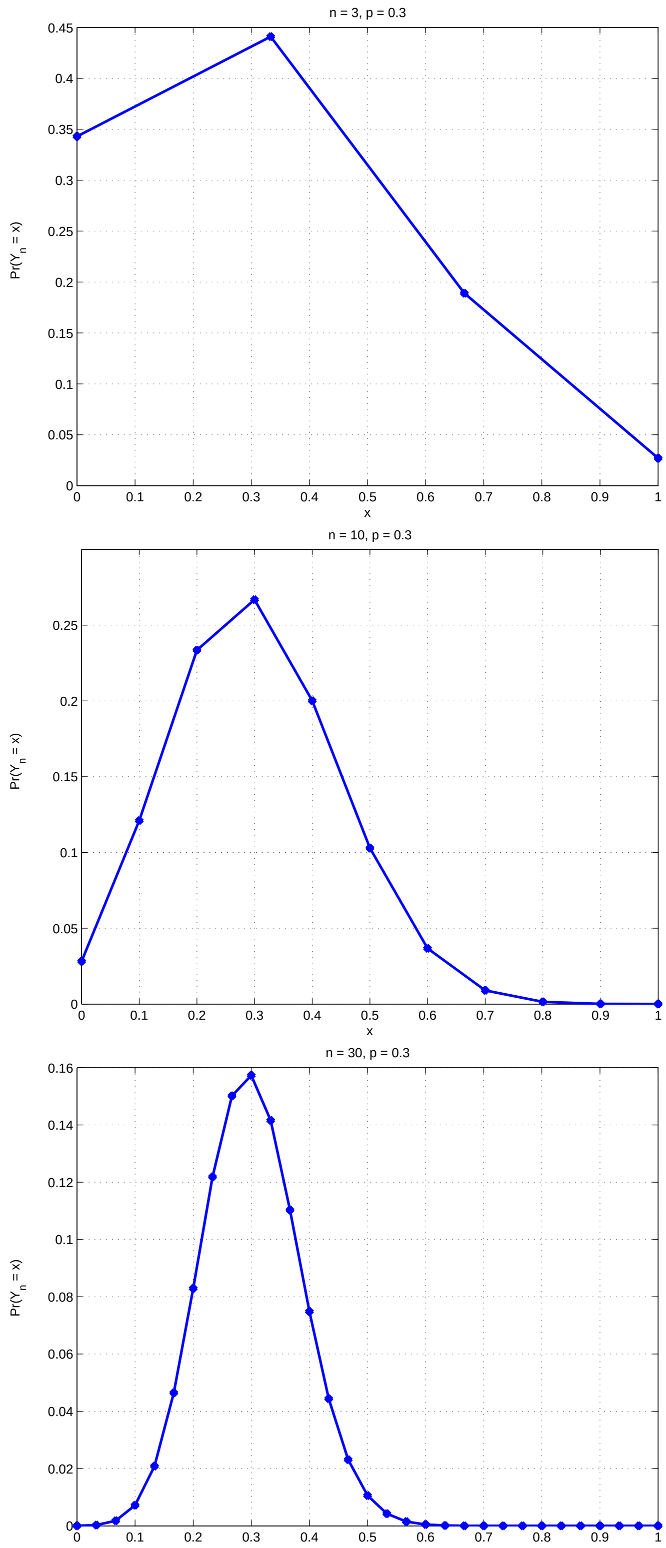

Figure 2: PMF of Y_n for different values of n and a favorite value of $p = 0.3$.

5 (a) The proof of being uniquely decodable is the same as the prefix free codes except we just need to start decoding from the end of the stream.

(b)

$$\begin{cases} a: & 1 \\ b: & 10 \\ c: & 00 \end{cases}$$

We can start decoding after receiving the last bit. Therefore the decoder might have to wait a long time before it can start decoding.

(c) Assume the codeword of length one is 1. Then if the code is prefix free the other two should start with 0 therefore one is 01 and the other is 00 and clearly it is not a suffix free code. The same argument applies when the codeword of length one is 0.