1. Binary random variables $X$, $Y$, and $Z$, where $X$ and $Z$ are independent and are both distributed uniformly and $Y = X \oplus Z$.

$$H(X) = -\frac{1}{2} \log \frac{1}{2} - \frac{1}{2} \log \frac{1}{2}$$
$$= 1$$
$$= H(Z).$$

$$P_Y(0) = P_X(1)P_Z(1) + P_X(0)P_Z(0)$$
$$= \frac{1}{2}.$$  

∴ $H(Y) = 1$.

$$H(X,Y) = H(X) + H(Y|X)$$
$$= H(X) + H(X \oplus Z|X)$$
$$= H(X) + H(Z)$$
$$= 2.$$  

\[P(X = 0, Y = 0|Z = 0) = P_X(0) = 1/2\]
\[P(X = 1, Y = 1|Z = 0) = P_X(1) = 1/2\]
\[P(X = 0, Y = 1|Z = 0) = 0\]
\[P(X = 1, Y = 0|Z = 0) = 0\]

∴ $H(X,Y|Z = 0) = 1$.

Similarly, $H(X,Y|Z = 1) = 1$.

Therefore, $H(X,Y|Z) = P_Z(0)H(X,Y|Z = 0) + P_Z(1)H(X,Y|Z = 1)$
$$= 1.$$  

From properties of entropy we know that

$$H(X,Y) = H(X) + H(Y) \iff X \perp \perp Y.$$  

Further,

$$H(X,Y|Z) = H(X|Z) + H(Y|Z) \iff X \text{ conditionally independent of } Y \text{ given } Z.$$  

Therefore, clearly, $X$ and $Y$ are independent but $X$ and $Y$ are not independent given $Z$. 

1
2. \( X \sim \text{Ber}(\frac{1}{2}) \), \( P_{Y|X}(0|0) = 0.5 \), \( P_{Y|X}(1|1) = 1 \).

\[ \therefore H(Y|X = 0) = 1. \]
\[ H(Y|X = 1) = 0. \]
\[ H(Y|X) = P_X(0)H(Y|X = 0) + P_X(1)H(Y|X = 1) \]
\[ = \frac{1}{2}. \]
\[ P_Y(0) = P_X(0)P_{Y|X}(0|0) + P_X(1)P_{Y|X}(0|1) \]
\[ = \frac{1}{2} \cdot \frac{1}{2} \]
\[ = \frac{1}{4} = 1 - P_Y(1). \]
\[ \therefore H(Y) = \frac{1}{4} \log 4 + \frac{1}{4} (2 - \log 3) \]
\[ = 0.603. \]
\[ H(X, Y) = H(X) + H(Y|X) \]
\[ = 1 + \frac{1}{2} = 1.5. \]
\[ H(X|Y) = H(X, Y) - H(Y) \]
\[ = 1.5 - 0.603 = 0.897. \]

3. (a) \textit{(Conditioning reduces entropy)} Using chain rule, \( H(X_1, X_2, X_3) \) can be expanded in the following two ways.

\[ 2H(X_1, X_2, X_3) = H(X_1, X_2) + H(X_3|X_1, X_2) + H(X_2, X_3) + H(X_1|X_2, X_3) \]
\[ = H(X_1, X_2) + H(X_2, X_3) + H(X_3|X_1, X_2) + H(X_1|X_2, X_3) \]
\[ \leq H(X_1, X_2) + H(X_2, X_3) + H(X_3|X_1, X_2) + H(X_1) \]
\[ \leq H(X_1, X_2) + H(X_2, X_3) + H(X_3|X_1) + H(X_1) \]
\[ = H(X_1, X_2) + H(X_2, X_3) + H(X_3, X_1). \]

(b) \textit{(Sub additivity of entropy)} Add and subtract \( H(X_1) + H(X_2) + H(X_3) \).

\[ H(X_1, X_2|X_3) + H(X_2, X_3|X_1) + H(X_3, X_1|X_2) \]
\[ = H(X_1, X_2|X_3) + H(X_3) + H(X_2, X_3|X_1) + H(X_1) + H(X_3, X_1|X_2) + H(X_2) \]
\[ - [H(X_1) + H(X_2) + H(X_3)] \]
\[ = 3H(X_1, X_2, X_3) - [H(X_1) + H(X_2) + H(X_3)] \]
\[ \leq 3H(X_1, X_2, X_3) - H(X_1, X_2, X_3) \]
\[ = 2H(X_1, X_2, X_3). \]

4. (i)

\[ H(X|Y) \leq H(X) \quad \text{ (Conditioning reduces entropy)} \]
\[ \leq \log |\mathcal{X}|. \quad \text{ (using the operational definition of entropy)} \]

Observe that equality holds when \( Y \perp \perp X \) and \( X \sim \text{Unif}(\mathcal{X}) \).

(ii) We know that for \( Z \sim \text{Geo}(p) \), \( \mathbb{E}[Z] = \frac{1}{p} \).

Let \( X \) be a r.v. such that \( X = i \) with probability \( P_X(i), i \in \mathbb{N} \) and \( \mathbb{E}[X] = \mu \).
Now let $Y \sim P_Y \equiv Geo(\frac{1}{\mu})$. Therefore, $\mathbb{E}[Y] = \mu$.

Now consider
\[
D(P_X||P_Y) = \sum_{i=1}^{\infty} P_X(i) \log \frac{P_X(i)}{P_Y(i)}
\]
\[
= \sum_{i=1}^{\infty} P_X(i) \log P_X(i) - P_Y(i) \log P_Y(i) + P_Y(i) \log P_Y(i) - P_X(i) \log P_Y(i)
\]
\[
= H(Y) - H(X) + \sum_{i=1}^{\infty} \left[ P_Y(i) \log P_Y(i) - P_X(i) \log P_Y(i) \right]. \tag{1}
\]

Since $P_Y(i) = \left(1 - \frac{1}{\mu}\right)^{i-1} \left(\frac{1}{\mu}\right)$,
\[
\sum_{i=1}^{\infty} P_X(i) \log P_Y(i) = \sum_{i=1}^{\infty} P_X(i) \cdot (i-1) \log(\mu - 1) - \sum_{i=1}^{\infty} P_X(i) \cdot i \cdot \log \mu
\]
\[
= (\mu - 1) \log(\mu - 1) - \mu \log \mu. \tag{2}
\]

From the entropy calculation of a Geometric r.v., we know that,
\[
\sum_{i=1}^{\infty} P_Y(i) \log P_Y(i) = \left(1 - \frac{1}{\mu}\right) \log \frac{1 - \frac{1}{\mu}}{1/\mu} + \left(\frac{1}{\mu}\right) \log \left(\frac{1}{\mu}\right)
\]
\[
= (\mu - 1) \log(\mu - 1) - \mu \log \mu. \tag{3}
\]

Substituting (2) and (3) in (1), we see that,
\[
H(Y) - H(X) = D(P_X||P_Y)
\]
\[
\geq 0.
\]

Therefore, for any r.v. $X \in \mathbb{N}$ with $\mathbb{E}[X] = \mu$, $H(X) \leq H(Y)$ where $Y \sim Geo(\frac{1}{\mu})$.

5. (i) For a Markov chain, $X \Rightarrow Y \Rightarrow Z$, by data processing inequality,
\[
I(X \land Y) \geq I(X \land Z)
\]
\[
\Rightarrow H(X) - I(X \land Y) \leq H(X) - I(X \land Z)
\]
i.e., $H(X|Y) \leq H(X|Z)$.

(ii) Let $\mathcal{X} = S_{52}$ denote the set of all permutations of numbers $\{1, 2, \ldots, 52\}$, namely each element $x \in \mathcal{X}$ represents an order of shuffled cards. A random shuffle of cards can be represented by a channel $W : X \rightarrow \mathcal{X}$. We say that a shuffle is good if it increases the “randomness” in ordering of cards. Formally, a shuffle $W$ is said to be good if for every pmf $P$ on $\mathcal{X}$,
\[
H(P) \leq H(PW).
\]

Claim: A shuffle is good if and only if it does not decrease the entropy of randomly ordered cards (here randomly ordered stand for $X$ distributed uniformly over $\mathcal{X}$).

Proof. Clearly, if a shuffle is good then for a uniform distribution $P_{\text{unif}}(\mathcal{X})$ on $\mathcal{X}$
\[
\log |\mathcal{X}| = H(P_{\text{unif}}(\mathcal{X})) \leq H(P_{\text{unif}}(\mathcal{X})W) \leq \log |\mathcal{X}|,
\]
which can only happen if \( H(P_{\text{unif}}(\mathcal{X})W) = \log |\mathcal{X}| \). Thus, the shuffle does not decrease the entropy of randomly ordered cards, and \( P_{\text{unif}}(\mathcal{X})W \) is uniform as well.

Conversely, suppose a shuffle does not decrease the entropy of randomly ordered cards. Then, \( H(P_{\text{unif}}(\mathcal{X})W) = H(P_{\text{unif}}(\mathcal{X})) = \log |\mathcal{X}| \), and so,
\[
P_{\text{unif}}(\mathcal{X})W = P_{\text{unif}}(\mathcal{X}).
\]

Note that for any pmf \( P \) on \( \mathcal{X} \)
\[
D(P\|P_{\text{unif}}(\mathcal{X})) = \log |\mathcal{X}| - H(P).
\]

Also, since \( P_{\text{unif}}(\mathcal{X})W = P_{\text{unif}}(\mathcal{X}) \),
\[
D(PW\|P_{\text{unif}}(\mathcal{X})W) = \log |\mathcal{X}| - H(PW).
\]

Thus, by the data processing inequality we get
\[
\log |\mathcal{X}| - H(PW) = D(PW\|P_{\text{unif}}(\mathcal{X})W) \\
\leq D(P\|P_{\text{unif}}(\mathcal{X})) \\
= \log |\mathcal{X}| - H(P),
\]

which gives
\[
H(P) \leq H(PW).
\]

Therefore, the shuffle is good if it does not reduce the entropy of randomly ordered cards.

Now, to answer the question asked in the homework, we show that the shuffle mentioned in homework is good. To that end, by the claim above, it suffices to show that it does not reduce the entropy of randomly ordered cards. Specifically, the shuffle in the homework can be described as
\[
W(y|x) = \begin{cases} 
\frac{1}{52} & \text{if } y = (x_i, x_1, ..., x_{i-1}, x_{i+1}, ..., x_{52}) \text{ for some } 1 \leq i \leq 52, \\
0 & \text{otherwise}.
\end{cases}
\]

For \( W \) above, it is easy to see that
\[
P_{\text{unif}}(\mathcal{X})W = P_{\text{unif}}(\mathcal{X}),
\]

which by the claim above shows that shuffle \( W \) is good, i.e.,
\[
H(Y) = H(PW) \geq H(P) = H(X).
\]

6. Let \( p \) denote the maximum probability of guessing \( X \) correctly. Clearly \( p = \max_x P_X(x) \). Let \( \hat{X} \) be the random variable denoting the guess for \( X \). The probability of correctness of the guess could be maximized by always guessing the \( \arg\max_x P_X(x) \). Then, by Fano’s inequality,
\[
H(X|\hat{X}) \leq h(1 - p) + (1 - p) \log(|\mathcal{X}| - 1)
\]

Since the guess is independent of the random variable itself, \( H(X|\hat{X}) = H(X) \).

For conditions of equality, verify from the proof of Fano’s inequality in the class that equality holds in Fano’s inequality if and only if
\[
H(X|\hat{X}, 1(X \neq \hat{X}) = 1) = \log(|\mathcal{X}| - 1).
\]
For the specific case here, this equality holds if and only if
\[ P(X = x | X \neq x_{\text{max}}) = \frac{1}{|\mathcal{X}| - 1}, \quad x \in \mathcal{X} \setminus \{x_{\text{max}}\}, \]
where \( x_{\text{max}} = \arg\max_x P_X(x) \). This in turn holds if and only if \( P_X(x) \) is the same for every \( x \neq x_0 \).

7. If \( X \leftrightarrow Y \leftrightarrow Z \),
\[
I(X \land Y | Z) = H(X | Z) - H(X | Y, Z)
\]
\[ = H(X | Z) - H(X | Y) \quad \text{(by Markovity)}
\]
\[ = H(X | Z) - H(X | Y) + H(X) - H(X)
\]
\[ = H(X | Z) + I(X \land Y) - H(X)
\]
\[ \leq I(X \land Y). \quad \text{(since } H(X | Z) \leq H(X)\text{)}
\]

It is easy to observe that equality is attained if and only if \( X \perp Z \).

- An example where \( I(X \land Y | Z) > I(X \land Y) \): Let \( X \sim \text{Ber}(\frac{1}{2}), Y \sim \text{Ber}(\frac{1}{2}) \) and \( X \perp Y \).
Thus, clearly, \( I(X \land Y) = 0 \). Let \( Z = X \oplus Y \). Verify that \( I(X \land Y | Z) = 1 \).

8. \textit{Shape of } \( D(W||Q|P) \)

(a) To show that \( D(W||Q|P) \) is convex in \( Q \) for a fixed \( P \), let \( Q = \alpha Q_1 + (1-\alpha)Q_2, 0 < \alpha < 1 \).

\[
D(W||Q|P) = \sum (P \circ W)(x, y) \log \frac{W(y|x)}{\alpha Q_1(y) + (1-\alpha)Q_2(y)}
\]
\[ = \sum (P \circ W)(x, y) \log W(y|x) - \sum (P \circ W)(x, y) \log \left[ \alpha Q_1(y) + (1-\alpha)Q_2(y) \right]
\]
\[ \leq \sum \left[ \alpha (P \circ W)(x, y) \log W(y|x) + (1-\alpha)(P \circ W)(x, y) \log W(y|x) \right]
\]
\[ - \sum \left[ \alpha (P \circ W)(x, y) \log Q_1(y) - (1-\alpha)(P \circ W)(x, y) \log Q_2(y) \right]
\]
\[ = \alpha \sum (P \circ W)(x, y) \log \frac{W(y|x)}{Q_1(y)} + (1-\alpha) \sum (P \circ W)(x, y) \log \frac{W(y|x)}{Q_2(y)}
\]
\[ = \alpha D(W||Q_1|P) + (1-\alpha)D(W||Q_2|P).
\]

where the inequality follows by applying Jensen’s inequality to the convex function \( -\log(\cdot) \).

(b) To show that \( D(W||Q|P) \) is linear in \( P \) for a fixed \( Q \), let \( P = aP_1 + bP_2, a, b \neq 0 \).

\[
D(W||Q|P) = \sum P(x)W(y|x) \log \frac{W(y|x)}{Q(y)}
\]
\[ = \sum \left[ aP_1(x) + bP_2(x) \right] W(y|x) \log \frac{W(y|x)}{Q(y)}
\]
\[ = \sum aP_1(x)W(y|x) \log \frac{W(y|x)}{Q(y)} + \sum bP_2(x)W(y|x) \log \frac{W(y|x)}{Q(y)}
\]
\[ = aD(W||Q|P_1) + bD(W||Q|P_2).
\]

Therefore, \( D(W||Q|P) \) is linear in \( P \) for a fixed \( Q \).

9. We will prove the if part first.

(a) Suppose there exists functions \( f : \mathcal{Y} \rightarrow \mathcal{U} \) and \( g : \mathcal{Z} \rightarrow \mathcal{U} \) satisfying
(a) $\mathbb{P}(f(Y) = g(Z)) = 1$
(b) $X \leftrightarrow f(Y) \leftrightarrow (Y, Z)$
(c) $X \leftrightarrow g(Z) \leftrightarrow (Y, Z)$.

Clearly,
\[
I(X \land f(Y)|Y, Z) = H(f(Y)|Y, Z) - H(f(Y)|X, Y, Z)
= 0 = I(X \land g(Z)|Y, Z)
\]

By Markovity,
\[
I(X \land f(Y)|Y, Z) = H(X|Y, Z) - H(X|f(Y))
\quad\text{and,}
I(X \land g(Z)|Y, Z) = H(X|Y, Z) - H(X|g(Z))
\]

Therefore,
\[
H(X|f(Y)) = H(X|Y, Z) = H(X|g(Z))
\quad\text{(4)}
\]

By “conditioning reduces entropy” and Equation (4),
\[
H(X|Y) = H(X|Y, f(Y))
\leq H(X|f(Y))
= H(X|Y, Z)
\leq H(X|Y).
\]

Therefore, all the inequalities above must be equalities. In particular,
\[
H(X|Y) = H(X|Y, Z)
\]

Thus,
\[
I(X \land Z|Y) = H(X|Y) - H(X|Y, Z) = 0 \quad\Rightarrow X \leftrightarrow Y \leftrightarrow Z.
\]

Similarly, $H(X|Z) = H(X|Y, Z)$, and,
\[
I(X \land Y|Z) = H(X|Z) - H(X|Y, Z) = 0 \quad\Rightarrow X \leftrightarrow Z \leftrightarrow Y.
\]

(b) Now, to show the other direction, assume $X \leftrightarrow Y \leftrightarrow Z$ and $X \leftrightarrow Z \leftrightarrow Y$. Then, it follows that
\[
I(X \land Z|Y) = I(X \land Y|Z) = 0.
\quad\text{(5)}
\]

Construct $f$ in the following manner. Divide $Y$ into equivalent classes $[y]$ wherein $y$ and $\hat{y}$ are equivalent if $P_{X|Y}(x|y) = P_{X|Y}(x|\hat{y})$ for all $x$. Let $f(y) \mapsto u$ for all $y \in [y]$. Let $U$ denote the r.v. $f(Y)$. Now,
\[
H(X|U) = -\sum_x \sum_u P_{X,U}(x, u) \log P_{X|U}(x|u)
= -\sum_x \sum_u \sum_{y: f(y) = u} P_{X,Y}(x, y) \log P_{X|Y}(x|y)
= -\sum_x \sum_y \log P_{X,Y}(x, y) \log P_{X|Y}(x|y)
= H(X|Y).
\quad\text{(6)}
Similarly, let \( g(z) \mapsto u \) for all \( z \in [z] \). Let \( V \) denote \( g(Z) \). Then, \( H(X|V) = H(X|Z) \).

Now,

\[
I(X \land YZ|f(Y)) = I(X \land Y|f(Y)) + I(X \land Z|Y)
\]

(by Equation 5)

\[
= I(X \land Y|f(Y))
\]

\[
= H(X|f(Y)) - H(X|Y,f(Y))
\]

(by Equation 6)

\[
\Rightarrow X \leftarrow f(Y) \leftarrow (Y,Z).
\]

Similarly, \( X \leftarrow g(Z) \leftarrow (Y,Z) \).

Now, it remains to be shown that \( P[f(Y) = g(Z)] = 1 \).

Since \( X \leftrightarrow Y \leftrightarrow Z \) and \( X \leftrightarrow Z \leftrightarrow Y \), \( P_{Y,Z}(xyz) = P_{X,Y}(x|y) = P_{X|Z}(x|z) \) for every \( y, z \) such that \( P_{Y,Z}(y,z) > 0 \). Thus, the conditional distribution \( P_{X|Y,Z} \) can be determined from \( y \) or \( z \). Therefore, we can choose the mappings \( f \) and \( g \) in such a way that for \( \tilde{y}, \tilde{z} \) such that \( P_{Y,Z}(\tilde{y},\tilde{z}) > 0 \), \( f(\tilde{y}) = u \) and \( P_{X|Y}(\cdot|\tilde{y}) = Q \), then \( g(\tilde{z}) = u \) for \( \tilde{z} \) with \( P_{X|Z}(\cdot|\tilde{z}) = Q \).

10. Let \( X \) be distributed uniformly over all subsets of \( \{1, ..., n\} \) of size less than or equal to \( np \).

Let \( X_i = 1 \) (\( i \in X \)), i.e., \( X_i \) is 1 if the random set contains the element \( i \) and 0 otherwise. Thus, \( X = (X_1, ..., X_n) \).

Note that the number of values taken by the random variable is \( \sum_{i \leq np} \binom{n}{i} \).

Thus,

\[
\log \sum_{i \leq np} \binom{n}{i} = H(X)
\]

\[
= H(X_1, ..., X_n)
\]

\[
\leq \sum_{i=1}^{n} H(X_i)
\]

\[
= nH(X_1),
\]

(7)

where in the last step we used the fact that random variables \( X_i \)'s have the same distribution.

To bound \( H(X_1) \), we bound \( P(X_1 = 1) \). To that end, note that for every \( \delta \leq p \)

\[
P(X_1 = 1|X = n\delta) = \frac{\text{number of subsets of } [n] \text{ of size } n\delta \text{ containing } 1}{\text{number of subsets of } [n] \text{ of size } n\delta}
\]

\[
= \frac{\binom{n-1}{n\delta-1}}{\binom{n}{n\delta}}
\]

\[
= \delta
\]

\[
\leq p.
\]

Therefore, \( P(X_1 = 1) \leq p \). Since \( h(\delta) \) is increasing in \( \delta \) for \( 0 \leq \delta \leq 1/2 \),

\[
H(X_1) = h(\mathbb{P}(X_1 = 1)) \leq h(p),
\]

which together with (7) completes the proof.