# Information Theory Notes

Sidney Golstein

April 9, 2020

## 1 Information Measures (ch2 p18)

Here, only for discrete random variables (RV).

### 1.1 Entropy

#### 1.1.1 General definition

Let $\mathbf{X}$ be a discrete RV with pmf $p(x)$. The entropy of $\mathbf{X}$ is the uncertainty about its outcome:

$$H(\mathbf{X}) = -\sum_{x \in \chi} p(x) \log p(x) = -E_{\mathbf{X}} \left( \log p(\mathbf{X}) \right) \tag{1}$$

where $\chi$ is the set of possible values of $x$, i.e., the alphabet.

#### 1.1.2 Conditional entropy

Measure of the remaining uncertainty about the outcome of $\mathbf{Y}$ given the observation $\mathbf{X}$. Denoted $H(X|Y)$

$$H(\mathbf{X}|\mathbf{Y}) = -E_{\mathbf{X},\mathbf{Y}} \left( \log p(\mathbf{Y}|\mathbf{X}) \right) \tag{2}$$

#### 1.1.3 Joint entropy

Let ($\mathbf{X}$,$\mathbf{Y}$) be a pair of discrete RV:

$$H(\mathbf{X}, \mathbf{Y}) = -E \left( \log p(\mathbf{X}, \mathbf{Y}) \right) \tag{3}$$

### 1.1.4 Properties

$$H(\mathbf{Y}|\mathbf{X}) \leq H(\mathbf{Y}) \quad (4)$$
$$H(\mathbf{X},\mathbf{Y}) = H(\mathbf{X}) + H(\mathbf{Y}|\mathbf{X}) = H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y}) \quad (5)$$
$$H(\mathbf{X},\mathbf{Y}) \leq H(\mathbf{X}) + H(\mathbf{Y}) \quad (6)$$

## 1.2 Mutual Information

### 1.2.1 General definition

Let ($\mathbf{X}$,$\mathbf{Y}$) be a pair of discrete RV. The information about $\mathbf{X}$ obtained from the observation $\mathbf{Y}$is the mutual information between $\mathbf{X}$ and $\mathbf{Y}$.

$$I(\mathbf{X};\mathbf{Y}) = \sum_{(x,y)\in(\chi,\Upsilon)} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} = H(\mathbf{X}) + H(\mathbf{Y}) - H(\mathbf{X},\mathbf{Y}) \quad (7)$$

$I(\mathbf{X};\mathbf{Y}) = 0$ i.i.f. $\mathbf{X}$ and $\mathbf{Y}$ are independent.

### 1.2.2 Conditional mutual information

The conditional mutual information etween $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{Z}$ is:

$$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) = H(\mathbf{X}|\mathbf{Z}) + H(\mathbf{Y}|\mathbf{Z}) - H(\mathbf{X},\mathbf{Y}|\mathbf{Z}) \quad (8)$$

#### Properties

- Independence:
  If $\mathbf{X}$ and $\mathbf{Z}$ are independent:
  $$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) \geq I(\mathbf{X};\mathbf{Y}) \quad (9)$$
- Conditional independence:
  If $\mathbf{Z} \to \mathbf{X} \to \mathbf{Y}$ for a Markov chain (prediction of the future state only depends on the present state and not on the previous ones):
  $$I(\mathbf{X};\mathbf{Y}|\mathbf{Z}) \leq I(\mathbf{X};\mathbf{Y}) \quad (10)$$

## 1.3 Summary

The entropy is a measure of information. The mutual entropy is a measure of information transfer.

# 2 Information Theoretic Secrecy (ch22 p549)

TEST ok