Shannon's Theory

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology Sri City

odelu.vanga@iiits.in

January 28, 2021

Today's Objectives

- Discrete Random Variable
- Probability Distribution
- Joint Probability
- Conditional Probability
- Bayes' Theorem

Introduction

- In 1949, Claude Shannon published a paper entitled "Communication Theory of Secrecy Systems" in the Bell Systems Technical Journal.
- This paper had a great influence on the scientific study of cryptography.

Computational security

- A cryptosystem is computationally secure if the best algorithm for breaking it requires at least N operations, where N is some specified, very large number.
- The problem is that no known practical cryptosystem can be proved to be secure under this definition.
- In practice, often we study the *computational security* of a cryptosystem w.r.t. certain specific type of attack. For example, exhaustive key search

Provable security

- Provide evidence of computational security by reducing the security of the cryptosystem to some well-studied problem that is thought to be difficult.
- For example, "a given cryptosystem is secure if a given integer n cannot be factored"
- This approach only provides a proof of security relative to some other problem, not an absolute proof of security.

Unconditional security

A cryptosystem is defined to be unconditionally secure if it cannot be broken, even with infinite computational resources

Discrete Random Variable

- An experiment is a procedure that yields one a given set of outcomes.
- Individual outcomes are called sample events
- The set of all possible outcomes called sample space, denoted by S.

Definition (Random Variable (r.v.))

A r.v. is a function, say X, is a function from the sample space S to the set of real numbers.

A r.v X takes finite or countably infinite number of values called a discrete r.v.

Probability Distribution

Definition (Discrete Probability Distribution)

Let X be a discrete r.v., and suppose that the possible values that it can take are x. The probability that the random variable X takes value x is denoted by $Pr[X = x]$, and must satisfy the following

$$Pr[X = x] \geq 0, \text{ for all } x \in X$$
$$\sum_{x \in X} Pr[X = x] = 1$$

Example: Tossing pair of fair coins

Joint and Conditional Probability

– probability that X takes on the value x by $Pr[x]$

– probability that Y takes on the value y by $Pr[y]$

Definition (Joint Probability)

Suppose X and Y are random variables. The joint probability $Pr[x, y]$ is the probability that X takes on the value x and Y takes on value y.

Definition (Conditional Probability)

The conditional probability $Pr[x|y]$ denotes the probability that X takes on the value x given that Y takes on the value y.

Example: Tossing pair of fair dice

Bayes' Theorem

Joint probability can be related to conditional probability by the formula

$$Pr[x, y] = Pr[x|y]Pr[y]$$

Then we have

$$Pr[x, y] = Pr[y|x]Pr[x]$$

Theorem (Bayes' Theorem)

If $Pr[y] > 0$, then

$$Pr[x|y] = \frac{Pr[x]Pr[y|x]}{Pr[y]}$$

The random variables X and Y are said to be independent if $Pr[x, y] = Pr[x]Pr[y]$ for all possible values x of X and y of Y.

Perfect Secrecy

Assumptions:

1. Cryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ is specified.
2. A particular key $k \in \mathcal{K}$ is used for only one encryption.
3. Plaintext $\mathcal{P}$ defines a r.v. denoted by X, and a priory probability that plaintext occurs denoted by $Pr[X = x]$.
4. The key chosen with some fixed probability distribution, so key also defines a r.v., denoted by K. Denote the probability that key K is chosen by $pr[K = k]$.
5. The probability distributions on $\mathcal{P}$ and $\mathcal{K}$ induce a probability distribution on $\mathcal{C}$. So, ciphertext also a r.v., denoted by Y.

Note that key is chosen before the plaintext knows, so that plaintext and key are independent r.v.'s.

Perfect Secrecy

- For a key $k \in \mathcal{K}$, we define

$$C(k) = \{E_k(x) : x \in \mathcal{P}\}$$

The set of all possible ciphertexts if k is the key

- For every $y \in \mathcal{C}$, we have

$$Pr[Y = y] = \sum_{\{k: y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]$$

Note $x = D_k(E_k(x)) = D_k(y)$

- For $y \in \mathcal{C}$ and $x \in \mathcal{P}$, we have

$$Pr[Y = y | X = x] = \sum_{\{k: x = D_k(y)\}} Pr[K = k]$$

Bayes' Theorem

$$Pr[X = x | Y = y] = \frac{Pr[X = x] \sum_{\{k : x = D_k(y)\}} Pr[K = k]}{\sum_{\{k : y \in C(k)\}} Pr[K = k] Pr[X = D_k(y)]}$$

Example

Let $\mathcal{P} = \{a, b\}$ with $Pr[a] = 1/4$, $Pr[b] = 3/4$
$\mathcal{K} = \{k_1, k_2, k_3\}$ with $Pr[k_1] = 1/2$, $Pr[k_2] = Pr[k_3] = 1/4$,
and $\mathcal{C} = \{1, 2, 3, 4\}$.
Suppose encryption rule is defined as

$E_k(x)$	a	b
k_1	1	2
k_2	2	3
k_3	3	4

Find the probability $Pr[X = x | Y = y]$