18733: Applied Cryptography Recitation

Discrete Probability Theory Review

Gihyuk Ko

January 20, 2017

Carnegiel Mellon University

Discrete Probability Theory and Cryptography

Q. What is Discrete Probability Theory?

- **Discrete** finite, countable sets
- **Probability** likelyhood, chance of event
- **Theory** formal representation, used for proof

A. A *formal representation* which deals with the *probability of events* that occur in *countable sample spaces*.

Q. Why are we using it to study Cryptography?
A. We want to *prove* that an adversary who tries to break a certain protocol has only miniscule(‘negligible’) *probability of succeeding* (and the protocol usually deals with *finite* number of events).

Probability Distribution

Sample Space U

U is a **finite** set, i.e. $|U| \in \mathbb{N}$

ex) coin flips $U = \{heads, tails\}, |U| = 2$

ex) dice roll $U = \{1, 2, 3, 4, 5, 6\}, |U| = 6$

ex) n-bit random number $U = \{0, 1\}^n, |U| = 2^n$

Probability Distribution P: $U \to [0, 1]$

P is a function from U to $[0, 1]$ s.t. $\displaystyle\sum_{x \in U} P(x) = 1$

Uniform Distribution

A probability distribution P s.t. $\forall x \in U. P(x) = \frac{1}{|U|}$

i.e., every *elements* in U have same *probability mass*

Events

Event $A \subseteq U$

An event A is a subset of sample space U.

Probability of event A:

$$Pr[A] = \sum_{a \in A} P(a)$$

Note the difference between $Pr[\cdot]$ and $P(\cdot)$

- More formally, $Pr[\cdot] : 2^U \to [0, 1]$
- $P(\cdot)$ is (normally) called a *probability mass function*

ex) odd-numbered fair dice roll:

$U = \{1, 2, 3, 4, 5, 6\}, A = \{1, 3, 5\}, P(i) = \frac{1}{6}$ for $\forall i$
$Pr[A] = \frac{1}{2}$

Example: Bernoulli(binomial) Distribution

Assume flipping n biased coins where each coins have probability of turning out head p ($0 \leq p \leq 1$).

Sample space $U = \{0, 1\}^n$

Probability distribution $P(x)$ for x which have k ones

$$P(x) = p^k(1 - p)^{n-k}$$

Event $A_k = \{a|$ **there are** k **ones in** $a\}$

$$P[A_k] = \binom{n}{k} p^k(1 - p)^{n-k}$$

Union Bound

For events A_1 and A_2:

$$Pr[A_1 \cup A_2] \leq Pr[A_1] + Pr[A_2]$$

The probability of the union of two events cannot exceed their sum

Useful when it is difficult to calculate exact probability

Random Variable

A **Random Variable** X is a function $X : U \to V$

ex) $X : \{0,1\}^n \to \{0,1\}, X(u) = lsb(u)\ \forall u \in \{0,1\}^n$

X *induces* a *probability distribution* on V from $P'(v) := Pr[X = v]$

1. $(X = v) := \{u | X(u) = v\}$ **Event**
2. $0 \leq Pr[X = v] \leq 1$ **Probability**
3. $P' : V \to [0,1]$ **Distribution**

$P'(v) := Pr[X = v]$ is a *probability distribution* on V!

X is called a **Uniform Random Variable** if the induced distribution is uniform

ex) Let r be the identity function sampled uniformly over U: $r(u) = u$

$r \leftarrow_R U, \forall a \in U : Pr[r = a] = \frac{1}{|U|}$

Independence

Events A and B are **independent** if

$$Pr[A \cap B] = Pr[A]Pr[B]$$

Random variables $X : U \to V$, $Y : U \to W$ are **independent** if

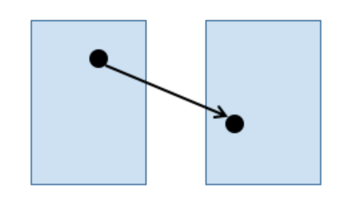
$$\forall v \in V, \forall w \in W. Pr[X = v \cap Y = w] = Pr[X = v]Pr[Y = w]$$

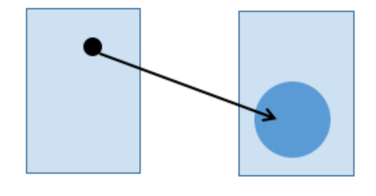
Randomized Algorithms

Deterministic Algorithm: $y \leftarrow A(m)$

Randomized Algorithm: $y \leftarrow A(m, r)$, $r \leftarrow_R \{0, 1\}^n$

r is given 'implicitly' as an output of a uniform random variable





Idea: Think of the input as a message and random factor as an "encryption key"

XOR: eXclusive OR

X	Y	$X \oplus Y$
0	0	0
0	1	1
1	0	1
1	1	0

Table 1: Exclusive Or Truth Table

$$x \oplus x = 0 \qquad x \oplus 0 = x$$

$$\begin{array}{cccccc l} 0 & 1 & 1 & 0 & 1 & 0 & \\ 1 & 1 & 0 & 0 & 1 & 1 & \oplus \\ \hline 1 & 0 & 1 & 0 & 0 & 1 & \end{array}$$

XOR: eXclusive OR (cont'd)

Let X, Y random variable over $\{0,1\}^n$. If X is a *uniform random variable independent* to Y, then $Z = X \oplus Y$ is uniform over $\{0,1\}^n$

Intuition: take something predictable, XOR it with something uniform, the result is completely uniform.

proof(n=1). Let $Pr[Y=0] = p, Pr[Y=1] = 1-p$

X	Y	$X \oplus Y$	$Pr[\cdot]$
0	0	0	$\frac{p}{2}$
0	1	1	$\frac{1-p}{2}$
1	0	1	$\frac{p}{2}$
1	1	0	$\frac{1-p}{2}$

from the given table, we have $Pr[Z=0] = Pr[Z=1] = \frac{1}{2}$. $\square$

... how can we prove when $n \geq 2$?

Birthday Paradox

In a set of n randomly chosen people, what is the probability of finding a pair with same birthday? – *Birthday Problem*

Let $r_1, \dots, r_n \in U$ be i.i.d.(*independent and identically distributed*) random variables
Theorem: when $n = 1.2 * \sqrt{|U|}$, then $Pr[r_i = r_j] \geq 0.5$

ex) $U = \{0, 1\}^{128}$, after sampling about 2^{64}, we will likely find a collision.

Application: Keys must be changed more quickly than we might expect in some applications, and “collision resistant” functions must be made sufficiently strong

Questions?