Probability Reminder

Cryptography and Protocols
Andrei Bulatov

Sample Space and Outcomes

- Experiment s and outcomes
- Sample space is the set of all possible outcomes
- Examples
  - flipping a coin Ω = {heads, tails}
  - flipping a pair of coins Ω = {HH, HT, TH, TT}
  - horse race (7 horses) Ω = {all 7! permutations of (1,2,3,4,5,6,7)}
  - tossing two dice Ω = {11,12, … , 66}

  flipping k coins $\Omega = \{0,1\}^k$

Events

- Event is any subset of the sample space
- Examples
  - any outcome is an event (a 1-element subset)
  - getting even number of heads when flipping a pair of coins
  - horse no. 4 came second
  - getting at least one 3 when tossing two dice
- Algebra of events
  - union of events
  - intersection
  - complement
  - mutually exclusive events

Probability: Case of Equally Likely Outcomes

- If all the outcomes are equally likely, then the probability of event A equals

$$Pr[A] = m/n$$

where m is the number of outcomes in A, and n the total number of outcomes

- Examples
  - getting even number of heads when flipping a pair of coins
  - horse no. 4 came second
  - getting at least one 3 when tossing two dice

Probability: General Case

- The probability of event A is a positive number $Pr[A]$
- Axioms:
  - $0 \le Pr[A] \le 1$
  - $Pr[\Omega] = 1$
  - for any events A, B such that $AB = \emptyset$

$$Pr[A \cup B] = Pr[A] + Pr[B]$$

- Examples
  - what is the probability to get both heads and tails flipping 3 identical coins?

Distribution

- In the general case each outcome a is associated with probability it happens Pr[{a}] , or just Pr[a]. The collection of these numbers is called a distribution
- Examples
  - uniform distribution: all outcomes are equally likely
  - important uniform distribution, U_n selecting an n-bit string
  - crooked die: Pr[1] = 1/3, Pr[2] = Pr[3] = Pr[4] = Pr[5] = 1/6, Pr[6] = 0

Properties of Probability

- $\Pr[\overline{A}] = 1 - \Pr[A]$
- If $A \subseteq B$ then $\Pr[A] \leq \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[AB]$
- Examples

  - what is the probability to get at least one heads flipping 33 coins?

Conditional Probability

- The probability of event A conditional on event B is the probability that A happened if it is known that B happened
- Example

  Toss two dice. What is the probability that the sum of the two dice is 8 if the first die is 3?
- Probability of A conditional on B is denoted Pr[A | B]
- This probability equals

$$\Pr[A \mid B] = \frac{\Pr[AB]}{\Pr[B]}$$

- Multiplication rule: Pr[AB] = Pr[A] · Pr[B|A]

Independent Events

- Events A,B are independent if $Pr[A|B] = Pr[A]$ and $Pr[B|A] = Pr[B]$
- Examples:
  - flipping two coins A = {first coin is heads} , B = {second coin is heads}
  - tossing two dice A = {sum of the dice is 3}, B = {first die is even}

Random Variables

- A random variable is a function of the outcomes
- Formally: $X\colon \Omega \to \mathbb{R}$
- Discrete random variable: $X : \Omega \to \{x_1, \ldots, x_k\}$
- Examples:
  - sum of two dice
  - number of heads
  - lifetime of an electric bulb
- Sum and product of random variables $X + Y$, XY, aX

Distribution of Random Variable

- Let X be a discrete random variable with values $x_1, \ldots, x_k$
Then its distribution is a collection of numbers $p_1, \ldots, p_k$ such that
$$\Pr[X = x_i] = p_k$$
- Note: $$\sum_{i=1}^{k} p_i = 1$$
- Examples:

  - uniform distribution : all probabilities are equal, e.g. random variable X with values 0 = heads and 1 = tails when flipping a coin (Bernoulli random variable)

  - sum of two dice is not uniform

  - number of heads when flipping k coins

  - more general – binomial random variable: the number of successes in k repetitions of the same experiment (*independent*!); each repetition is successful with probability p

Binomial Random Variable

- Suppose that the outcomes of the experiment are bits 0 and 1

  1 happens with probability p
- The probability of a particular string with m 1s: $p^m(1-p)^{k-m}$
- The probability of a string with m 1s:

$$\Pr[N=m]=\binom{k}{m}p^m(1-p)^{k-m}$$

- Let N_i be the random variable that equals the number of successes in the i'th experiment. Then

$$N = N_1+\cdots+N_k$$

Expectation

- The expectation of a random variable is its `median' value
- Formally, if V is the set of possible values of a random variable X, then

$$\mathbb{E}(X) = \sum_{v \in V} v \cdot \Pr[X = v]$$

- Properties of expectation:
  - let X be a random variable, let a be a number then

    $\mathbb{E}(aX) = a \cdot \mathbb{E}(X)$

  - let X and Y be random variables then

    $\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$

Expectation (cntd)

- Example

  Lottery: 1000000 tickets, 4 tickets win \$1000000, 5 tickets win \$100000, 5000 tickets win \$1000. What is the average win?

- Expectation of Bernoulli random variable

  Pr[N=1] = p, Pr[N=0] = 1-p

  E(N) = p

- Expectation of the binomial random variable (k trials):

$$E(N) = E(N_1 + \cdots + N_k)$$
$$= E(N_1) + \cdots + E(N_k) = k \cdot p$$

Independent Random Variables

- Random variables X and Y are independent if for any value v of X and any value w of Y the events $X = v$ and $Y = w$ are independent
- Example
  - flipping 2 coins, N and N_1 are independent
- Properties of expectation
  - if X and Y are independent then $\mathbb{E}(XY) = \mathbb{E}(X) \cdot \mathbb{E}(Y)$

Markov's Inequality

- If a random variable X is non-negative, then

$$\Pr[X \geq k] \leq \frac{\mathbb{E}(X)}{k}$$

- Examples

  - $\Omega = \{0,1\}^k, \qquad X = N$

$$\underbrace{\Pr[X \geq k]}_{= 1/2^k} \leq \frac{\mathbb{E}(X)}{k} = \frac{k/2}{k} = \frac{1}{2}$$

  - $\Omega = \{00\ldots0, 11\ldots1\}$ $\qquad \underbrace{\Pr[X \geq k]}_{= 1/2} \leq \frac{\mathbb{E}(X)}{k} = \frac{k/2}{k} = \frac{1}{2}$

Randomized Algorithms

- An algorithm that has access to random bits, that is can flip coins, is called randomized
- The sample space associated with such an algorithm is the set of possible bit strings
- A random variable associated with it is, for instance, the running time