Design and Analysis of Algorithms I

Probability Review

Part II

Topics Covered

- Conditional probability
- Independence of events and random variables

See also:

- Lehman-Leighton notes (free PDF)
- Wikibook on Discrete Probability

Concept #1 – Sample Spaces

Sample Space Ω : "all possible outcomes"
[in algorithms, Ω is usually finite]

Also : each outcome $i \in \Omega$ has a probability p(i) >= 0

Constraint : $\sum_{i \in \Omega} p(i) = 1$

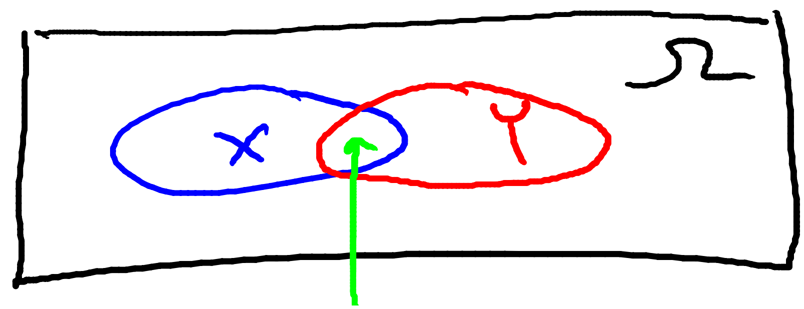
An event is a subset $S \subseteq \Omega$

The probability of an event S is $\sum_{i \in S} p(i)$

Tim Roughgarden

Concept #6 – Conditional Probability

$$Let \quad X, Y \subseteq \Omega \quad be \quad events.$$



$X \cap Y$

$$Then \quad Pr[X|Y] = \frac{Pr[X \cap Y]}{Pr[Y]}$$

("X given Y")

Ter
ver

Suppose you roll two fair dice. What is the probability that at least one die is a 1, given that the sum of the two dice is 7?

- $^1/_{36}$
- $^1/_6$
- $^1/_3$
- $^1/_2$

X = at least one die is a 1

Y = sum of two dice = 7

= {(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)}

$$=> X \cap Y = \{(1,6),(6,1)\}$$

$$Pr[X|Y] = \frac{Pr[X \cap Y]}{Pr[Y]} = \frac{(2/36)}{(6/36)} = \frac{1}{3}$$

Concept #7 – Independence (of Events)

<u>Definition</u> : Events $X, Y \subseteq \Omega$ are independent if (and only if) $Pr[X \cap Y] = Pr[X] \cdot Pr[Y]$

<u>You check</u> : this holds if and only if Pr[X | Y] = Pr[X]
<==> Pr[Y|X] = Pr{Y]

<u>WARNING</u> : can be a very subtle concept.
(intuition is often incorrect!)

Independence (of Random Variables)

Definition : random variables A, B (both defined on Ω)
are independent if and only if the events Pr[A=1], Pr[B=b] are independent for all a,b. [<==> Pr[A = a and B = b] = Pr[A=z]*Pr[B=b]]

Claim : if A,B are independent, then E[AB] = E[A]*E[B]

Proof :
$$E[AB] = \sum_{a,b} (a \cdot b) \cdot Pr[A = a \ and \ B = b]$$
$$= \sum_{a,b} (a \cdot b) \cdot Pr[A = a] \cdot Pr[B = b]$$ (Since A,B independent)
$$= \underbrace{\left(\sum_a a \cdot Pr[A = a]\right)}_{E[A]} \underbrace{\left(\sum_b b \cdot Pr[B = b]\right)}_{E[B]}$$

Q.E.D.

Tim Roughgarden

Example

Let $X_1, X_2 \in \{0,1\}$ be random, and $X_3 = X_1 \overset{\text{XOR}}{\oplus} X_2$

formally : $\Omega = \{000, 101, 011, 110\}$, each equally likely.

Claim : X_1 and X_3 are independent random variables (you check)

Claim : X_1X_3 and X_2 are not independent random variables.

Proof : suffices to show that

$$\underbrace{E[X_1X_2X_3]}_{=0} \neq \underbrace{E[X_1X_3]}_{= E[X1]E[X3] = 1/4}\,\overbrace{E[X_2]}^{= 1/2}$$

Since X_1 and X_3 independent

Tim Roughgarden