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

Review

<u>Sample space Ω</u> = "all possible outcomes"

[in algorithms, Ω is usually finite]

<u>Also</u>: each outcome $i \in \Omega$ has a <u>probability</u> $p(i) \geq 0$.

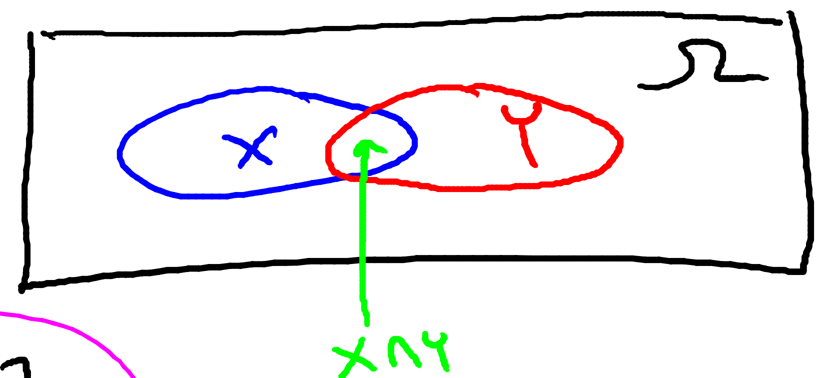
<u>Constraint</u>: $\sum_{i \in \Omega} p(i) = 1$.

An <u>event</u> is a subset $S \subseteq \Omega$.

The <u>probability of an event S</u> is $\sum_{i \in S} p(i)$.

Concept #6 – Conditional Probability

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



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

("X given Y")

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

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

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

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

Concept #7 – Independence (of Events)

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

You check: this holds $\Longleftrightarrow \Pr[X | Y] = \Pr[X]$

$\Longleftrightarrow \Pr[Y | X] = \Pr[Y]$

WARNING: 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 $\Leftrightarrow$ the events $\Pr[A=a]$, $\Pr[B=b]$ are independent for all a, b. [$\Leftrightarrow \Pr[A=a$ and $B=b] = \Pr[A=a] \cdot \Pr[B=b]$)

Claim: if A, B are independent, then $E[A \cdot B] = E[A] \cdot E[B]$.

Proof: $E[A \cdot B] = \sum_{a,b} (a \cdot b) \cdot \Pr[A=a \text{ and } B=b]$

$= \sum_{a,b} (a \cdot b) \cdot \Pr[A=a] \cdot \Pr[B=b]$ (since A, B independent)

$= \underbrace{\sum_a a \cdot \Pr[A=a]}_{E[A]} \underbrace{\left(\sum_b b \cdot \Pr[B=b]\right)}_{E[B]}$ QED!

Tim Roughgarden

Example

XOR

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

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

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

Claim: $X_1 X_3$ and X_2 are not independent random variables.

Proof: Suffices to show that

$$\underbrace{E[X_1 X_3 X_2]}_{=0} \neq \underbrace{E[X_1 X_3]}_{E[X_1]E[X_3] = 1/4} \overbrace{E[X_2]}^{1/2}$$

since X_1 and X_3 independent

QED!

Tim Roughgarden