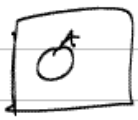
Probability for Crypto

Note Title 2/14/2006

Let P a function that assigns values to sets.

$A \subseteq E$ $\quad \phi^c = E$



a) $P(\phi) = 0$

b) $P(A) \leq 1$

c) $P(A^c) + P(A) = 1$

d) $A_1, A_2 \quad A_1 \cap A_2 = \phi \Rightarrow P(A_1 \cup A_2) = P(A_1) + P(A_2)$

Example: choose a number m between $\{0, \ldots, n-1\}$ Let $n = p_1^{e_1} \cdots p_r^{e_r}$.

Let A_i be $p_i \mid m$

what is $Pr\{\bar{A}_1 \cap \bar{A}_2 \cdots \bar{A}_r\} = ?$

$= \frac{\phi(n)}{n}$

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

Bayes Rule

Let $A_1, \ldots, A_\infty$ be a partition of the sample space & B be any set

$$P(A_i|B) = \frac{P(B|A_i)\, P(A_i)}{\sum P(B|A_j)\, P(A_j)}$$

Assume D_1, D_2, D_3

$D_i = 1$ if it has a car.

D_2 is chosen, D_3 is opened

Do you switch to D_1?

$Pr\{$ stay with 1 | one is open $\} = \frac{1}{3}$

$Pr\{$ switch | one bad door is open $\}$

$=$

$Pr\{$ good is chosen $\} = \frac{1}{3}$

$Pr\{$ Bad is chosen $\} = \frac{2}{3}$

$$0 \cdot \frac{1}{3} + 1 \cdot \frac{2}{3} = \frac{2}{3}$$

A & B indep. $\Leftrightarrow$ $P(A \cap B) = P(A) \cdot P(B)$

A r.v. is a function from a sample space S into the real numbers.

Experiment: Toss two dice

R.V. X = sum of the numbers

$P(X = x_i) = P(s_j \in S,\ X(s_j) = x_i)$

$P(X=10) = P((s_1, s_2) \in S,\ X((s_1, s_2)) = s_1 + s_2 = 10)$

$= \frac{1}{12}$

c.df of r.v

$F_X(x) = P_X(X \leq x)$

3 coins, X = number of heads observed

$$F_X(x) = \begin{cases} 0 & \text{if } -\infty < x < 0 \\ \frac{1}{8} & \text{if } 0 \le x < 1 \\ \frac{1}{2} & \text{if } 1 \le x < 2 \\ \frac{7}{8} & \text{if } 2 \le x < 3 \\ 1 & \text{if } 3 \le x < \infty \end{cases}$$

$$E(X) = \begin{cases} \sum_{x \in X} x f_x(x) \\ \sum_{x \in X} x P(X = x) \end{cases}$$

$$X_1 = \begin{cases} 1 & p \\ 0 & 1-p \end{cases}$$

$$E(X_1) = 1 \cdot p + 0 \cdot (1-p) = p$$

$$E(X_1 + X_2) = E(X_1) + E(X_2)$$

Linearity of Expectation

$$Var(X) = E[(X - E(X))^2]$$
$$= E[X^2 - 2X E[X] + E^2[X]]$$
$$= E[X^2] - E^2[X]$$

$$Var(aX+c) = a^2 Var(X)$$

$$cov(X,Y) = E((X-\mu_x).(Y-\mu_y))$$

$\mu_x = E[X]$, $\mu_y = E[Y]$

X & Y indep : $E[X.Y] = E[X].E[Y]$

$\Rightarrow cov(X,Y) = 0$

$E[X - E[X]] = E[X] - E[E[X]] = 0$

$$corr(X,Y) = \frac{cov(X,Y)}{\sqrt{Var(X).Var(Y)}}$$

$X' = X - \mu_x$

$Y' = Y - \mu_y$

$E[X'.Y'] = E[X'].E[Y']$

$E[X - \mu_x]$

$= E[X] - \mu_x = 0$

---

corr (X, X)

---

chebycheuls Inequality

$$P(X \geq r) \leq \frac{E(X)}{r}$$ X is positive r.v

Proof:

$$E(X) = \sum_x x\,P(x)$$

$$= \sum_{x<r} x\,P(x) + \sum_{x\geq r} x\,P(x)$$

$$\geq \sum_{x\geq r} x\,P(x) \quad \text{(why?)}$$

$$\geq \sum_{x\geq r} r\,P(x) \overset{?}{\geq} r\,P(x\geq r)$$ □

Bernoulli trials with n, p i.e $B(n,p)$

$$E(B(n,p)) = np$$

$$Var(B(n,p)) = np(1-p)$$

$$P(X=x \mid n,p) = \binom{n}{x} p^x (1-p)^{n-x}$$

ERROR: undefined
OFFENDING COMMAND:

STACK: