mit math lectures 20 and 21

Yunhua Zhao

November 16, 2020

1 Chapter 20 Summary

1.1 Independent Definition

Def: If $P(A|B) = P(A)$, then A is independent of B

1. disjoint can not get independent
eg. two events A and B are disjoint, then $P(A|B) = 0 \neq P(A)$

2. Theorem(Product Rule For Independent Events): If A is independent of B, then $P(A \wedge B) = P(A)P(B)$
It is an equivalent definition, which means if $P(A \wedge B) = P(A)P(B)$, then A is independent of B

3. Theorem(Symmetry of Independence): If A is independent of B,then If B is independent of A

1.2 Mutually Independent

Def: Events $A_1, A_2...$ are mutually independent,
if $\forall_i$ and $\forall J \subseteq [1, n] - i$, $P(A_i | \bigcap_{j \in J} A_j) = P(A_i)$ or $P(\bigcap_{j \in J} A_j) = 0$
Equivalent Def:(Product Rule Form): $A_1, A_2...$ are mutually independent,
If $\forall J \subseteq [1, n]$, $P(\cap_{j \in J} A_j) = \prod_{j \in J} P(A_j)$

Note: all the events are independent with each other, and put them together also independent

1.3 Pairwise Independent

Def: Events $A_1, A_2...$ are pairwise independent,
if $\forall i$, j $(i \neq j)$, A_i and $A_j$are independent.

Note: all the events are independent with each other, but put them together not sure if it is independent

Note:
pairwise $\nRightarrow$ mutual
mutual $\Rightarrow$ pairwise

Stirling's formula: $N! \sim \sqrt{2\pi N}(\frac{N}{e})^N$

1.4 Birthday Principle: x collides with y

hash: $L \to S$, and $L' \subseteq L$, L' is pretty small, we want L' after hash matched one by one
Def: x collides with y, if $h(x) = h(y)$, but $x \neq y$
Def Birthday Principle: If $|S| \geqq 100$, $L' \subseteq L$, $|L'| \geqq 1.2\sqrt{|S|}$, and if the values of h on L' are random(uniform) and mutually independent, then with prob $\geqq 1/2$, $\exists x, y \in L'$, such that $x \neq y$, but $h(x) = h(y)$

2 Chapter 21 Summary

2.1 Random Variable

Def: A random variable R is a function
$R : S \to R$, first IR is the random variable, S is the sample space, the second IR is the reals.
Def: $P(R = x) = \sum^{w:R(w)=x} P(w)$, which means the probability of the random variable is x equal to the probability of the event happens. Suit for the set also.
Def: Two random variable($r.v.$) R_1 and R_2 are independent if
$\forall x_1, x_2 \in IR$, $P(IR_1 = x_1 | IR_2 = x_2) = P(IR_1 = x_1)$ or $P(IR_2 = x_2)$
Equivalent Def: $\forall x_1, x_2 \in IR$, $P(IR_1 = x_1 \wedge IR_2 = x_2) = P(IR_1 = x_1)P(IR_2 = x_2)$

Note: If asked to show independent, need to show everything required, if dependent just find one

2.2 Indicator

Def An indicator(known as Bernoulli or Characteristic):
$r.v.$ is a $r.v.$ with range $0, 1$
$w|R(w) = x$ is the event that $R = x$, R is the random variable

2.3 Mutually Independent

Def mutually independent $r.v.$: $R_1, R_2, ...$ are mutually independent
if $\forall x_1, x_2 ... \in IR$, $P(IR_1 = x_1 \wedge IR_2 = x_2 \wedge ...) = P(IR_1 = x_1)P(IR_2 =$

$x_2)P(IR_3 = x_3)$...

2.4 Distribution Function

Def: Given a *rv* R, the probability(also point) distribution function (pdf) for R is $f(x) = P(R = x)$
Def: The cumulative distribution function F for R is $F(x) = P(R \leqq x) = \sum_{y \leqq x} P(R = y)$

2.5 Winning Strategy—Random Guess(uniform distribution problem eg)

Note: Improve the probability to win
$1/2 + (z - y)/2n \geqq 1/2 + 1/2n$

2.6 Binomial Distribution

Def Unbiased Binomial Distribution:
$f_n(k) = \binom{n}{k} 2^{-n}\ n \geqslant 1,\ 0 \leqslant k \leqslant n$
Def Normal Binomial Distribution:
$f_{n,p}(k) = \binom{n}{k} p^k (1-p)^{n-k}\ n \geqslant 1,\ 0 \leqslant k \leqslant n,\ 0 < p < 1$

Note: Unbiased Binomial Distribution is when $p = 1/2$