Lecture-13

Birthday Matching Problem:

In a group of n-people, consider the following two questions:

(1) What is the prob. that two or more persons will have the same birthday? (month & date)

(2) What is the prob. that some-one in that has one same birthday as you?

Ans (1): There are $N = 365$ equally likely ways where the birthdays of each person can fall independently.

A: Two or more persons have the same birthday. $P(A) = ?$

B: No two persons share same birthday.

It is clear that $\overline{A} = B$

$$\Rightarrow P(A) = 1 - P(B)$$

To Compute the number of ways no matching birthday can occur among n-persons:

persons:

Note that there are N ways for the first person to have a birthday, N-1 ways for the second person without matching birthday with first person.

finally, $N-(n-1) = N-n+1$ ways for the last person without matching any others.

Using the independence assumption that gives $N(N-1)\cdots(N-n+1)$ possible "no matches".

Without any such restrictions, there are N choices for each person birthday and there are total of N^n ways of assigning birthdays to n-persons.

$$\Rightarrow P(B) = \frac{N(N-1)\cdots(N-n+1)}{N^n}$$

$$= \prod_{k=1}^{n-1}\left(1-\frac{k}{N}\right)$$

and hence the probability of the desired event A i.e.

$$P(A) = P(\bar{B}) = 1 - P(B)$$

$$= 1 - \prod_{k=1}^{n-1} \left(1 - \frac{k}{N}\right)$$

$$\simeq 1 - e^{-\sum_{k=1}^{n-1} \frac{k}{N}}$$

$$= 1 - e^{-n(n-1)/2N}$$

$e^{-x} \simeq 1 - x$ for small values of x. $\frac{k}{n}$ is very small, $e^{-\frac{k}{n}}$

In other words,

$$P\left(\begin{array}{c}\text{two people have}\\ \text{same birthday}\end{array}\right) = 1 - P\left(\begin{array}{c}\text{all } n\text{- people}\\ \text{have different}\\ \text{birthdays}\end{array}\right)$$

$$= 1 - \prod_{k=1}^{n} P\left(\begin{array}{c}k\text{-th person does not have}\\ \text{the same birthday as any of}\\ \text{the previous } (k-1) \text{ people}\end{array}\right)$$

$$= 1 - \prod_{k=1}^{n} \frac{N-(k-1)}{N} = 1 - \prod_{k=1}^{n} \left(1 - \frac{k-1}{N}\right)$$

$$= 1 - \prod_{k=1}^{n-1} \left(1 - \frac{k}{n}\right)$$

---

for example, $n = 23$, $P(A) \simeq 0.5$

i.e. $n = 23$ gives the prob of at least one match to be 0.5,

$n = 40$, $P(A) \simeq 0.891$

$n = 40$, $P(A) \simeq 0.891$

$n = 50$, $P(A) \simeq 0.97$

$n = 60$, $P(A) = ?$

(b)

$$P\left(\begin{matrix}\text{some one has}\\ \text{your birthday}\end{matrix}\right) = 1 - P\left(\begin{matrix}\text{None of } n\text{-person}\\ \text{has your birthday}\end{matrix}\right)$$

$$= 1 - \prod_{k=1}^{n} P\left(\begin{matrix}k\text{-th person does not}\\ \text{have your birthday}\end{matrix}\right)$$

$$= 1 - \prod_{k=1}^{n} \frac{N-1}{N}$$

$$= 1 - \prod_{k=1}^{n} \left(1 - \frac{1}{N}\right)$$

$$= 1 - \left(1 - \frac{1}{N}\right)^{n}$$

$$\simeq \boxed{1 - e^{-\frac{n}{N}}}$$

$1 - \frac{1}{N} \simeq e^{-\frac{1}{N}}$ as $\frac{1}{N}$ is very small

$n = 253$, there are 50 % Chances that some one share his/her birthday with you.

$n = 1000$, 93 %

$X = \{1, 2, 3, \ldots\ldots n\}$ ✓

$X = \{1, 2, 3, \text{——} n\}$ ✓

$Y = \{1, 2, 3, \text{——} N = 365\}$ ✓

Person : 1 2 3 —— j —— n

Birthday f : f(1) f(2) f(3) f(j) —— f(n)

$f(i) \neq f(j)$ for any $i \neq j$

f is 1-1.

$f : X \longrightarrow Y$

$f : \{1, 2, \text{——} 3\} \longrightarrow \{1, 2, 3, \text{——} N = 365\}$

Possible total number of functions

$f = (365)^n$

Ro: There are total no. of 1-1 functions

are $= \prod_{R=1}^{n} N - (R-1) = {}^{N}P_{n}$ ☐

$P(B) = P\left(\begin{array}{l}\text{all } n \text{ points in } X \\ \text{have different images in } Y\end{array}\right)$

$$= \frac{\prod_{k=1}^{n} N - (k-1)}{N^n} \text{ ——}$$

Searching algorithm

Searching algorithm

Collision Algorithm

An Introduction to Mathematical Cryptography.

J. Hoffstein, J. Pipher, J. H. Silverman.