Equality Checking Protocol

Alice $\longleftrightarrow$ Bob

Files: A B

- Alice (Bob) has a file A (resp. B). Each file is n-bits long.
- Design a communication protocol to test $A \stackrel{?}{=} B$, by sending as few bits as possible.

Brute-force: Alice sends A to Bob. #bits $= n$. Better?

Deterministic protocol not possible?

We give a probabilistic one, using number theory!

Protocol: 1) Turn A into number $N_A := \sum_{i<n} a_i \cdot 2^i$.

2) Pick a random prime $p \in [t]$.

3) Compute residue $R_A := N_A \bmod p$ [$\Rightarrow \lg t$-bits]
4) Send (R_A, p) to Bob. [$2\lg t$-bits]
5) Bob checks $R_A \stackrel{?}{=} R_B$. [Output YES iff $R_A = R_B$.]

Qn: What's min t, to get a "good" success prob.?

Analysis:

- $\pi(t) :=$ # primes in $[t]$ $\approx t/\lg t$ [Why?] (Prime Number Thm.)

▷ $P(R_A = R_B \mid A = B) = 1$.

▷ $A \neq B \Rightarrow N_A - N_B \neq 0$ has $\leq \lg|N_A - N_B| \leq n$ prime factors.

$$\Rightarrow P(R_A = R_B \mid A \neq B) = \frac{\#\text{primeFactors}(N_A - N_B)}{\#\text{prime in } [t]}$$

$$< n/\pi(t) \leq n\lg t/t. \quad [\text{So fix } t := 4n^2 \lg n.]$$

$$= n \cdot \frac{\lg(4n^2) + \lg\lg n}{4n^2 \cdot \lg n} < n \cdot \frac{3\lg n}{4n^2 \lg n} < 1/n.$$

Thm: The protocol transmits $2 \cdot \lg t = O(\lg n)$ bits & succeeds with prob. $> (1 - \frac{1}{n})$.

↳ $(\lg n)$-bits are needed to even index a bit in file A. So, the protocol is amazingly efficient!

- Let's look at another random variable:

5) Poisson random var. It's best described by an example.

Eg. Suppose phone-calls satisfy two properties:

i) #calls in a time-interval are proportional to its length.

ii) #calls in disjoint intervals are mutually independent.

. Say, $\alpha :=$ expected #calls in 12-1pm.

$X :=$ #calls in 12-1pm.

Qn: What's $P(X=k) = ?$

- Because of the continuous nature of calls, we divide the interval into n discrete parts:

$$P(\text{call in one part}) = \alpha/n =: p \quad (\text{large } n.)$$

$\triangleright$ $P(X=k) = \binom{n}{k} \cdot p^k \cdot (1-p)^{n-k} = \dfrac{n \cdots (n-k+1)}{k!} \cdot \left(\dfrac{\alpha}{n}\right)^k \cdot \left(1-\dfrac{\alpha}{n}\right)^{n-k}$

$$= \left(1-\frac{1}{n}\right) \cdots \left(1-\frac{k-1}{n}\right) \cdot \frac{\alpha^k}{k!} \cdot \left(1-\frac{\alpha}{n}\right)^n \cdot \left(1-\frac{\alpha}{n}\right)^{-k}$$

$$\Rightarrow \lim_{n\to\infty} P(X=k) = 1 \cdot \frac{\alpha^k}{k!} \cdot e^{-\alpha} \cdot 1 = \frac{\alpha^k}{k!} \cdot e^{-\alpha}.$$

$\triangleright$ $\displaystyle\sum_{k\geq 0} P(X=k) = \sum_k e^{-\alpha} \cdot \frac{\alpha^k}{k!} = \underline{1}.$

$\triangleright$ $\displaystyle E[X] = \sum_{k\geq 0} P(X=k) \cdot k = \sum e^{-\alpha} \cdot \alpha \cdot \frac{\alpha^{k-1}}{(k-1)!} = e^{-\alpha} \cdot \alpha \cdot e^{\alpha} = \underline{\alpha}.$

- **Defn:** Rnd. var. X over prob. space (Ω, P) is Poisson random variable with parameter α, if:
  - X takes values $\{0,1,2,\dots\} =: \mathbb{W}$, and
  - $P(X=k) = e^{-\alpha} \cdot \alpha^k / k!$; $\forall k \in \mathbb{W}$.

Exercise: Poisson rnd. var. approximates the Binomial " ".