From last week: Majonty element.

Given a sequence $S = x_1, x_2, \ldots, x_n$ of numbers

Q: is there an index $i \in \{1,2,\ldots,n\}$ s.t
x_i occurs $> \frac{n}{2}$ times in S?

Easy to solve in time (# comparison) $O(n \log n)$ using sorting

A:
```
Randomized majonty (S, m)
    Repeat m times
        select random i∈[n]
        If x_i is the majonty, then return 'true'   O(n)
    end
    return 'false'
```

If A returns 'true' then then is a majonty, so the anwer is correct

If A returns 'false', then then could still be a majonty element, however the probability p that A is wrong is at most $\left(\frac{1}{2}\right)^m$ $\left(p < \left(\frac{1}{2}\right)^m\right)$

Why? in each round, the probability of not selecting the majonty x (assuming then is one) is less than 1/2

$x_j = x$	$x_{j \neq} \neq x$
$> \frac{1}{2}n$	$< \frac{1}{2}n$

Is this enough to be usefull?

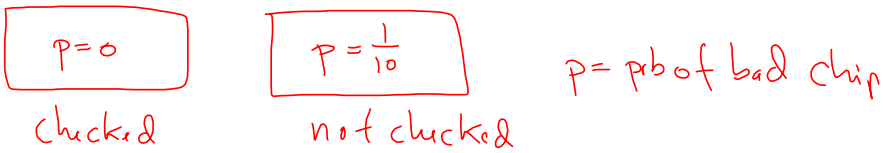
Yes because we can make p arbitranly small:

m	10	20	30
p	2^{-10}	2^{-20}	2^{-30}

A1 is an example of a Monte-Carlo alg
these have two outputs 'true'/'false'
one of which is always correct and the
other only wrong with a fixed prob.

Ex 15 Quality control

know: if container was checked
then no bad chips
otherwise 10% of chips are bad

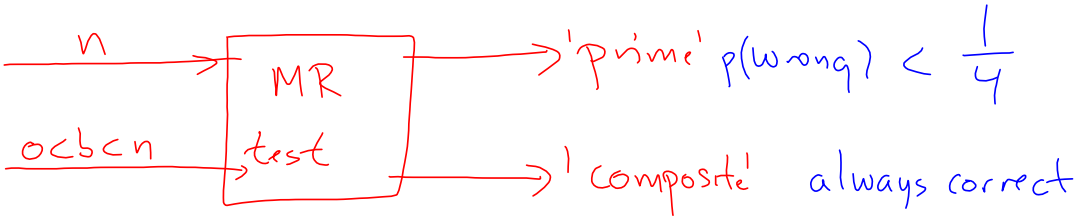


Monte-carlo strategy (m)
Repeat m times
pick random chip
if bad then return 'false'
end
return 'true'

B

Observations B is always correct if it returns 'false'
B is wrong (by answering 'true')
with probality at most $(1-p)^m$
in this case $p=\frac{1}{10}$ so wrong with
prob $< \left(\frac{9}{10}\right)^m$
if $m = 136$ then error with prob $< 10^{-6}$

Prime testing (Miller-Rabin) MR



MC algorithm (n, m)
  repeat m times
    select random b ∈ {1, 2, ..., n-1}
    do MR-test(n, b)
    if 'composite' then return 'composite'
  end
  return 'prime'

M

M is wrong with probability at most $\left(\frac{1}{4}\right)^m$

Ex 13 Birthday problem.

Q: what is the minimum # of persons in a room so that prob^{y} that two have the same birthday is at least $1/2$?

assumption · 1 year = 366 days
· all birthdays are equally likely

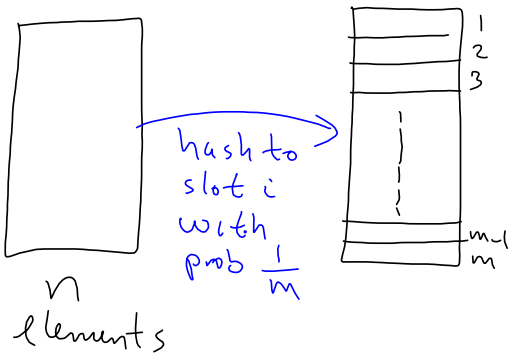
$q = (1-p)$ is prob. of all different

(We want n s.t $q < \frac{1}{2}$)

366 dates for person 1
365 - - - —— 2
⋮
367-j ... — — — j

$$q = \frac{366}{366}\cdot\frac{365}{366}\cdot \cdots \frac{(367-n)}{366} \approx \begin{cases} 0.525 & n=22 \\ 0.494 & n=23 \end{cases}$$

Ex 14 Collisions in hashing



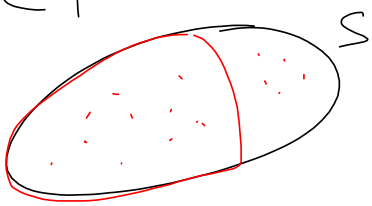
Q: how large does n have to be before $p(\text{collision}) \geq \frac{1}{2}$?

We calculate q = prob. of no collision

$$q = \frac{m}{m} \cdot \frac{m-1}{m} \cdot \ldots \cdot \frac{m-n+1}{m} < \frac{1}{2} \text{ when } n \geq 1.177\sqrt{m}$$

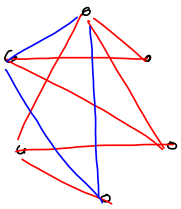
Probabilistic method

basic idea if $p(E) < 1$
then event $\overline{E} \neq \emptyset$



Back to Ramsey theory

recall that $\forall$ 2-colouring of the edges of K_6 then is a monochromatic K_3



rest !

define $r(k,k)$ is minimum n s.t
every 2-col of K_n has a monochromatic K_k

We already know that $r(2,2) = 2 = 2^{2/2}$ $k=2$
$r(3,3) = 6 > 2^{3/2}$

Theorem (Erdös)

$$\forall k \in \mathbb{Z}^+ \quad r(k,k) \geq 2^{k/2}$$

P: assume $n \leq 2^{k/2}$, and $k \geq 4$
consider a random 2-colouring of the edges of K_n
(for each independently: colour it red with $p = \frac{1}{2}$)

We prove that prob that a randomly coloured K_n has a monochr. K_k is < 1.

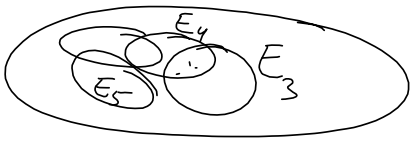
First enumerate all the distinct k-sets of $\{1,2,\dots n\}$

$S_1, S_2, \dots, S_{\binom{n}{k}}$ ← each correspond to a unique K_k of K_n

E_i: all edges of S_i have the same colour

$p(E_i) = \left(\frac{1}{2}\right)^{\binom{k}{2}} \cdot 2$

$\bigcup E_i = E_1 \cup E_2 \cup \dots \cup E_{\binom{n}{k}}$ is the event that at least one K_k is monochr.



$p(\bigcup E_i) \le \sum p(E_i)$

(union bound)

$p(\bigcup E_i) \le \sum_{i=1}^{\binom{n}{k}} p(E_i)$

$= \binom{n}{k} \cdot 2 \cdot \left(\frac{1}{2}\right)^{\binom{k}{2}}$

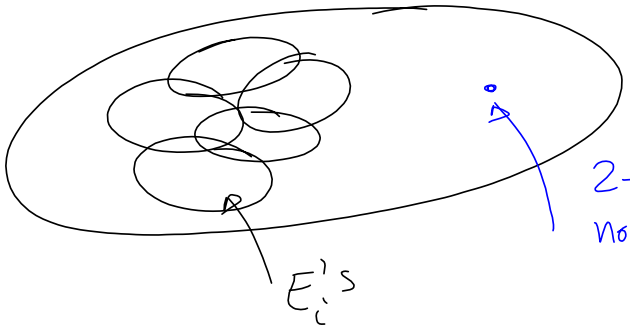
$\binom{n}{k} < \frac{n^k}{2^{k-1}}$

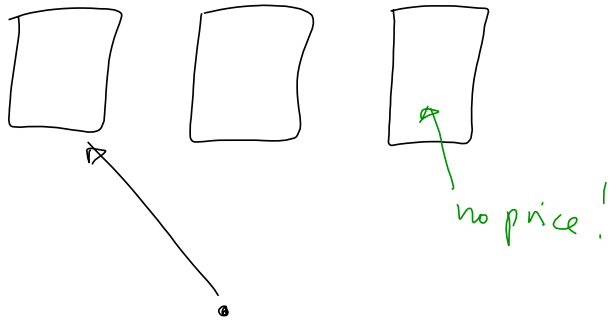
$< \frac{n^k}{2^{k-1}} \cdot 2 \cdot 2^{-\frac{k}{2}(k-1)}$

$n < 2^{k/2}$

$< \frac{2^{k^2/2}}{2^{k-1}} \cdot 2 \cdot 2^{-\frac{k}{2}(k-1)} = 2^{2-\frac{k}{2}} \le 1$ as $k \ge 4$

Look at the set of all possible 2-colourings of K_n $2^{\binom{n}{2}}$ such





Bayes theorem. If E and F are events with $p(E), p(F) > 0$ then

$$p(F|E) = \frac{p(E|F) \cdot p(F)}{p(E|F) \cdot p(F) + p(E|\bar{F}) \cdot p(\bar{F})}$$

P:

By definition $p(F|E) \overset{(\triangle)}{=} \frac{p(F \cap E)}{p(E)}$

and $p(F \cap E) = p(E \cap F) \overset{(\square)}{=} p(E|F) \cdot p(F)$

we also have

$p(E) = p(E \cap F) + p(E \cap \bar{F})$ as $F \cup \bar{F} = S$ and $F \cap \bar{F} = \emptyset$

$\overset{(*)}{=} p(E|F) \cdot p(F) + p(E|\bar{F}) \cdot p(\bar{F})$

inserting $(\square)$ and $(*)$ in $(\triangle)$ we get

$$p(F|E) = \frac{p(F \cap E)}{p(E)} = \frac{p(E \cap F)}{p(E)} = \frac{p(E|F)\,p(F)}{p(E|F)\,p(F) + p(E|\bar{F})\,p(\bar{F})}$$