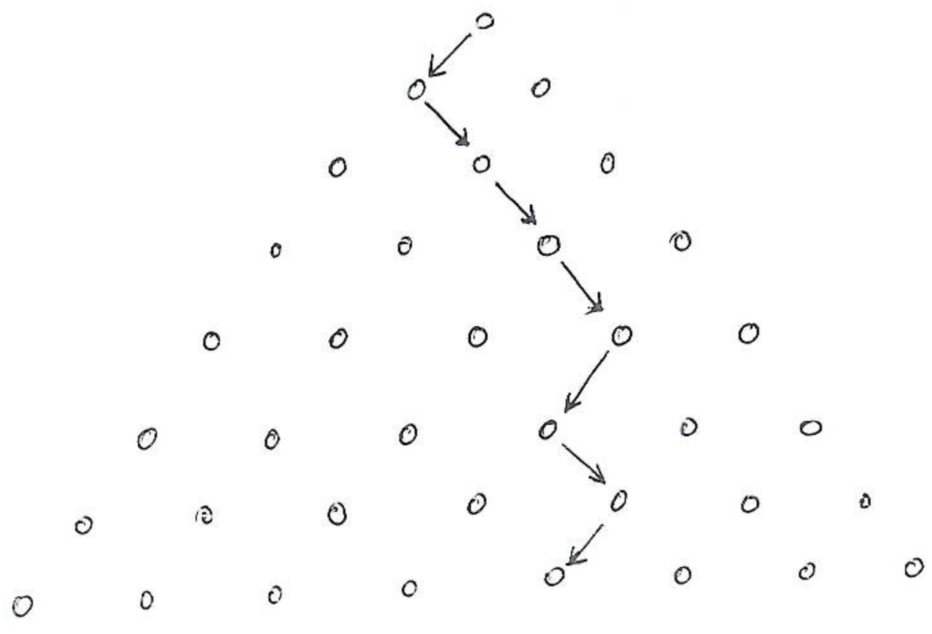
UNIVERSITY COLLEGE DUBLIN
School of Mathematical Sciences
Mathematical Enrichment Class, 1 February 2014
Professor Gary McGuire

For more information see website www.irmo.ie and follow link to UCD.

1. Suppose a hacker can check 1000 passwords in one second. How long will it take a hacker to check all passwords with three characters? How about with eight characters?

2. How many paths are there from the top circle to any lower circle?



3. What are the chances of winning the lotto?

Suppose passwords are chosen from 26 small letters

26 capital letters

10 digits

10 others (say)

72

A password with two characters has

$$72 \times 72 = 72^2 = 5184 \text{ possibilities.}$$

So it takes 5.184 seconds to try them all.

With three characters $72^3 = 373,248$ passwords.

Takes about 6 minutes.

With four characters $72^4 = 26873856$

Takes about 7½ hours, to check them all.

With eight characters, $72^8 = 722204136308736$

$$\approx 7.2 \times 10^{14}$$

72^n

Takes about 22,900 years.

Long passwords are more secure!

72^8 = number of ways to choose 8 characters from 72

where order matters and they need not be distinct.

The number of ways of choosing k characters from n, where order matters and they need not be distinct, is

$$n^k$$

$$\underset{1}{\underline{\ a\ }}\ \underset{2}{\underline{\ x\ }}\ \underset{3}{\underline{\ a\ }}\ \cdots\cdots\ \underset{k}{\underline{\ 3\ }}$$

(n choices in each place)

If the choices need to be distinct, then

$$\underset{1}{\underline{\quad}}\ \underset{2}{\underline{\quad}}\ \underset{3}{\underline{\quad}}\ \cdots\cdots\ \underset{k}{\underline{\quad}}$$

there are $n(n-1)(n-2)\cdots(n-k+1)$ ways

(order matters, choices distinct)

Suppose $k=n$.

There are $\underbrace{n(n-1)(n-2)\cdots\cdots(3)(2)(1)}_{\text{This is denoted } n!}$ ways.

e.g. $n=3$

123
132
213
231
312
321

$$3! = (3)(2)(1) = 6$$

In how many ways can you rearrange the letters of the word RANDOM ?

$6!$

COLOSH
HLCSOO

What about SCHOOL ?

$$\frac{6!}{2}$$

What about CARAVAN ?

$$\frac{7!}{3!}$$

How many ways can you choose a captain and vice-captain from a team of 11 ?

$$11 \times 10 = 110$$

How many ways can you choose two objects from n objects (a) if order matters (b) if order doesn't matter

$$n(n-1) \qquad \frac{n(n-1)}{2}$$

Given n points, we join each pair by a line. How many lines are there ?

$$\frac{n(n-1)}{2}$$

How many different ways are there to draw <u>some</u> of the lines ?

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

$n=4$ $2^6=64$

Consider a set with n elements.
How many subsets of size k are there?

$n=0$ 1

$n=1$ $\underbrace{k=0}_{1}$ $\underbrace{k=1}_{1}$

$n=2$ $\underbrace{k=0}_{1}$ $\underbrace{k=1}_{2}$ $\underbrace{k=2}_{1}$

$n=3$ $\underbrace{k=0}_{1}$ $\underbrace{k=1}_{3}$ $\underbrace{k=2}_{3}$ $\underbrace{k=3}_{1}$

$n=4$ a b c d $\underbrace{k=0}_{1}$ $\underbrace{k=1}_{4}$ $\underbrace{k=2}_{6}$ $\underbrace{k=3}_{4}$ $\underbrace{k=4}_{1}$

ab bc
ac bd
ad cd

$n=5$

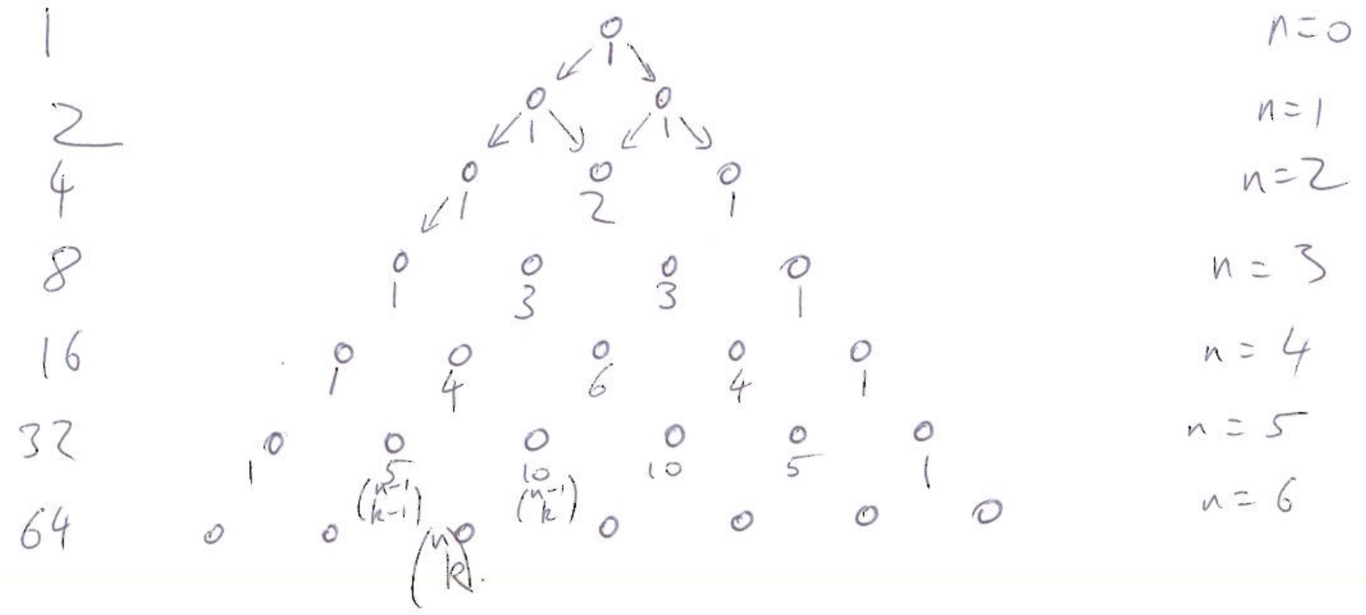
a b c d e $\underbrace{k=0}_{1}$ $\underbrace{k=1}_{5}$ $\underbrace{k=2}_{10}$ $\underbrace{k=3}_{10}$ $\underbrace{k=4}_{5}$ $\underbrace{k=5}_{1}$

ab bc cd de
ac bd ce
ad be
ae

Let $\binom{n}{k}$ = number of subsets of size k of a set of size n

= number of ways of choosing k objects from n, where order does not matter and choices are distinct.

e.g. $\binom{n}{2} = \frac{n(n-1)}{2}$



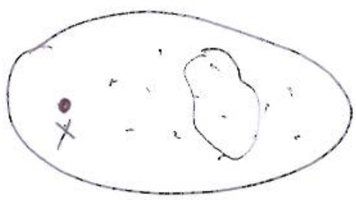
So $\binom{n}{k}$ is the number of paths from the top to the k-th circle in the n-th row

Notice ① $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

② $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n$

What do these mean in terms of subsets?

①



$$\underbrace{\binom{n}{k}}{} = \underbrace{\binom{n-1}{k}}_{\text{do not contain } x} + \underbrace{\binom{n-1}{k-1}}_{\text{do contain } x}$$

②

$2 \cdot 2 \cdot 2 \cdots 2 = 2^n$

How many sequences with 8 0's and 5 1's can you make

0 0 0 0 0 0 0 0 1 1 1 1 1

13 $\quad \underline{0}\ \underline{0}\ \_\ \underline{0}\ \_\ \_\ \underline{0}\ \underline{0}\ \_\ \_\ \underline{0}\ \underline{0}\ \underline{0}$

$$\binom{13}{8} = \binom{13}{5}$$

$$= \frac{13!}{8!\,5!}$$

$$(x+y)^1 = x + y$$

$$(x+y)^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

Show that

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$$