Lecture 13

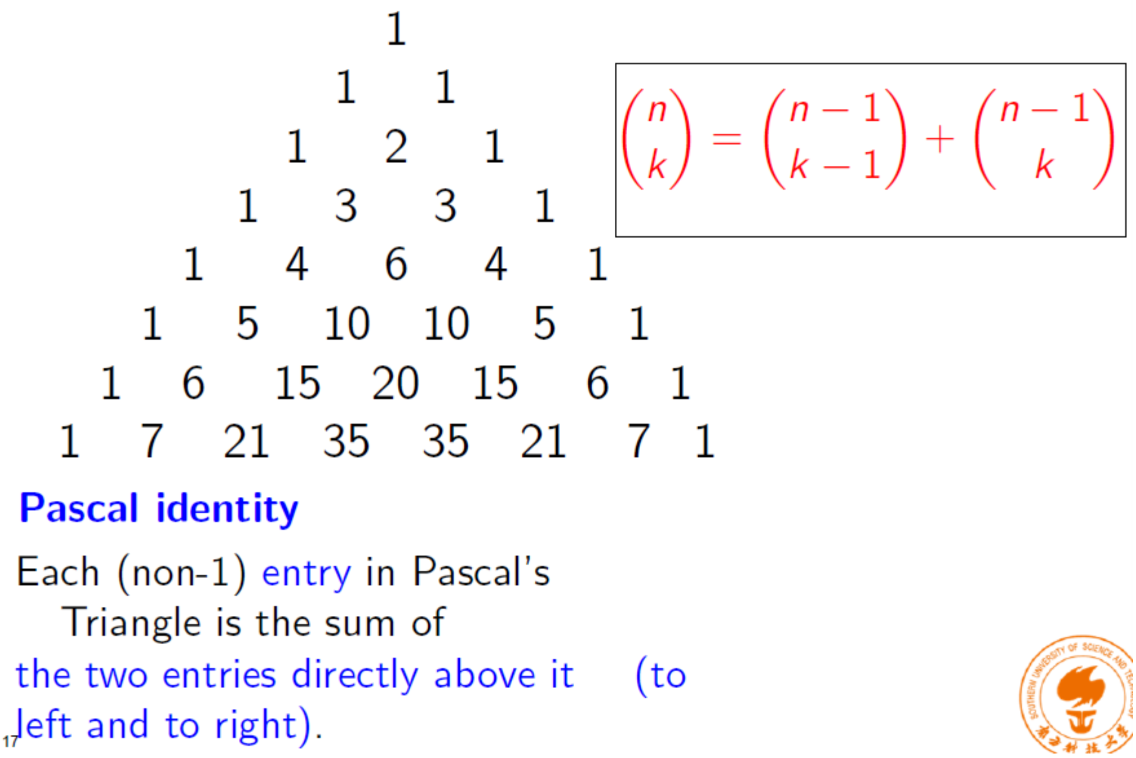
Some Properties of Binomial Coefficients（二项式系数）

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$
$$\binom{n}{0} = 1$$
$$\binom{n}{n} = 1$$
$$\binom{n}{k} = \binom{n}{n-k}$$
$$\sum_{i-0}^{n} \binom{n}{i} = 2^n$$

Pascal's Identity

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

由帕斯卡三角形推出，或者说是杨辉三角——对于任意一个非第一个元素，都是由两个上方相邻的元素相加求和得到



proof

Proof: Apply sum rule.

Let S_1 be set of all k-element subsets.

To apply sum rule, partition S_1 into S_2 and S_3.

Let S_2 be set of k-element subsets that contain x_n.

Let S_3 be set of k-element subsets that don't contain x_n.

The binomial Theorem

$$(x+y)^n = \binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\binom{n}{2}x^{n-2}y^2+\ldots+\binom{n}{n-1}xy^{n-1}+\binom{n}{n}y^n$$

$$(x+y)^n = \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i.$$

Labelling and Trinomial Coefficients

When $k_1+k_2+k_3=n$, we call

$$\frac{n!}{k_1!k_2!k_3!}$$

a *trinomial coefficient* and denote it as

$$\binom{n}{k_1\quad k_2\quad k_3}$$

The Birthday Paradox

A_n : n students in class, at least two of them share a birthday

B_n : n students in class, none of them share a birthday

$|S|$: Sample Space—— $|S|=365^n$

$\#B_n = 365 * 364 * \ldots * (365-(n-1))$

$\#A_n + \#B_n = 365^n$

When n >= 23 the probability bigger then 0.5.

Birthday Attacks

Let $n(p;H)$ be the smallest number of values we have to choose, such that the probability for finding a collision is at least p. By inverting the expression above, we have

$$n(p;H) \approx \sqrt{2Hln\frac{1}{1-p}}$$
$$H\ is\ sapce\ of\ chosen$$

such like above, H is 365