南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CS201 DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room413, CoE South Tower
Email: wangqi@sustech.edu.cn

The Bijection Principle

- The following loop is a part of program to determine the number of triangles formed by n points in the plane.

```
trianglecount = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

- The following loop is a part of program to determine the number of triangles formed by n points in the plane.

```
(1) trianglecount = 0
(2)    for i = 1 to n
(3)       for j = i+1 to n
(4)          for k = j+1 to n
(5)             if points i, j, k are not collinear
(6)                trianglecount = trianglecount + 1
```

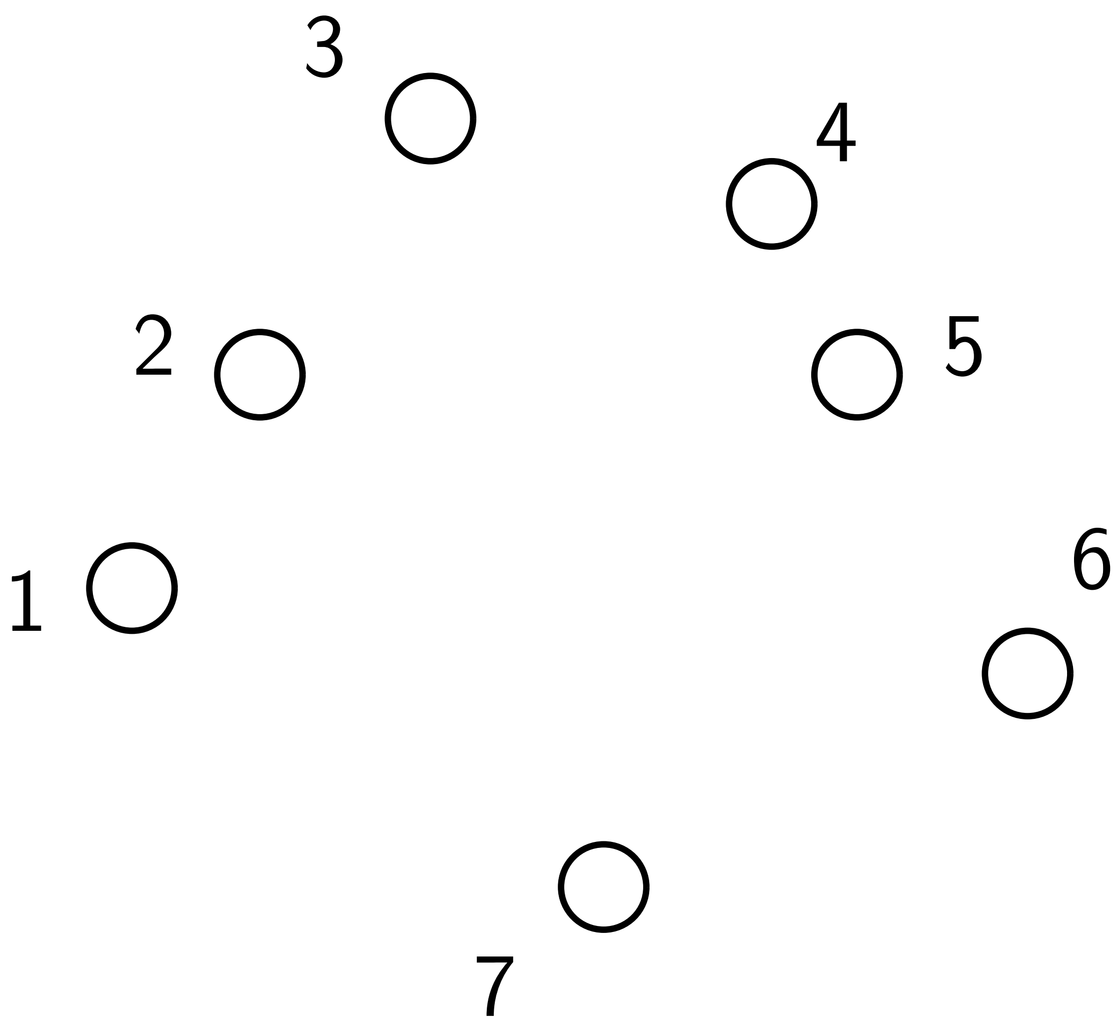
Among all iterations of line 5, what is the total number of times this line checks three points to see if they are collinear?

Counting Triangles

- 3 points form a triangle if and only if they are non collinear

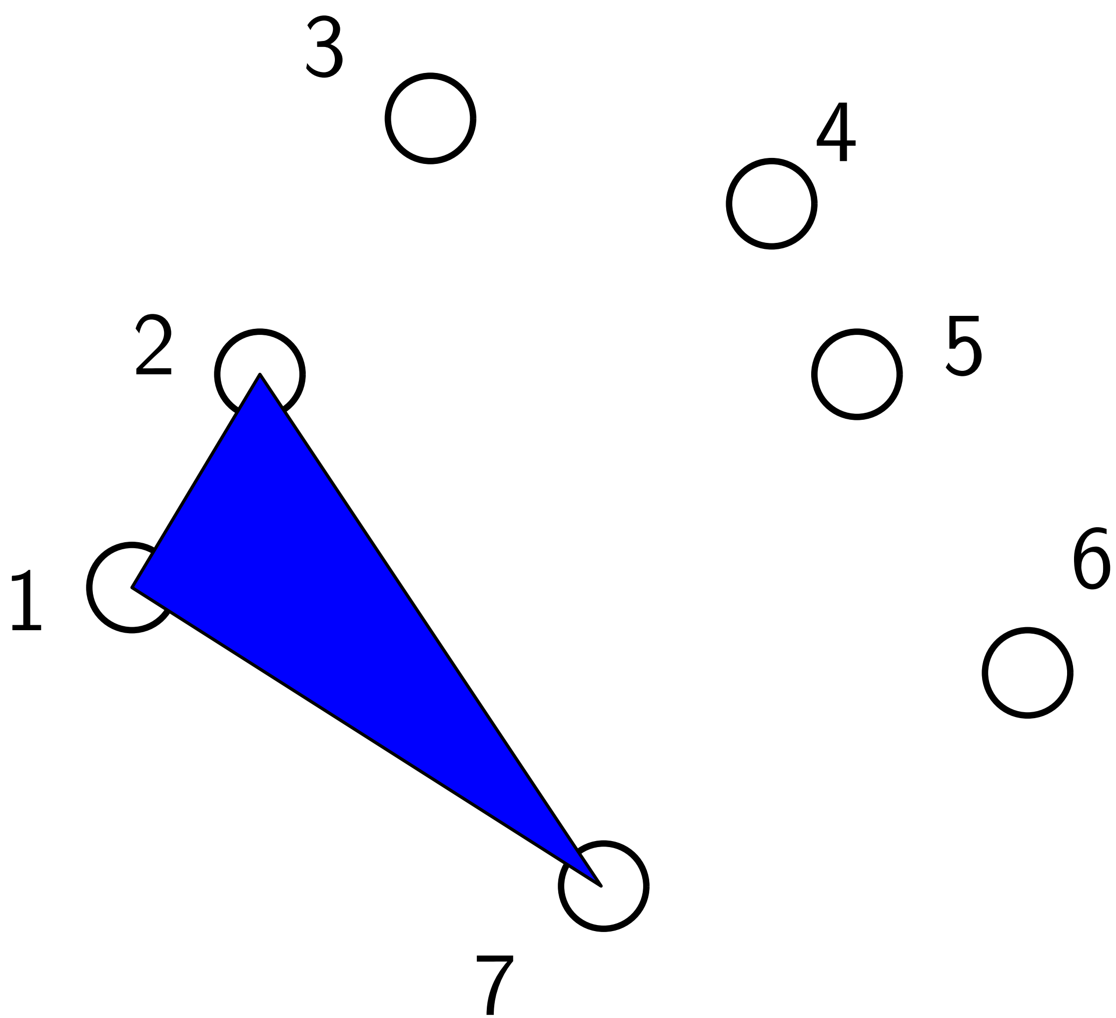
Counting Triangles

- 3 points form a triangle if and only if they are non collinear



Counting Triangles

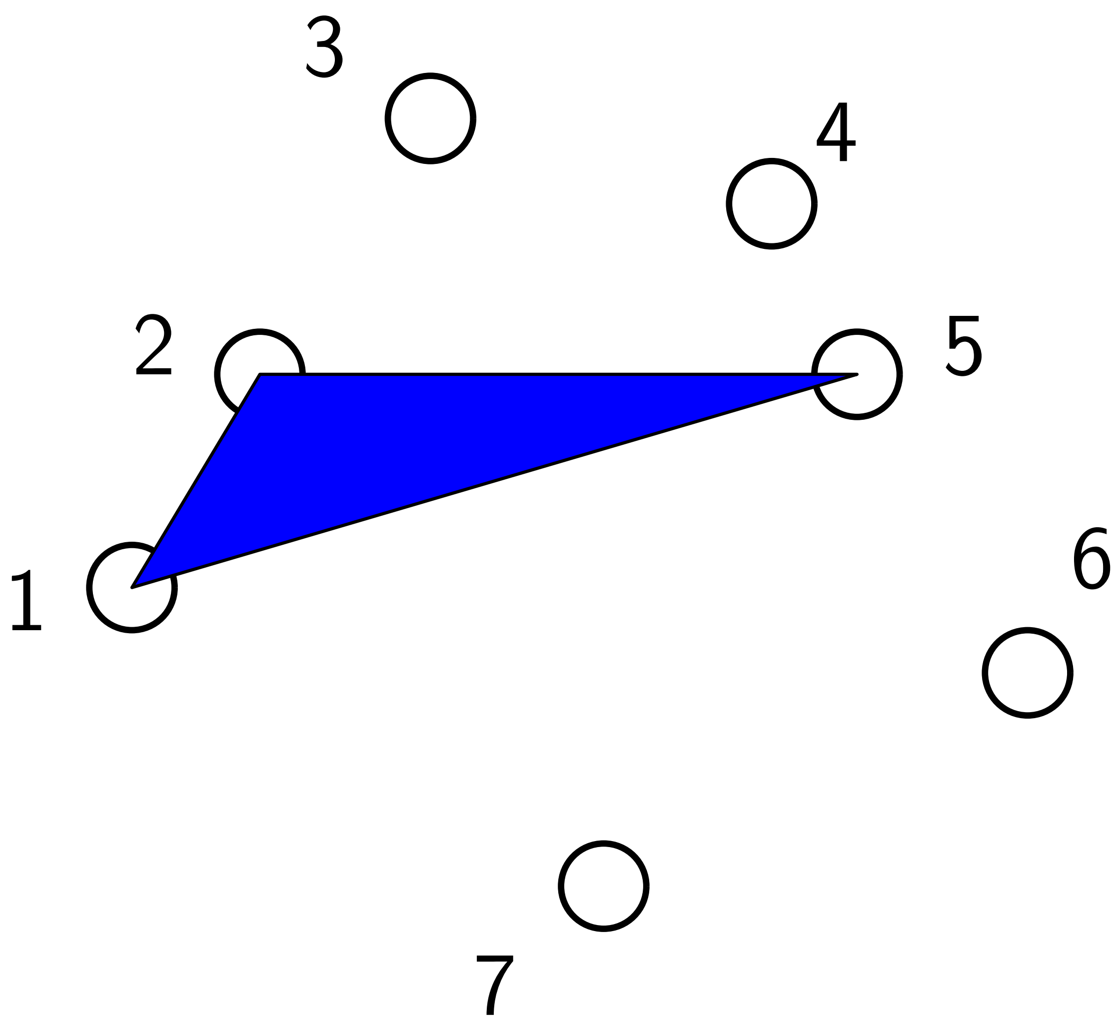
- 3 points form a triangle if and only if they are non collinear



$1 - 2 - 7$: yes

Counting Triangles

- 3 points form a triangle if and only if they are non collinear

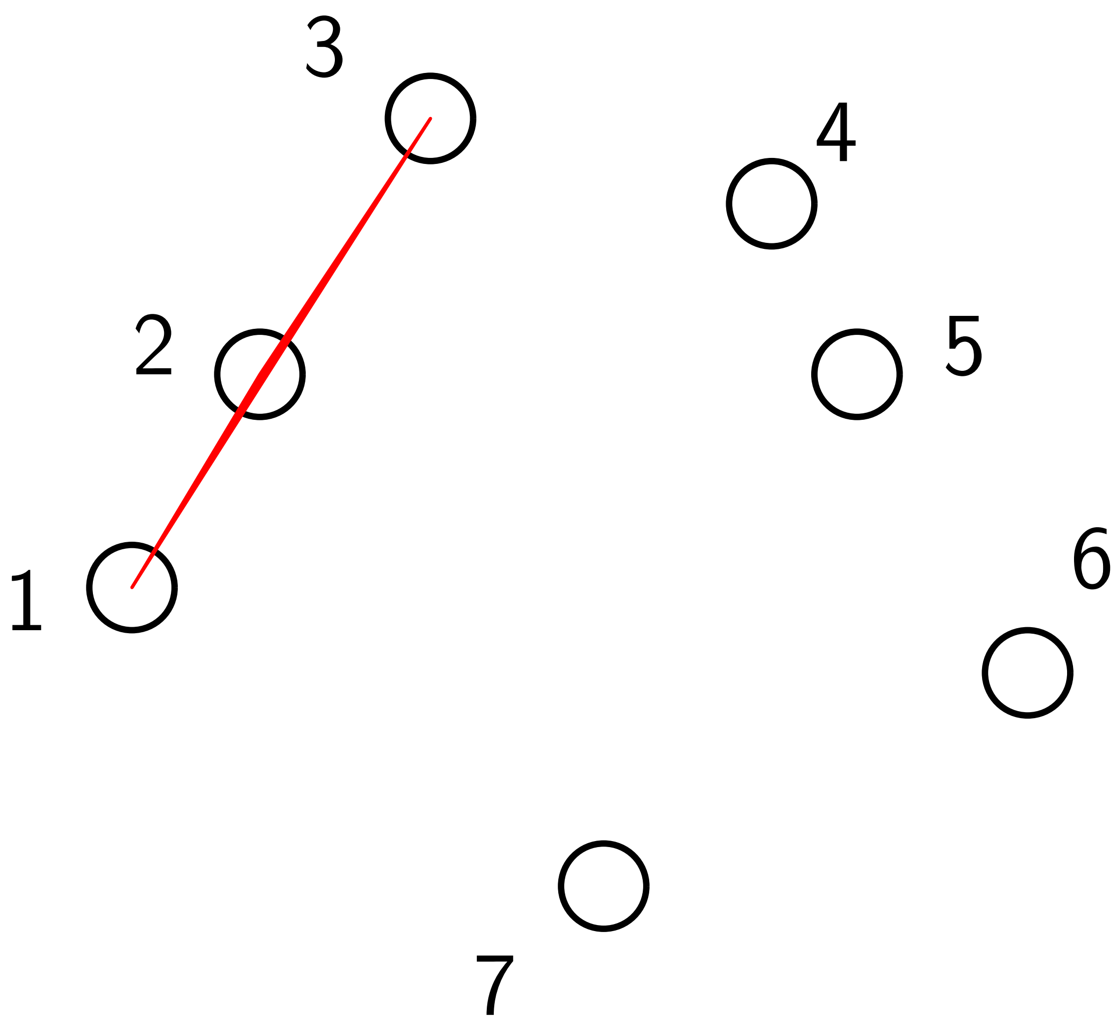


$1 - 2 - 7$: yes

$1 - 2 - 5$: yes

Counting Triangles

- 3 points form a triangle if and only if they are non collinear



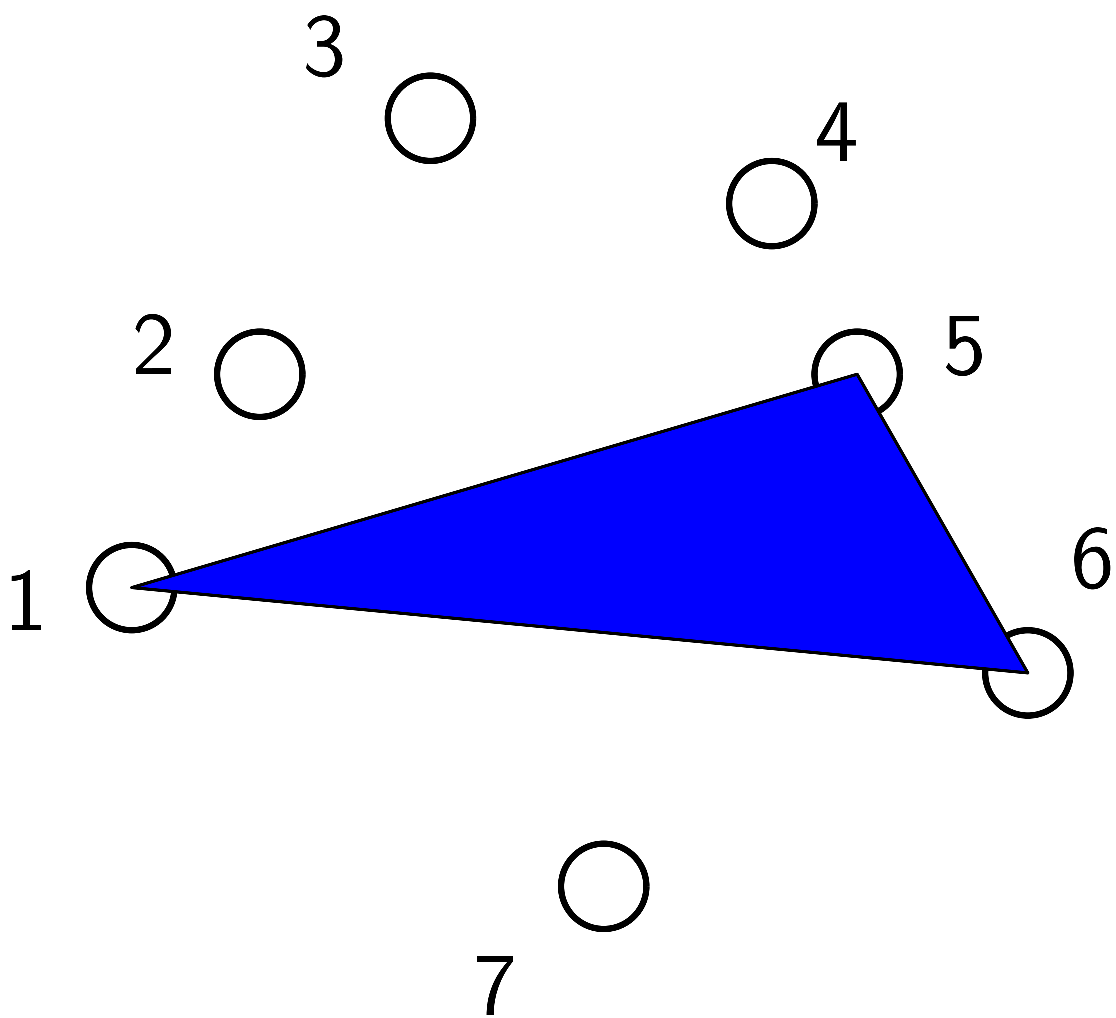
1 — 2 — 7: yes

1 — 2 — 5: yes

1 — 2 — 3: no

Counting Triangles

- 3 points form a triangle if and only if they are non collinear



1 – 2 – 7: yes

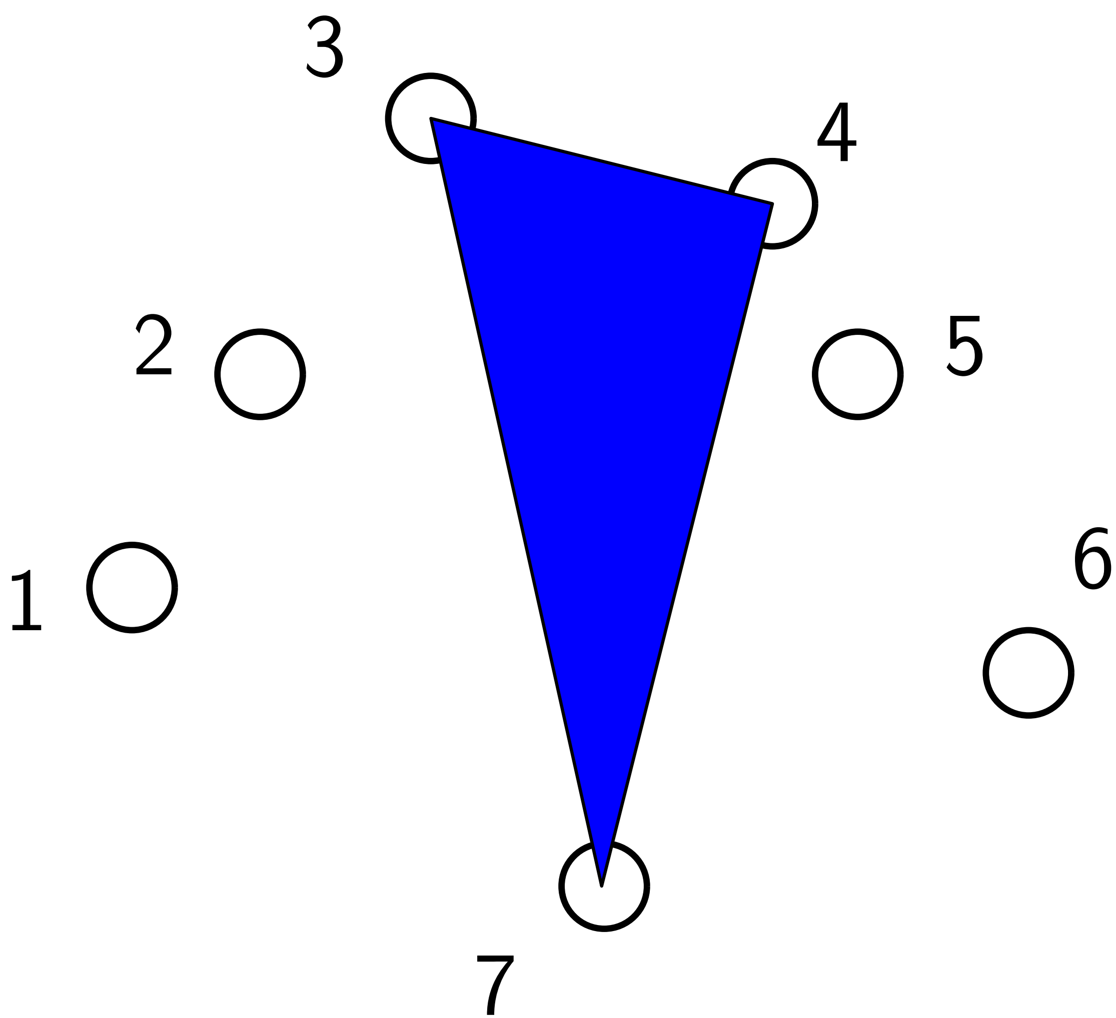
1 – 2 – 5: yes

1 – 2 – 3: no

1 – 5 – 6: yes

Counting Triangles

- 3 points form a triangle if and only if they are non collinear



$1 - 2 - 7$: yes

$1 - 2 - 5$: yes

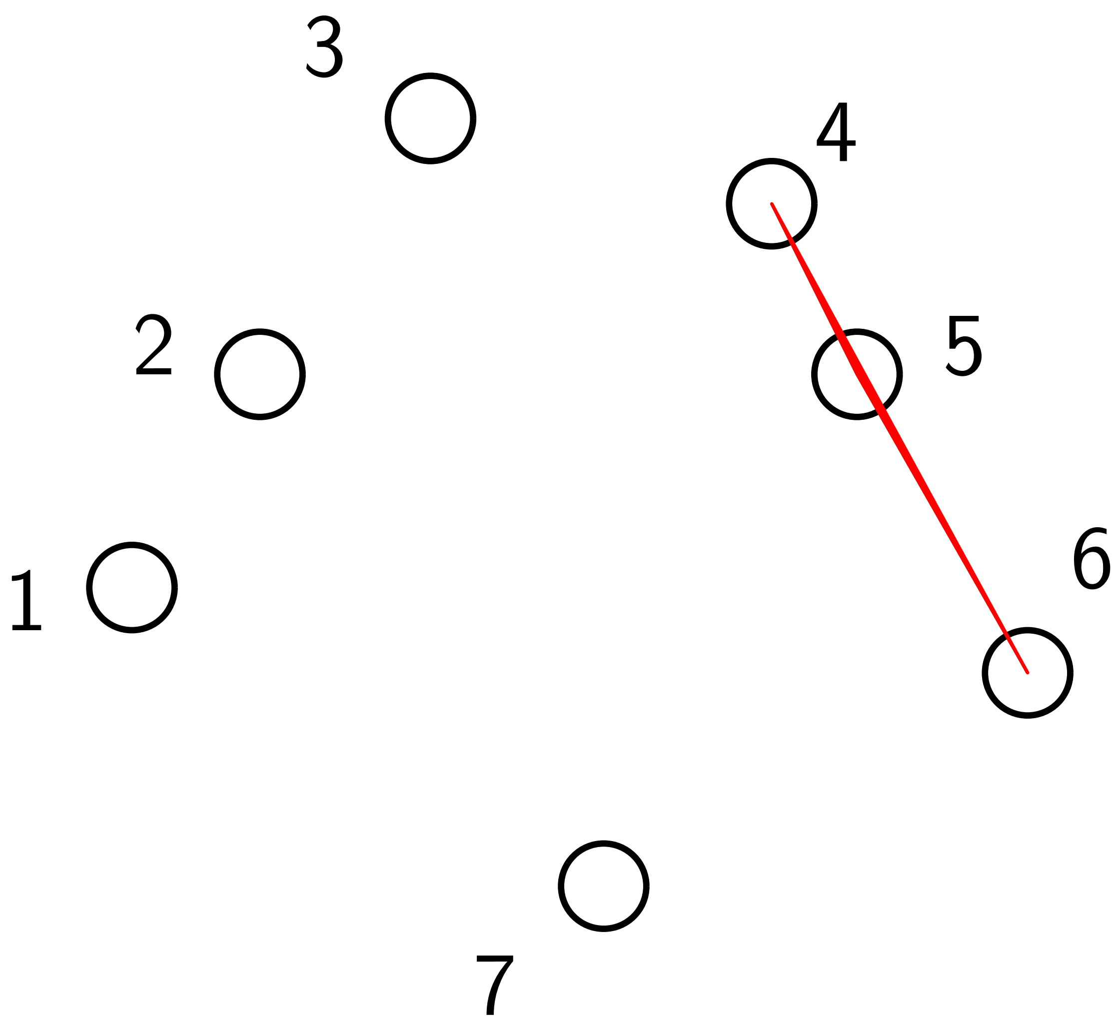
$1 - 2 - 3$: no

$1 - 5 - 6$: yes

$3 - 4 - 7$: yes

Counting Triangles

- 3 points form a triangle if and only if they are non collinear



$1 - 2 - 7$: yes

$1 - 2 - 5$: yes

$1 - 2 - 3$: no

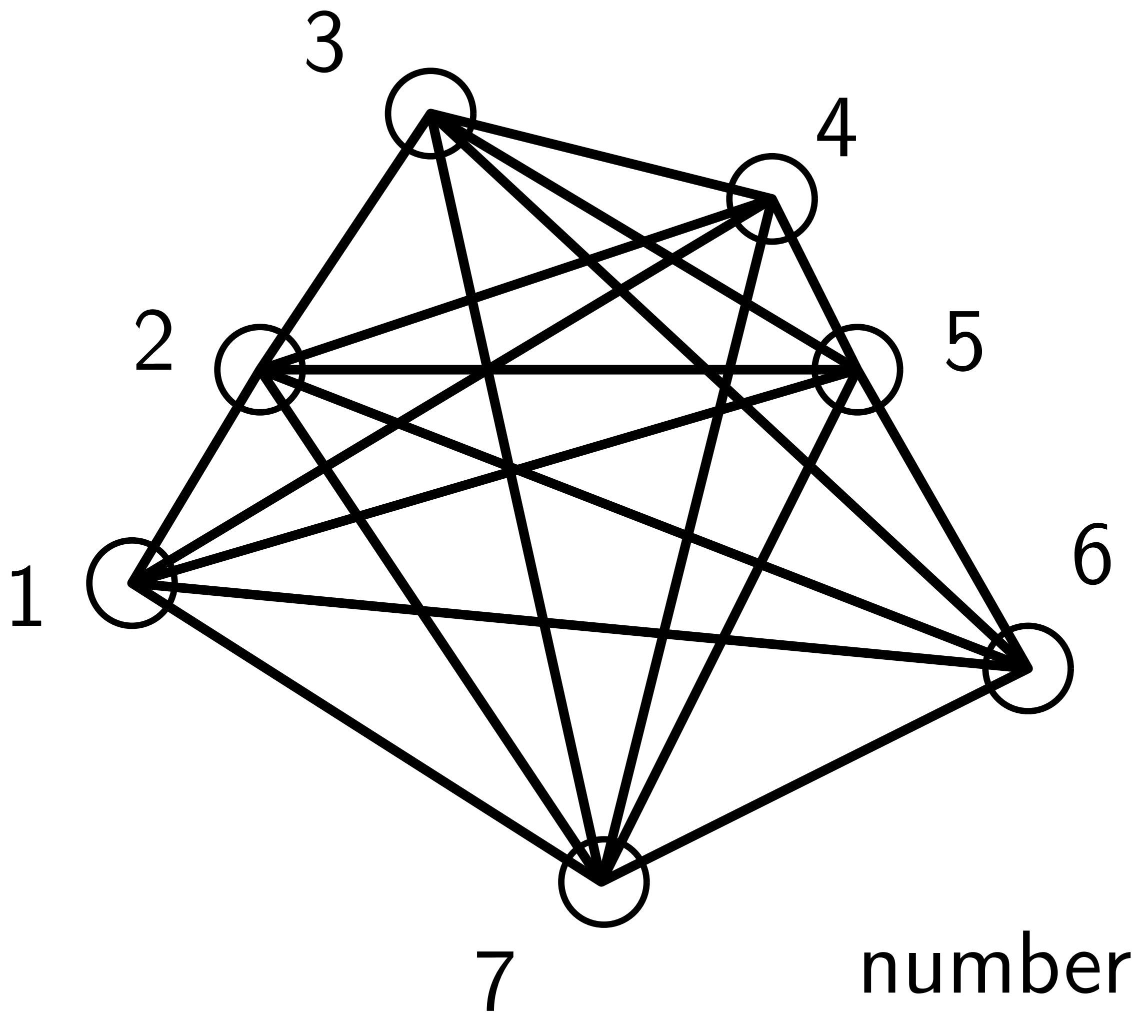
$1 - 5 - 6$: yes

$3 - 4 - 7$: yes

$4 - 5 - 6$: no

Counting Triangles

- 3 points form a triangle if and only if they are non collinear



$1 - 2 - 7$: yes

$1 - 2 - 5$: yes

$1 - 2 - 3$: no

$1 - 5 - 6$: yes

$3 - 4 - 7$: yes

$4 - 5 - 6$: no

number of triangles: 33

Counting Triangles

```
trianglecount = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

Counting Triangles

```
triianglecount = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

A loop

Counting Triangles

```
(1) trianglecount = 0
(2)   for i = 1 to n
(3)     for j = i+1 to n
(4)       for k = j+1 to n
(5)         if points i, j, k are not collinear
(6)           trianglecount = trianglecount + 1
```

A loop embedded in a loop

Counting Triangles

```
triangleCount = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          triangleCount = triangleCount + 1
```

A loop embedded in a loop embedded in another loop.

Counting Triangles

```
trianglecount = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

A loop embedded in a loop embedded in another loop.

Second loop begins with $j = i + 1$ and j increases up to n.
Third loop begins with $k = j + 1$ and k increases up to n.

Counting Triangles

```
triangle count = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

A loop embedded in a loop embedded in another loop.

Second loop begins with $j = i + 1$ and j increases up to n.
Third loop begins with $k = j + 1$ and k increases up to n.

Thus each triple i, j, k with $i < j < k$ is examined exactly once.

Counting Triangles

```
triangle count = 0
  for i = 1 to n
    for j = i+1 to n
      for k = j+1 to n
        if points i, j, k are not collinear
          trianglecount = trianglecount + 1
```

A loop embedded in a loop embedded in another loop.

Second loop begins with $j = i + 1$ and j increases up to n.
Third loop begins with $k = j + 1$ and k increases up to n.

Thus each triple i, j, k with $i < j < k$ is examined exactly once.

For example, if $n = 4$, then triples (i, j, k) used by algorithm are (1,2,3), (1,2,4), (1,3,4), and (2,3,4).

Counting Triangles

- Want to compute the number of *increasing triples* (i, j, k) with $1 \leq i < j < k \leq n$.

Counting Triangles

- Want to compute the number of
  increasing triples (i, j, k) with $1 \leq i < j < k \leq n$.

  Claim: Number of increasing triples is exactly the same as number of 3-element subsets from $\{1, 2, \ldots, n\}$

Counting Triangles

- Want to compute the number of
  increasing triples (i, j, k) with $1 \leq i < j < k \leq n$.

  Claim: Number of increasing triples is exactly the same as number of 3-element subsets from $\{1, 2, \ldots, n\}$

  Why? Let $X =$ set of increasing triples and
  $Y =$ set of 3-element subsets from $\{1, 2, \ldots, n\}$

Counting Triangles

- Want to compute the number of
  increasing triples (i, j, k) with $1 \leq i < j < k \leq n$.

Claim: Number of increasing triples is exactly the same as number of 3-element subsets from $\{1, 2, \ldots, n\}$

Why? Let $X =$ set of increasing triples and
$Y =$ set of 3-element subsets from $\{1, 2, \ldots, n\}$

Define: $f : X \to Y$ by $f((i, j, k)) = \{i, j, k\}$
Claim: f is a **bijection** (why) so $|X| = |Y|$

Counting Triangles

- Want to compute the number of
  increasing triples (i, j, k) with $1 \leq i < j < k \leq n$.

Claim: Number of increasing triples is exactly the same as number of 3-element subsets from $\{1, 2, \ldots, n\}$

Why? Let $X =$ set of increasing triples and
$Y =$ set of 3-element subsets from $\{1, 2, \ldots, n\}$

Define: $f : X \to Y$ by $f((i, j, k)) = \{i, j, k\}$
Claim: f is a **bijection** (why) so $|X| = |Y|$

f is a bijection because

f is one-to-one

if $(i, j, k) \neq (i', j', k') \Rightarrow f(\,(i, j, k)\,) \neq f(\,(i', j', k'))$

f is onto

if γ is a 3-element subset then it can be written as $\gamma = \{i, j, k\}$
where $i < j < k$ so $f(\,(i, j, k)\,) = \gamma$.

Counting Pairs

- The number of

  increasing pairs (i, j) with $1 \leq i < j \leq n$

  is the same as the number of

  2-sets from $\{1, 2, \ldots, n\}$

Counting Pairs

- The number of

  $\text{increasing pairs } (i, j) \text{ with } 1 \leq i < j \leq n$

  is the same as the number of

  $\text{2-sets from } \{1, 2, \ldots, n\}$

  Define $f : X \to Y$ by $f(\,(i, j)\,) = \{i, j\}$

  Claim: f is a **bijection** so $|X| = |Y|$

Counting Pairs

- The number of
  increasing pairs (i, j) with $1 \leq i < j \leq n$
  is the same as the number of
  2-sets from $\{1, 2, \ldots, n\}$

  Define $f : X \to Y$ by $f(\,(i, j)\,) = \{i, j\}$
  Claim: f is a **bijection** so $|X| = |Y|$

  We actually already saw that $|X| = |Y| = \binom{n}{2}$

The Bijection Principle

- Two sets have the same size if and only if there is a one-to-one function from one set onto the other.

The Bijection Principle

- Two sets have the same size if and only if there is a one-to-one function from one set onto the other.

  A standard first step in counting the size of a set is to use a bijection to show that it has the same size as a 2nd set, and then count the 2nd set instead.

The Bijection Principle

- Two sets have the same size if and only if there is a one-to-one function from one set onto the other.

  A standard first step in counting the size of a set is to use a bijection to show that it has the same size as a 2nd set, and then count the 2nd set instead.

  In practice, in real problems we often only *implicitly* use the bijection and don't *explicitly* describe it

The Bijection Principle

- Two sets have the same size if and only if there is a one-to-one function from one set onto the other.

  A standard first step in counting the size of a set is to use a bijection to show that it has the same size as a 2nd set, and then count the 2nd set instead.

  In practice, in real problems we often only *implicitly* use the bijection and don't *explicitly* describe it

  Currently, we started with the problem of counting the # of increasing triples and changed it to the problem of counting the # of 3-element sets from $\{1, 2, \ldots, n\}$

Inclusion-Exclusion Principle

- Used in counts where the decomposition yields two independent counting tasks with overlapping elements

Inclusion-Exclusion Principle

- Used in counts where the decomposition yields two independent counting tasks with overlapping elements

  If we use the sum rule, some elements would be counted twice.

Inclusion-Exclusion Principle

- Used in counts where the decomposition yields two independent counting tasks with overlapping elements

  If we use the sum rule, some elements would be counted twice.

  Inclusion-Exclusion Principle: uses a sum rule and then corrects for the overlapping elements.

Inclusion-Exclusion Principle

- Used in counts where the decomposition yields two independent counting tasks with overlapping elements

  If we use the sum rule, some elements would be counted twice.

Inclusion-Exclusion Principle: uses a sum rule and then corrects for the overlapping elements.

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Inclusion-Exclusion Principle

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

  ◇ it is easy to count bit strings starting with '1':

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

  - it is easy to count bit strings starting with '1': 2^7

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

  - ◇ it is easy to count bit strings starting with '1': 2^7
  - ◇ it is easy to count bit strings ending with '00':

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

  - ◇ it is easy to count bit strings starting with '1': 2^7
  - ◇ it is easy to count bit strings ending with '00': 2^6

- **Example**

  How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

  - ◇ it is easy to count bit strings starting with '1': 2^7
  - ◇ it is easy to count bit strings ending with '00': 2^6

  Overcounting!!!

- **Example**

How many bit strings of length 8 either start with a '1' bit or end with the two bits '00'?

◇ it is easy to count bit strings starting with '1': 2^7

◇ it is easy to count bit strings ending with '00': 2^6

Overcounting!!!

◇ deduct the number of strings starting with '1' and ending with "00":

- **Example**

How many bit strings of length 8 either start with a ‘1’ bit or end with the two bits ‘00’?

◇ it is easy to count bit strings starting with ‘1’: 2^7

◇ it is easy to count bit strings ending with ‘00’: 2^6

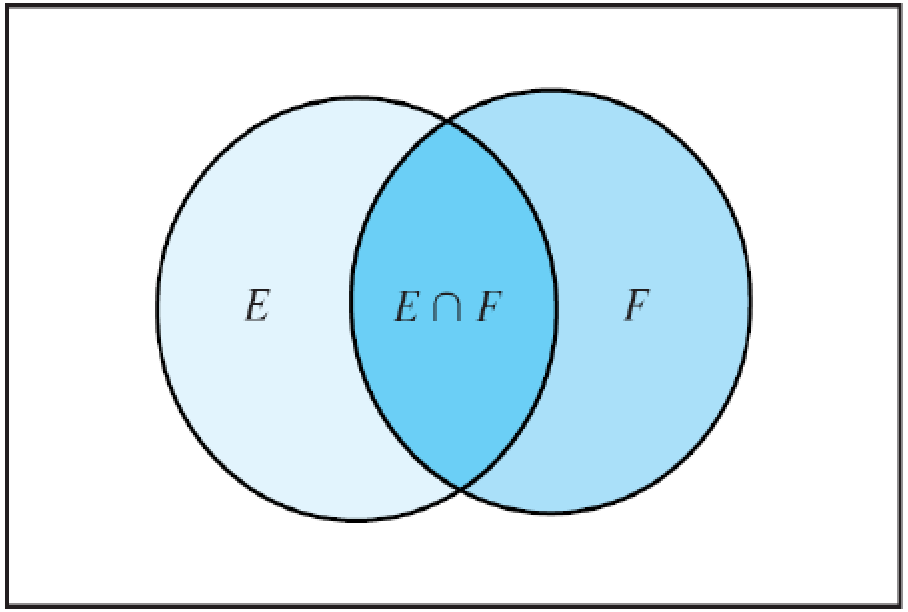
Overcounting!!!

◇ deduct the number of strings starting with ‘1’ and ending with “00”: 2^5

Inclusion-Exclusion Principle

- Two sets

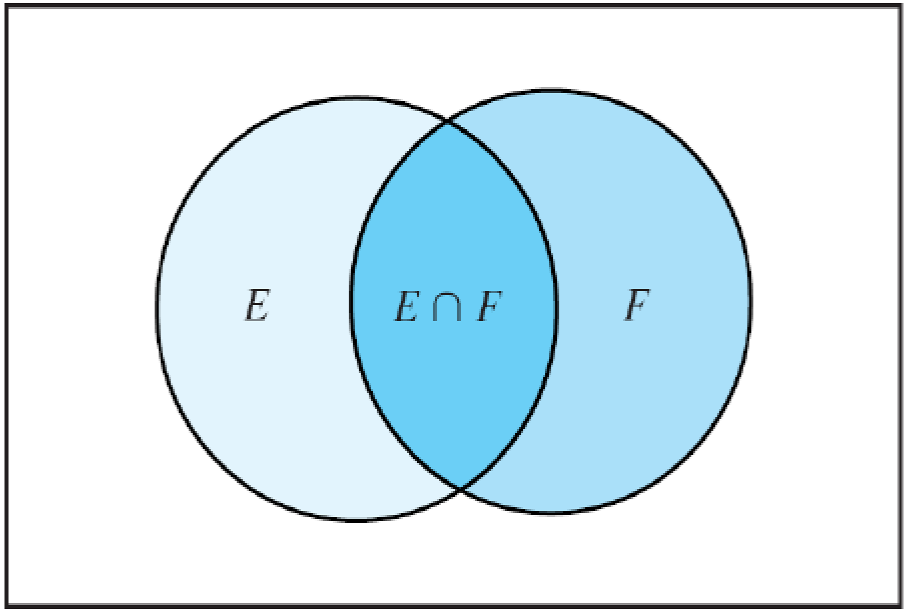
$$|E \cup F| = |E| + |F| - |E \cap F|$$



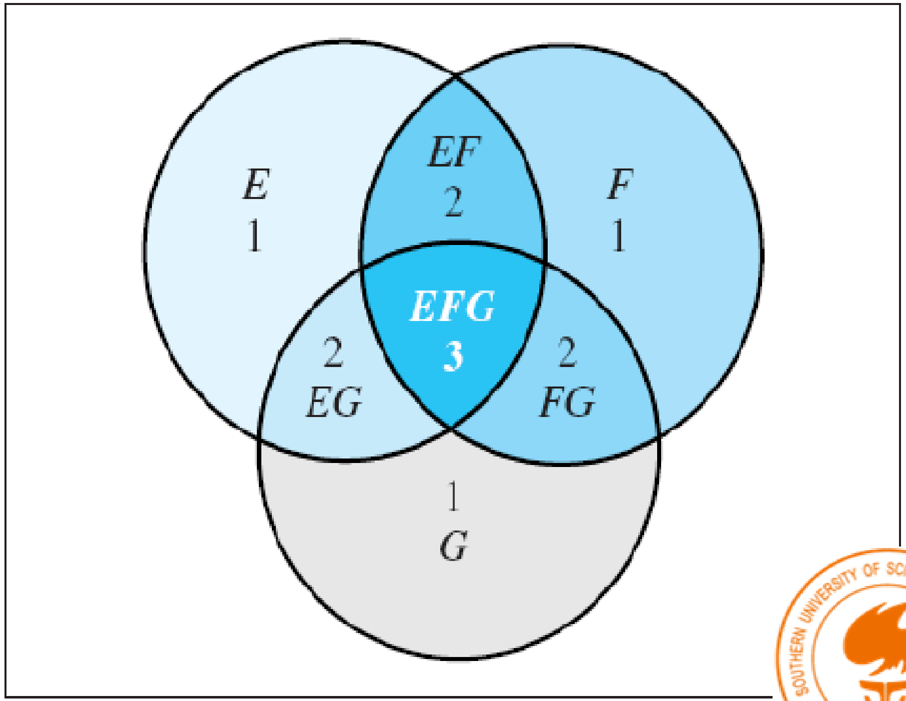
Inclusion-Exclusion Principle

- Two sets

$$|E \cup F| = |E| + |F| - |E \cap F|$$



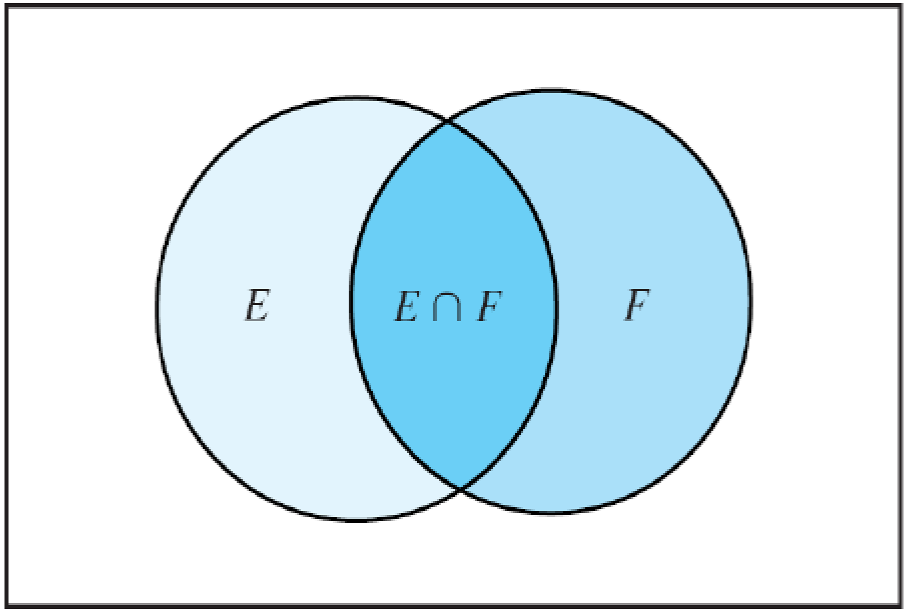
Three sets



Inclusion-Exclusion Principle

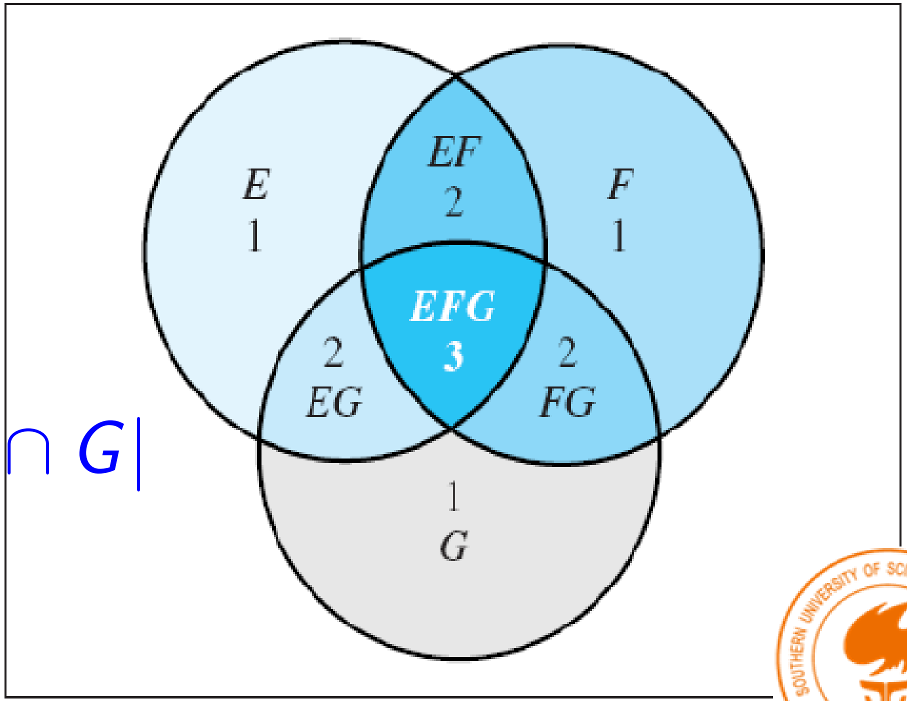
- Two sets

$$|E \cup F| = |E| + |F| - |E \cap F|$$



Three sets

$$\begin{aligned} & |E \cup F \cup G| \\ = & |E| + |F| + |G| \\ & -|E \cap F| - |E \cap G| - |F \cap G| \\ & +|E \cap F \cap G| \end{aligned}$$



Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

Proof by induction

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

Proof by induction

Base case $(n = 2)$

$$|E \cup F| = |E| + |F| - |E \cap F|$$

$$\left|\cup_{i=1}^{n} E_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} \left|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}\right|$$

Proof by induction

Base case $(n = 2)$

$$|E \cup F| = |E| + |F| - |E \cap F|$$

Inductive Hypothesis

$$\left|\cup_{i=1}^{n-1} E_i\right| = \sum_{k=1}^{n-1} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n-1} \left|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}\right|$$

Inclusion-Exclusion Principle

- Inductive step

  Set $E = E_1 \cup \cdots \cup E_{n-1}$, and $F = E_n$.

Inclusion-Exclusion Principle

- Inductive step

  Set $E = E_1 \cup \cdots \cup E_{n-1}$, and $F = E_n$.

  By $|E \cup F| = |E| + |F| - |E \cap F|$

Inclusion-Exclusion Principle

- Inductive step

  Set $E = E_1 \cup \cdots \cup E_{n-1}$, and $F = E_n$.

  By $|E \cup F| = |E| + |F| - |E \cap F|$

$$|\cup_{i=1}^{n} E_i| = \left|\cup_{i=1}^{n-1} E_i\right| + |E_n| - \left|\left(\cup_{i=1}^{n-1} E_i\right) \cap E_n\right|$$

Inclusion-Exclusion Principle

- Inductive step

  Set $E = E_1 \cup \cdots \cup E_{n-1}$, and $F = E_n$.

  By $|E \cup F| = |E| + |F| - |E \cap F|$

$$|\cup_{i=1}^{n} E_i| = \boxed{\left|\cup_{i=1}^{n-1} E_i\right|} + |E_n| - \left|\left(\cup_{i=1}^{n-1} E_i\right) \cap E_n\right|$$

  The first term is given by i.h.

Inclusion-Exclusion Principle

- Inductive step

  Set $E = E_1 \cup \cdots \cup E_{n-1}$, and $F = E_n$.

  By $|E \cup F| = |E| + |F| - |E \cap F|$

$$|\cup_{i=1}^{n} E_i| = \boxed{\left|\cup_{i=1}^{n-1} E_i\right|} + |E_n| - \boxed{\left|\left(\cup_{i=1}^{n-1} E_i\right) \cap E_n\right|}$$

  The first term is given by i.h.

  For the third term, by distributive law,

$$\left|\left(\cup_{i=1}^{n-1} E_i\right) \cap E_n\right| = \left|\cup_{i=1}^{n-1} (E_i \cap E_n)\right| = \left|\cup_{i=1}^{n-1} G_i\right|$$

  where $G_i = E_i \cap E_n$.

Inclusion-Exclusion Principle

- So far

$$\left|\cup_{i=1}^{n} E_i\right| = \left|\cup_{i=1}^{n-1} E_i\right| + |E_n| - \left|\cup_{i=1}^{n-1} G_i\right|$$

where $G_i = E_i \cap E_n$.

Inclusion-Exclusion Principle

- So far

$$\left|\cup_{i=1}^{n} E_i\right| = \left|\cup_{i=1}^{n-1} E_i\right| + |E_n| - \left|\cup_{i=1}^{n-1} G_i\right|$$

where $G_i = E_i \cap E_n$.

Note that (why?)

$$-(-1)^{k+1}|G_{i_1} \cap G_{i_2} \cap \cdots \cap G_{i_k}|$$
$$= (-1)^{k+2}|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k} \cap E_n|$$

- So far

$$\left|\cup_{i=1}^{n} E_i\right| = \left|\cup_{i=1}^{n-1} E_i\right| + |E_n| - \left|\cup_{i=1}^{n-1} G_i\right|$$

where $G_i = E_i \cap E_n$.

Note that (why?)

$$-(-1)^{k+1}|G_{i_1} \cap G_{i_2} \cap \cdots \cap G_{i_k}|$$
$$= (-1)^{k+2}|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k} \cap E_n|$$

Some discussion:
first summation sums $(-1)^{k+1}|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$ over all lists $i_1, i_2, \ldots, i_k$ that do not contain n
$|E_n|$ and second summation together sum $(-1)^{k+1}|E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$ over all lists $i_1, i_2, \ldots, i_k$ that do contain n

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

  This can be used to determine the number of onto functions

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

  This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

  This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

Inclusion-Exclusion Principle

- $$|\cup_{i=1}^{n} E_i| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$$

  This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

  $$\#(a) + \#(b) = n^m$$

Inclusion-Exclusion Principle

- This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

$$\#(a) + \#(b) = n^m$$

Inclusion-Exclusion Principle

- This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

$$\#(a) + \#(b) = n^m$$

  Set E_i – set of functions that map nothing to element i of B

Inclusion-Exclusion Principle

- This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

$$\#(a) + \#(b) = n^m$$

  Set E_i – set of functions that map nothing to element i of B

  $\#(b) = |\cup_{i=1}^{n} E_i|$

Inclusion-Exclusion Principle

- This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

$$\#(a) + \#(b) = n^m$$

  Set E_i – set of functions that map nothing to element i of B

  $\#(b) = |\cup_{i=1}^{n} E_i|$

  $= \sum_{k=1}^{n}(-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$

Inclusion-Exclusion Principle

- This can be used to determine the number of onto functions

  A, B are two sets with $|A| = m$ and $|B| = n$.

  (a) How many onto functions are there from A to B?

  (b) How many functions are there from A to B that map nothing to at least one element of B?

$$\#(a) + \#(b) = n^m$$

Set E_i – set of functions that map nothing to element i of B

$\#(b) = |\cup_{i=1}^{n} E_i|$

$= \sum_{k=1}^{n}(-1)^{k+1} \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} |E_{i_1} \cap E_{i_2} \cap \cdots \cap E_{i_k}|$

$= \sum_{k=1}^{n}(-1)^{k+1} \binom{n}{k} (n-k)^m$

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

  A list of k *distinct* elements chosen from a set N is called a **k-element permutation of N**

k-Element Permutations of a Set

- In how many ways can we choose **an ordered triple** of distinct elements from $\{1, 2, \ldots, n\}$?

  More generally, in how many ways can we choose a list of k distinct elements from $\{1, 2, \ldots, n\}$?

  A list of k *distinct* elements chosen from a set N is called a **k-element permutation of N**

  Note that the case of $k = n$ is special;
  An n-element permutation of a set N of size $|N| = n$ is what we earlier simply called a permutation.

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

    For each way of choosing first number there are $n - 1$ choices for the second

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

  For each way of choosing first number there are $n - 1$ choices for the second

  For each way of choosing first two numbers,there are $n - 2$ choices for the third number

k-Element Permutations of a Set

- How many three-element permutations of $\{1, 2, \ldots, n\}$ are there?

  n choices for first number

  For each way of choosing first number there are $n-1$ choices for the second

  For each way of choosing first two numbers,there are $n-2$ choices for the third number

  By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

Ex: When $n = 4$, there are $4 \times 3 \times 2 = 24$ 3 -element permutations of $\{1, 2, 3, 4\}$

$$L = \{123, 124, 132, 134, 142, 143, 213, 214, 231, 234, 241, 243, 312, 314, 321, 324, 341, 342, 412, 413, 421, 423, 431, 432\}.$$

An Example

- By product rule, there are $n(n-1)(n-2)$ ways to choose the permutation

Ex: When $n = 4$, there are $4 \times 3 \times 2 = 24$
3 -element permutations of $\{1, 2, 3, 4\}$

$$L = \{123, 124, 132, 134, 142, 143, 213, 214, 231, 234, 241, 243$$
$$312, 314, 321, 324, 341, 342, 412, 413, 421, 423, 431, 432\}.$$

Note: This type of "dictionary" ordering of tuples (assuming that we treat numbers the same as letters) is called a *lexicographic ordering* and is used quite often.

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n, k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n,k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n, k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

  Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n, k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

  Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

  $(\#$ 3-element perms$) = 6 \times (\#$ 3-element subsets$)$

k-Element Permutations of a Set

- **Theorem** If N is a positive integer and k is an integer with $1 \leq k \leq n$, then there are
  $P(n,k) = n(n-1)(n-2)\cdots(n-k+1)$
  k-element permutations with n distinct elements.

  How does this help us solve our original problem(from triangle program) of counting $\#$ of 3-element subsets?

  Note that every 3-element subset $\{i, j, k\}$ can be made into exactly 6 3-element perms

  $(\#$ 3-element perms$) = 6 \times (\#$ 3-element subsets$)$

  $$P(n,3) = 3! \cdot C(n,3)$$

Binomial Coefficient

- **Theorem** For integers n and k with $0 \leq k \leq n$, the number of k-element subsets of an n-element set is

$$\binom{n}{k} = C(n,k) = \frac{P(n,k)}{k!} = \frac{n!}{k!(n-k)!}.$$

This is the number of k-combinations of a set with n elements.

Some Properties of Binomial Coefficients

- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is the number of k-element subsets of an n-element set.

  $\binom{n}{0} = 1$ only one set of size 0.

  $\binom{n}{n} = 1$ only one set of size n.

  $\binom{n}{k} = \binom{n}{n-k}$ Obvious from equation. Can you think of a simple bijection that explains this?

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

  Use Sum Rule

  Let P = set of all subsets of $\{1,2,\ldots,n\}$

  S_i = set of all i subsets of $\{1,2,\ldots,n\}$

Some Properties of Binomial Coefficients (cont.)

- $$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

  Use Sum Rule

  Let P = set of all subsets of $\{1,2,\ldots,n\}$

  S_i = set of all i subsets of $\{1,2,\ldots,n\}$

  $$\Rightarrow |P| = \sum_{i=0}^{n} |S_i| = \sum_{i=0}^{n} \binom{n}{i}$$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L} = \text{set of all such lists} \Rightarrow \; |\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L} = \text{set of all such lists} \Rightarrow \ |\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by

$$i \in S \ \Leftrightarrow \ L_i = 1$$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0,1\}$

  If $\mathcal{L}$ = set of all such lists $\Rightarrow$ $|\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by

  $$i \in S \;\Leftrightarrow\; L_i = 1$$

  f is a *bijection* between $\mathcal{L}$ and P (why?) so $|\mathcal{L}| = |P|$

Some Properties of Binomial Coefficients (cont.)

- Let $L = L_1 L_2 \ldots L_n$ be a list of size n from $\{0, 1\}$

  If $\mathcal{L} = \text{set of all such lists} \Rightarrow \ |\mathcal{L}| = 2^n$

  There is a *bijection* between $\mathcal{L}$ and P so
  $|P| = 2^n$ and we are done.

  Define the following function $f : \mathcal{L} \to P$

  If $L \in \mathcal{L}$ then $f(L)$ is the set $S \subseteq \{1, 2, \ldots, n\}$ defined by

  $$i \in S \ \Leftrightarrow \ L_i = 1$$

  f is a *bijection* between $\mathcal{L}$ and P (why?) so $|\mathcal{L}| = |P|$

Ex: $n = 5$

$$f(10101) = \{1, 3, 5\}, \ f(11101) = \{1, 2, 3, 5\}, \ f(00000) = \emptyset$$

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Binomial Coefficients

n \ k	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Second half of each row is the reverse of the first half.

Binomial Coefficients

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Each row begins with a 1 because $\binom{n}{0} = 1$

Each row ends with a 1 because $\binom{n}{n} = 1$.

Each row increases at first then decreases.

Second half of each row is the reverse of the first half.

Sum of items on n-th row is 2^n

Pascal's Triangle

Take the table

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

Pascal's Triangle

Take the table

$n \backslash k$	0	1	2	3	4	5	6
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1

and shift each row slightly so that middle element is in middle

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

Pascal's Triangle

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

Pascal's Triangle

						1						
					1		1					
				1		2		1				
			1		3		3		1			
		1		4		6		4		1		
	1		5		10		10		5		1	
1		6		15		20		15		6		1

What is the next row in the table?

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

Pascal identity

Each (non-1) entry in Pascal's Triangle is the sum of the two entries directly above it (to left and to right).

Pascal's Triangle

							1							
						1		1						
					1		2		1					
				1		3		3		1				
			1		4		6		4		1			
		1		5		10		10		5		1		
	1		6		15		20		15		6		1	
1		7		21		35		35		21		7		1

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

Pascal identity

Each (non-1) entry in Pascal's Triangle is the sum of the two entries directly above it (to left and to right).

Pascal's Identity

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

Pascal's Identity

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

A purely *algebraic* proof (manipulating formulas) is possible.

Pascal's Identity

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

  A purely *algebraic* proof (manipulating formulas) is possible.

  We will use a combinatorial proof.

A Combinatorial Proof

- $\binom{n}{k}$ is the number of k-element subsets of an n-element set.

A Combinatorial Proof

- $\binom{n}{k}$ is the number of k-element subsets of an n-element set.

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

Therefore, each term (left and right) represents the number of subsets of a particular size chosen from an appropriately sized set.

A Combinatorial Proof

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

A Combinatorial Proof

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

  Number of k-subsets of an n-element set.

A Combinatorial Proof

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

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

A Combinatorial Proof

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

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

  Number of k-subsets of an $(n-1)$-element set.

A Combinatorial Proof

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

  Number of k-subsets of an n-element set.

  Number of $(k-1)$-subsets of an $(n-1)$-element set.

  Number of k-subsets of an $(n-1)$-element set.

Try to use sum principle to explain relationship among these three terms.

Example: $n = 5$, $k = 2$

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \\ \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S can be partitioned into 2 disjoint parts.

S_2 the 2-subsets that contain E and

S_3, the set of 2-subsets that do not contain E.

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \\ \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

$$\binom{5}{2} = \binom{4}{1} + \binom{4}{2}.$$

Consider $S = \{A, B, C, D, E\}$.

Set S_1 of 2-subsets of S can be partitioned into 2 disjoint parts.

S_2 the 2-subsets that contain E and

S_3, the set of 2-subsets that do not contain E.

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \\ \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

$$S_1 = \{\{A, B\}, \{A, C\}, \{A, D\}, \{A, E\}, \{B, C\}, \\ \{B, D\}, \{B, E\}, \{C, D\}, \{C, E\}, \{D, E\}\}.$$

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

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

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

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

Proof: Apply sum rule.

- If n and k are integers satisfying $0 < k < n$, then

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

Proof: Apply sum rule.

Let S_1 be set of all k-element subsets.

A Combinatorial Proof

- If n and k are integers satisfying $0 < k < n$, then

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

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.

Blaise Pascal

Born 1623; Died 1662

French Mathematician

A Founder of Probability Theory

Inventor of one of the first mechanical calculating machines

Pascal Programming Language named for him

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

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

The Binomial Theorem

$$(x+y) = \binom{1}{0}x + \binom{1}{1}y$$

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

$$\begin{aligned}(x+y)^3 &= x^3 + 3x^2y + 3xy^2 + y^3 \\ &= \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3\end{aligned}$$

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x + y)^n$.

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

The Binomial Theorem For any integer $n \geq 0$,

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

The Binomial Theorem

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

The Binomial Theorem For any integer $n \geq 0$,

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

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

- Number of k-element subsets of an n-element set is called a **binomial coefficient** because of its role in the algebraic expansion of a binomial $(x+y)^n$.

The Binomial Theorem For any integer $n \geq 0$,

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

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

Proof?

Application of the Binomial Theorem

- We may use the Binomial Theorem to prove

$$\boxed{\sum_{i=0}^{n} \binom{n}{i} = 2^n}$$

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n-k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n-k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

  Show that if we have k_1 labels of one kind, e.g., red, k_2 labels of a second kind, e.g., blue, and $k_3 = n - k_1 - k_2$ labels of a third kind, then there are $\frac{n!}{k_1!k_2!k_3!}$ ways to apply these labels to n objects

Labelling and Trinomial Coefficients

- Suppose we have k labels of one kind, e.g., red and $n-k$ labels of another, e.g., blue. In how many different ways can we apply these labels to n objects?

  Show that if we have k_1 labels of one kind, e.g., red, k_2 labels of a second kind, e.g., blue, and $k_3 = n - k_1 - k_2$ labels of a third kind, then there are $\frac{n!}{k_1!k_2!k_3!}$ ways to apply these labels to n objects

  What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x+y+z)^n$?

Labelling and Trinomial Coefficients

- There are $\binom{n}{k_1}$ ways to choose the red items There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n - k_1$. The remaining k_3 items get labelled a third color.

Labelling and Trinomial Coefficients

- There are $\binom{n}{k_1}$ ways to choose the red items There are then $\binom{n-k_1}{k_2}$ ways to choose the blue items from the remaining $n - k_1$. The remaining k_3 items get labelled a third color.

  Using the *product rule* the total number of labellings is

$$
\begin{aligned}
\binom{n}{k_1}\binom{n-k_1}{k_2} &= \frac{n!}{k_1!(n-k_1)!}\,\frac{(n-k_1)!}{(k_2)!(n-k_1-k_2)!} \\
&= \frac{n!}{k_1!k_2!(n-k_1-k_2)!} = \frac{n!}{k_1!k_2!k_3!}
\end{aligned}
$$

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

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

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

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

What is the coefficient of $x^{k_1}y^{k_2}z^{k_3}$ in $(x+y+z)^n$?

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than $1/2$! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

  We may assume that a year has 365 days and there are no twins in the room.

The Birthday Paradox

- Suppose that 25 students are in a room. What is the probability that at least two of them share a birthday?

  It's greater than 1/2! (only need 23)

  A_n – "there are n students in a room and at least two of them share a birthday."

  We may assume that a year has 365 days and there are no twins in the room.

  This will be very similar to the analysis of hashing n keys into a table of size 365.

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

  $\#B_n = 365 \times 364 \times \cdots \times (365 - (n-1))$

The Birthday Paradox

- A_n – "there are n students in a room and at least two of them share a birthday."

  Sample space: $|S| = 365^n$

  B_n – "there are n students in a room and none of them share a birthday."

  $\#B_n = 365 \times 364 \times \cdots \times (365 - (n-1))$

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

The Birthday Paradox

n	A_n	B_n	n	A_n	B_n
1	0.00000000	1.00000000	16	0.28360400	0.71639599
2	0.00273972	0.99726027	17	0.31500766	0.68499233
3	0.00820416	0.99179583	18	0.34691141	0.65308858
4	0.01635591	0.98364408	19	0.37911852	0.62088147
5	0.02713557	0.97286442	20	0.41143838	0.58856161
6	0.04046248	0.95953751	21	0.44368833	0.55631166
7	0.05623570	0.94376429	22	0.47569530	0.52430469
8	0.07433529	0.92566470	23	0.50729723	0.49270276
9	0.09462383	0.90537616	24	0.53834425	0.46165574
10	0.11694817	0.88305182	25	0.56869970	0.43130029
11	0.14114137	0.85885862	26	0.59824082	0.40175917
12	0.16702478	0.83297521	27	0.62685928	0.37314071
13	0.19441027	0.80558972	28	0.65446147	0.34553852
14	0.22310251	0.77689748	29	0.68096853	0.31903146
15	0.25290131	0.74709868	30	0.70631624	0.29368375

"Birthday" attacks

- Event A: at least two people in the room have the same birthday

  Event B: no two people in the room have the same birthday

  $\Pr[A] = 1 - \Pr[B]$

$$\begin{aligned}\Pr[B] &= \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdot \cdots \cdot \left(1 - \frac{n-1}{365}\right) \\ &= \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right).\end{aligned}$$

$\Pr[A] = 1 - \prod_{i=1}^{n-1} \left(1 - \frac{i}{365}\right)$

"Birthday" attacks

- Event A: at least two people in the room have the same birthday

  Event B: no two people in the room have the same birthday

  $\Pr[A] = 1 - \Pr[B]$

$$\begin{aligned}\Pr[B] &= \left(1-\frac{1}{365}\right)\cdot\left(1-\frac{2}{365}\right)\cdot\cdots\cdot\left(1-\frac{n-1}{365}\right)\\ &= \prod_{i=1}^{n-1}\left(1-\frac{i}{365}\right).\end{aligned}$$

  $\Pr[A] = 1 - \prod_{i=1}^{n-1}\left(1-\frac{i}{365}\right)$

  $p(n;H) := 1 - \prod_{i=1}^{n-1}(1-\frac{i}{H})$

"Birthday" attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

"Birthday" attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

"Birthday" attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

  Recall that $p(n; H) := 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{H})$

  This probability can be approximated as

$$p(n; H) \approx 1 - e^{-n(n-1)/2H} \approx 1 - e^{-n^2/2H}.$$

“Birthday” attacks

- Since $e^x = 1 + x + \frac{x^2}{2!} + \cdots$, for $|x| \ll 1$, $e^x \approx 1 + x$

  Thus, we have $e^{-i/H} \approx 1 - \frac{i}{H}$.

  Recall that $p(n; H) := 1 - \prod_{i=1}^{n-1}(1 - \frac{i}{H})$

  This probability can be approximated as

  $$p(n; H) \approx 1 - e^{-n(n-1)/2H} \approx 1 - e^{-n^2/2H}.$$

  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

  $$n(p; H) \approx \sqrt{2H \ln \frac{1}{1-p}}.$$

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$. (this will be proved later.)

Euclidean Algorithm

- The Euclidean algorithm in pseudocode

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x\{gcd(a, b) is x\}

The number of divisions required to find $\gcd(a, b)$ is $O(\log b)$, where $a \geq b$. (this will be proved later.)

Why ?

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \le r_3 < r_2, \\
&\ \ \vdots \\
r_{n\text{-}2} &= r_{n\text{-}1} q_{n\text{-}1} + r_n && 0 \le r_n < r_{n\text{-}1}, \\
r_{n\text{-}1} &= r_n q_n \, .
\end{aligned}
$$

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}$$

Observation:

$$r_{i+2} = r_i \bmod r_{i+1}$$

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\;\;\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n \,.
\end{aligned}
$$

Observation:

$r_{i+2} = r_i \bmod r_{i+1}$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \le r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

Observation:

$$r_{i+2} = r_i \bmod r_{i+1}$$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Case (i): $r_{i+1} \le \frac{1}{2} r_i$: $r_{i+2} < r_{i+1} \le \frac{1}{2} r_i$.

Case (ii): $r_{i+1} > \frac{1}{2} r_i$: $r_{i+2} = r_i \bmod r_{i+1} = r_i - r_{i+1} < \frac{1}{2} r_i$.

Euclidean Algorithm

- Key steps in the Euclidean algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \le r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 & 0 \le r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \le r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

See [Theorem 1 p. 347].

Observation:

$r_{i+2} = r_i \bmod r_{i+1}$

We claim that $r_{i+2} < \frac{1}{2} r_i$

Case (i): $r_{i+1} \le \frac{1}{2} r_i$: $r_{i+2} < r_{i+1} \le \frac{1}{2} r_i$.

Case (ii): $r_{i+1} > \frac{1}{2} r_i$: $r_{i+2} = r_i \bmod r_{i+1} = r_i - r_{i+1} < \frac{1}{2} r_i$.

Next Lecture

- solving linear recurrence ...