COUNTING

DISCRETE STRUCTURES II

DARRYL HILL

BASED ON THE TEXTBOOK:

DISCRETE STRUCTURES FOR COMPUTER SCIENCE: COUNTING, RECURSION, AND PROBABILITY

BY MICHIEL SMID

Product Rule Revisited

Strings of length 75 – each character is an Upper Case letter or a digit

Procedure – write each character from left to right

- We have 26 letters plus 10 digits
- Task 1 = choose from 36 choices for first character
- Task 2 = choose from 36 choices for second character
- …
- Task 75 = choose from 36 choices for 75th character
- = 36^{75}

More Complex Passwords

Slight adjustment: Strings of length 75 – each character is an Upper Case letter or a digit – must contain **at least** one digit

In counting the 36^{75} strings we have counted strings that contain no digits

We want to NOT count these no digit strings.

Ideas?

- count all strings with 1 digits
- add all strings with 2 digits
- add all strings with 3 digits
- …
- add all strings with 75 digits

More Complex Passwords

Slight adjustment: Strings of length 75 – each character is an Upper Case letter or a digit – must contain **at least** one digit

In counting the 36^{75} strings we have counted strings that contain no digits

We want to NOT count these no digit strings.

Ideas?

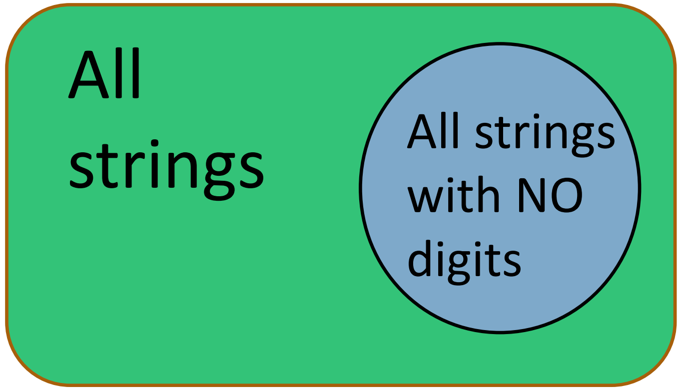
- count all strings with 1 digits
- add all strings with 2 digits
- add all strings with 3 digits
- …
- add all strings with 75 digits

75 different calculations

…easy for a computer, not for a person

Complement Rule

Slight adjustment: Strings of length 75 – each character is an Upper Case letter or a digit – must contain **at least** one digit



We can count all strings

What about all the strings with NO digits?

This is the **complement** of the set of elements that we are looking for.

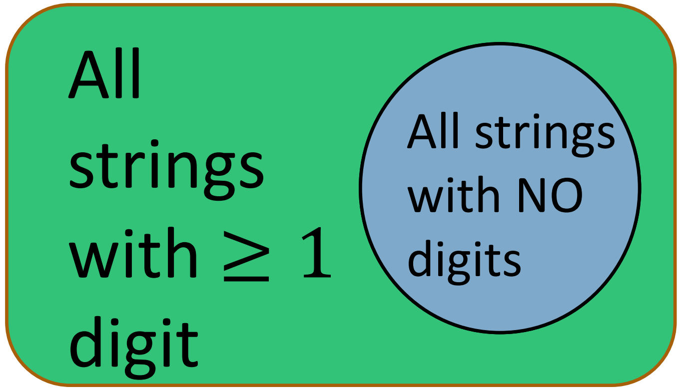
Can we count those?

75 Upper Case letters = 26^{75} - easy to count

So now is there a way to count how many strings have at least one digit?

Complement Rule

Slight adjustment: Strings of length 75 – each character is an Upper Case letter or a digit – must contain **at least** one digit



We can count all strings

What about all the strings with NO digits?

This is the **complement** of the set of elements that we are looking for.

Can we count those?

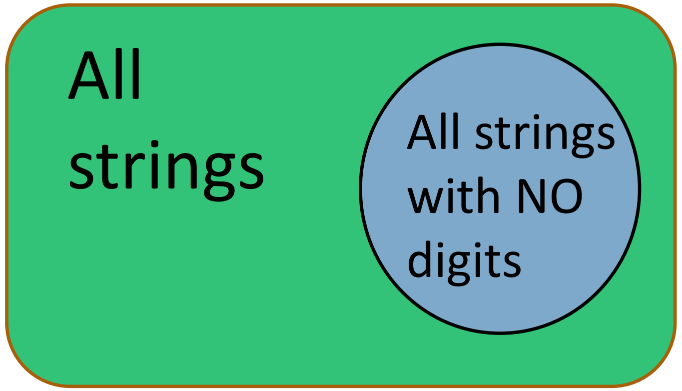
75 Upper Case letters = 26^{75} - easy to count

So now is there a way to count how many strings have at least one digit?

Complement Rule

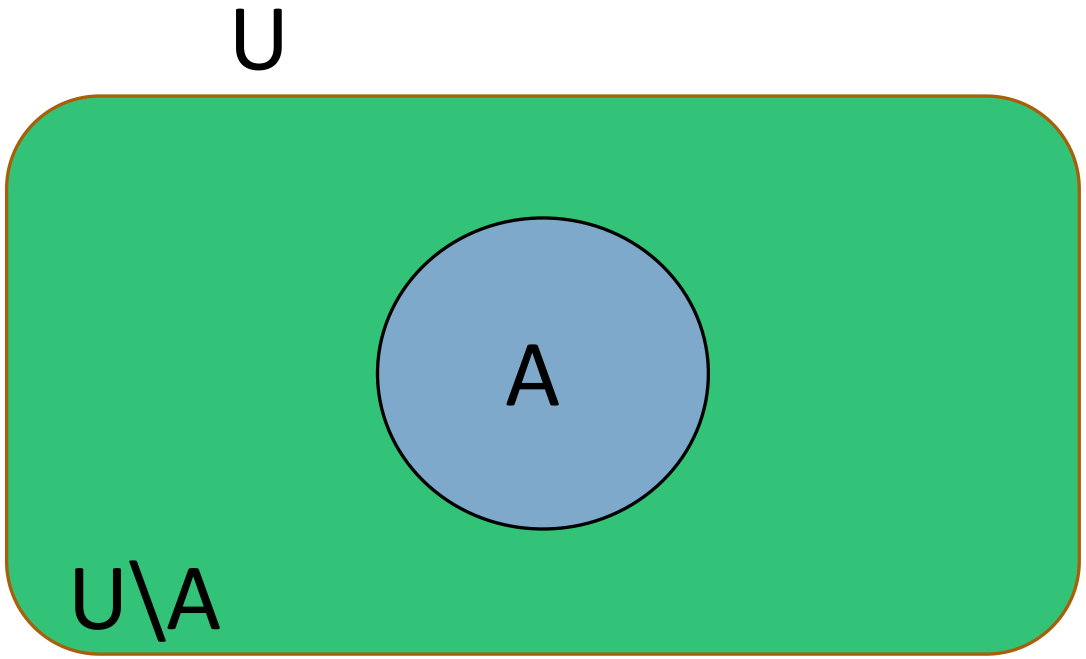
Slight adjustment: Strings of length 75 – each character is an Upper Case letter or a digit – must contain at least one digit

- Count number of strings with no restrictions = 36^{75} subtract all strings with NO digits $= 26^{75}$
- All strings with at least one digit $= 36^{75} - 26^{75}$
- Known as the **Complement Rule**



Complement Rule

- Known as the Complement Rule
- If we want to find |A| but it is too difficult, then we can substitute:
- $|A| = |U| - |U \backslash \mathrm{A}|$
- In this example U = all strings with either a digit or upper case letter
- U/A = all strings with no digits
- A = all strings with at least one digit



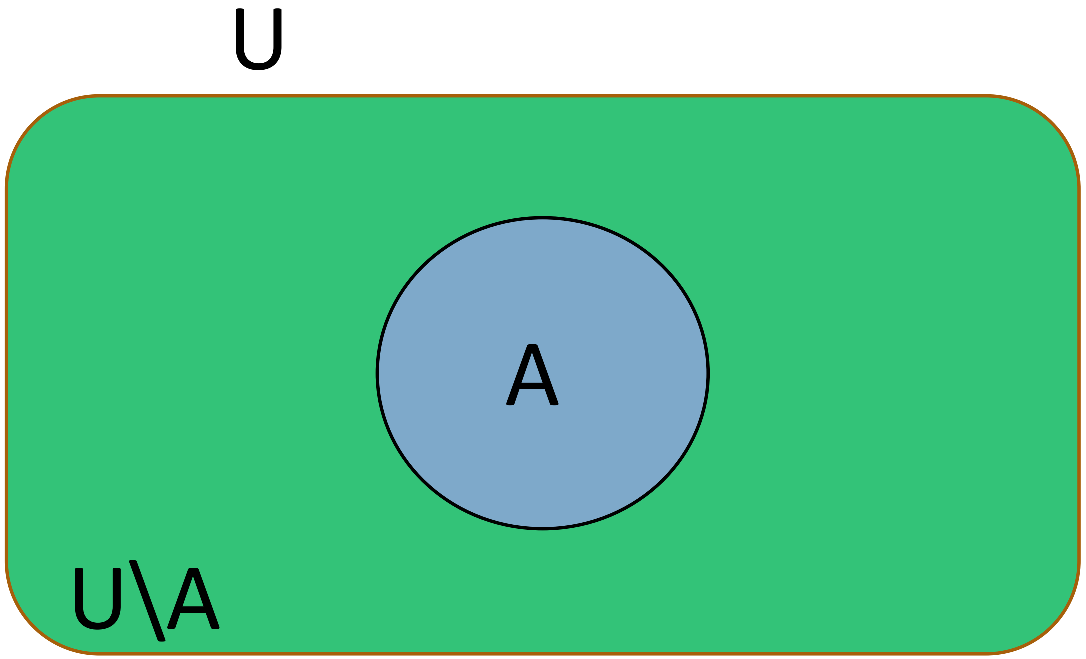
$= \{x | x \in U \wedge x \notin A\}$

Complement Rule

- Complement Rule
- $|A| = |U| - |U \backslash A|$

- Can be used if we do not know how to count A, or if counting A directly is too painstaking

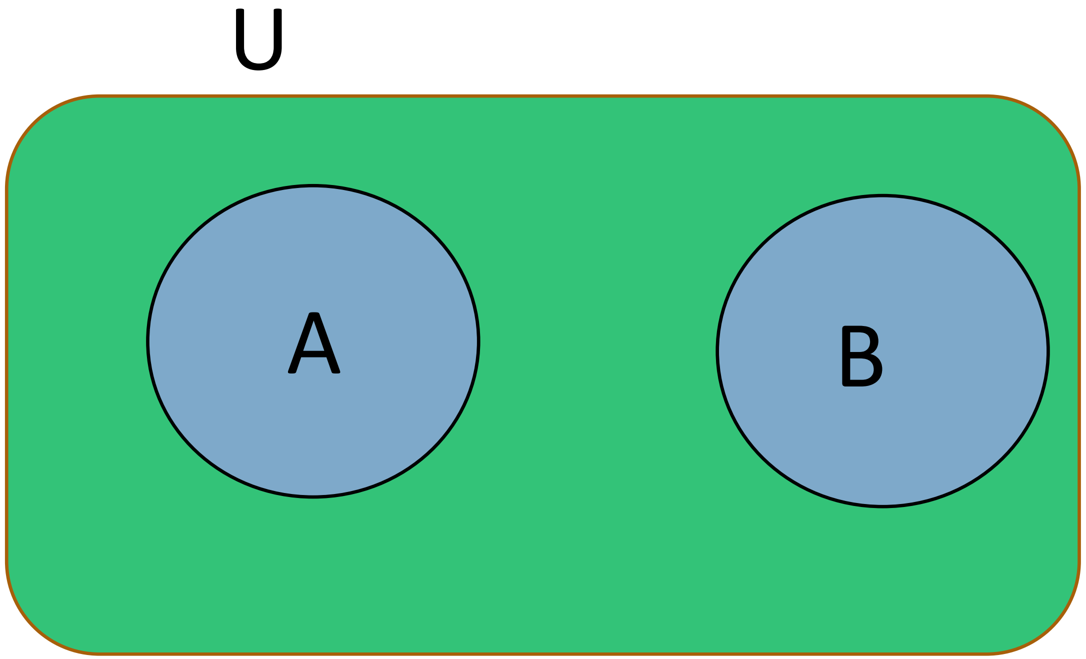
- but |U| is easy to determine and |U\A| is easy to determine



$= \{x | x \in U \wedge x \notin A\}$

Sum Rule

- If A and B are disjoint then
- $|A \cup B| = |A| + |B|$
- Find all strings of length 75 or 76
- There are no strings that have length 75 **and** length 76
  - thus these sets are pairwise disjoint

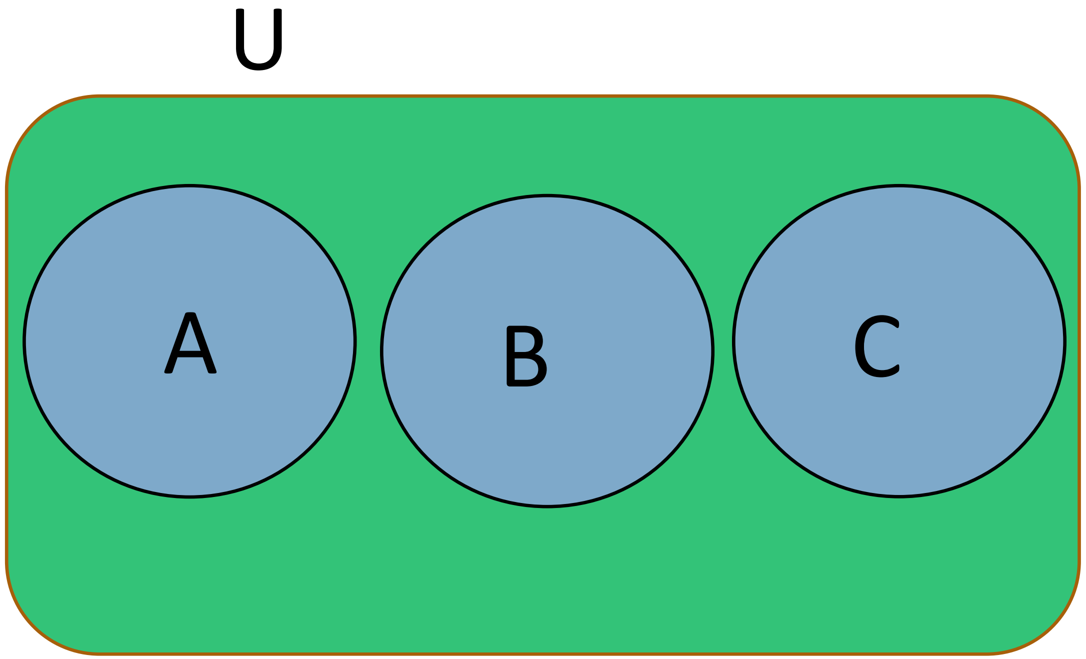


Sum Rule

- If A and B and C are disjoint then
- $|A \cup B \cup C| = |A| + |B| + |C|$

- Example: Find all strings of length 75 or 76 or 77 with digits or Upper Case letters and ≥ 1 digit
- $|A| = (36^{75} - 26^{75})$
- $|B| = (36^{76} - 26^{76})$
- $|C| = (36^{77} - 26^{77})$

- $|A \cup B \cup C| = |A| + |B| + |C|$
  $= (36^{75} - 26^{75}) + (36^{76} - 26^{76}) + (36^{77} - 26^{77})$

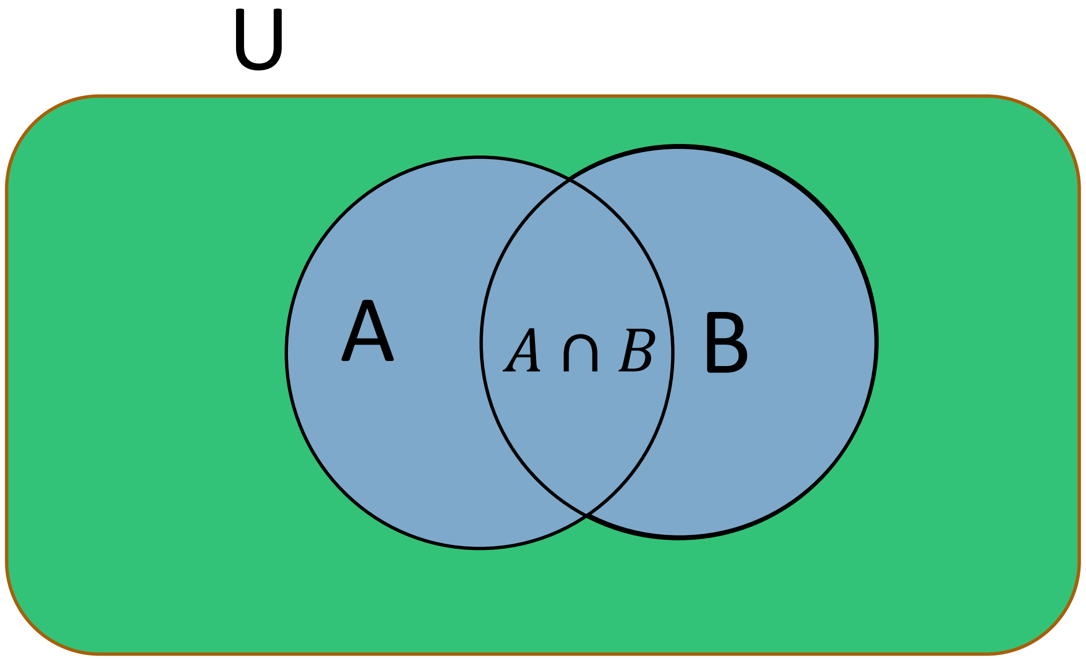


Inclusion - Exclusion

- What if A and B are NOT disjoint? How do we determine $|A \cup B|$?

- Start with:
- $|A \cup B| = |A| + |B|$

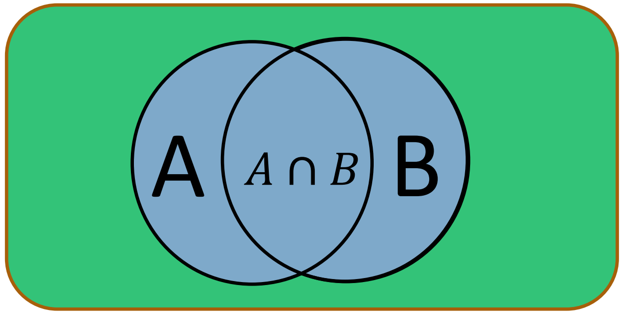
- But we have counted the elements in $|A \cap B|$ twice.
- Subtract it once to get the correct counting



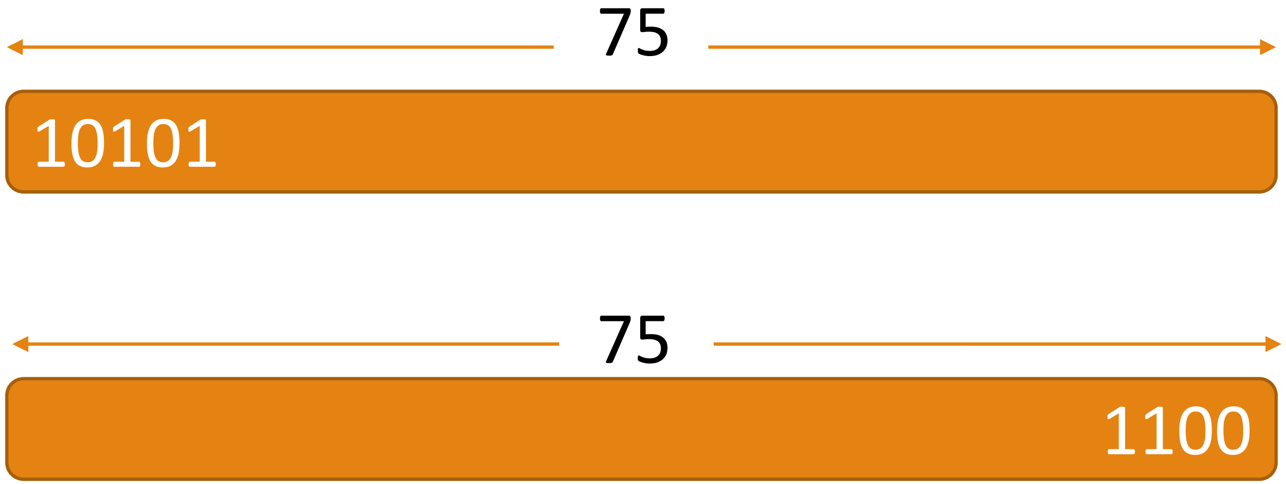
- $|A \cup B| = |A| + |B| - |A \cap B|$

Inclusion - Exclusion

- bitstrings of length 75
  - start with 10101 – set A
  - or end with 1100 – set B



- Cannot apply the sum rule, since we have strings that are in both A and B

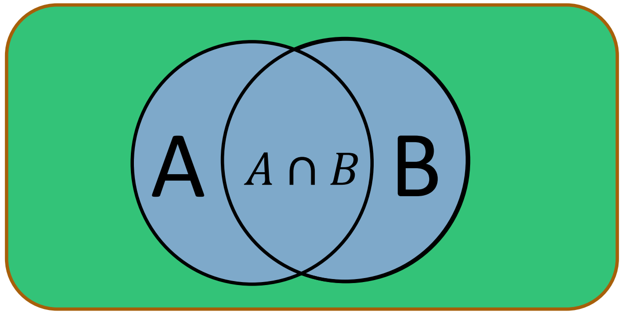


- Apply inclusion/exclusion:
- $|A \cup B| = |A| + |B| - |A \cap B|$

- Start by determining A and B individually

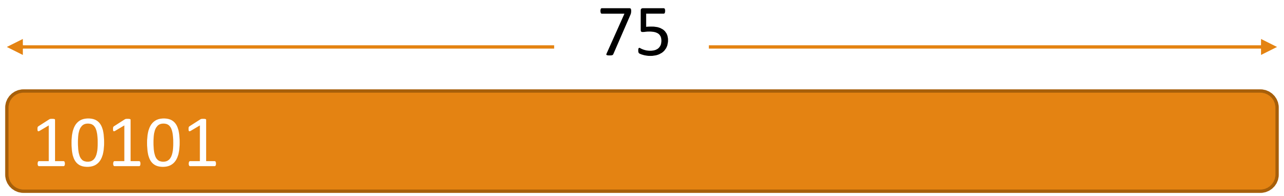
Inclusion - Exclusion

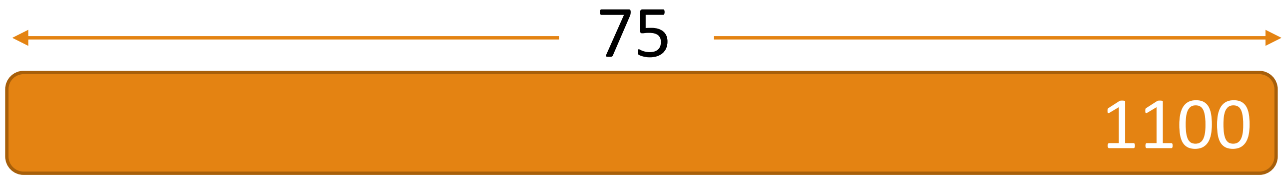
- $|A \cup B| = |A| + |B| - |A \cap B|$



- Start by determining A and B individually

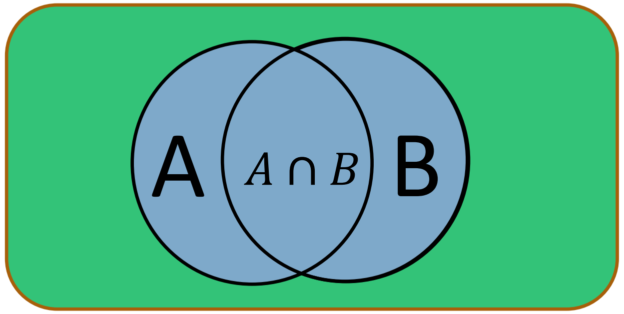
- A has first 5 bits fixed so:
- $|A| = 2^{75-5} = 2^{70}$
- B has last 4 bits fixed so:
- $|B| = 2^{75-4} = 2^{71}$
- $A \cap B$ has 9 bits fixed so
- $|A \cap B| = 2^{75-9} = 2^{66}$

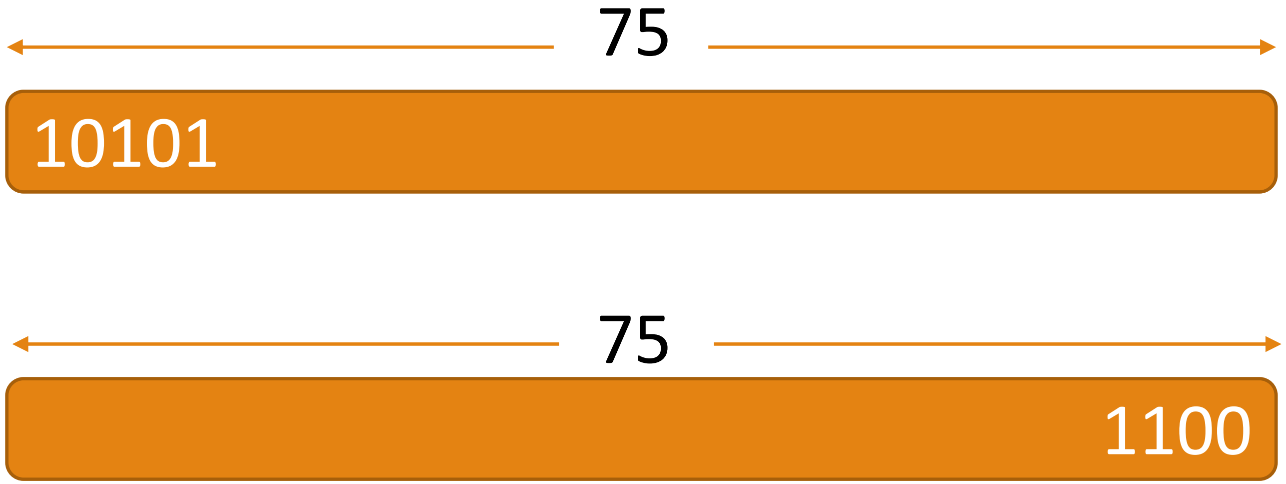




Inclusion - Exclusion

- bitstrings of length 75
  - start with 10101 – set A
  - or end with 1100 – set B





- $|A| = 2^{75-5} = 2^{70}$
- $|B| = 2^{75-4} = 2^{71}$
- $|A \cap B| = 2^{75-9} = 2^{66}$
- Thus:
- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \cup B| = 2^{70} + 2^{71} - 2^{66}$

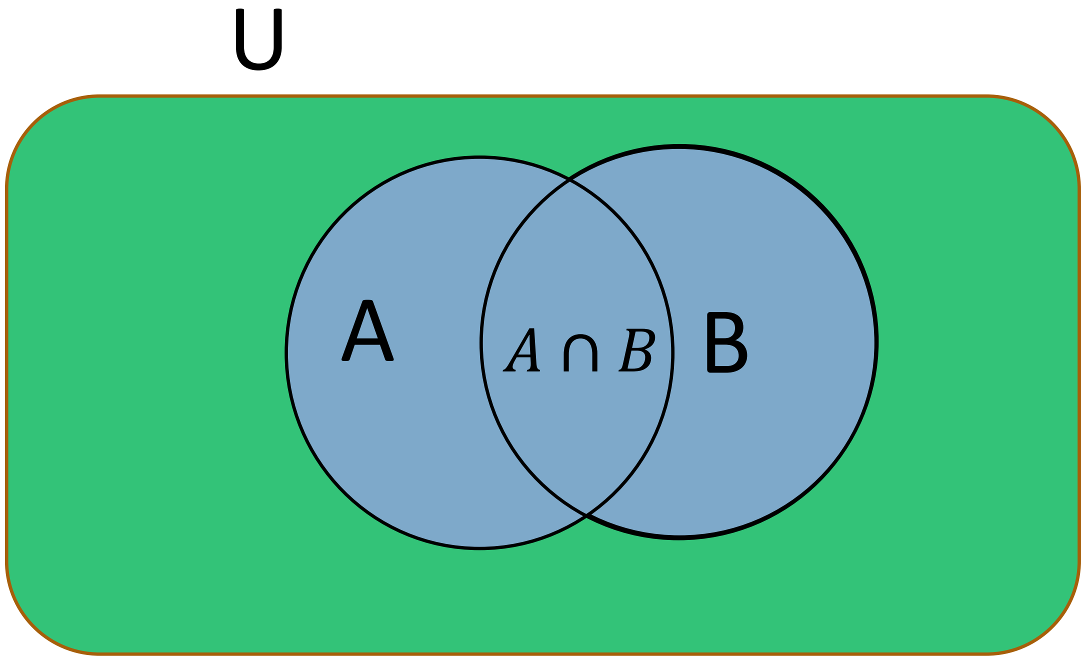
Inclusion - Exclusion

- Inclusion - Exclusion still applies if A and B are disjoint

- However it means that $|A \cap B| = 0$

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \cup B| = |A| + |B| - 0$
- $|A \cup B| = |A| + |B|$

- Which is the sum rule



Inclusion - Exclusion

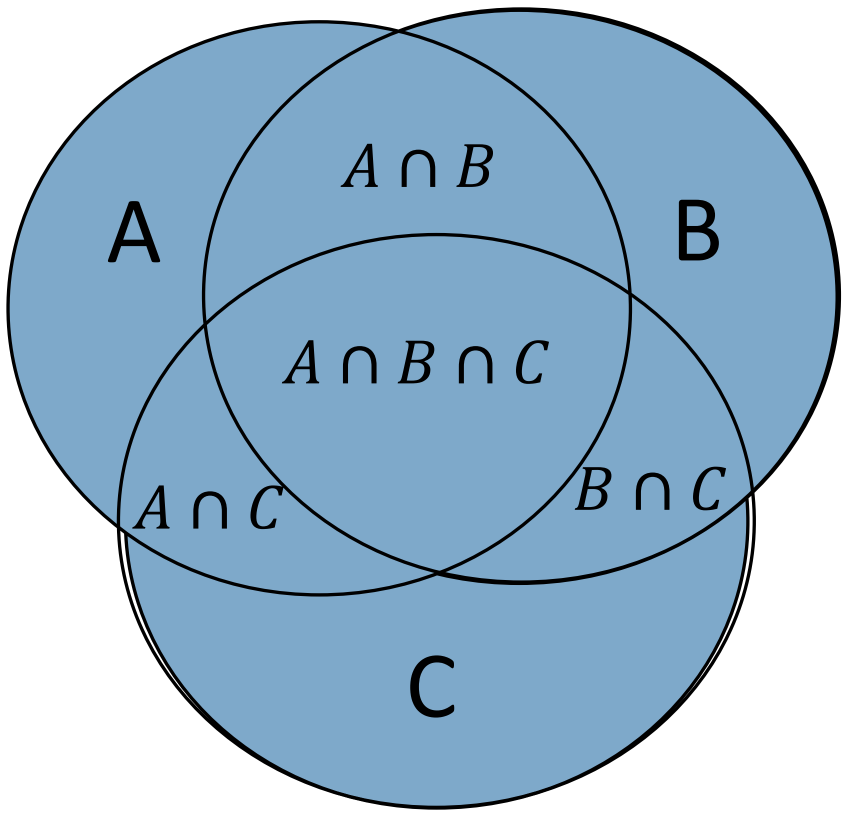
- With 3 sets:

- If we count $|A| + |B| + |C|$ what have we counted?

- $|A \cap B|$ twice – once with $|A|$ and once with $|B|$
- $|A \cap C|$ twice – once with $|A|$ and once with $|C|$
- $|B \cap C|$ twice – once with $|B|$ and once with $|C|$
- $|A \cap B \cap C|$ three times – with $|A|$, with $|B|$, and with $|C|$

$$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|$$

Now what have we done?



Inclusion - Exclusion

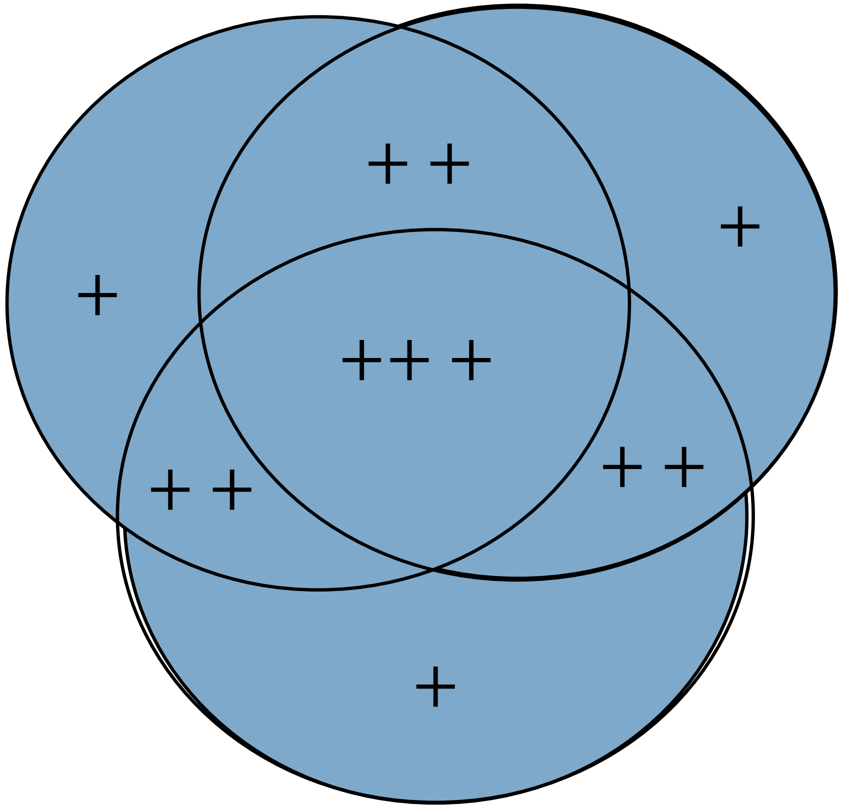
- With 3 sets:

- If we count $|A| + |B| + |C|$ what have we counted?

- $|A \cap B|$ twice – once with $|A|$ and once with $|B|$
- $|A \cap C|$ twice – once with $|A|$ and once with $|C|$
- $|B \cap C|$ twice – once with $|B|$ and once with $|C|$
- $|A \cap B \cap C|$ three times – with $|A|$, with $|B|$, and with $|C|$

$$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|$$

Now what have we done?



Inclusion - Exclusion

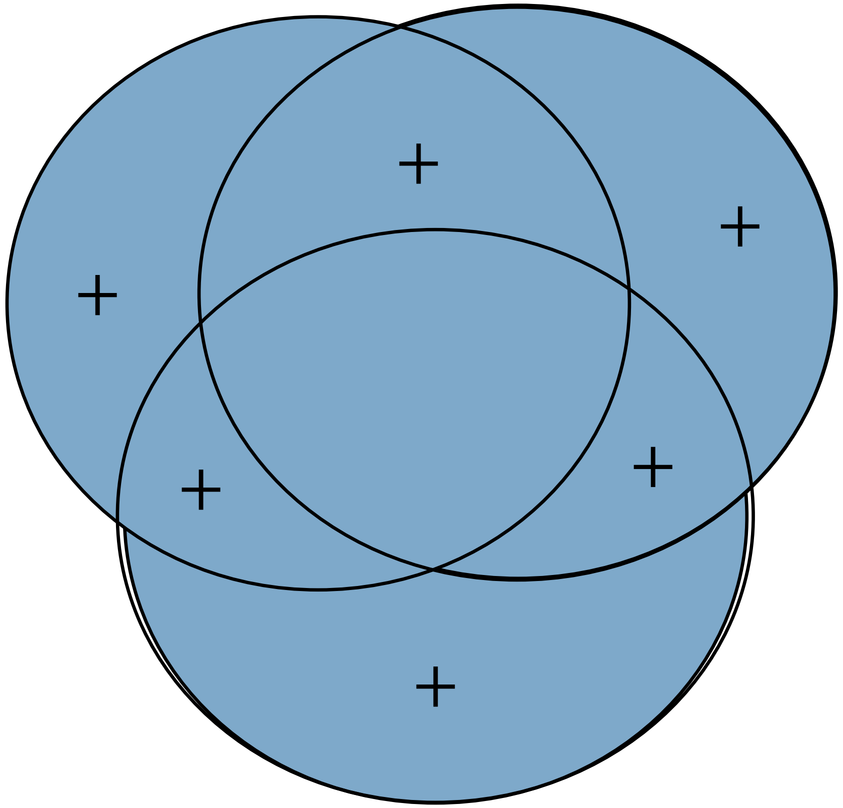
- With 3 sets:

- If we count $|A| + |B| + |C|$ what have we counted?

- $|A \cap B|$ twice – once with $|A|$ and once with $|B|$
- $|A \cap C|$ twice – once with $|A|$ and once with $|C|$
- $|B \cap C|$ twice – once with $|B|$ and once with $|C|$
- $|A \cap B \cap C|$ three times – with $|A|$, with $|B|$, and with $|C|$

$$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|$$

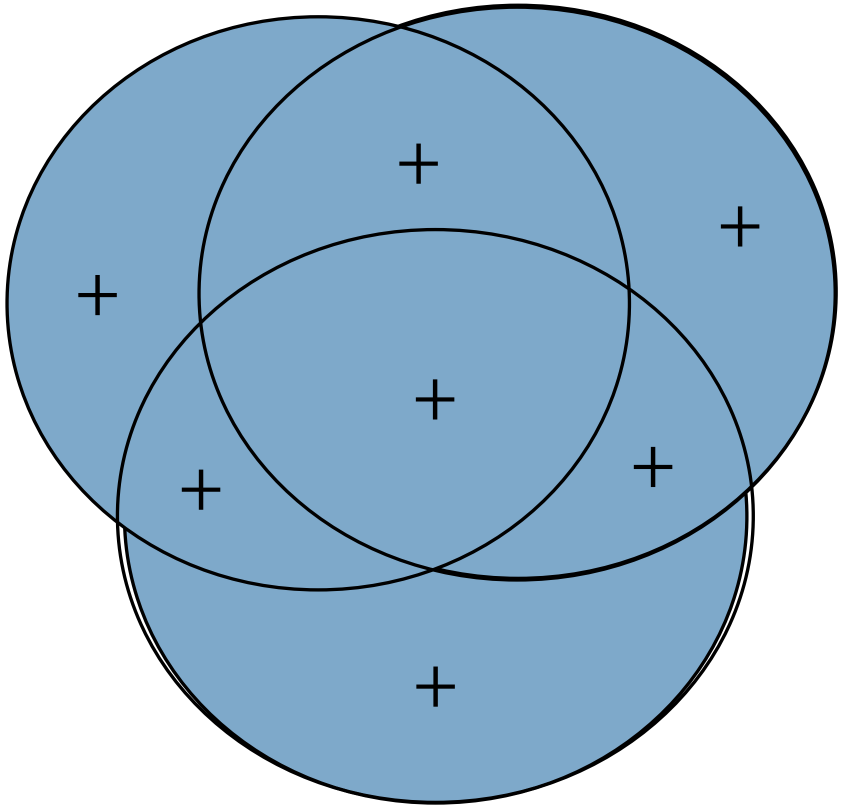
Now what have we done?



Inclusion - Exclusion

$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|$

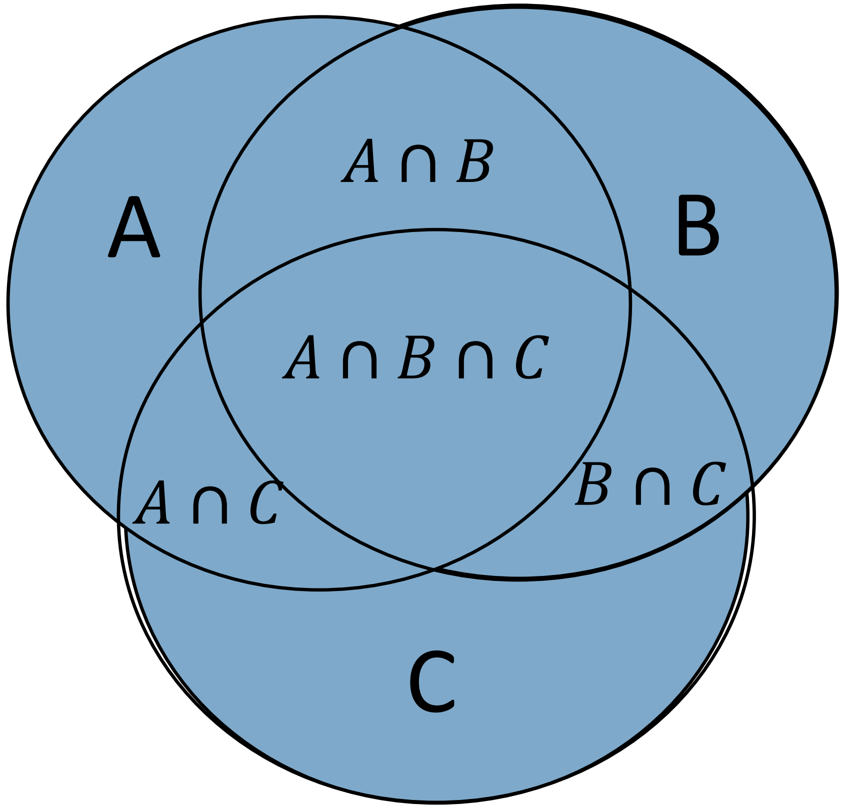
- We've subtracted $|A \cap B \cap C|$ three times
- Since $|A| + |B| + |C|$ counts $|A \cap B \cap C|$ three times, and we've subtracted it three times, now we have not counted it at all. So add it back in:
- $|A \cap B \cap C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$



Inclusion - Exclusion

$|A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C|$

- We've subtracted $|A \cap B \cap C|$ three times
- Since $|A| + |B| + |C|$ counts $|A \cap B \cap C|$ three times, and we've subtracted it three times, now we have not counted it at all. So add it back in:
- $|A \cap B \cap C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

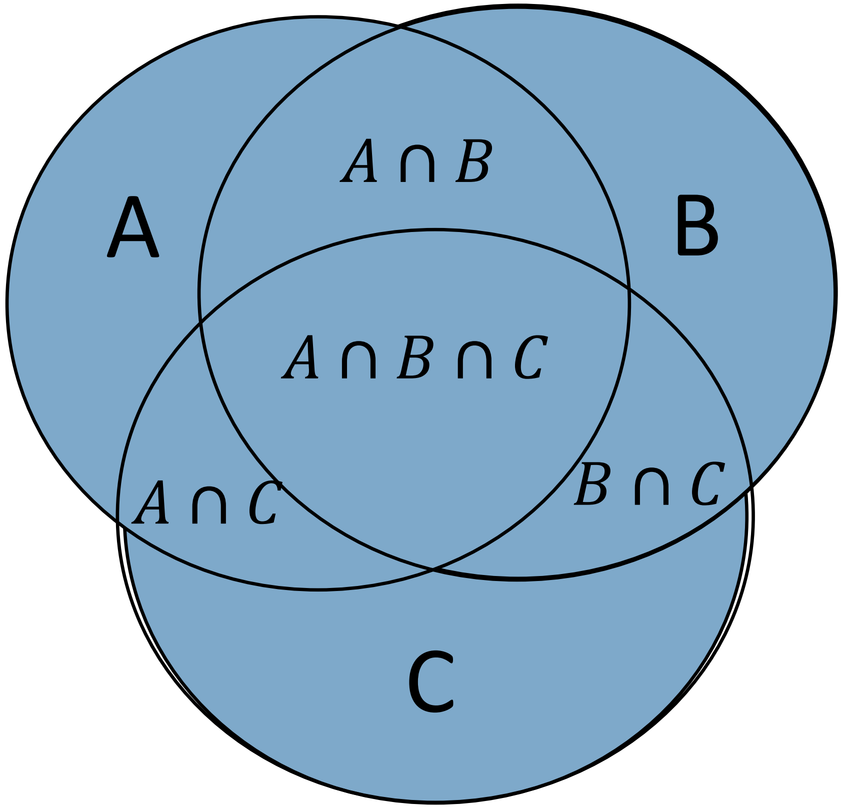


Inclusion - Exclusion

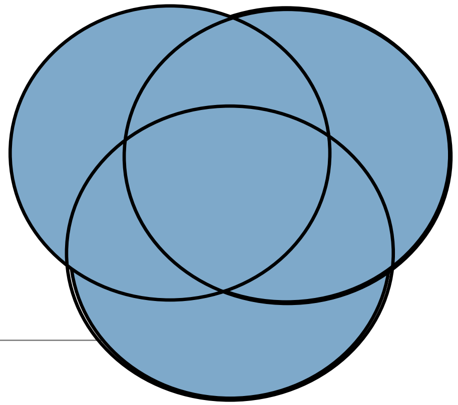
Can be done with 4 sets:

$$|A| + |B| + |C| + |D| - |A \cap B| - |B \cap C| - |A \cap C| - |A \cap D| - |B \cap D| - |C \cap D| + |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - |A \cap B \cap C \cap D|$$

- Can be done for any number of sets, alternating including and excluding
- In this course we will only go up to 3 sets



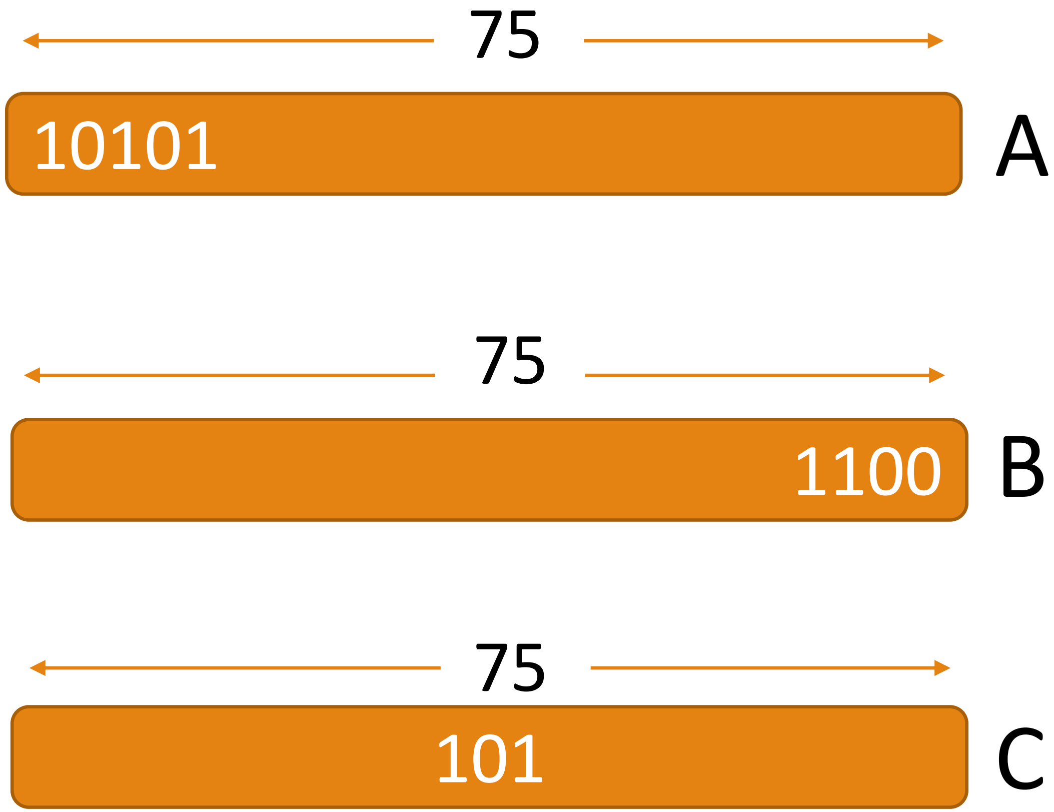
Inclusion - Exclusion



- bitstrings of length 75
  - start with 10101 – set A
  - or end with 1100 – set B
  - or have 101 at 36,37,38 – set C

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

$$= 2^{70} + 2^{71} + 2^{72}$$
$$-2^{66} - 2^{67} - 2^{68}$$
$$+2^{63}$$



Permutations of a Finite Set S

Permutation of a set S: an ordered sequence where each element of S appears exactly once

Example: for a set $S = \{a, b, c\}$ the permutations are:

$$abc, acb, bac, bca, cab, cba$$

For $|S| = n$, we can count the number of permutations using the product rule.

Procedure: Select a (previously unselected) element from S, make it the next element of the sequence.

Permutation of a Finite Set S

Procedure: Select a (previously unselected) element from S, make it the next element of the permutation.

Task 1: n choices for the 1st location

Task 2: $n - 1$ choices for the 2nd location

Task 3: $n - 2$ choices for the 3rd location

…

Task $n - 1$: 2 choices

Task n: 1 choice

Number of choices for each element of the sequence:

n	n-1	n-2	n-3	…	3	2	1

Permutation of a Finite Set S

Procedure: Select a (previously unselected) element from S, make it the next element of the permutation.

Number of choices for each element of the sequence:

n	**n-1**	**n-2**	**n-3**	**...**	**3**	**2**	**1**

Number of permutations for a set S, $|S| = n$ are:

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$$
$$= n!$$

Permutation of a Finite Set S

Number of permutations for a set $S, |S| = n$ is $n!$

n	n-1	n-2	n-3	…	3	2	1

Another way to say this is that the number of distinct **sequences** of n elements is $n!$

Subsets of Set S

$$S = \{a, b, c, d, e\}$$

How many subsets of size 3?

(These are sets, so their order does NOT matter)

All subsets of size 3 that contain a are:

$\{a, b, c\}$
$\{a, b, d\}$
$\{a, b, e\}$
$\{a, c, d\}$
$\{a, c, e\}$
$\{a, d, e\}$

All subsets of size 3 that do not contain a are:

$\{b, c, d\}$
$\{b, c, e\}$
$\{b, d\ e\}$
$\{c, d, e\}$

10 subsets total.

What if we had a set of size 1 000 000?

Subsets of Set S

For a set S, $|S| = n$, the number of subsets of size k is given by the notation:

$$\binom{n}{k}$$

"n choose k" – binomial coefficient

Since these are sets, order does not matter

$$\binom{5}{3} = 10$$

$$\binom{5}{2} = ?$$

Subsets of Set S

For a set S, $|S| = n$, the number of subsets of size k is given by the notation:

$$\binom{n}{k}$$

"n choose k" – binomial coefficient

Since these are sets, order does not matter

$$\binom{5}{3} = 10$$

$$\binom{5}{2} = 10$$

Subsets of Set S

For a set $S, |S| = n$, what is:

$$\binom{n}{1} =?$$

$$\binom{n}{n} =?$$

$$\binom{n}{0} =?$$

Subsets of Set S

What is:

$$\binom{75}{77} = ?$$

$$\binom{0}{0} = ?$$

Subsets of Set S

What is:

$$\binom{75}{77} = 0$$

$$\binom{0}{0} = 1$$

What is a general formula for $\binom{n}{k}$? Our claim is:

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

Subsets of Set S

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

$$\binom{5}{3} = \frac{5!}{3!(5-3)!}$$

$$= \frac{5!}{3!\,(2)!} = \frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{1 \cdot 2 \cdot 3 \cdot (1 \cdot 2)}$$

$$= \frac{4 \cdot 5}{2} = 10$$

We will prove this.