

# Book of Proof I: Fundamentals

January 16, 2018

# Sets: A mathematical structure

$$\{1, 2, 3\}$$

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

$$\{cat, dog, pig\}$$

$$\{2, 4, 6, 8, \dots\}$$

$$\emptyset = \{\}$$

$$\emptyset \neq \{\emptyset\}$$

Note:  $\{1, 2, 3\}$  is not the same as  $1, 2, 3$  or  $(1, 2, 3)$  or *etc.*

## Sets have no order or duplicates

$$\begin{aligned}\{1, 2, 3\} &= \{2, 3, 1\} \\ &= \{2, 1, 3\} \\ &= \{1, 1, 2, 2, 3, 3\} \\ &= \{2, 3, 3, 2, 1, 1, 1, 1, 2, 3, 2, 2, 2, 3, 1\}\end{aligned}$$

## Some important sets

The integers, the natural numbers, the nonnegative integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$$

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

$$\mathbb{N}^0 = \{0, 1, 2, 3, 4, \dots\}$$

We won't have much use for the real numbers,  $\mathbb{R}$ .

# The size of a finite set

$$3 = |\{a, b, c\}|$$

$$5 = |\{a, b, c, d, e\}|$$

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

$$0 = |\emptyset|$$

$$1 = |\{\emptyset\}|$$

$$1 = |\{\{\emptyset\}\}|$$

## Membership and subsets

$$3 \in \{1, 2, 3, 4, 5\}$$

$$3 \notin \{2, 4, 6, 8\}$$

$$\textit{cat} \in \{\textit{cat}, \textit{dog}, \textit{pig}\}$$

$$3 \in \mathbb{N}^0$$

$$\pi \notin \mathbb{Z}$$

$$\{2, 5, 8\} \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\{2, 5, 8\} \not\subseteq \{1, 2, 3, 4, 5, 6, 7\}$$

$$\{3\} \subseteq \{1, 2, 3, 4, 5\}$$

$$\{3\} \not\subseteq \{2, 4, 6, 8\}$$

$$\mathbb{N}^0 \subseteq \mathbb{Z}$$

$$\mathbb{R} \not\subseteq \mathbb{N}$$

## Set builder notation

$$\{n : n \text{ is odd and } 4 \leq n \leq 16\} = \{5, 7, 9, 11, 13, 15\}$$

$$\{2n + 5 : n \in \{3, 6, 7\}\} = \{11, 17, 19\}$$

$$\{2n : n \in \mathbb{N}^0\} = \{0, 2, 4, 6, 8, \dots\}$$

$$\{n \in \mathbb{N} : n < 5\} = \{1, 2, 3, 4\}$$

$$\{3n : n \in \mathbb{N} \text{ and } n < 5\} = \{3, 6, 9, 12\}$$

## Ordered pairs, triples, $n$ -tuples

$$(2, 4) \neq (4, 2)$$

$$(2, 2) \neq (2)$$

$$(1, 2, 3) \neq (3, 2, 1)$$

$$(1, 1, 2) \neq (1, 2)$$

$$(5, 3, 2, 1, 6) \neq (1, 2, 3, 5, 6)$$



## Cartesian product

$$A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$$

$$\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$

If  $A$  and  $B$  are finite sets, then  $|A \times B| = |A| \cdot |B|$ .

## Higher order Cartesian products

$$A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}$$

$$A^n = A \times A \times A \times \dots \times A$$

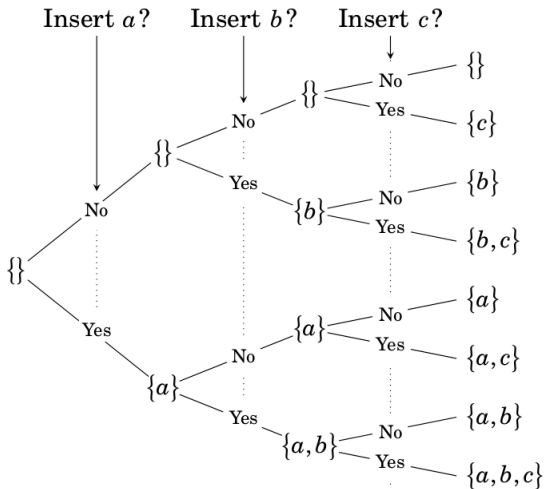
$$= \{(x_1, x_2, x_3, \dots, x_n) : x_1, x_2, x_3, \dots, x_n \in A\}$$

## Power set: the set of all subsets

$$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

How many subsets are there?

If  $|A| = n$  then  $|\mathcal{P}(A)| = 2^n$



## Union, Intersection, Difference

$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

$$A - B = \{x : x \in A \text{ and } x \notin B\}$$

$$A = \{1, 2, 3, 4, 5\}$$

$$B = \{4, 5, 6, 7, 8\}$$

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7, 8\}$$

$$A \cap B = \{4, 5\}$$

$$A - B = \{1, 2, 3\}$$

# Complement

$$\overline{A} = \{x : x \notin A\}$$

$$\overline{\{2, 4, 6, 8, \dots\}} = \{1, 3, 5, 7, \dots\}$$

Usually relative to some implied **universal set** or **universe**, in this case,  $\mathbb{N}$ .

# Indexed Sets

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n$$

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap A_3 \cap \dots \cap A_n$$

## Indexed Sets

$$A_i = \{ni : n \in \mathbb{N}\}$$

$$A_1 = \{1, 2, 3, 4, \dots\}$$

$$A_2 = \{2, 4, 6, 8, \dots\}$$

$$A_3 = \{3, 6, 9, 12, \dots\}$$

$$A_4 = \{4, 8, 12, 16, \dots\}$$

...

$$\bigcup_{i=2}^4 A_i = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, \dots\}$$

$$\bigcap_{i=2}^4 A_i = \{12, 24, 36, 48, 72, \dots\}$$



# The Division Algorithm

Given  $a, b \in \mathbb{Z}$  with  $b > 0$ , there exist  $q, r \in \mathbb{Z}$  with

$$a = qb + r$$

$$0 \leq r < b$$

# Logic

1. Circle  $X$  has radius equal to 3.
  2. If any circle has radius  $r$ , then its area is  $\pi r^2$ .
- 

3. Circle  $X$  has area  $9\pi$ .

# Statements

NOT Statements:	Statements
Add 5 to both sides.	Adding 5 to both sides of $x - 5 = 37$ gives $x = 42$ .
$\mathbb{Z}$	$42 \in \mathbb{Z}$
42	42 is not a number.
What is the solution of $2x = 84$ ?	The solution of $2x = 84$ is 42.

We use the letters  $P$ ,  $Q$ ,  $R$  and  $S$  to stand for statements.

## Examples

$P$  : The function  $f(x) = x^2$  is continuous.

$P(x)$  : If an integer  $x$  is a multiple of 6, then  $x$  is even.

$Q(x)$  : The integer  $x$  is even.

A sentence whose truth value depends on the value of variables is called an **open sentence**.

## And, Or, Not

- $P$  : The number 4 is even.  
 $Q$  : The number 7 is even.  
 $P \wedge Q$  : The number 4 is even **and** the number 7 is even.  
 $P \vee Q$  : The number 4 is even **or** the number 7 is even.  
 $\sim P$  : The number 4 is **not** even.  
 $\sim Q$  : The number 7 is **not** even.

# Truth Tables

$P$	$Q$	$P \wedge Q$
$T$	$T$	$T$
$T$	$F$	$F$
$F$	$T$	$F$
$F$	$F$	$F$

$P$	$Q$	$P \vee Q$
$T$	$T$	$T$
$T$	$F$	$T$
$F$	$T$	$T$
$F$	$F$	$F$

$P$	$\sim P$
$T$	$F$
$F$	$T$

$P$	$Q$	$P \oplus Q$
$T$	$T$	$F$
$T$	$F$	$T$
$F$	$T$	$T$
$F$	$F$	$F$

# Conditional Statements

$R(a)$  : **If** the integer  $a$  is multiple of 6, **then**  $a$  is divisible by 2.

$P(a)$  : The integer  $a$  is multiple of 6.

$Q(a)$  :  $a$  is divisible by 2.

$R(a)$  : If  $P$ , then  $Q$ .

$R(a)$  :  $P \Rightarrow Q$

$P$	$Q$	$P \Rightarrow Q$
$T$	$T$	$T$
$T$	$F$	$F$
$F$	$T$	$T$
$F$	$F$	$T$

# Indexed Sets

If  $P$  then  $Q$ .  
 $P$  only if  $Q$ .  
 $Q$ , if  $P$ .  
 $Q$  whenever  $P$ .  
 $Q$ , provided that  $P$ .  
Whenever  $P$ , then also  $Q$ .  
 $P$  is sufficient for  $Q$ .  
 $Q$  is necessary for  $P$ .

}  $P \Rightarrow Q$



## Biconditional or Equivalence Statements

$P$  if and only if  $Q$ .  
 $P$  iff  $Q$ .  
 $P$  is necessary and sufficient for  $Q$ .  
If  $P$ , then  $Q$ , and conversely.  
 $P$  is logically equivalent to  $Q$ .  
 $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

}  $P \iff Q$

$P$	$Q$	$P \iff Q$
$T$	$T$	$T$
$T$	$F$	$F$
$F$	$T$	$F$
$F$	$F$	$T$

## Truth Tables for Complex Statements

$P$	$Q$	$(P \vee Q)$	$(P \wedge Q)$	$\sim (P \wedge Q)$	$(P \vee Q) \vee \sim (P \wedge Q)$
$T$	$T$	$T$	$T$	$F$	$F$
$T$	$F$	$T$	$F$	$T$	$T$
$F$	$T$	$T$	$F$	$T$	$T$
$F$	$F$	$F$	$F$	$T$	$F$

# Quantifiers

## Universal quantifier

- For every  $n \in \mathbb{Z}$ ,  $2n$  is even.
- $\forall n \in \mathbb{Z}, 2n$  is even.
- $\forall n \in \mathbb{Z}, E(2n)$

## Existential quantifier

- There exists a subset  $X$  of  $\mathbb{N}$  for which  $|X| = 5$ .
- $\exists X, (X \subseteq \mathbb{N}) \wedge (|X| = 5)$
- $\exists X \subseteq \mathbb{N}, |X| = 5$
- $\exists X \in \mathcal{P}(\mathbb{N}), |X| = 5$

## Negating statements

$$\sim (P \Rightarrow Q) \iff P \wedge (\sim Q)$$

$$\sim (P \wedge Q) \iff (\sim P) \vee (\sim Q)$$

$$\sim (P \vee Q) \iff (\sim P) \wedge (\sim Q)$$

$$\sim (\forall x \in S, P(x)) \iff \exists x \in S, \sim P(x)$$

$$\sim (\exists x \in S, P(x)) \iff \forall x \in S, \sim P(x)$$

## Negating Statements, Example

$R$  : The square of every real number is non-negative.

$R$  :  $\forall x \in \mathbb{R}, x^2 \geq 0$

$\sim R$  :  $\sim (\forall x \in \mathbb{R}, x^2 \geq 0)$

$\sim R$  :  $\exists x \in \mathbb{R}, \sim (x^2 \geq 0)$

$\sim R$  :  $\exists x \in \mathbb{R}, x^2 < 0$

$\sim R$  : There exists a real number whose square is negative.

## Negating Statements, Example

$R$  :

For every real number  $x$  there is a real number  $y$  for which  $y^3 = x$ .

$$\begin{aligned} R &= \forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x \\ \sim R &= \sim (\forall x \in \mathbb{R}, \exists y \in \mathbb{R}, y^3 = x) \\ &= \exists x \in \mathbb{R}, \sim (\exists y \in \mathbb{R}, y^3 = x) \\ &= \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, \sim (y^3 = x) \\ &= \exists x \in \mathbb{R}, \forall y \in \mathbb{R}, y^3 \neq x \end{aligned}$$

$\sim R$  :

There is a real number  $x$  for which  $y^3 \neq x$  for all real numbers  $y$ .

# Tuples or Lists or Strings

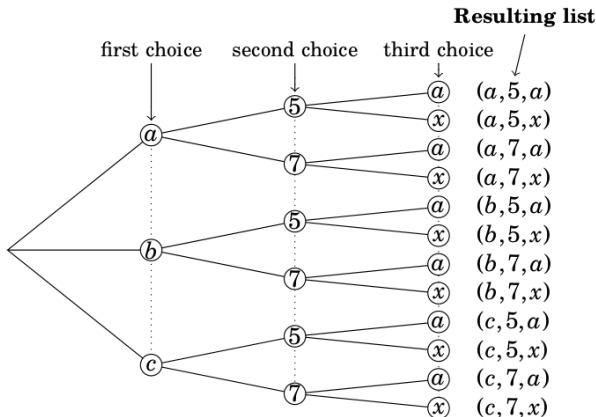
$$(a, b, c, d, e) \neq (b, a, c, d, e)$$

$$(a, b, c, d, e) \neq (a, a, b, c, d, e)$$

$$SOS = (S, O, S)$$

## Counting Tuples: Multiplication Principle

How many different lists of length 3 are there, where  
the first entry must be an element of  $\{a, b, c\}$ ,  
the second entry must be an element of  $\{5, 7\}$ ,  
and the third entry must be an element of  $\{a, x\}$ ?





## Some notation: falling factorial powers

$$7^5 = 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$$

$$7^{\underline{5}} = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$$

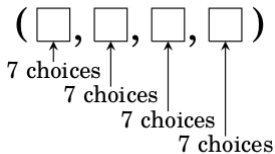
$$\begin{aligned} 7! &= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 7^{\underline{7}} \end{aligned}$$

## Lists with repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is allowed?

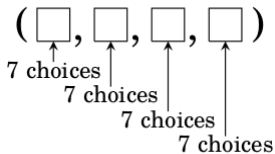
## Lists with repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is allowed?



## Lists with repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is allowed?



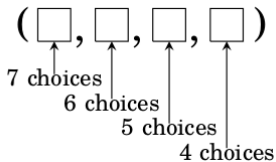
$$7 \cdot 7 \cdot 7 \cdot 7 = 7^4$$

## Lists without repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is not allowed?

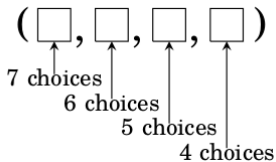
## Lists without repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is not allowed?



## Lists without repetitions

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , where repetition is not allowed?



$$7 \cdot 6 \cdot 5 \cdot 4 = 7^4$$

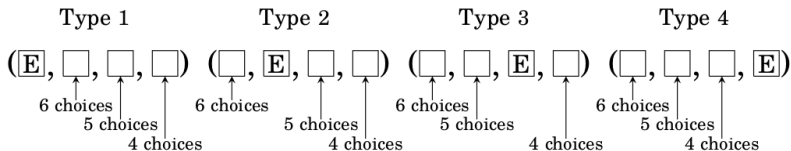
## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , without repetitions, and the symbol  $E$  must appear somewhere in the list?



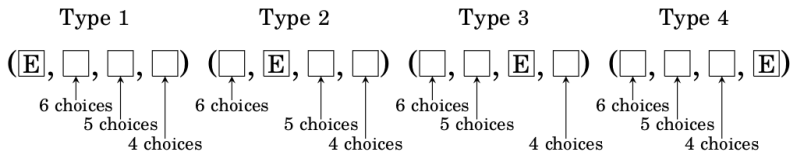
## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , without repetitions, and the symbol  $E$  must appear somewhere in the list?



## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , without repetitions, and the symbol  $E$  must appear somewhere in the list?



$$4 \cdot 6 \cdot 5 \cdot 4 = 4 \cdot 6^3$$

## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , repetition is allowed, and the list must contain an  $E$ ?

## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , repetition is allowed, and the list must contain an  $E$ ?

- There are  $7^4$  lists where repetition is allowed.

## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , repetition is allowed, and the list must contain an  $E$ ?

- There are  $7^4$  lists where repetition is allowed.
- There are  $6^4$  lists that do not contain  $E$ .

## More complex lists

How many lists of length 4 with selections from  $\{A, B, C, D, E, F, G\}$ , repetition is allowed, and the list must contain an  $E$ ?

- There are  $7^4$  lists where repetition is allowed.
- There are  $6^4$  lists that do not contain  $E$ .

$$7^4 - 6^4$$

## More about falling factorial powers

$$7^{\underline{3}} = 7 \cdot 6 \cdot 5$$

$$7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

$$7^{\underline{3}} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1}$$

$$= \frac{7!}{4!}$$

$$= \frac{7!}{(7-3)!}$$

$$n^{\underline{k}} = \frac{n!}{(n-k)!}$$

$$n! = n^{\underline{n}}$$

# Permutations

How many lists with repetitions of length  $k$  can be made from  $n$  symbols?  
*AAAA, BBBB, BABA, EBAB, CABC, ...*



# Permutations

How many lists with repetitions of length  $k$  can be made from  $n$  symbols?  
*AAAA, BBBB, BABA, EBAB, CABC, ...*

$$n^k$$

# Permutations

How many lists with repetitions of length  $k$  can be made from  $n$  symbols?  
*AAAA, BBBB, BABA, EBAB, CABC, ...*

$$n^k$$

How many lists without repetitions of length  $k$  can be made from  $n$  symbols?  
*ABCD, DCBA, BCDE, EBAC, CABE, ...*

# Permutations

How many lists with repetitions of length  $k$  can be made from  $n$  symbols?  
*AAAA, BBBB, BABA, EBAB, CABC, ...*

$$n^k$$

How many lists without repetitions of length  $k$  can be made from  $n$  symbols?  
*ABCD, DCBA, BCDE, EBAC, CABE, ...*

$$n^{\underline{k}}$$

# Permutations

How many lists with repetitions of length  $k$  can be made from  $n$  symbols?  
*AAAA, BBBB, BABA, EBAB, CABC, ...*

$$n^k$$

How many lists without repetitions of length  $k$  can be made from  $n$  symbols?  
*ABCD, DCBA, BCDE, EBAC, CABE, ...*

$$n^{\underline{k}}$$

$$\frac{n!}{(n-k)!}$$

# Counting subsets

How many subsets of size  $k$  can be made by selecting elements from a set of size  $n$ ?

# Counting subsets

How many subsets of size  $k$  can be made by selecting elements from a set of size  $n$ ?

The number of lists without repetitions?

# Counting subsets

How many subsets of size  $k$  can be made by selecting elements from a set of size  $n$ ?

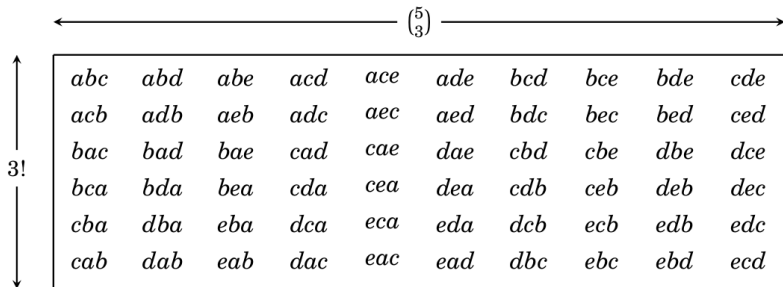
The number of lists without repetitions?

$$n^k$$

But these contain set-equivalent pairs, such as  $abc$  and  $cba$ .

# Eliminating the duplicates

$$\binom{5}{3} 3! = 5^3$$

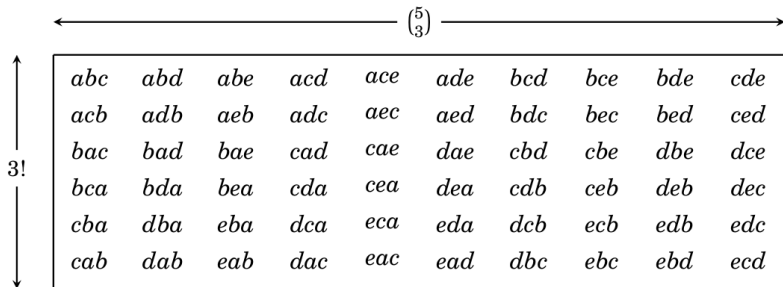


<i>abc</i>	<i>abd</i>	<i>abe</i>	<i>acd</i>	<i>ace</i>	<i>ade</i>	<i>bcd</i>	<i>bce</i>	<i>bde</i>	<i>cde</i>
<i>acb</i>	<i>adb</i>	<i>aeb</i>	<i>adc</i>	<i>aec</i>	<i>aed</i>	<i>bdc</i>	<i>bec</i>	<i>bed</i>	<i>ced</i>
<i>bac</i>	<i>bad</i>	<i>bae</i>	<i>cad</i>	<i>cae</i>	<i>dae</i>	<i>cbd</i>	<i>cbe</i>	<i>dbe</i>	<i>dce</i>
<i>bca</i>	<i>bda</i>	<i>bea</i>	<i>cda</i>	<i>cea</i>	<i>dea</i>	<i>cdb</i>	<i>ceb</i>	<i>deb</i>	<i>dec</i>
<i>cba</i>	<i>dba</i>	<i>eba</i>	<i>dca</i>	<i>eca</i>	<i>eda</i>	<i>dcb</i>	<i>ecb</i>	<i>edb</i>	<i>edc</i>
<i>cab</i>	<i>dab</i>	<i>eab</i>	<i>dac</i>	<i>eac</i>	<i>ead</i>	<i>dbc</i>	<i>ebc</i>	<i>ebd</i>	<i>ecd</i>



## Eliminating the duplicates

$$\binom{5}{3} 3! = 5^3$$



<i>abc</i>	<i>abd</i>	<i>abe</i>	<i>acd</i>	<i>ace</i>	<i>ade</i>	<i>bcd</i>	<i>bce</i>	<i>bde</i>	<i>cde</i>
<i>acb</i>	<i>adb</i>	<i>aeb</i>	<i>adc</i>	<i>aec</i>	<i>aed</i>	<i>bdc</i>	<i>bec</i>	<i>bed</i>	<i>ced</i>
<i>bac</i>	<i>bad</i>	<i>bae</i>	<i>cad</i>	<i>cae</i>	<i>dae</i>	<i>cbd</i>	<i>cbe</i>	<i>dbe</i>	<i>dce</i>
<i>bca</i>	<i>bda</i>	<i>bea</i>	<i>cda</i>	<i>cea</i>	<i>dea</i>	<i>cdb</i>	<i>ceb</i>	<i>deb</i>	<i>dec</i>
<i>cba</i>	<i>dba</i>	<i>eba</i>	<i>dca</i>	<i>eca</i>	<i>eda</i>	<i>dcb</i>	<i>ecb</i>	<i>edb</i>	<i>edc</i>
<i>cab</i>	<i>dab</i>	<i>eab</i>	<i>dac</i>	<i>eac</i>	<i>ead</i>	<i>dbc</i>	<i>ebc</i>	<i>ebd</i>	<i>ecd</i>

$$\binom{5}{3} = \frac{5!}{3!(5-3)!} = \frac{5^3}{3!} = \frac{5^3}{3^1}$$

# Counting subsets

How many subsets of size  $k$  can be made by selecting elements from a set of size  $n$ ?

# Counting subsets

How many subsets of size  $k$  can be made by selecting elements from a set of size  $n$ ?

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

Easy to prove theorem?

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

## Using set theory in counting

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

How many 3-card hands are there for which all 3 cards are red, or all three cards are face cards?

$A$  = 3-card hands, all red cards       $B$  = 3-card hands, all face cards

$$|A| = \binom{13}{3}$$

$$|B| = \binom{12}{3}$$

$$|A \cap B| = \binom{6}{3}$$

$$|A \cup B| = |A| + |B| - |A \cap B| = \binom{13}{3} + \binom{12}{3} - \binom{6}{3}$$