

# Proofs

Jason Soegondo

## Contents

<b>1</b>	<b>Fundamentals</b>	<b>2</b>
1.1	Sets . . . . .	2
1.1.1	Cartesian Product . . . . .	3
1.1.2	Subsets . . . . .	3
1.1.3	Power Sets . . . . .	3
1.1.4	Set Operations . . . . .	3
1.1.5	Complement . . . . .	4
1.1.6	Indexed Sets . . . . .	4
1.1.7	Zermelo-Fraenkel Axioms . . . . .	4
1.2	Logic . . . . .	4
1.2.1	Quantifiers . . . . .	5
1.2.2	English to Symbolic Logic . . . . .	5
1.2.3	Logical Inference . . . . .	5
1.2.4	Closing Notes . . . . .	5
<b>2</b>	<b>Counting</b>	<b>6</b>
2.1	Multiplication Principle . . . . .	6
2.2	Addition and Subtraction Principle . . . . .	6
2.3	Factorials . . . . .	7
2.3.1	Permutations . . . . .	8
2.4	Counting Sets . . . . .	8
2.5	Pascal's Triangle and the Binomial Theorem . . . . .	9
2.6	Inclusion-Exclusion Principle . . . . .	9
2.7	Counting Multisets . . . . .	10
2.8	Division and Pigeonhole Principles . . . . .	12
2.8.1	Pigeonhole Principle . . . . .	12
<b>3</b>	<b>Proofs</b>	<b>13</b>
3.1	Direct Proofs . . . . .	13
3.1.1	Steps to a Direct Proof . . . . .	13
3.1.2	Notes on Working Backwards . . . . .	13
3.1.3	Cases . . . . .	14
3.2	Contrapositive Proof . . . . .	14

3.3	Proof by Contradiction . . . . .	14
3.4	Non-Conditional Proofs . . . . .	15
3.4.1	If-and-only-if . . . . .	15
3.4.2	Equivalence Statements . . . . .	15
3.4.3	Existence . . . . .	15
3.4.4	Constructive and Non-Constructive Proofs . . . . .	15
3.5	Uniqueness Proofs . . . . .	15
3.6	Relations . . . . .	15

## 1 Fundamentals

### 1.1 Sets

Anything can be described as a set or a subset of a larger set. For example

- $0 = \{\emptyset\}$
- $1 = \{0\}$
- $2 = \{0, 1\}$
- $3 = \{0, 1, 2\}$
- $4 = \{0, 1, 2, 3\}$

and so on.

For negative numbers you can use any representation you want, its all just an abstraction at the end of the day.

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

Sets are commonly denoted with a capital character  
Some common sets are:

- Natural Numbers:  $A = \mathbb{N}$
- Integers:  $A = \mathbb{Z}$
- Rational Numbers:  $A = \mathbb{Q}$
- Real Numbers:  $A = \mathbb{R}$
- The empty set:  $\{\}$  or  $\emptyset$

Notation used to describe a value is in a set:  $n \in A$

If a set is finite, its *cardinality* or *size* is denoted as  $|A| = n$

*Set-builder notation* is used to describe sets that are too big to list in braces:

$E = \{2n : n \in A\}$ .

In general:  $X = \{A(x) : P\}$  in words, “for all  $A(x)$  such that  $P$  is true”

Intervals can be described with set-builder notation:

- Closed interval:  $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- Open interval:  $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- Infinite interval:  $(-\infty, b] = \{x \in \mathbb{R} : x \leq b\}$
- and the rest

### 1.1.1 Cartesian Product

An *ordered pair* is a list  $(x, y)$  of two things.

The *Cartesian product* of two sets  $A$  and  $B$  is another set denoted as  $A \times B$  which is defined as  $A \times B = \{(a, b) : a \in A, b \in B\}$

Example:  $A = \{k, l, m\}$  and  $B = \{q, r\}$

$A \times B = (k, q), (k, r), (l, q), (l, r), (m, q), (m, r)$

The set  $\mathbb{R} \times \mathbb{R}$  is the set of points of the Cartesian plane

The set  $\mathbb{R} \times \mathbb{N}$  would be a bunch of horizontal lines starting from  $y = 1$

And the set  $\mathbb{N} \times \mathbb{N}$  would just be a bunch of points in the first quadrant of a cartesian plane

Cartesian products can be done with more than two sets. The dimensionality of the ordered list would equal the amount of sets multiplied together.

The Cartesian power  $A^n$  is

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

### 1.1.2 Subsets

A set  $A$  is a subset of another set  $B$  if all elements in  $A$  are in  $B$ :  $A \subseteq B$  otherwise,  $A \not\subseteq B$ .

**Fact:**  $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

**Fact:** the empty set is a subset of all sets  $B$ :  $\emptyset \subseteq B$

For each element in a set, it can either be in the set or not. Therefore, the amount of subsets that a finite set that has  $n$  elements is  $2^n$

### 1.1.3 Power Sets

If  $A$  is a set, the *power set* is another set denoted as  $\mathcal{P}(A)$  and is the set of all subsets of  $A$ :  $\mathcal{P}(A) = \{X : X \subseteq A\}$

If  $A$  is a finite set then  $|\mathcal{P}(A)| = 2^{|A|}$  Where  $||$  denotes cardinality  $\mathcal{P}(\mathbb{R}^2)$  contains anything that can or will ever be displayed in a 2D plane.

#### 1.1.4 Set Operations

The *union* of two sets  $A$  and  $B$  is:  $A \cup B = \{x : x \in A \text{ or } x \in B\}$

The *intersection* of two sets  $A$  and  $B$  is:  $A \cap B = \{x : x \in A \text{ and } x \in B\}$

The *difference* of two sets  $A$  and  $B$  is:  $A - B = \{x : x \in A \text{ and } x \notin B\}$

In other words,  $A \cup B$  is the set of all elements in  $A$ , in  $B$ , or both.  $A \cap B$  is the set of all elements in both  $A$  and  $B$ .  $A - B$  is the set of all elements in  $A$  but not in  $B$

Notice that when  $A = \{(x, x^2) : x \in \mathbb{R}\}$  and  $B = \{(x, x + 2) : x \in \mathbb{R}\}$ ; in other words, when  $A$  and  $B$  are a set of function input and output pairs,  $A \cap B$  is a set containing the point(s) of intersection between the two functions.

Two sets,  $A$  and  $B$  are said to be disjoint sets if they share no elements in common.

#### 1.1.5 Complement

A *universal set* is a set that another set would naturally be the subset of. Sets like  $\mathbb{N}$ ,  $\mathbb{R}$ ,  $\mathbb{Q}$  and more are considered universal sets.

The *complement* of the set  $A$  whose universal set is  $U$  would be  $\bar{A} = U - A$

#### 1.1.6 Indexed Sets

$$\bigcap_{i=1}^n A_i = A_1 \cap A_2 \cap A_3 \cap A_4 \cdots \cap A_n = \{x : x \in A_i, \text{ for } 1 \leq i \leq n\}$$

where  $x$  is in every set  $A_i$

$$\bigcup_{i=1}^n A_i = A_1 \cup A_2 \cup A_3 \cup A_4 \cdots \cup A_n = \{x : x \in A_i, \text{ for } 1 \leq i \leq n\}$$

where  $x$  is in at least one set  $A_i$

Given  $A_i$  for  $i \in I$  where  $I$  is the set of possible subscripts, The set  $I$  is called the *index set*. We can rewrite the above using indexed notation:

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 \cap A_4 \cdots \cap A_n = \{x : x \in A_i \text{ for every set } A_i, \text{ for } 1 \leq i \leq n\}$$

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3 \cup A_4 \cdots \cup A_n = \{x : x \in A_i, \text{ for at least one set } A_i, \text{ for } 1 \leq i \leq n\}$$

### 1.1.7 Zermelo-Fraenkel Axioms

- *Well-ordered Principle*: a set is considered well-ordered if each non-empty subset has a smallest number
- *Axiom of Foundation*: For all non-empty sets  $X$ ,  $\exists x \in X$  such that  $X \cap x = \emptyset$ . Remember that elements are defined as sets eg:  $4 = \{0, 1, 2, 3\}$ . So, it follows that  $x$  must be the smallest element, because the proposition  $X \cap x = \emptyset$  only holds for the smallest element in  $X$ . This axiom also rules out circularly defined “sets” such as  $A = \{A\}$

## 1.2 Logic

Quick section for anything new. READ THE LOGIC NOTES for more details about propositional logic.

### 1.2.1 Quantifiers

$\forall$  represents phrase ‘for all’ or ‘for each’. called the *universal qualifier*

$\exists$  represents phrase ‘there exists’ or ‘there is a’. called the *existential qualifier*

### 1.2.2 English to Symbolic Logic

Given a set  $X$  and  $Q(X)$  a proposition about  $x$ . The following statements mean the same thing:

- $\forall x \in X, Q(x)$
- $(x \in X) \rightarrow Q(X)$

In english:

- for all  $x$  in  $X$ ,  $Q(x)$
- if  $x$  is in  $X$ , then  $Q(x)$

Oftentimes it is more practical to think of a universally quantified statement as a conditional.

### 1.2.3 Logical Inference

Assuming that the given proposition is actually true, we can make inferences given certain information:

- *Modus Ponens*:  $(P \rightarrow Q)$ , given  $P$ , we can infer  $Q$
- *Modus Tollens*:  $(P \rightarrow Q)$ , given  $\neg Q$ , we can infer  $\neg P$
- *Elimination*:  $(P \vee Q)$ , given  $\neg P$ , we can infer  $Q$

### 1.2.4 Closing Notes

Logic is important because:

- Truth tables tell us the exact meaning of words such as “and” and “or”. Logic also tells us exactly what constructs like “if...then” mean.
- Rules of inference provide a system in which we can produce new information (propositions) from known information.
- Logical rules like De Morgan’s laws help us to correctly change the forms of certain propositions to potentially make them more useful.

## 2 Counting

### 2.1 Multiplication Principle

A list  $(a, b, c)$  where  $a, b, c$  can have  $a_i, b_i, c_i$  different choices for each value respectively, can form multiple unique lists. The amount of unique lists that can be formed can be found using the *Multiplication Principle*.

#### Definition

Given a list of length  $n$ , there are  $a_1$  possible choices for the first entry,  $a_2$  possible choices for the second entry, and so on. The total number of different lists that can be made this way is the product  $a_1 * a_2 * a_3 \cdots a_n$

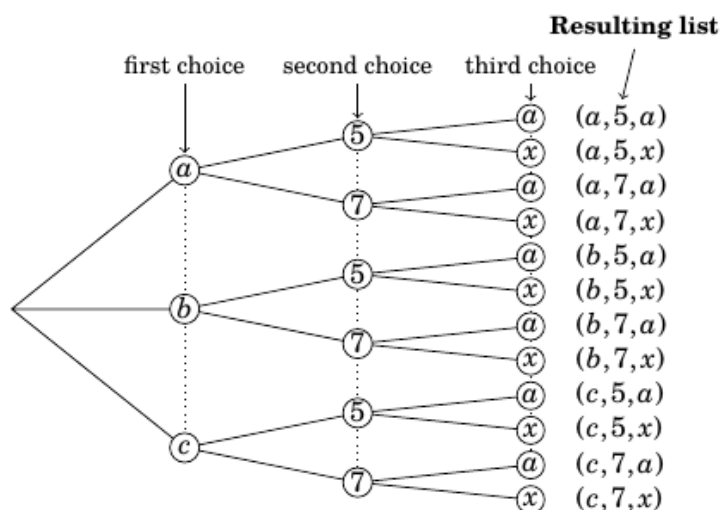


Figure 1: A tree showing how the multiplication principle works

## 2.2 Addition and Subtraction Principle

### Addition Principle

Given a finite set  $X$ ,  $X$  can be decomposed as a union

$X = X_1 \cup X_2 \cup X_3 \cdots \cup X_n$  whenever  $X_i \cap X_j = \emptyset$  whenever  $i \neq j$ .

In otherwords, each set does not share an element with any other set.

Then,  $|X| = |X_1| + |X_2| + |X_3| \dots + |X_n|$

### Example

Suppose you want to find how many strings of *length* 4 made up of the letters  $a, b, c, d, e, f, g$  contain the letter  $e$ . You would start by arranging it into 4 possibilites

$X_1$	e			
$X_2$		e		
$X_3$			e	
$X_4$				e

Using the multiplication principle we can find the amount of unique lists that could be made out of each possibility

$X_i$					$ X_i $
$X_1$	1	6	5	4	120
$X_2$	6	1	5	4	120
$X_3$	6	5	1	4	120
$X_4$	6	5	4	1	120

Finally, using the *addition principle* add up the cardinality of the 4 subsets to find the cardinality of the set  $X$  of unique 4 character strings that can be made using only the letters  $a, b, c, d, e, f, g$  and contain  $e$ .

### Subtraction Principle

Given  $X$  is a subset of a finite set  $U$ , remember that the complement of  $X$ , is  $\bar{X} = U - X$ . It follows that  $|\bar{X}| = |U| - |X|$ .

In otherwords, if  $X \subseteq U$ , then  $|U - X| = |U| - |X|$

### Example

Suppose you want to find how many strings of length 4 made up of the letters  $a, b, c, d, e, f, g$  contain the letter  $e$  with repitition allowed; that is, letters can be used multiple times)

Using the multiplication principle, we can find the set of unique 4 character strings that can be made using the letters  $a, b, c, d, e, f, g$ :  $7^4 = 2401$ .

7	7	7	7	2401
---	---	---	---	------

We can also find the set of unique 4 character strings that only do not contain  $e$ , but contain  $a, b, c, d, f, g$ :  $6^4 = 1296$

6	6	6	6	1269
---	---	---	---	------

Finally using the subtraction principle we can take the *difference* between the two sets,  $2401 - 1296 = 1105$ , which results in a set of unique 4 character strings that contain *e*.

## 2.3 Factorials

Given  $n$  is a non-negative integer,  $n!$  is the number of lists of length  $n$  that can be made from  $n$  symbols, without repetition.

0!	()	1
1!	a	1
2!	ab ba	2
3!	abc acb bac bca cab cba	6
$\vdots$	$\vdots$	$\vdots$

As seen above, factorials can be calculated using the multiplication principle.

### Proof

$0! = 1$  must be true because the generalized equation for a factorial is  $n! = n(n-1)!$ . If  $0! = 0$  then  $1! = 0$  which is obviously wrong, so  $0! = 1$  must be true.

### 2.3.1 Permutations

In general a set of  $n$  elements will have  $n!$  amount of permutations.

A *permutation* of  $X$  is a non-repetitive list made from all elements of  $X$ .

A *k-permutation* of  $X$  is a non-repetitive list made from  $k$  elements of  $X$ .

For example: the amount of non-repetitive lists made from two elements of a set  $\{a, b, c, d\}$  is 12 because using the multiplication principle, there are 4 choices for the first element and 3 choices for the second element:  $3 * 4 = 12$

*ab ac ad ba bc bd ca cb cd da db dc*

### Notation:

$P(n, k)$  represents the number of  $k$ -permutations of a set of size  $n$

For example:

$$P(4, 5) = 0$$

$P(2, 0) = 1$ , here the empty list  $()$  is the only possible permutation

### Definition:

$$P(n, k) = n(n-1)(n-2)\dots(n-k+1)$$

if  $0 \leq k \leq n$  then the above can be rewritten as:

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

## 2.4 Counting Sets

When permuting a *list*, changing the position of an element creates a new list eg: *ab* and *ba* are two different permutations. The same cannot be said



when permuting subsets where it would only results in a single subset  $\{a, b\}$   
 Take  $A = \{a, b, c, d, e\}$ ,  $P(5, 2) = 20$  possible lists.

$ab\ ac\ ad\ ae\ ba\ bc\ bd\ be\ ca\ cb\ cd\ ce\ da\ db\ dc\ de\ ea\ eb\ ec\ ed$

But  $A$  only has 10 subsets

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

### Definition

Given that  $n$  and  $k$  are integers,  $\binom{n}{k}$  denotes the number of subsets that can be made by choosing  $k$  elements of an  $n$ -element set.

Notice that  $\binom{n}{k} * k! = P(k)$

because each subset has  $k!$  possible permutations.

substitute:  $\binom{n}{k} * k! = \frac{n!}{(n-k)!}$

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

## 2.5 Pascal's Triangle and the Binomial Theorem

Notice the pattern:  $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$  given  $1 \leq k \leq n$

To understand this, think of  $\binom{n+1}{k}$  as the amount of  $k$ -subsets resulting from the set  $A = (0, 1, 2, 3 \dots n)$ .  $\binom{n}{k}$  is the amount of  $k$ -subsets resulting from the set  $(1, 2, 3 \dots n)$ ; in other words,  $\binom{n}{k}$  counts the subsets of  $A$  that **do not** contain 0.  $\binom{n}{k-1}$  is the amount of subsets of  $A$  that **do** contain 0 because if you were to start each subset with  $\{0\}$ , you can append an additional  $k-1$  elements to each subset.

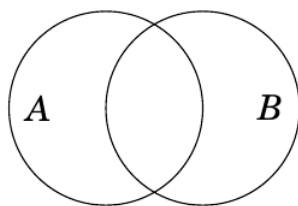
Pascal's triangle can be written with this pattern in mind.

$$\begin{array}{c} 1 \\ 1\ 1 \\ 1\ 2\ 1 \\ 1\ 3\ 3\ 1 \\ 1\ 4\ 6\ 4\ 1 \\ 1\ 5\ 10\ 10\ 5\ 1 \end{array}$$

$$\begin{array}{c} \binom{0}{0} \\ \binom{1}{0}\ \binom{1}{1} \\ \binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \end{array}$$

The binomial theorem can also be written with this pattern in mind.

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



## 2.6 Inclusion-Exclusion Principle

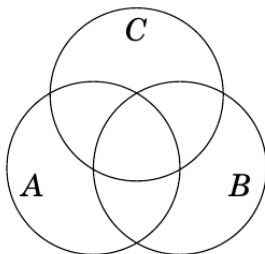
The cardinality  $|A \cup B|$  is relatively easy to find.  $|A| + |B|$  is close, but not quite because it does not exclude the elements in **both**  $A$  and  $B$ .

**Definition:**  $|A \cup B| = |A| + |B| - |A \cap B|$

### Example

A hand of 3-card hand is dealt from a standard deck of 52 cards. How many hands have all red or all face cards?

1. Let  $|A|$  = the amount of possible 3-card hands that contain all red cards
2. Let  $|B|$  = the amount of possible 3-card hands that contain all face cards
3.  $|A| = \binom{26}{3}$
4.  $|B| = \binom{12}{3}$
5. Since you can freely rearrange a hand, we will consider them as sets as opposed to lists.
6. The deck only has 6 red faced cards, so  $|A \cap B| = \binom{6}{3}$ .
7. Using the equation derived previously,  $|A \cup B| = \binom{26}{3} + \binom{12}{3} - \binom{6}{3}$



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

Looking at the venn diagram above, this equation can easily be derived.

## 2.7 Counting Multisets

Multisets are sets that contain duplicate elements. The **cardinality** of the set  $A$ ,  $|A|$  is the amount of elements in the set while the **multiplicity** of  $x \in A$  is the amount of times  $x$  appears in  $A$ .

Although there are no *subsets* of cardinality 5 in the set  $X = \{a, b, c, d, e\}$ , there are multiple multisets of cardinality 5 from  $X$

eg:  $\{a, a, a, a, a\}$   $\{a, a, b, c, d, e\}$   $\{b, b, b, b, b\}$  etc.

The amount of multisets that can be created from a list can be described using the following diagram. Take the case of  $X = \{a, b, c, d\}$ .

Multisets
$aa b c d$
$a bb c d$
$a bb cc d$
$aaa   dd$
$aaaaa   $

If the list keeps going we end up with  $\binom{8}{3} = \frac{8!}{3!(5)!} = 56$ .

Notice that all  $k$ -element multisets of  $X$  can be represented using  $k$  elements and  $n - 1$  bars separating each unique element.

\*\*\*\*|\*\*\*\*|\*\*\*\*...|\*\*\*\*

with  $k$  stars and  $n - 1$  bars separating the stars into  $n$  groups.

### Definition

In general, the  $k$ -multiset of a set with  $n$  elements is:

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

Rather than treating each element as a numerical value, think of  $k + n - 1$  as the possible positions that the bar(|) can be placed on the set,  $\{@@@@@@@@\}$  where each symbol represents a location on the multiset of size  $k$ .

### Definition

If a multiset with  $n$  values has  $p_1, p_2, p_3 \dots p_k$  multiplicities. The total number of permutations possible on the multiset is:

$$\frac{n!}{p_1! p_2! p_3! \dots p_k!}$$

For example, BANANA is a multiset where  $p_1 = 1$ ,  $p_2 = 3$ ,  $p_3 = 2$ . Using the equation above, the amount of permutations of BANANA is  $\frac{6!}{3!2!} = 60$ .

The idea behind the formula is to remove the amount of permutations where repeated characters are swapped with one another from the total number of permutations( $n!$ ). Given an element with a *multiplicity* of  $k$ , there are  $k!$  ways to permute said elements in their given positions eg: the A in BANANA has a multiplicity of 3 and therefore,  $3!$  in place permutations:

BA <sub>1</sub> NA <sub>2</sub> NA <sub>3</sub>
BA <sub>2</sub> NA <sub>1</sub> NA <sub>3</sub>
BA <sub>3</sub> NA <sub>2</sub> NA <sub>1</sub>
BA <sub>1</sub> NA <sub>3</sub> NA <sub>2</sub>
BA <sub>2</sub> NA <sub>3</sub> NA <sub>1</sub>
BA <sub>3</sub> NA <sub>1</sub> NA <sub>2</sub>

For N in BANANA it's 2!

BAN <sub>1</sub> AN <sub>2</sub> A
BAN <sub>2</sub> AN <sub>1</sub> A

Combining the two multiplicities,  $2!3! = 12$

BA <sub>1</sub> N <sub>1</sub> A <sub>2</sub> N <sub>2</sub> A <sub>3</sub>
BA <sub>2</sub> N <sub>1</sub> A <sub>1</sub> N <sub>2</sub> A <sub>3</sub>
BA <sub>3</sub> N <sub>1</sub> A <sub>2</sub> N <sub>2</sub> A <sub>1</sub>
BA <sub>1</sub> N <sub>1</sub> A <sub>3</sub> N <sub>2</sub> A <sub>2</sub>
BA <sub>2</sub> N <sub>1</sub> A <sub>3</sub> N <sub>2</sub> A <sub>1</sub>
BA <sub>3</sub> N <sub>1</sub> A <sub>1</sub> N <sub>2</sub> A <sub>2</sub>
BA <sub>1</sub> N <sub>2</sub> A <sub>2</sub> N <sub>1</sub> A <sub>3</sub>
BA <sub>2</sub> N <sub>2</sub> A <sub>1</sub> N <sub>1</sub> A <sub>3</sub>
BA <sub>3</sub> N <sub>2</sub> A <sub>2</sub> N <sub>1</sub> A <sub>1</sub>
BA <sub>1</sub> N <sub>2</sub> A <sub>3</sub> N <sub>1</sub> A <sub>2</sub>
BA <sub>2</sub> N <sub>2</sub> A <sub>3</sub> N <sub>1</sub> A <sub>1</sub>
BA <sub>3</sub> N <sub>2</sub> A <sub>1</sub> N <sub>1</sub> A <sub>2</sub>

This pattern holds true for all unique permutations of the multiset. In conclusion, permutations of BANANA can be placed into groups of 12 **repeated** permutations; that is,  $\frac{6!}{2!3!} = \frac{720}{12}$  gives us the amount of **unique** permutations. Or more generally  $\frac{n!}{p_1!p_2!\dots p_k!}$

## 2.8 Division and Pigeonhole Principles

Given a number  $x$ , its *floor*,  $\lfloor x \rfloor$  is the number rounded **down** to the nearest integer. The ceiling,  $\lceil x \rceil$  is the number rounded **up** to the nearest integer.

### 2.8.1 Pigeonhole Principle

There are  $n$  pigeons in  $k$  pigeonholes. Some of the  $k$  boxes may contain more than one pigeon, but the average number of pigeons per box must be  $\frac{n}{k}$ . Obviously one or more boxes contain at least  $\lceil \frac{n}{k} \rceil$  or more pigeons. Similarly, at least one or more boxes contain at least  $\lfloor \frac{n}{k} \rfloor$  or less pigeons.

#### Division Principle

Supposed  $n$  objects are placed in  $k$  boxes.

Then at least one box contains  $\lceil \frac{n}{k} \rceil$  or more objects

and at least one box contains  $\lfloor \frac{n}{k} \rfloor$  or fewer objects.

### Pigeonhole Principle

If  $n > k$  then at least one box contains more than one object  
(because  $\frac{n}{k} < 1$ )

If  $n < k$  then at least one box is empty  
(because  $\frac{n}{k} < 1$ )

### Example

Pick six numbers out of  $[0, 9]$ . Prove that in any combination of the six numbers, there will be two numbers that sum up to 9.

List all possible sum of two numbers (in the range) that add to 9:

$(0, 9), (1, 8), (2, 7), (5, 4), (6, 3)$

Notice that there are only 5 possible “boxes”. No matter what 6 numbers we choose,  $\frac{5}{6} < 1$ . Which means that at least one box will have more than 1 number. So we have proven the above conjecture.

## 3 Proofs

### 3.1 Direct Proofs

#### Example

Prove that  $2\sqrt{xy} \leq x + y$  given  $x, y \in \mathbb{N}$ .

**Proposition:**  $2\sqrt{xy} \leq x + y$

*Proof*

- Notice that  $0 \leq (x - y)^2$ , that is  $0 \leq x^2 - 2xy + y^2$  is true by a given axiom.
- Adding  $4xy$  to both sides, we get  $4xy \leq x^2 + 2xy + y^2$ , that is  $4xy \leq (x + y)^2$
- Square root both sides:  $2\sqrt{xy} \leq x + y$  ■

#### 3.1.1 Steps to a Direct Proof

1. Note the definitions of each part of the proposition eg: what set a variable is in, whether it's positive, negative, etc.
2. Remember certain axioms that may be useful for the proof eg: the definition of an even number is  $x = 2z$  for  $z \in \mathbb{Z}$ , etc.
3. Initially, it may be a good idea to write down the first and last lines of the proof first, so that you know the “start” and the “endgoal”.
4. If a proposition seems obviously true, it may be easier to prove the proposition by working backwards such as in the proof of  $2\sqrt{xy} \leq x + y$ .

You can start by squaring both sides resulting in  $4xy \leq x^2 + 2xy + y^2$ . Then, subtracting  $4xy$  from both sides we get  $0 \leq (x - y)^2$  which is true by another axiom.

### 3.1.2 Notes on Working Backwards

In short, a proof by working backwards starts by *assuming* that the proposition is true.

If that is the case, then there must be a process in which the proposition can be transformed into another proposition that we know to be true.

Reverse the process and you get the proof.

### 3.1.3 Cases

Sometimes a proof may have multiple cases such as the proof that the expression  $1 + (-1)^n(2n - 1)$  is a multiple of 4. Just looking at the expression you can kind of guess that the two cases are the scenarios where  $n$  is either even or odd.

**Proof** If  $k$  is a multiple of 4, then  $1 + (-1)^n(2n - 1) = k$

**case**  $n = 2n$  (even)

$$1 + (-1)^{(2n)}(2(2n) - 1) = k$$

$$\text{notice } -1^{2n} = 1$$

$$1 + (4n - 1) = k$$

$$4n = k$$

**case**  $n = 2n + 1$  (odd)

$$1 + (-1)^{(2n+1)}(2(2n + 1) - 1) = k$$

$$\text{notice } -1^{2n+1} = -1$$

$$1 - (4n + 1) = k$$

$$-4n = k$$

Sometimes cases are so similar that you can omit the second proof and say that “Without loss of generality...”

## 3.2 Contrapositive Proof

A contrapositive proof in short is that  $P \rightarrow Q$  is equivalent to  $\neg P \rightarrow \neg Q$ . Keep *De Morgan's Law* in mind when doing a contrapositive proof.  $\neg(P \wedge Q)$  is equivalent to  $\neg P \vee \neg Q$

Integers  $a$  and  $b$  are congruent modulo  $n$ ,  $a \equiv b(\text{mod } n)$ . If  $n|(a - b)$ . This is the same as saying that  $n|a$  and  $n|b$  have the same remainder.

### 3.3 Proof by Contradiction

We can prove an if-then statement by assuming the opposite of the proposition. If the assumption leads to a contradiction, then we know that the statement must be true.

Example:

$a \rightarrow b$

assume that  $\neg b$

but  $\neg b$  contradicts  $a$

therefore,  $b$ .

#### Definition

A real number,  $x$ , is rational if  $x = \frac{a}{b} \quad \forall a, b \in \mathbb{Z}$ . A real number,  $x$ , is irrational if  $x \neq \frac{a}{b} \quad \forall a, b \in \mathbb{Z}$ .

### 3.4 Non-Conditional Proofs

#### 3.4.1 If-and-only-if

To prove a biconditional, just prove the conditional, then prove the converse.

#### 3.4.2 Equivalence Statements

An equivalence statement asserts that the statements  $A, B, C, D \dots$  are all equivalent to each other. Which is to say, either they are all true, or they are all false. Therefore to prove equivalence, we create a loop of conditionals. that is,  $A \rightarrow B \rightarrow C \rightarrow D \rightarrow A$ , and we must prove that every conditional in this loop holds.

The conditionals do not need to be proven in a loop though. Biconditionals can be used instead. The only “requirement” is that at least one statement is proven by another statement.

#### 3.4.3 Existence

To prove existence, just provide an example to the existentially qualified statement

#### 3.4.4 Constructive and Non-Constructive Proofs

Existence proofs fall into two categories. Constructive proofs provide an example to the statement while a non-constructive proof proves that an example exists but does not give a specific one.

### 3.5 Uniqueness Proofs

Some propositions ask for existence as well as uniqueness. Proving existence is obvious enough, but to prove uniqueness, you need to show that assuming the existence of more than one value will lead to a contradiction.

### 3.6 Relations

All relations of the elements in the set  $A$  can be represented by a subset of  $A \times A$ . For example, consider the set  $\{1, 2, 3, 4, 5\}$ , the set  $\{(2, 1), (3, 1), (4, 1), (5, 1), (3, 2), (4, 2), (5, 2), (4, 3), (5, 3), (5, 4)\}$  is used to represent the relation  $>$  for the elements in the former set. Again, all relations can be represented as some subset of the cartesian product of the set which the elements lie.

$xRy$  is short for  $(x, y) \in R \subseteq A \times A$  where  $x, y \in A$ .

Additionally, if  $xRx$  then the relation is reflexive.

If  $xRy$  and  $yRz$  implies  $xRz$ , then the relation is transitive.

If  $xRy$  and  $yRx$ , then the relation is symmetric.

Equivalence relations are reflexive, transitive, and symmetric. Examples of equivalence statements include  $(=)$ , (x and y have the same parity), (x and y have the same sign).

A function is injective (one-to-one) if every distinct element in its domain is mapped to a distinct element in its codomain.

A function is surjective (onto) function is a function where the set of all possible outputs (range) of the function is equal to the codomain. Equivalently if  $f : X \rightarrow Y$ , then for all  $x \in X$  there is a corresponding  $y \in Y$ .

A function is bijective if it is both injective and surjective. That is,  $f : X \rightarrow Y$ . For every unique  $x \in X$ , there is a one-to-one mapping to a unique  $y \in Y$ .

Parameter	Position
h	Place the float <i>here</i> , i.e., <i>approximately</i> at the same point it occurs in the source text (however, not <i>exactly</i> at the spot)
t	Position at the <i>top</i> of the page.
b	Position at the <i>bottom</i> of the page.
p	Put on a special <i>page</i> for floats only.
!	Override internal parameters LaTeX uses for determining "good" float positions.
H	Places the float at precisely the location in the L <sup>A</sup> T <sub>E</sub> X code. Requires the float package, though may cause problems occasionally. This is somewhat equivalent to h!.

Figure 2: