

# Book of Proof Summary

Raphaël Hermans

February 2026

Contains examples, theorems, proofs, exercises and definitions from the book that I found important, not every detail

## 1 Fundamentals

### 1.1 Sets

- **Powerset:**  $\mathcal{P}(A)$  is the the powerset of  $A$ , i.e. the set of all subsets, sometimes denoted  $2^A$ , because for a set with cardinality  $n$ , there are  $2^n$  subsets.
- **Russel's paradox:** The set  $X = \{A \text{ is a set} \mid A \in A\}$  implies the logic inconsistency  $X \in X \iff X \notin X$ . Following the Zermelo–Fraenkel axioms avoids Russel's paradox
- **Set builder notation:**  $\{x \in A \mid P(x)\}$  is the set of all elements  $x$  in  $A$  such that  $P(x)$  is true
- **Universal set:**  $U$  is generally considered to be the universal set and is context dependent. E.g. for  $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ ,  $U = \mathbb{R}^2$
- **Complement:**  $\bar{A} = A^c$  is the complement of  $A$ ,  $U - A$

### 1.2 Logic

- $\neg(\forall x, P(x)) \iff \exists x, \neg P(x)$
- $\neg(\exists x, P(x)) \iff \forall x, \neg P(x)$
- $(P \implies Q) \iff (\neg P \vee Q)$
- Exercise in English (personal solution of 2.10 P12): "Whenever I have to choose between two evils, I choose the one I haven't tried yet." equates to "For all choices of two evils, if I have not tried an evil, I pick that evil.", which translates to

$$\forall(e_1, e_2) \in E, \forall e \in (e_1, e_2), \neg \text{tried}(e) \implies \text{pick}(e).$$

Negating this gives

$$\neg(\forall(e_1, e_2) \in E, \forall e \in (e_1, e_2), \neg \text{tried}(e) \implies \text{pick}(e))$$

$$\exists(e_1, e_2) \in E, \exists e \in (e_1, e_2), \neg(\text{tried}(e) \vee \text{pick}(e))$$

$$\exists(e_1, e_2) \in E, \exists e \in (e_1, e_2), \neg \text{tried}(e) \wedge \neg \text{pick}(e)$$

Translating this back into English gives: "There exists a choice of two evils, for which there is an evil which I haven't tried and didn't pick."

### 1.3 Counting

- **Lists**  $(a, b, c, \dots)$  are ordered and can contain duplicates. Sets  $\{a, b, c, \dots\}$  are unordered and do not contain duplicates
- $\binom{n}{k}$  is read as " $n$  choose  $k$ "
- **Multisets** are sets which can contain elements multiple times. They are denoted with  $\llbracket \rrbracket$  brackets
- The cardinality of a multiset  $A$  is the number of elements in  $A$  including repetitions
- The number of  $k$ -element multisets that can be made from an  $n$ -element set is  $\binom{k+n-1}{n-1} = \binom{k+n-1}{k}$

*Proof.* We can organize the elements of any multiset in alphabetical order, so that any multiset can be written as a sequence of  $k$  characters  $*$  and  $n - 1$  characters  $|$ . In such a representation, the character  $*$  denotes the appearance of an element from the set and  $|$  denotes a separator, i.e. a shift to the next element of the set. E.g. the multiset  $\llbracket a, a, b, c \rrbracket$  generated from  $\{a, b, c\}$  can be written as the sequence  $**|*|*$ . Thus, there are as many multisets as there are configurations of the characters. And since there are exactly  $k + n - 1$  spots to place the  $n - 1$  bars, the number of possible multisets is  $\binom{k+n-1}{n-1}$ .  $\square$

- **Division Principle:** Suppose you divide  $n$  objects into  $k$  boxes. At least one box must contain at least  $\lceil n/k \rceil$  and one box must contain at most  $\lfloor n/k \rfloor$  objects.

*Proof.* We will prove that the negation of the division principle is false, proving that the principle is, in fact, true. Assume  $B$  the set of boxes and  $|b|$  the number of elements in box  $b$ . Suppose now that the division principle does not hold. Then we know that

$$\neg((\exists b \in B, |b| \geq \lceil n/k \rceil) \wedge (\exists b \in B, |b| \leq \lfloor n/k \rfloor))$$

$$(\forall b \in B, |b| < \lceil n/k \rceil) \wedge (\forall b \in B, |b| > \lfloor n/k \rfloor)$$

$$\forall b \in B, \lfloor n/k \rfloor < |b| < \lceil n/k \rceil.$$

Now there are two possible cases:  $\lfloor n/k \rfloor = \lceil n/k \rceil$  and  $\lfloor n/k \rfloor = \lceil n/k \rceil - 1$ . Both cases immediately lead to an impossible solution, since there is no valid number of elements  $|b|$  to choose. Therefore, if the division principle does not hold, there is no way to distribute the elements in a valid way.  $\square$

- **Pigeonhole Principle:** *Suppose you divide  $n$  objects into  $k$  boxes. If  $n > k$ , then at least one box contains more than one object. If  $n < k$ , then at least one box is empty.*
- Example proof using the division principle (personal solution of 3.9 P10): Given a sphere  $S$ , a great circle of  $S$  is the intersection of  $S$  with a plane through its center. Every great circle divides  $S$  into two parts. A hemisphere is the union of the great circle and one of these two parts. Show that if five points are placed arbitrarily on  $S$ , then there is a hemisphere that contains four of them.

*Proof.* Consider the first two points. They define a unique great circle. The remaining three points are to be placed in either one of the two hemispheres. Now, according to the division principle, at least one hemisphere must contain at least  $\lceil 3/2 \rceil = 2$  points. Thus, there is a hemisphere containing at least the first two points and two of the remaining three points, i.e. four points in total.  $\square$

- **Combinatorial proof** is a method of proving two different expressions are equal by showing that they are both answers to the same counting question
- Example of combinatorial proof (personal solution of 3.10 P12): Show that  $\sum_{k=1}^n k \binom{n}{k} \binom{k}{m} = \binom{n}{m} 2^{n-m}$ .

*Proof.* Assume we have a set of  $n$  ordered elements. Then the right hand side of the equation counts the number of ways in which we can choose a subset  $A$  of size  $m$  and then choose whether or not to include the remaining  $n-m$  elements in a second set  $B$ . The left hand side of the equation counts the same thing in a different way. First, we choose the number of elements  $k$  to include in the total subset  $A \cup B$ . Now, for each possible  $k$ , there are  $\binom{n}{k}$  ways to choose the  $k$  elements from the original set. From these  $k$  elements, we need to choose  $m$  elements to be in the first subset  $A$ . The remaining elements will be part of the second subset  $B$ . There are  $\binom{k}{m}$  ways to make this choice, so that the total number of ways to choose such a subset is  $\sum_{k=1}^n k \binom{n}{k} \binom{k}{m}$ .  $\square$

## 2 How to Prove Conditional Statements

### 2.1 Direct Proof

- **Theorem:** A true, significant statement to be proved
- **Lemma:** An auxiliary theorem used to prove a larger theorem
- **Corollary:** A theorem that follows easily from another theorem
- **Proposition:** A true statement that is not as significant as a theorem

### 2.2 Contrapositive Proof

### 2.3 Proof by Contradiction

## 3 More on Proof

### 3.1 Proving Non-Conditional Statements

### 3.2 Proofs Involving Sets

### 3.3 Disproof

### 3.4 Mathematical Induction

## 4 Relations, Functions, and Cardinality

### 4.1 Relations

### 4.2 Functions

### 4.3 Proofs in Calculus

### 4.4 Cardinality of Sets