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 (3rd edition)

1 Fundamentals

1.1 Sets

- **Powerset:** $\mathcal{P}(A)$ is 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 $X = \{A \text{ is a set } | A \in A\}$ implies the logical inconsistency $X \in X \iff X \notin X$. Following the Zermelo–Fraenkel axioms avoids Russel's paradox
- **Set builder notation:** $\{x \in A | P(x)\}$ 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 $\{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$, $U = \mathbb{R}^2$
- **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 [] 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 $[a, a, b, c]$ 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 $\binom{k+n-1}{n-1}$. □

- **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

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

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

Now we have an expression of the form $P \vee Q$, which is false if both P and Q are false. The first proposition must be false, since $k\lceil n/k \rceil \leq n$, so if $|b| < \lceil n/k \rceil$ for all b, then the amount of objects in boxes is $k|b| < n$, i.e. not all the boxes are filled. A similar argument holds for the second proposition. □

- **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, the according to the division pricniple, 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. □

- **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 $\sum_{k=1}^{n} \binom{n}{k}\binom{k}{m} = \binom{n}{m}2^{n-m}$.

  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 to include the remaining $n-m$ elements in a second set B. The left-hand side of the equation counts the same thing differently. 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 $\sum_{k=1}^{n} \binom{n}{k}\binom{k}{m}$. □

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
- **Parity:** Two integers have the same parity if they are both even or both odd, otherwise they have opposite parity
- **Composite:** A positive integer that is not prime
- If a divides b we write $a|b$, i.e. $\exists c \in \mathbb{Z}, b = ac$
- The greates common divisor of a and b is denoted $\gcd(a, b)$, the least common multiple is denoted $\text{lcm}(a, b)$
- **Division Algorithm:** $\forall a, b \in \mathbb{Z}, b > 0, \exists! q, r \in \mathbb{Z}, 0 \leq r < b$ such that $a = bq + r$
- In direct proofs, it can be a good idea to work at the proof from both ends, from the assumptions down, and from the conclusion up, until both sides meet
- WLOG means "without loss of generality", and is generally used when a proof for one case can be easily adapted to the other cases
- Direct proof example (personal solution of 4 P28): Let $a, b, c \in \mathbb{Z}$. Suppose a and b are not both zero, and $c \neq 0$. Prove that $c \cdot \gcd(a, b) \leq \gcd(ca, cb)$.

  Proof. Let d be the greatest common divisor of a and b, so that $d_1 = \gcd(a, b)$. Then there exist integers x_1 and y_1 such that $d_1 x_1 = a$ and $d_1 y_1 = b$. Now, consider $d_2 = \gcd(ca, cb)$. There exist integers x_2 and y_2 such that $d_2 x_2 = ca$ and $d_2 y_2 = cb$. Substituting a and b in these equations gives $ca = cd_1 x_1$ and $cb = cd_1 y_1$. Thus, cd_1 divides both ca and cb. And since d_2 is the greatest common divisor of ca and cb, we have that $cd_1 \leq d_2$, or $c \cdot \gcd(a, b) \leq \gcd(ca, cb)$. □

2.2 Contrapositive Proof

- **Contrapositive:** The contrapositive of the statement $P \implies Q$ is the logically equivalent statement $\neg Q \implies \neg P$
- It is said that a and b are "congruent modulo n" if $n|(a - b)$, otherwise stated as $a \equiv b \mod n$
- General guidelines for good proofs:

- Begin each sentence with a word, not a symbol, otherwise it might create ambiguity
- End each sentence with a period, even when the sentence ends in a mathematical expression.
- Always separate mathematical expressions with text to avoid ambiguity
- Use the first-person plural ("we") to make the reader feel included
- Each new symbol must be explained when it is first introduced
- Watch out for the words "it" and "this" as they can be ambiguous
- It is helpful to tip the reader off as to what type of proof you are using: direct, contrapositive, contradiction, induction, etc.

- Example of contrapositive proof (personal solution of 5 P32): If $a \equiv b \mod n$, then a and b have the same remainder when divided by n.

  Proof. Assume a and b have a different remainder when divided by n, such that

  $$a = nq_1 + r_1$$
  $$b = nq_2 + r_2$$

  with $0 \leq r_1, r_2 < n$ and $r_1 \neq r_2$. Now, we can write that $a - b = n(q_1 - q_2) + (r_1 - r_2)$. Since $r_1 \neq r_2$, we know that $a - b$ does not divide n, so that $a \not\equiv b \mod n$. Thus, by contrapositive, if $a \equiv b \mod n$, then a and b have the same remainder when divided by n. □

2.3 Proof by Contradiction

- In proof by contradiction, we assume $\neg P$ and logically derive a contradiction $C \wedge \neg C$ to conclude P. This is a vald proof, since $\neg P \implies C \wedge \neg C$ is logically equivalent to P.

  Proof.

  $$\begin{aligned} \neg P &\implies C \wedge \neg C \\ &\iff P \vee (C \wedge \neg C) \\ &\iff P \vee F \\ &\iff P \end{aligned}$$

  □

- Example of proof by contradiction (personal solution of 6 P24): The number $\log_2 3$ is irrational.

Proof. Assume $\log_2 3$ is rational, so that $\log_2 3 = \frac{a}{b}$ with a and b positive integers. Thus, $2^{\frac{a}{b}} = 3$, so that $2^a = 3^b$. This is a contradiction since 2^a is even and 3^b is odd. The proposition that 2^a is even can easily be proven through mathematical induction. The same goes for the second proposition, that 3^b is odd. We will analyze only the second proposition. The base case is trivial: 3^1 is an odd number. Now assume 3^{b-1} is odd, then $3^{b-1} = 2k + 1$ with $k \in \mathbb{Z}$, so that $3^b = 3 \cdot (2k + 1) = 6k + 3 = 2 \cdot (3k + 1) + 1 = 2n + 1$ with $n \in \mathbb{Z}$. □

3 More on Proof

3.1 Proving Non-Conditional Statements

- In case of a biconditional theorem ($P \iff Q$), we need to prove both $P \implies Q$ and $Q \implies P$. If we envision the implications as edges of a graph and the propositions as vertices, we are trying to make the graph fully connected.
- In case of multiple equivalent statements, $P \iff Q \iff R \iff \ldots$ we don't have to prove every possible conditional statement. Instead, we can prove the easiest conditional statements that make the graph fully connected.

  Proof. A fully connected graph of implications implies that if any of the propositions are true, all of them must be true. This can be proven by Following the chain of implications through the graph. If it is truly fully connected, then the chain will reach every proposition, necessarily making all of them true.Likewise if one of them is false, they must all be false. □

- In case of multiple equivalent statements, a circular pattern yields the fewest conditional statements that must be proved
- There are two types of existsence proofs: contstructive and non-contstructive proofs. Constructive proofs display an explicit example that proves the theorem, while non-constructive proofs prove an example exists without actually giving one.

3.2 Proofs Involving Sets

- Proving $A \subseteq B$ is done by proving $a \in A \implies a \in B$
- Proving $A = B$ is done by proving $A \subseteq B \wedge B \subseteq A$
- There is an equivalence relationship between sets and propositional logic where sets correspond to propositions $P(x)$, operator $\cup$ corresponds to $\vee$, operator $\cap$ to $\wedge$, and $^-$ to $\neg$.

- Equivalences that work for propositional logic also works for sets. E.g. DeMorgan's law, $\overline{A \cap B} = \overline{A} \cup \overline{B}$ and $\overline{A \cup B} = \overline{A} \cap \overline{B}$. This also works for distributive laws, associate laws, etc.
- **Perfect number:** A number $p \in \mathbb{N}$ is perfect when it equals the sum of its positive divisors less than itself. E.g. $6 = 1 + 2 + 3$.
- Example of a proof involving sets (personal solution of 8 P31). Suppose $B \neq \emptyset$ and $A \times B \subseteq C \times C$. Prove that $A \subseteq C$.

  Proof. Since the order of the Cartesian products matters, we know that if $A \times B \subseteq B \times C$, it must also be true that $A \subseteq B$ and $B \subseteq C$ (this can easily be proven through proof by contradiction). Thus, due to the transitive property of sets, $A \subseteq C$ is also true. □

3.3 Disproof

- **Conjecture:** A statement which we don't know to be true or false
- Disproving a statement P boils down to proving $\neg P$. For that we can just use the aforementioned techniques.
- Example of disproof (personal solution to 9 P34). If $X \subseteq A \cup B$, then $X \subseteq A$ or $X \subseteq B$.

  Proof. We will disprove this proposition through a counterexample. Suppose $A = \{a, c\}$ and $B = \{b, c\}$, then $A \cup B = \{a, b, c\}$. Now suppose that $X = \{a, b, c\}$. Then $X \subseteq A \cup B$, but not $X \subseteq A$ or $X \subseteq B$. □

3.4 Mathematical Induction

- Strong induction assumes $S_1, S_2, \ldots, S_k$ to prove S_{k+1}, while weak induction only assumes S_k
- **Proof by Smallest Counterexample:** A hybrid of mathematical induction and proof by contradiction. It has four steps
  1. Check that S_1 holds
  2. Suppose that not every S_n holds
  3. Let S_k be the first false statement
  4. Use the fact that S_{k-1} is true and S_k false to get a contradiction
- **Fundamental Theorem of Arithmetic:** *Any integer k greater than 1 has a unique prime factorization $k = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ with $p_1, p_2, \ldots, p_n$ primes*

4 Relations, Functions, and Cardinality

4.1 Relations

- Any subset R of a set $A \times A$ can be considered a relation
- We often abbreviate $(x, y) \in R$ as xRy
- A relation is **reflexive** if $\forall x \in A, xRx$
- A relation is **symmetric** if $\forall x, y \in A, xRy \implies yRx$
- A relation is **transitive** if $\forall x, y, z \in A((xRy) \wedge (yRz)) \implies xRz$
- **Equivalence relation:** A relation that is reflexive, symmetric and transitive
- **Equivalence class:** A subset of A containing only element that are equal under a certain equivalence relation, usually denoted with a representative element a. Equivalence classes are usually written as $[a] = \{x \in A : xRa\}$
- Equivalence relations arise in many fields of mathematics. They are often hidden under the surface. E.g. the set of antiderivatives $F(x) + c$ are considered equal
- Partitions and equivalence relations have a one-to-one correspondence.
- Relations can also arise from two different sets, so that $R \subseteq A \times B$
- Proving anything related to relations boils down to applying the definitions of reflexive, symmetric and transitive relations along with the aforementioned methods of proof

4.2 Functions

- A function f from A to B (denoted $f : A \to B$) is a relation $f \subseteq A \times B$ that contains exactly one pair of the form (a, b) for every a in A (denoted $f(a) = b$).
- A function $f : A \to B$ contains a pair (a, b) for every value a in its domain A, although it must not have a pair for every value b in its codomain B
- The range is the subset $\{f(a) : a \in A\}$ of the codomain B
- Since a function is really just a relation and a relation is really just a set, a function is also just a set, in theory
- We consider functions to be equal ($f = g$) when their set representations are equal, i.e. when $f(x) = g(x)$ for every $x \in A$
- **Injection:** $\forall a, a' \in A, a \neq a' \implies f(a) \neq f(a')$ (one-to-one)
- **Surjection:** $\forall b \in B, \exists a \in A, f(a) = b$ (onto)
- **Bijection:** injection and surjection

- Proving anything about function, like proving anything about relations boils down to applying the definitions of injections, surjections, bijections and the aforementioned methods of proof
- **Pigeonhole Principle:** (applied to functions) For a function $f : A \to B$:
  1. If $|A| > |B|$, then f is not injective
  2. If $|A| < |B|$, then f is not surjective
- The inverse relation R^{-1} is defined as $\{(y, x) : (x, y) \in R\}$
- The inverse function can only be defined when f is bijective, in which case f^{-1} is defined such that $f \circ f^{-1} = i_B$ and $f^{-1} \circ f = i_A$
- **Image:** $f(X) = \{f(x) : x \in X\}$
- **Preimage:** $f^{-1}(X) = \{f^{-1}(x) : x \in X\}$
- Example proof using functions (personal solution 12 P14): Let $f : A \to B$ be a function, and $Y \subseteq B$. Prove or disprove: $f^{-1}(f(f^{-1}(Y))) = f^{-1}(Y)$.

  Proof. This statement is obviously true, but to prove it, we need to revisit definitions. $f^{-1}(f(f^{-1}(Y)))$ is defined as $\{f^{-1}(x) : x \in C\}$ with $C = f(f^{-1}(Y))$, so if we can prove that $C = Y$, then we are done. C is defined as

$$\begin{aligned} C &= \{f(x) : x \in f^{-1}(Y)\} \\ &= \{f(x) : x \in \{f^{-1}(x') : x' \in Y\}\} \\ &= \{f(f^{-1}(x')) : x' \in Y\} \\ &= \{i_B(x') : x' \in Y\} \\ &= Y \end{aligned}$$

  □

4.3 Proofs in Calculus

- **Limit:** $\lim_{x \to c} f(x) = L$ if $\forall \epsilon > 0, \exists \delta > 0, (0 < |x - c| < \delta) \implies (|f(x) - L| < \epsilon)$
- The rest of this chapter mostly recaps high-school level calculus, not interesting

4.4 Cardinality of Sets

- Two sets are said to have the same cardinality, written $|A| = |B|$, if there exists a bijection $f : A \to B$
- Any set with equal cardinality to $|\mathbb{N}|$ is considered countably infinite. E.g. $|\mathbb{N}| = |\mathbb{Z}|$.

Proof. Consider the bijection $f : \mathbb{N} \to \mathbb{Z}$ where $f(n) = n/2$ if n even and $f(n) = -\frac{n-1}{2}$ if n uneven $f : \{1, 2, 3, 4, 5, \dots\} \mapsto \{0, 1, -1, 2, -2, \dots\}$. To prove this is a bijection, we must prove it is both an injection and a surjection. Firstly, it is a surjection, since $\forall z \in \mathbb{Z}, \exists n \in \mathbb{N}, f(n) = z$, namely $n = 2z$ if $z > 0$ and $n = -2z + 1$ if $z \leq 0$. Secondly, it is an injection, since $n \neq n' \implies f(n) \neq f(n')$. □

- It was George Cantor who first recognized that $|\mathbb{N}| \neq |\mathbb{R}|$ by proving that there are no surjective functions $f : \mathbb{N} \to \mathbb{R}$ (diagonal in the table argument). It is said that $\mathbb{R}$ is uncountably infinite
- Intervals in $\mathbb{R}$ are generally all uncountably infinite, since there are an infinite number of bijective function that can take you from any continuous interval to any other continuous interval in $\mathbb{R}$
- A set is considered countable if it is finite
- We use the first Hebrew letter "alpeh" to denote cardinalities. We write $\aleph_0 = |\mathbb{N}|$ and $\aleph_1 = |\mathbb{R}|$
- A set A is countably infinite if we can arrange its elements in an infinite list $a_1, a_2, a_3, ...$, since $f : \mathbb{N} \to A : f(n) \mapsto a_n$ is a bijection
- The set of rational numbers $\mathbb{Q}$ is countably infinite

  Proof. Every element in $\mathbb{Q}$ can be denoted as $\frac{a}{b}$ with a and b integers with $b > 0$. If we place the values for a in the columns of a table and the values b in the rows of a table, we can construct an infinite list that covers the whole table by drawing a line through the diagonals of the table. □

- The Cartesian product of two countably infinite sets is also countably infinite. The proof is analogous to that of $|\mathbb{Q}| = \aleph_0$. Therefor A^n must also be countably infinite if A is countably infinite
- We say that $|A| < |B|$ when there is an injective function $f : A \to B$, but no bijective function
- We can prove that $\aleph_0 < \aleph_1$ with a similar argument as the one that is used to prove that $|\mathbb{R}| \neq |\mathbb{N}|$ (digits on the diagonal argument)
- If A is any set, then $|A| < |\mathcal{P}(A)|$

  Proof. To prove this theorem, we must prove that there is an injection $f : A \to \mathcal{P}(A)$, but no bijection. Proving there is an injection is easy, take $f(x) = \{x\}$ for example. Proving there is no bijection can be done by proving there is no surjection. Suppose

$$B = \{x \in A : x \notin f(x)\} \subseteq A.$$

This set has the property $B \in \mathcal{P}(A)$, but also $f(a) \neq B$ for all $a \in A$. Since this set exists for any function f, no f can be surjective. To prove that $f(a) \neq B$ for all $a \in A$, consider the following cases.
Case 1: If $a \notin f(a)$ then $a \in B$. Consequently, $f(a) = B$ is impossible, since it would imply that $a \in B$.
Case 2: If $a \in f(a)$ then $a \notin B$. Consequently, $f(a) = B$ is impossibly, since it would imply that $a \notin B$.
Simply put, no element a can be mapped onto B, because if it were, then B could not contain a, but if it does not contain a it must contain a, leading to a contradiction. □

- **Cantor-Bernstein-Schröder theorem:** To prove that $|A| = |B|$ it suffices to prove that there exists and injection from A to B and from B to A
- The Cantor-Bernstein-Schröder theorem can be used to prove that $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$
- **Continuum hypothesis:** There exists no set with cardinality between that of $\mathbb{N}$ and that of its powerset
- It has been proven that the continuum hypothesis cannot be proven true or false. Therefor, accepting it as true leads to one version of set theory, while accepting it as false leads to another, both different, but valid versions