Book of Proof Summary

Raphaël Hermans

February 2026

Contains important examples, theorems, proofs and definitions from the book, not every detail

1 Sets

- $\mathcal{P}(A)$ is the powerset of A
- Russel's paradox: $X = \{A \text{ is a set} \mid A \in A\}$. Now $X \in X \iff X \notin X$
- Following the Zermelo–Fraenkel axioms avoids Russel's paradox
- U is the universal set and is context dependent
- $\bar{A} = A^c$ is the complement of A, $U - A$

2 Logic

- $\neg(\forall x, P(x)) \iff \exists x, \neg P(x)$
- $\neg(\exists x, P(x)) \iff \forall x, \neg P(x)$
- $(P \implies Q) \iff (\neg P \lor Q)$
- Exercise in English: "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

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

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

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

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."

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

- **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. $\square$