CS 4TH3: Computability Theory

Term 1, 2019/20
Instructor: J. Zucker
TA: M. Armstrong

1. Introduction; Mathematical Preliminaries

Computability theory (or ***recursive function theory***) originated in the 1930's in the research of ***Church***, ***Gödel***, ***Turing***, ***Kleene*** and others, who formalised the notion of computable (or "recursive") function in different ways, e.g., by Turing machines, lambda-calculus, definability by μ-recursive schemes, and definability by sets of equations. Corresponding to each of these formalisms is a ***Church-Turing Thesis*** which identifies computability by that formalism with intuitive algorithmic computability.

We use ***computability by a simple imperative programming language*** as our basic notion. Also, we take computability of ***partial functions*** ("partial recursiveness") as basic.

References

These notes are based closely on [PZ93], which in turn was directly inspired by [DW83]. We have also benefitted from the classic references [Kle52] and [Rog67]. [DDS78] give a useful set-theoretic background. The collection [Dav65] contains interesting articles by the pioneers in the field: Church, Gödel, Turing and others. [Dav00] is a very readable history of the subject.

[PZ93] L. Pretorius and J.I. Zucker. "Introduction to Computability Theory". *South African Computer Journal*, 9, pages 3–30.

[DW83] M. Davis and E. Weyuker. *Computability, Complexity and Languages.* Academic Press, 1983.

[Kle52] S. C. Kleene. *Introduction to Metamathematics.* North-Holland, 1952.

[Rog67] H. Rogers, Jr. *Theory of Recursive functions and Effective Computability.* McGraw-Hill, 1967. (Chapters 1, 2, 5).

[DDS78] D. van Dalen, H. C. Doets and H. de Swart. *Sets: Naive, Axiomatic and Applied.* Pergamon Press, Oxford, 1978.

[Dav65] M. Davis (ed.) *The Undecidable.* Raven Press, 1965.

[Dav00] M. Davis. *The Universal Computer*. Norton, 2000

Mathematical Preliminaries

We review some basic concepts.

Sets and n-tuples

- $A \subseteq B$ means: A is a subset of B, i.e., $\forall x(x \in A \Rightarrow x \in B)$.
- $A \subset B$ means: A is a *proper* subset of B, i.e., $A \subseteq B$ but $A \neq B$.
- $a \in A$ means: a is an element of the set A.
- The order of writing, or repetition of, elements of a set $\{a_1, a_2, \ldots, a_n\}$ is irrelevant.
- The order in an *n-tuple* $\vec{a} = (a_1, a_2, \ldots, a_n)$ is important:
  $(a_1, \ldots, a_m) = (b_1, \ldots, b_n) \iff m = n \ \wedge \ a_1 = b_1 \ \wedge \ \ldots \ \wedge \ a_n = b_n.$
- $A_1 \times \cdots \times A_n \ = \ \{(a_1, \ldots, a_n) \mid a_1 \in A_1, \ \ldots \ , a_n \in A_n\}$
  $A^n \ = \ \underbrace{A \times \cdots \times A}_{n \text{ times}}.$

Natural numbers

- $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of *natural numbers*.

By "*number*" we will mean natural number.

$\mathbb{N}$ will be our *basic domain of computation*.

Relations

- An n-ary relation on a set A is a subset of A^n, for $n = 1, 2, 3, \ldots$
- When $n = 2$, this is a *binary relation* on A — often use *infix*.
  E.g., write '$x < y$' for '$<(x, y)$'.
- If B and C are two n-ary relations on A, define:

$$\begin{aligned} B \cup C &= \{\, \vec{x} \in A^n \mid \vec{x} \in B \text{ or } \vec{x} \in C \,\}, \\ B \cap C &= \{\, \vec{x} \in A^n \mid \vec{x} \in B \text{ and } \vec{x} \in C \,\}, \\ B \backslash C &= \{\, \vec{x} \in A^n \mid \vec{x} \in B \text{ and } \vec{x} \notin C \,\}, \\ B^{\mathsf{C}} &= A^n \backslash B. \end{aligned}$$

- By "relation" we will usually mean: *relation on* $\mathbb{N}$.

Functions

A *(partial) function* $f : A \rightharpoonup B$ is a subset of $A \times B$ such that for all $a \in A$ there is *at most one* $b \in B$ (denoted $f(a)$) such that $(a, b) \in f$.

The *domain* and *range* of f are defined by

$$\begin{aligned} \boldsymbol{dom}(f) &= \{\, x \in A \mid \exists y \in B : (x, y) \in f \,\} \\ \text{and} \quad \boldsymbol{ran}(f) &= \{\, y \in B \mid \exists x \in A : (x, y) \in f \,\}, \end{aligned}$$

Notation.

- $f(x)\uparrow$ ("diverges") if $x \notin \boldsymbol{dom}(f)$,
- $f(x)\downarrow$ ("converges") if $x \in \boldsymbol{dom}(f)$, and
- $f(x)\downarrow y$ ("converges to y") if $x \in \boldsymbol{dom}(f)$ *and* $(x, y) \in f$.

  Also write: $f(x) = y$.

- If $A = A_1 \times \cdots \times A_n$, we write $f(x_1, \ldots, x_n)$ and say f is a *function* of n *arguments*, or an n*-ary* function, or a function of *arity* n.
  (We call f ***unary*** if $n = 1$ and ***binary*** if $n = 2$.)

- A function $f : A \rightharpoonup B$ is ***total*** if $\boldsymbol{dom}(f) = A$ (written $f : A \to B$).

Definitions. A total function $f : A \to B$ is called

- ***injective*** or ***1-1***, or an ***embedding*** of A into B, written $f \colon A \hookrightarrow B$, if $\forall x, y \in \boldsymbol{dom}(f)\, (f(x) = f(y) \Rightarrow x = y)$;
- ***surjective*** or ***onto*** B, written $f \colon A \twoheadrightarrow B$, if $\boldsymbol{ran}(f) = B$, i.e., $\forall y \in B\, \exists x \in A\, (f(x) = y)$;
- ***bijective*** or a ***bijection*** between A and B, or a ***1-1 correspondence*** between A and B, written $f \colon A \approx B$, if it is ***both 1-1 and onto*** B

Notation.

- $A \hookrightarrow B$ means $\exists f[f \colon A \hookrightarrow B]$.
- $A \twoheadrightarrow B$ means $\exists f[f \colon A \twoheadrightarrow B]$.
- $A \approx B$ means $\exists f[f \colon A \approx B]$.
  In this case we also say: A and B are ***equinumerous***.

Note. For our purposes,

partial functions are the more basic concept,

and totality of functions should *not* be assumed unless explicitly stated.

In fact we will be concerned mainly with n-ary partial functions on $\mathbb{N}$, i.e. functions $f : \mathbb{N}^n \rightharpoonup \mathbb{N}$, for some $n > 0$. So by "function" we will generally mean *partial function on* $\mathbb{N}$, denoted by f, g, $h, \ldots$

- We will use ***lambda-notation*** informally.
  E.g., $\lambda x, y \cdot (x^2 + 3y + 1)$ denotes the function $f : \mathbb{N}^2 \to \mathbb{N}$ such that for all x, $y \in \mathbb{N}$, $f(x, y) = x^2 + 3y + 1$.

Definitions. (1) 1_A is the *identity function* on A.

(2) If $f \colon A \rightharpoonup B$ and $g \colon B \rightharpoonup C$, then
$g \circ f \colon A \rightharpoonup C$ is their ***composition*** $\lambda x \cdot g(f(x))$.

Lemma 1.1. *(a) Let $f\colon A \rightharpoonup B$. Then $f \circ 1_A = f = 1_B \circ f$.*

(b) Let $f\colon A \rightharpoonup B$, $g\colon B \rightharpoonup C$ and $h\colon C \rightharpoonup D$. Then $h \circ (g \circ f) = (h \circ g) \circ f$. We therefore write this as $h \circ g \circ f$.

Lemma 1.2. *Let $f\colon A \rightharpoonup B$ and $g\colon B \rightharpoonup C$. Then*

(a) f, g total $\Longrightarrow$ $g \circ f$ total.

Suppose f, g total. Then

(b) f, g 1-1 $\Longrightarrow$ $g \circ f$ 1-1.

(c) f, g onto $\Longrightarrow$ $g \circ f$ onto. ***Hence:***

(d) f, g bijective $\Longrightarrow$ $g \circ f$ bijective.

Proof: EXERCISES. $\square$

Corollary 1.3. *Equinumerosity is an equivalence relation on the universe of sets, i.e.,*

(a) $A \approx A$

(b) $A \approx B \implies B \approx A$

(c) $A \approx B \approx C \implies A \approx C$.

Proof: EXERCISES. (*Note*: For (b), use Cor. 1.5(c) below.) $\square$

Definitions. (3) Suppose $f\colon A \to B$ and $g\colon B \to A$.

(a) g is a *left inverse* of f if $g \circ f = 1_A$.

(b) g is a *right inverse* of f if $f \circ g = 1_B$.

(c) g is a *2-sided inverse* of f if g is both a left and a right inverse of f.

Note. g is a left inverse of f $\iff$ f is a right inverse of g.

Predicates

We identify $\mathbb{2} = \{0, 1\}$ with the set of *truth values*,
i.e. $0 = \mathsf{false}$ and $1 = \mathsf{true}$.

- A *predicate* on a set A is a total function $P : A \to \mathbb{2}$.
  An n-ary predicate on A is a predicate on A^n.

- Given $B \subseteq A$, the ***characteristic function*** or ***characteristic predicate*** of B on A is the function $\chi_B : A \to \mathbb{2}$ such that $\forall x \in A$:

$$\chi_B(x) = \begin{cases} 1 & \text{if } x \in B \\ 0 & \text{otherwise.} \end{cases}$$

- Conversely, given a predicate $P : A \to \mathbb{2}$, the *characteristic set* of P on A is the set $\mathcal{S}_P = \{x \in A \mid P(x) = 1\} \subseteq A$. Hence (by Cor. 1.5($c$) below)

$$\wp A \approx \mathrm{PRED}(A)$$

  where $\wp A$ is the power set (the set of all subsets) of A and $\mathrm{PRED}(A)$ is the set of predicates on A.

Note. We will usually take $A = \mathbb{N}$, i.e. we will be working mainly with n-ary relations on $\mathbb{N}$ and n-ary predicates on $\mathbb{N}$ (for $n \geq 1$).

(For some background, a good reference is [DDS78].)

Theorem 1.4. *Suppose $A \neq \emptyset$. The following are equivalent:*

(1) *there is a (total) injection* $f\colon A \hookrightarrow B$

(2) *there is a (total) surjection* $g\colon B \twoheadrightarrow A$.

Further, given either f or g as above, the other can be chosen so that $g \circ f = 1_A$.

Proof: (Done in class.) $\square$

Corollary 1.5. *Suppose $A \neq \emptyset$ and f, g total.*

(a) $f\colon A \to B$ *is injective* $\iff$ f *has a left inverse* $g\colon B \to A$.

(b) $g\colon B \to A$ *is surjective* $\iff$ g *has a right inverse* $f\colon A \to B$.

(c) $f\colon A \to B$ *is bijective* $\iff$ f *has a 2-sided inverse* $g\colon B \to A$.

Note. Part (c) of Corollary 1.5 was used in the proof of Cor. 1.3(b), and also in the proof (p. 1-6) that $\wp A \approx \mathrm{PRED}(A)$.

Note.

(a) A *right inverse* need not be a *left inverse*, and *vice versa*.

(b) A 1-sided inverse need *not* be *unique*.

(c) However a 2-sided inverse *is unique*.

We write the (unique) inverse of f (if it exists) as f^{-1}.

Proof: Exercises. (*Hint*: For (a), (b), take $A = \mathbb{2}$, $B = \mathbb{N}$.) $\square$

Finite and Infinite sets

Definition. $\boldsymbol{seg}(n) =_{df} \{0, \dots, n-1\}$.

Note. $\boldsymbol{seg}(0) = \emptyset$.

Definition (Finite set). (a) A is ***finite*** $\iff \exists n \in \mathbb{N}[A \approx \boldsymbol{seg}(n)]$.

(b) A is ***infinite*** otherwise.

If A is finite, with $A \approx \boldsymbol{seg}(n)$, write $A = \{a_0, \dots, a_{n-1}\}$.

Q. Is it possible that $B \subset A$ but $B \approx A$?

This question is answered by the following theorems, especially Cor. 1.10.

Lemma 1.6. *(a)* $B \subseteq \boldsymbol{seg}(n),\ B \approx \boldsymbol{seg}(n) \implies B = \boldsymbol{seg}(n)$.

(b) $B \subset \boldsymbol{seg}(n) \implies \exists m < n[B \approx \boldsymbol{seg}(m)]$.

Proof: Exercise. (By induction on n.) $\square$

Corollaries 1.7.

(a) $\boldsymbol{seg}(m) \approx \boldsymbol{seg}(n) \implies m = n.$ [by Lemma 1.6(a)]

(b) $B \subset A \approx \boldsymbol{seg}(n) \implies \exists m < n[B \approx \boldsymbol{seg}(m)].$ [by Lemma 1.6(b)]

(c) $B \subset A$, A *finite* $\implies B \not\approx A.$ [by (a) and (b)]

(d) $A \approx \boldsymbol{seg}(\boldsymbol{n})$ *for at most one* $\boldsymbol{n} \in \mathbb{N}$. [by ($a$)]

We call this $\boldsymbol{n}$ *the* ***cardinal (number) of*** A, *written* ***card***(A) *or* $|A|$. *We say:* A *has* $\boldsymbol{n}$ *elements.*

Lemma 1.8. $\mathbb{N} \approx$ *a proper subset of* $\mathbb{N}$.

Proof: Ex. $\square$

Theorem 1.9. *For any set* A, *the following are equivalent:*

(1) A *is infinite*

(2) $\mathbb{N} \hookrightarrow A$

(3) $A \approx$ *some proper subset of* A

Proof: (1) $\Rightarrow$(2): (Details in class).

(2) $\Rightarrow$(3): Exercise.

(3) $\Rightarrow$(1): From Cor. 1.7(c). $\square$

Note. By Theorem 1.4, we can re-write Theorem 1.9 as:

Theorem 1.9$^+$. *For any set* A, *the following are equivalent:*

(1) A *is infinite*

(2) $\mathbb{N} \hookrightarrow A$

(3) $A \twoheadrightarrow \mathbb{N}$

(4) $A \approx$ *some proper subset of* A

From Theorem 1.9, we get:

Corollary 1.10.
A set is equinumerous with some proper subset of itself iff it is infinite.

Theorem 1.11 (Countability). *For any A, the foll. are equiv:*

(1) $A \hookrightarrow \mathbb{N}$

(2) $A = \emptyset$ *or* $\exists g \colon \mathbb{N} \twoheadrightarrow A$.

(3) A *is finite, or* $\exists h \colon \mathbb{N} \approx A$.

*A is called **countable** or **enumerable** if any of the above conditions holds.*

Proof: (1)⇔(2): Thm 1.4 (p. 1-7), with $B = \mathbb{N}$.

(3)⇒(1): Clear.

(2)⇒(3): Replace g by a bijection $h \colon \boldsymbol{seg}(n) \approx A$ or $h \colon \mathbb{N} \approx A$ by *deleting repetitions*. □

Corollary 1.12. *For any $A \neq \emptyset$:* $\qquad A \hookrightarrow \mathbb{N} \iff \mathbb{N} \twoheadrightarrow A$.

Notes.

(a) In (2) above, g is called an ***enumeration*** or ***listing with repetitions***, since g enumerates or lists A:

$$A = \{a_0, a_1, a_2, \dots\} \qquad\qquad \text{where } \ a_i = g(i).$$

Similarly, in (3), h is an ***enumeration without repetitions***.

(b) By (3) above, if A is countable but not finite, then $A \approx \mathbb{N}$, and A is called ***countably infinite***.

(c) A set which is not countable is called ***uncountable*** (or ***uncountably infinite***).

(d) A subset of a finite set is finite. (By Cor. 1.7(b).)

(e) A subset of a countable set is countable. (EXERCISE.)

(f) If $A \approx B$ and A is ***finite***, ***countably infinite*** or ***uncountable*** (resp.), then so is B. (EXERCISE.)
Thus all sets can be *classified by size* as

- finite,
- countably infinite,
- uncountably infinite.

Roughly speaking, countable infinity is the "smallest" infinity.

Uncountable sets

Recall the notation: B^A is the set of (total) functions from A to B.

(Reason for the notation: For finite sets A and B, what is ***card***(B^A)?)

Let $\mathrm{TFN}^{(1)} = \mathbb{N}^{\mathbb{N}}$ be the set of total unary functions on $\mathbb{N}$.

Theorem 1.13 (Cantor).
The sets $(a)\,\mathrm{TFN}^{(1)}$, (b) $\wp\mathbb{N}$ *and* (c) PRED$(\mathbb{N})$ *are uncountably infinite.*

Proof: The proofs use a ***diagonalisation method***, which we will encounter many times in this course.

(a) Let $F = \{f_0, f_1, f_2, \dots\}$ be any countable subset of $\mathrm{TFN}^{(1)}$.
We will exhibit a function

$$f \in \mathrm{TFN}^{(1)} \backslash F,$$

i.e. a *witness* that $F \subset \mathrm{TFN}^{(1)}$. Define

$$f(n) = f_n(n) + 1.$$

Then for all n, $f(n) \neq f_n(n)$, and so $f \neq f_n$. Hence $f \notin F$.

(b) Let $\mathcal{S} = \{X_0, X_1, X_2, \dots\}$ be any countable subset of $\wp\mathbb{N}$.
We can similarly define a witness that $\mathcal{S} \subset \wp\mathbb{N}$, namely

$$X =_{df} \{n \mid n \notin X_n\},$$

since for all n, $n \in X \Leftrightarrow n \notin X_n$, and so $X \neq X_n$.
Hence $X \notin \mathcal{S}$.

(c) EXERCISE. $\square$

Some theorems on countability (See [DDS78], pp. 118 ff.)

Recall Thm 1.11 (p. 10): If $A \neq \emptyset$, then A is ***countable*** $\iff$

(a) $A \hookrightarrow \mathbb{N}$ ***or*** (b) $\mathbb{N} \twoheadrightarrow A$.

In case (a), if $f\colon A \hookrightarrow \mathbb{N}$, then f is a ***coding*** of A,
and for $x \in A$, $f(x)$ is the ***code*** of x under f.
If f is *effective*, then it is an ***effective coding*** or ***Gödel numbering*** of A (studied later).

In case (b), if $g\colon \mathbb{N} \twoheadrightarrow A$, then g is an ***enumeration*** or ***listing*** of A:

$$(a_0, a_1, a_2, \dots) \qquad \text{(where } a_i = g(i))$$

— with or without repetitions.

If g is *effective*, then it is an ***effective enumeration*** of A (studied later).

The following results are proved in class.

Theorem 1.14 (Countable sets).

(1) A, B *countable* $\implies$ $A \cup B$ *countable.*

Example: $\mathbb{Z}$ is countable.

(2) $A_0, \dots, A_n$ *countable* $\implies$ $A_0 \cup \dots \cup A_n$ *countable.*

(3) $A_0, A_1, A_2, \dots$ *countable* $\implies$ $\bigcup_{i=0}^{\infty} A_i$ *countable.*

(4) A, B *countable* $\implies$ $A \times B$ *countable.*

Example: $\mathbb{Q}$ is countable.

(5) $A_0, \dots, A_n$ *countable* $\implies$ $\prod_{i=0}^{n} A_i =_{df} A_0 \times \dots \times An$ *is countable.*

(6) A *countable* $\implies$ A^n *countable* $(n \geq 0)$

(7) A *countable* $\implies$ $A^* =_{df} A^{<\omega} = \bigcup_{n=0}^{\infty} A^n$ *is countable.*

Example: $\mathbb{N}^*$ is countable.

Q. What about $A^\omega \approx A^{\mathbb{N}}$ for A countable?

A note on cardinal numbers

We showed (p. 1-9) how to define cardinal numbers for finite sets A:

$$\boldsymbol{card}(A) \;=\; \text{the unique } n \text{ such that } A \approx \boldsymbol{seg}(n).$$

The ***card*** operation has the property that for finite A, B:

$$\boldsymbol{card}(A) = \boldsymbol{card}(B) \iff A \approx B. \tag{1}$$

Georg Cantor, the founder of modern set theory, developed a theory of cardinal numbers for *all* sets, so as to satisfy (1).
Bertrand Russell defined $\boldsymbol{card}(A)$ as the equivalence class of A under the equivalence relation '$\approx$'. (Recall Cor. 1.3.)

Notation.

- $\aleph_0 \;=_{df}\; \boldsymbol{card}(\mathbb{N})$
- $\mathsf{c} \;=_{df}\; \boldsymbol{card}(\mathbb{R})$ (the cardinality of the real continuum)

Definitions.

(1) $\boldsymbol{card}(A) \le \boldsymbol{card}(B) \quad \Longleftrightarrow_{df} \quad A \hookrightarrow B$ ***or*** $B \twoheadrightarrow A$.

(2) $\boldsymbol{card}(A) < \boldsymbol{card}(B) \quad \Longleftrightarrow_{df} \quad A \hookrightarrow B$ ***but not*** $A \approx B$

(or equiv: $A \hookrightarrow B$ ***but not*** $B \hookrightarrow A$).

It can then be shown:

- $\aleph_0$ is the smallest infinite cardinal
- $\boldsymbol{card}(A) < \aleph_0 \iff A$ is finite
- $\boldsymbol{card}(A) \le \aleph_0 \iff A$ is countable $\iff A \hookrightarrow \mathbb{N} \iff \mathbb{N} \twoheadrightarrow A$
- $\boldsymbol{card}(A) = \aleph_0 \iff A$ is countably infinite $\iff A \approx \mathbb{N}$
- $\boldsymbol{card}(A) \ge \aleph_0 \iff A$ is infinite $\iff \mathbb{N} \hookrightarrow A \iff A \twoheadrightarrow \mathbb{N}$
- $\boldsymbol{card}(A) > \aleph_0 \iff A$ is uncountable
- ${\aleph_0}^{\aleph_0} \;=\; \boldsymbol{card}(\mathbb{N}^{\mathbb{N}}) \;=\; \mathsf{c} \;>\; \aleph_0$ by Cantor's Thm.
- $2^{\aleph_0} \;=\; \boldsymbol{card}(\mathbb{2}^{\mathbb{N}}) \;=\; \boldsymbol{card}(\mathrm{PRED}(\mathbb{N})) \;=\; \boldsymbol{card}(\wp\mathbb{N}) \;=\; \mathsf{c} > \aleph_0$ also.

For more information, see, e.g., [DDS78].

Truth tables: basic operations on truth values

Let p and q be *boolean variables*, i.e. ranging over $\mathbb{2}$. The operations *not*, *and*, and *or*, denoted by $\neg$, $\wedge$, and $\vee$ respectively, are defined by the truth tables

p	$\neg p$
1	0
0	1

and

p	q	$p \wedge q$	$p \vee q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

.

Now we can form new predicates from old, for if P and Q are predicates on A, then so are $\neg P$, $P \wedge Q$, and $P \vee Q$, where for $x \in A$:

$$\neg P(x) \ = \ 1 - P(x),$$

$$(P \wedge Q)(x) = P(x) \wedge Q(x) = \begin{cases} 1 & \text{if } P(x) = 1 \text{ and } Q(x) = 1 \\ 0 & \text{otherwise,} \end{cases}$$

$$(P \vee Q)(x) = P(x) \vee Q(x) = \begin{cases} 1 & \text{if } P(x) = 1 \text{ or } Q(x) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

The corresponding ***characteristic sets*** are

$$\begin{aligned} \mathcal{S}_{\neg P} \ &= \ \ A \backslash \mathcal{S}_P \ \ = \{\, x \in A \mid \neg P(x) \,\}, \\ \mathcal{S}_{P \wedge Q} &= \mathcal{S}_P \cap \mathcal{S}_Q = \{\, x \in A \mid P(x) \wedge Q(x) \,\}, \\ \mathcal{S}_{P \vee Q} &= \mathcal{S}_P \cup \mathcal{S}_Q = \{\, x \in A \mid P(x) \vee Q(x) \,\}. \end{aligned}$$

We will use De Morgan's laws:

$$\neg(p \wedge q) = \neg p \vee \neg q,$$

$$\neg(p \vee q) = \neg p \wedge \neg q.$$

We define $p \rightarrow q$ to mean $\neg p \vee q$ ***or*** $\neg(p \wedge \neg q)$.

Quantifiers

We usually quantify over $\mathbb{N}$, so that $\forall x\, R(x)$ means $(\forall x \in \mathbb{N})\, R(x)$ and $\exists x\, R(x)$ means $(\exists x \in \mathbb{N})\, R(x)$. Quantifiers can also be *relativised* to predicates P on $\mathbb{N}$, thus:

$$
\begin{aligned}
(\forall x)_{P(x)} R(x) &= \forall x \left[P(x) \to R(x)\right], \\
(\exists x)_{P(x)} R(x) &= \exists x \left[P(x) \wedge R(x)\right].
\end{aligned}
$$

In particular, we have *bounded* quantifiers:

$$
\begin{aligned}
(\forall x \leq n) P(x) &= (\forall x)_{x \leq n} P(x), \\
(\forall x < n) P(x) &= (\forall x)_{x < n} P(x), \\
(\exists x \leq n) P(x) &= (\exists x)_{x \leq n} P(x), \\
(\exists x < n) P(x) &= (\exists x)_{x < n} P(x).
\end{aligned}
$$

De Morgan's laws for quantifiers are

$$
\begin{aligned}
\neg \forall x R(x) &= \exists x \neg R(x), \\
\neg \exists x R(x) &= \forall x \neg R(x), \\
\neg (\forall x)_{P(x)} R(x) &= (\exists x)_{P(x)} \neg R(x), \\
\neg (\exists x)_{P(x)} R(x) &= (\forall x)_{P(x)} \neg R(x).
\end{aligned}
$$

Mathematical induction

We give three different (but equivalent) formulations of this principle.
Let P be a predicate on $\mathbb{N}$.

- **Simple induction (SI)**

  If $P(0)$ *and* $\forall n\,[P(n) \Rightarrow P(n+1)]$
  then $\forall n P(n)$.

- **Course-of-values induction (CVI)**

  If $\forall n[(\forall m < n\ P(m)) \Rightarrow P(n)]$
  then $\forall n P(n)$.

- **Least number principle (LNP)**

  If $\exists n P(n)$
  then $\exists$ *least* $n\ P(n)$,
  that is, $\exists n\,[P(n) \wedge \forall m < n\ \neg P(m)]$.

Exercise. Prove the equivalence of these three *induction schemes*.