CM0081 Automata and Formal Languages
§ 1.4 Formal Proofs

Andrés Sicard-Ramírez

Universidad EAFIT

Semester 2024-1

Preliminaries

Conventions

- The number and page numbers assigned to chapters, examples, exercises, figures, quotes, sections and theorems on these slides correspond to the numbers assigned in the textbook [Hopcroft, Motwani and Ullman 2007].
- The natural numbers include the zero, that is, $\mathbb{N} = \{0, 1, 2, \dots\}$.
- The power set of a set A, that is, the set of its subsets, is denoted by $\mathcal{P}\,A$.

Proofs by Contradiction and Proofs of Negations

Proof by contradiction
(or *reductio ad absurdum*)

$$\frac{\begin{matrix}[\neg\beta] \\ \vdots \\ \bot\end{matrix}}{\beta}$$

Proof of negation [Bauer 2017]

$$\frac{\begin{matrix}[\beta] \\ \vdots \\ \bot\end{matrix}}{\neg\beta}$$

Proofs by Contradiction and Proofs of Negations

Proof by contradiction
(or *reductio ad absurdum*)

$$\dfrac{\begin{array}{c}[\neg\beta]\\ \vdots\\ \bot\end{array}}{\beta}$$

Proof of negation [Bauer 2017]

$$\dfrac{\begin{array}{c}[\beta]\\ \vdots\\ \bot\end{array}}{\neg\beta}$$

Justifications

$$\dfrac{\dfrac{\dfrac{\begin{array}{c}[\neg\beta]\\ \vdots\\ \bot\end{array}}{\neg\beta \to \bot}\ \text{(conditional proof)}}{\neg\neg\beta}\ (\neg\alpha := \alpha \to \bot)}{\beta}\ (\vdash \neg\neg\alpha \to \alpha)$$

$$\dfrac{\dfrac{\begin{array}{c}[\beta]\\ \vdots\\ \bot\end{array}}{\beta \to \bot}\ \text{(conditional proof)}}{\neg\beta}\ (\neg\alpha := \alpha \to \bot)$$

Inductive Proofs: Mathematical Induction

The induction principle

Let $S(n)$ be a property about natural numbers. If

(i) we prove $S(i)$ (basis step) and

(ii) we prove that for all natural number $n \geq i$, $S(n)$ implies $S(n+1)$ (inductive step),

then we may conclude $S(n)$ for all $n \geq i$.

Inductive Proofs: Structural Induction

The structural induction principle

Let $S(X)$ be a property about structures X that are defined by some recursive/inductive definition. If

(i) we prove $S(X)$ for the basis structure(s) of X (basis step) and

(ii) given a structure X whose recursive/inductive definition says it is formed from $Y_1, \dots, Y_k$, we prove $S(X)$ assuming that the properties $S(Y_1), \dots, S(Y_k)$ hold (inductive step),

then $S(X)$ is true for all X.

Inductive Proofs: Mutual Induction

Example

Given the functions $f, g, h : \mathbb{N} \to \mathbb{N}$ and properties R, S, T,

$$f(0) = 0, \qquad g(0) = 1, \qquad h(0) = 0,$$
$$f(n+1) = g(n), \qquad g(n+1) = f(n), \qquad h(n+1) = 1 - h(n),$$

$$R(n)\colon h(n) = 1 - g(n), \qquad S(n)\colon h(n) = f(n), \qquad T(n) : S(n) \land R(n),$$

Inductive Proofs: Mutual Induction

Example

Given the functions $f, g, h : \mathbb{N} \to \mathbb{N}$ and properties R, S, T,

$$f(0) = 0, \qquad g(0) = 1, \qquad h(0) = 0,$$
$$f(n+1) = g(n), \qquad g(n+1) = f(n), \qquad h(n+1) = 1 - h(n),$$

$$R(n)\colon h(n) = 1 - g(n), \qquad S(n)\colon h(n) = f(n), \qquad T(n) : S(n) \wedge R(n),$$

1. To prove $(\forall n)R(n)$ (impossible!)
2. To prove $(\forall n)S(n)$ (impossible!)

Inductive Proofs: Mutual Induction

Example

Given the functions $f, g, h : \mathbb{N} \to \mathbb{N}$ and properties R, S, T,

$$f(0) = 0, \qquad g(0) = 1, \qquad h(0) = 0,$$
$$f(n+1) = g(n), \qquad g(n+1) = f(n), \qquad h(n+1) = 1 - h(n),$$

$$R(n) \colon h(n) = 1 - g(n), \qquad S(n) \colon h(n) = f(n), \qquad T(n) : S(n) \wedge R(n),$$

1. To prove $(\forall n) R(n)$ (impossible!)
2. To prove $(\forall n) S(n)$ (impossible!)
3. To prove $(\forall n) T(n)$ (by mutual induction)

(continued on next slide)

Inductive Proofs: Mutual Induction

Proof

- Basis step $T(0)$. Easy.

Inductive Proofs: Mutual Induction

Proof

- Basis step $T(0)$. Easy.
- Induction step $T(n) \Rightarrow T(n+1)$:

$$
\begin{aligned}
S(n): \quad h(n+1) &= 1 - h(n) && \text{(def. of } h\text{)} \\
&= g(n) && \text{(IH } R(n)\text{)} \\
&= f(n+1) && \text{(def. of } f\text{)}
\end{aligned}
$$

$$
\begin{aligned}
R(n): \quad h(n+1) &= 1 - h(n) && \text{(def. of } h\text{)} \\
&= 1 - f(n) && \text{(IH } S(n)\text{)} \\
&= 1 - g(n+1) && \text{(def. of } g\text{)}
\end{aligned}
$$

∎

References

Bauer, A. (2017). Five States of Accepting Constructive Mathematics. Bulletin of the American Mathematical Society 54.3, pp. 481–498. DOI: 10.1090/bull/1556 (cit. on pp. 3, 4).

Hopcroft, J. E., Motwani, R. and Ullman, J. D. [1979] (2007). Introduction to Automata Theory, Languages, and Computation. 3rd ed. Pearson Education (cit. on p. 2).