Formal Proof Systems

A formal system is one way to make precise the arguments and reasoning used in everyday mathematics. Cutland gives a definition for a formal system \((\mathcal{A}, \mathcal{D})\) with respect to a language \(L\).

- \(\mathcal{A}\) is a set of axioms, that is sentences that we hold to be implicitly provable (where depending on our choice of \(\mathcal{A}\) we have a different definition of “implicitly provable”). Thus, \(\mathcal{A} \subseteq \mathcal{I}\).
- \(\mathcal{D}\) is an explicit definition of the notion of a formal proof in this system, satisfying two conditions.
  - Proofs are finite objects (hence capable of being coded by natural numbers).
  - In particular, it is important to have the property that if \(\mathcal{A}\) is recursive then the set of proofs is also recursive.

\`
\'p is a proof of the statement \(\sigma\) from the axioms \(\mathcal{A}\)’
\`

is decidable. This means that the set of proofs of \((\mathcal{A}, \mathcal{D})\) is recursive.

This all seems very abstract, so we will consider a few concrete examples. These examples are formal systems for first-order logic (without any nonlogical function, relation, or constant symbols). But, each of these examples can be expanded (by adding axioms or rules of inferences) to describe proofs of sentences in the language of arithmetic.

In particular, we will be interested in adding to any axiomatisation of first-order logic the axioms/rules of inference of Peano Arithmetic, in the language of arithmetic \(L = (+, \times, 0, 1)\).

- \(\forall x (0 \neq x + 1)\)
- \(\forall x \forall y (x + 1 = y + 1 \rightarrow x = y)\)
- \(\forall x (x + 0 = x)\)
- \(\forall x \forall y (x + (y + 1) = (x + y) + 1)\)
- \(\forall x (x \times 0 = 0)\)
- \(\forall x \forall y (x \times (y + 1) = (x \times y) + x)\)
- For each formula \(\phi\) with free variables \(x, y_1, \ldots, y_n\)
  \(\forall y_1 \ldots \forall y_n (\phi(0, y_1, \ldots, y_n) \land \forall x (\phi(x, y_1, \ldots, y_n) \rightarrow \phi(x + 1, y_1, \ldots, y_n))) \rightarrow \forall x \phi(x, y_1, \ldots, y_n)\)
Formal system based on many axioms and a single rule of inferences

In this deductive system we have infinitely many axioms and a single inference rule. The one rule of inference is modus ponens: from the formulas $\alpha$ and $\alpha \to \beta$, we may infer $\beta$. This is often written as

$$\frac{\alpha, \alpha \to \beta}{\beta}.$$

We take as basic only the logical symbols $\neg, \to, \forall$: other connectives are defined in terms of these.

We arrange the axioms into six kinds. An axiom is any generalization of well-formed formulas of the following kinds. Note that a generalization of a well-formed formula $\forall x_1 \cdots \forall x_n \phi$ (for any variables $x_1, \ldots, x_n$).

- **Tautologies** of sentential logic where we replace sentence symbol by any well-formed formula of $L$. E.g. replacing $A, B$ in the contrapositive $[A \to \neg B] \to [B \to \neg A]$, we get

$$[\forall x(x = x) \to \neg \exists x(\neg x = x)] \to [\exists x(\neg x = x) \to \neg \forall x(x = x)].$$

- **Substitution** For a term $t$,

$$\forall x \alpha \to \alpha[x/t].$$

- **Generalization** If $x$ does not occur free in $\alpha$,

$$\alpha \to \forall x \alpha.$$ 

- **Identity** $x = x$.

- **Indistinguishability of identicals** If $\alpha$ is atomic and $\alpha'$ is obtained from $\alpha$ by replacing $x$ in zero or more (but not necessarily all) places by $y$,

$$x = y \to (\alpha \to \alpha').$$

A deduction (or proof) of $\phi$ from a set of formulas $\Gamma$ is a finite sequence $\langle \alpha_0, \ldots, \alpha_n \rangle$ of formulas such that $\alpha_n$ is $\phi$ and for each $k \leq n$ either $\alpha_k$ is in $\Gamma$ or is an axiom, or $\alpha_k$ is obtained by modus ponens from two earlier formulas in the proof.

**Note**: this definition of proof satisfies the two conditions Cutland describes for proof systems.

Example: The following is a deduction for the sentence $\forall x \phi(x) \to \neg \forall x \neg \phi(x)$.

$$\begin{align*}
\forall x \phi(x) &\to \phi(c) \\
\forall x \neg \phi(x) &\to \neg \phi(c) \\
[\forall x \neg \phi(x) \to \neg \phi(c)] &\to [\neg \phi(c) \to \neg \forall x \neg \phi(x)] \\
\neg \phi(c) &\to \neg \forall x \neg \phi(x) \\
\phi(c) &\to \neg \neg \phi(c) \\
[\phi(c) \to \neg \neg \phi(c)] &\to \{[\neg \neg \phi(c) \to \neg \forall x \neg \phi(x)] \to [\phi(c) \to \neg \forall x \neg \phi(x)]\} \\
[\neg \neg \phi(c) &\to \neg \forall x \neg \phi(x)] \to [\phi(c) \to \neg \forall x \neg \phi(x)] \\
\phi(c) &\to \neg \forall x \neg \phi(x) \\
[\forall x \phi(x) &\to \phi(c)] \to \{[\phi(c) \to \neg \forall x \neg \phi(x)] \to [\forall x \phi(x) \to \neg \forall x \neg \phi(x)]\} \\
[\phi(c) &\to \neg \forall x \neg \phi(x)] \to [\forall x \phi(x) \to \neg \forall x \neg \phi(x)] \\
\forall x \phi(x) &\to \neg \forall x \neg \phi(x).
\end{align*}$$

Each line is either an axiom or the result of applying modus ponens to previous lines in the proof. Note that on two occasions, we use the sentential tautology $[A \to B] \to \{[B \to C] \to [A \to C]\}$. We also use the tautology associated with contrapositives, $[A \to B] \to [\neg B \to \neg A]$, and the tautology associated with double negation, $A \to \neg \neg A$. 


Formal system based on no axioms but many rules of inference

The sequent calculus formalizes proofs as finite sequences of lines where each line is

\[ \Gamma \Rightarrow \Delta, \]

where \( \Gamma, \Delta \) are sets of sentences and the intended meaning is that any interpretation of the non-logical symbols which makes all sentences in \( \Gamma \) true will make at least one sentence in \( \Delta \) true.

*We take as basic only the logical symbols \( \neg, \lor, \exists \); other connectives are defined in terms of these.*

We have the following rules of the sequent calculus.

\[
\frac{\text{\{A\} \Rightarrow \{A\}}}{\Gamma \Rightarrow \Delta} \quad \text{(1)}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Gamma' \Rightarrow \Delta'} \quad \text{where } \Gamma \subseteq \Gamma', \Delta \subseteq \Delta' \quad \text{(2)}
\]

\[
\frac{\Gamma \Rightarrow \{\neg A\} \cup \Delta}{\Gamma \Rightarrow \{A, B\} \cup \Delta} \quad \text{(3)}
\]

\[
\frac{\Gamma \Rightarrow \{A\} \cup \Delta}{\Gamma \cup \{A\} \Rightarrow \Delta} \quad \text{(4)}
\]

\[
\frac{\Gamma \Rightarrow \{A\} \cup \Delta}{\Gamma \Rightarrow \{(A \lor B)\} \cup \Delta} \quad \text{(5)}
\]

\[
\frac{\Gamma \Rightarrow \{A(s)\} \cup \Delta}{\Gamma \Rightarrow \{\exists xA(x)\} \cup \Delta} \quad \text{(6)}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Gamma \cup \{\exists xA(x)\} \Rightarrow \Delta} \quad \text{where } c \text{ does not appear in } \Gamma, \Delta, A(x). \quad \text{(7)}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Gamma \cup \{A(c)\} \Rightarrow \Delta} \quad \text{(8)}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Gamma \cup \{s = t\} \Rightarrow \Delta} \quad \text{(9)}
\]

\[
\frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \{A(\bar{s})\} \cup \Delta} \quad \frac{\Gamma \cup \{A(t)\} \Rightarrow \Delta}{\Gamma \cup \{s = \bar{t}, A(s)\} \Rightarrow \Delta} \quad \text{(10)}
\]

A deduction (or proof) of a sentence \( \sigma \) from a set of premises \( \Gamma \) is a finite sequence of sequents whose last line is \( \Gamma \Rightarrow \{\sigma\} \) and such that each sequent is obtainable from previous ones by applying one of the rules of inference.

*Note: this definition of proof satisfies the two conditions Cutland describes for proof systems.*

**Example:** The following is a deduction for the sentence \( \neg \exists x \neg \phi(x) \rightarrow \exists x \phi(x) \), i.e. the sentence \( \exists x \neg \phi(x) \lor \exists x \phi(x) \) (because \( A \rightarrow B \) is an abbreviation for \( \neg A \lor B \)).

\[
\{\phi(c)\} \Rightarrow \{\phi(c)\}
\]

\[
\emptyset \Rightarrow \{\phi(c), \neg \phi(c)\}
\]

\[
\emptyset \Rightarrow \{\exists x \phi(x), \neg \phi(c)\}
\]

\[
\emptyset \Rightarrow \{\exists x \neg \phi(x) \lor \exists x \phi(x)\}
\]