Formal Proofs and their Lengths III

Frege systems II

Definition 1 (Frege rule)**.** Let L be a complete system of logical connectives. An ℓ-ary *Frege rule* is a an $(\ell+1)$-tuple of formulas $A_1, \ldots, A_l, A_0$ (using just the connectives from L, L-formulas) written as

$$\frac{A_1, \ldots, A_l}{A_0},$$

such that $A_1, \ldots, A_n \models A_0$. A 0-ary Frege rule is called a *Frege axiom scheme.*

Definition 2 (Frege proof)**.** Let F be a finite set of Frege rules in a finite set of connectives L. An F-proof of an L-formula C from formulas $B_1, \ldots, B_t$ is any sequence of formulas $D_1, \ldots, D_k$, such that:

- $D_k = C$
- For all $i = 1, \ldots, k$ at least one of the following holds:
  - $D_i \in \{B_1, \ldots, B_t\}$
  - There is a Frege rule
  $$\frac{A_1, \ldots, A_\ell}{A_0} \in F,$$
  and numbers $j_1, \ldots, j_\ell < i$ and a substitution[1] σ such that
  $$\sigma(A_1) = D_{j_1}, \ldots, \sigma(A_\ell) = D_{j_\ell}, \text{ and } \sigma(A_0) = D_i.$$

The fact that π is an F-proof of C from $B_1, \ldots, B_t$ is denoted

$$\pi : B_1, \ldots, B_t \vdash_F C,$$

if we drop the 'π :' part, we just mean that such a π exists.

We call the number of formulas in a proof k the *number of steps* and denote it $\mathbf{k}(\pi)$. We call the length of the longest formula in π the *width* of π and denote it $\mathbf{w}(\pi)$. We call the size of π the sum of the lengths of all formulas in π and denote it $|\pi|$.

Definition 3 (Frege system)**.** A finite set of Frege rules F, with formulas using the connectives from a finite complete set L, is a *Frege proof system* if it is *sound* (cannot derive a non-tautology) and *implicationally complete* that is: For any L-formulas $B_1, \ldots, B_t, C$ we have

$$B_1, \ldots, B_t \models C \iff B_1, \ldots, B_t \vdash_F C.$$

Fact 4. The textbook Frege system is implicationally complete.

[1] A mapping from variables to formulas, when applied to a formula it outputs a formula where each variable is replaced by the respective formula according to σ.

Exercise 5. Show that the textbook Frege system is a Frege system. How many Frege rules does it have?

Exercise 6 (Frege can prove substitutions!)**.** Show that if F is a Frege system in finite complete set of connectives L and $\pi = (D_1, \ldots, D_k)$ fulfills

$$\pi : B_1, \ldots, B_t \vdash_F C,$$

and σ is a substitution then for some π',

$$\sigma(B_1), \ldots, \sigma(B_t) \vdash_F \sigma(C).$$

What's the smallest $\mathbf{k}(\pi')$ you can achieve?

Lemma 7 (Deduction lemma)**.** Let F be a Frege system. Assume that

$$\pi : A, B_1, \ldots, B_t \vdash_F C,$$

then there is π' such that

$$\pi' : B_1, \ldots, B_t \vdash_F A \to C,$$

with $\mathbf{k}(\pi') = O(\mathbf{k}(\pi))$, $\mathbf{w}(\pi') = O(\pi)$ and $|\pi'| \leq O(|\pi|^2)$.

Exercise 8. Show that there is a proof of $\neg\neg a \to a$ in the textbook Frege system using the Deduction lemma. That is, find a proof:

$$\pi : \neg\neg a \vdash_{\text{textbook Frege}} a$$

Fact 9. Let C be a tautology which is not a substitution instance of any shorter tautology and let F be a Frege system. Then any $\pi : \vdash_F C$, must have $\mathbf{k}(\pi) = \Omega(ldp(C))$ and $|\pi| = \Omega(m)$, where $ldp(C)$ is the logical depth of C which is defined to be the length of the longest path in the representation tree of C and m is the sum of all lengths of subformulas of C.

Exercise 10. Use the previous fact to prove that any Frege proof

$$\pi : \vdash_F \overbrace{\neg \ldots \neg}^{2n}(a \to a),$$

must have $\mathbf{k}(\pi)$ at least $\Omega(n)$ and $|\pi|$ at least $\Omega(n^2)$.

Fact 11 (Reckhow's Theorem)**.** Any two Frege systems F_1 and F_2 have sizes of their shortest proofs of any particular sequence of tautologies polynomially related.

Open problem 12. Let F be a Frege system. Prove any lower bound on the size of F-proofs on a sequence aby sequence that is larger than $\Omega(n^2)$.

Propositional sequent calculus

Definition 13. Let $A_1, \ldots, A_n$ and $B_1, \ldots, B_m$ be propositional formulas. A sequent is a symbol of the form

$$A_1, \ldots, A_n \longrightarrow B_1, \ldots, B_m.$$

The semantics for a sequent are the same as for the formula

$$\bigwedge_i A_i \to \bigvee_i B_i,$$

which is semantically equivalent to

$$\bigvee_i \neg A_i \vee \bigvee_i B_i.$$

Definition 14. The Sequent calculus is a propositional proof system (which proves sequents), whose proves are given as follows.

A proof of a sequent S is a sequence of sequents, $S_1, \ldots, S_k$, where $S_k = S$ and each S_i is either an *initial sequent*

$$x \longrightarrow x,$$

where x is a propositional variable or was derived from $S_j, S_l, 1 \leq j \leq l \leq$ by one of the following rules.

Weak Structural Rules

$$(\text{Exchange:L})\frac{\Gamma, A, B, \Pi \longrightarrow \Delta}{\Gamma, B, A, \Pi \longrightarrow \Delta} \qquad (\text{Exchange:R})\frac{\Gamma \longrightarrow \Delta, A, B, \Lambda}{\Gamma \longrightarrow \Delta, B, A, \Lambda}$$

$$(\text{Contraction:L})\frac{\Gamma, A, A, \Pi \longrightarrow \Delta}{\Gamma, A, \Pi \longrightarrow \Delta} \qquad (\text{Contraction:R})\frac{\Gamma \longrightarrow \Delta, A, A, \Lambda}{\Gamma \longrightarrow \Delta, A, \Lambda}$$

$$(\text{Weakening:L})\frac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \qquad (\text{Weakening:R})\frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}$$

The Cut Rule

$$(\text{Cut})\frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma, A \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

The Propositional Rules

$$(\neg\text{:L})\frac{\Gamma \longrightarrow \Delta, A}{\Gamma, \neg A \longrightarrow \Delta} \qquad (\neg\text{:R})\frac{\Gamma, A \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A}$$

$$(\wedge\text{:L})\frac{\Gamma, A, B \longrightarrow \Delta}{\Gamma, A \wedge B \longrightarrow \Delta} \qquad (\wedge\text{:R})\frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}$$

$$(\vee\text{:L})\frac{\Gamma, A \longrightarrow \Delta \qquad \Gamma, B \longrightarrow \Delta}{\Gamma, A \vee B \longrightarrow \Delta} \qquad (\vee\text{:R})\frac{\Gamma \longrightarrow \Delta, A, B}{\Gamma \longrightarrow \Delta, A \vee B}$$

Sequent calculus is denoted LK (for Logischer Kalkülus) or PK for the propositional version.

Fact 15. $LK \equiv_p F$

Definition 16. LK^- is the subsystem of LK, which forbids the use of the cut rule.

Exercise 17. Prove $LK^- \vdash \longrightarrow A \vee \neg A$

Exercise 18. Prove $LK^- \vdash \longrightarrow (A \vee \neg A) \wedge (B \vee \neg B)$

Exercise 19. Prove $LK^- \vdash \longrightarrow (A \wedge B) \vee (A \wedge \neg B) \vee (A \wedge \neg B) \vee (\neg A \wedge \neg B)$

Exercise 20. Prove LK^- is complete.

Exercise 21. Is LK^- implicationally complete?