Formal Proofs and their Lengths III

Frege systems I

Example 1. Prove $a \to a$ in the textbook Frege system.

A Little Bit of Complexity

Definition 2. A predicate $f : \{0,1\}^* \to \{0,1\}$ is in **NP** if there is a predicate $g(x,y)$ in **P** and a polynomial p such that for every $x \in \{0,1\}^n$:

$$f(x) = 1 \iff (\exists y \in \{0,1\}^{\leq p(n)})\, g(x,y) = 1,$$

if such a y exists it is called the *witness*.

Definition 3. A predicate $f : \{0,1\}^* \to \{0,1\}$ is in **coNP** if there is a predicate $g(x,y)$ in **P** and a polynomial p such that for every $x \in \{0,1\}^n$:

$$f(x) = 0 \iff (\exists y \in \{0,1\}^{\leq p(n)})\, g(x,y) = 0.$$

Exercise 4. Show that $f(x) \in \mathbf{NP}$ if and only if $\neg f(x) \in \mathbf{coNP}$.

Definition 5. CNF-SAT is the predicate which assigns 1 exactly to those CNF formulas which are satisfiable. DNF-TAUT is the predicate which assigns 1 exactly to those CNF formulas which are satisfiable.

Theorem 6 (Cook-Levin)**.** The following equalities hold:

- $\mathbf{P} = \mathbf{NP}$ if and only if CNF-SAT $\in \mathbf{P}$.
- $\mathbf{P} = \mathbf{coNP}$ if and only if DNF-TAUT $\in \mathbf{P}$
- $\mathbf{NP} = \mathbf{coNP}$ if and only if DNF-TAUT $\in \mathbf{NP}$
  if and only if CNF-SAT $\in \mathbf{coNP}$

Theorem 7 (Cook-Reckhow)**.** $\mathbf{NP} = \mathbf{coNP}$ if and only if there is a propositional proof system P which has polynomial sized P-proofs of every tautology.

Exercise 8. Prove the Cook-Reckhow theorem.

Frege systems II

Definition 9 (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 10 (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 11 (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 12. The textbook Frege system is implicationally complete.

Exercise 13. Show that the textbook Frege system is a Frege system. How many Frege rules does it have?

Exercise 14 (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?

[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.

Lemma 15 (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 16. 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 17. 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 18. 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 19 (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 20. 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 $\Omega(n^2)$.