Formal Proofs and their Lengths II

Propositional Proof Systems

Definition 1. Let A be a finite set of symbols. We define $A^{\leq n} := \bigcup_{i=0}^{n} A^i$ and $A^* := \bigcup_{i\geq 0} A^i$.

Definition 2. A predicate $f : \{0,1\}^* \to \{0,1\}$ is in $\mathbf{P}$ if there is a Turing machine M computing f in polynomial time[1].

Definition 3 (Cook-Reckhow)**.** A *propositional proof system* (or a PPS) P is determined by a predicate $f(x,y)$ in $\mathbf{P}$ such that for every propositional formula A:

- Soundness:

$$(\exists y \in \{0,1\}^*)\, f(A,y) = 1 \implies A \text{ is a tautology},$$

- Completeness:

$$(\exists y \in \{0,1\}^*)\, f(A,y) = 1 \impliedby A \text{ is a tautology},$$

here we interpret f to be a predicate checking that y is a valid "proof" of A. That is, if $f(A,y) = 1$, then we say y is a P-proof of A.

Example 4. The truth-table proof system is a system determined by a predicate

$$f(A,y) = \begin{cases} 1 & y \text{ is the truth-table of } A,\ (\forall \overline{x})\mathbf{tt}_A(\overline{x}) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 5. Show that the truth-table proof system is a propositional proof system by the definition of Cook-Reckhow.

Exercise 6 (First lower bound!)**.** Show that all truth-table proofs of some family of tautologies are exponentially long in the size of the corresponding tautology.

A Little Bit of Complexity

Definition 7. A predicate $f : \{0,1\}^* \to \{0,1\}$ is in $\mathbf{NP}$ if there is a function $g(x,y)$ in $\mathbf{P}$ 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*.

[1] The precise definition of a Turing machine in fact does not matter. If you have never encountered the definition of a Turing machine, it is enough to consider the intuitive idea of an algorithm, whose number of steps does not exceed a specific polynomial in the length of the input and this itself just means, that the algorithm is somehow feasible — does not run too long. For example, such an algorithm cannot look at every truth assignment of a formula it receives as an input.

Definition 8. A predicate $f : \{0,1\}^* \to \{0,1\}$ is in **coNP** if there is a function $g(x,y)$ 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 9. Show that $f(x) \in \mathbf{NP}$ if and only if $\neg f(x) \in \mathbf{coNP}$.

Definition 10. 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 11 (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 12 (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 13. Prove the Cook-Reckhow theorem.

Frege systems I

Definition 14. The textbook Frege proof system is determined by the proofs of the following form:

The connectives in every formula in the system are just $\{\neg, \to\}$. A proof of a formula A is a sequence of propositional formulas $(B_1, \ldots, B_k)$, where $B_k = A$ and for each $1 \leq i \leq k$ one of the following is true:

- B_i has any of the forms
  1. $p \to (q \to p)$
  2. $(p \to (q \to r)) \to ((p \to q) \to (p \to r))$
  3. $(\neg p \to \neg q) \to (q \to p)$,

  where p, q and r are arbitrary formulas. Such a B_i is called an axiom (in the textbook Frege system).
- There are $1 \leq j_1, j_2 < i$ such that $B_{j_1} = p$, $B_{j_2} = (p \to q)$ and $B_i = q$. Such a B_i is said to be introduced by the *modus ponens* rule:

$$\frac{p, p \to q}{q}$$

Example 15. Prove $(a \to a) \to (a \to (a \to a))$ in the textbook Frege system.

Example 16. Prove $(a \to b) \to (a \to a)$ in the textbook Frege system.

Example 17. Prove the textbook Frege system is sound.

Example 18 (Bonus)**.** Prove $a \to a$ in the textbook Frege system.

Open problem 19. Does every tautology have a polynomial sized proof in the textbook Frege system?