

## Formal Proofs and their Lengths II

**Example 1.** The DNF  $(x_1 \wedge y_1) \vee (x_2 \wedge y_2) \vee \cdots \vee (x_n \wedge y_n)$  when expressed as CNF has at least  $2^n$  clauses.

### Propositional Proof Systems

**Definition 2.** Let  $A$  be a finite set of symbols. We define  $A^{<n} := \bigcup_{i=0}^n A^i$  and  $A^* := \bigcup_{i \geq 0} A^i$ .

**Definition 3.** A predicate  $f : \{0, 1\}^* \rightarrow \{0, 1\}$  is in  $\mathbf{P}$  if there is a Turing machine  $M$  computing  $f$  in polynomial time<sup>1</sup>.

**Definition 4** (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:

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

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 5.** The truth-table proof system is a system determined by a predicate

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

**Exercise 6.** Show that the truth-table proof system is a propositional proof system by the definition of Cook-Reckhow.

**Exercise 7** (First lower bound!). Show that some truth-table proof of a tautology is exponentially long in the size of that tautology.

---

<sup>1</sup>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.

## A Little Bit of Complexity

**Definition 8.** A predicate  $f : \{0, 1\}^* \rightarrow \{0, 1\}$  is in **NP** if there is a function  $g(x, y)$  in **P** and a polynomial  $p$  such that for every  $x \in \{0, 1\}^n$ :

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

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

**Definition 9.** A predicate  $f : \{0, 1\}^* \rightarrow \{0, 1\}$  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 10.** Show that  $f(x) \in \mathbf{NP}$  if and only if  $\neg f(x) \in \mathbf{coNP}$ .

**Definition 11.** 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 12** (Cook-Levin). The following equalities hold:

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

**Theorem 13** (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 14.** Prove the Cook-Reckhow theorem.

## Frege systems I

**Definition 15.** The textbook Frege proof system is determined by the proofs of the following form:

The connectives in every formula in the system are just  $\{\neg, \rightarrow\}$ . A proof of a formula  $A$  is a sequence of propositional formulas  $(B_1, \dots, B_k)$ , 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.  $p \rightarrow (q \rightarrow p)$
  2.  $(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r))$
  3.  $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$ ,

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  $B_{j_1} = p$ ,  $B_{j_2} = (p \rightarrow q)$  and  $B_i = q$ . Such a  $B_i$  is said to be introduced by the *modus ponens* rule:

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

**Example 16.** Prove  $(a \rightarrow a) \rightarrow (a \rightarrow (a \rightarrow a))$  in the textbook Frege system.

**Example 17.** Prove  $(a \rightarrow b) \rightarrow (a \rightarrow a)$  in the textbook Frege system.

**Example 18.** Prove the textbook Frege system is sound.

**Example 19 (Bonus).** Prove  $a \rightarrow a$  in the textbook Frege system.

**Open problem 20.** Does every tautology have a polynomial sized proof in the textbook Frege system?