Propositional proof systems

Definition 1. A propositional formula $\varphi(x_1, \dots, x_n)$ is a *tautology* if it obtains the value 1 under any assignment of its variables.

Exercise 2. Give an example of a tautology!

Definition 3 (Cook-Reckhow)**.** A propositional proof system P is a relation between propositional formulas and binary strings, such that

$$\varphi \text{ is a tautology} \iff \exists \pi : P(\varphi, \pi),$$

and $P(\varphi, \pi)$ can be checked in polynomial time.

Definition 4. The propositional proof system LK (or Sequent Calculus) is the system whose proofs operate on *sequents* which are expressions of the form

$$A_1, \dots, A_n \longrightarrow B_1, \dots, B_m,$$

where A_i's and B_i's are formulas, which is interpreted the same as the formula

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

A valid proof in LK is a list of sequents $\pi = (S_1, \dots, S_k)$ such that each sequent S_i is obtained as one of the initial sequents or from the previous sequents by one of the following rules:

- **Intial sequents:** $0 \longrightarrow$, $\longrightarrow 1$, $p \longrightarrow p$, where p is a propositional variable.
- **Structural rules:**
  - the weakening rules
  $$\frac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta} \text{ and } \frac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A},$$
  - the exchange rules
  $$\frac{\Gamma_1, A, B, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, B, A, \Gamma_2 \longrightarrow \Delta} \text{ and } \frac{\Gamma \longrightarrow \Delta_1, A, B, \Delta_2}{\Gamma \longrightarrow \Delta_1, B, A, \Delta_2},$$
  - the contraction rules
  $$\frac{\Gamma_1, A, A, \Gamma_2 \longrightarrow \Delta}{\Gamma_1, A, \Gamma_2 \longrightarrow \Delta} \text{ and } \frac{\Gamma \longrightarrow \Delta_1, A, A, \Delta_2}{\Gamma \longrightarrow \Delta_1, A, \Delta_2},$$
- **Logical rules:**
  - $(\neg)$-introduction rules:
  $$\frac{\Gamma \longrightarrow \Delta, A}{\neg A, \Gamma \longrightarrow \Delta} \text{ and } \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A},$$

– ($\bigwedge$)-introduction rules

$$\frac{\Gamma \longrightarrow \Delta, A_1 \quad \dots \quad \Gamma \longrightarrow \Delta, A_n}{\Gamma \longrightarrow \Delta, \bigwedge_i A_i} \text{ and } \frac{\Gamma, A_1, \dots, A_n \longrightarrow \Delta}{\Gamma, \bigwedge_i A_i \longrightarrow \Delta},$$

– ($\bigvee$)-introduction rules

$$\frac{\Gamma, A_1 \longrightarrow \Delta \quad \dots \quad \Gamma, A_n \longrightarrow \Delta}{\Gamma, \bigvee_i A_i \longrightarrow \Delta} \text{ and } \frac{\Gamma \longrightarrow \Delta, A_1, \dots, A_n}{\Gamma \longrightarrow \Delta, \bigvee_i A_i},$$

- **The cut rule:**

$$\frac{\Gamma \longrightarrow \Delta, A \quad A, \Gamma \to \Delta}{\Gamma \to \Delta}.$$

Exercise 5. Prove $\longrightarrow \neg(p \wedge \neg p)$ in LK.

Fact 6. The system LK is complete, it proves all tautologies.

Definition 7. A depth of a formula in an LK-proof is defined as follows: Propositional variables and constants have the depth 0, and

$$\text{depth}(\bigwedge(A_1, \dots, A_r)) = 1 + \max_i(\text{depth}(A_i)),$$

$$\text{depth}(\bigvee(A_1, \dots, A_r)) = 1 + \max_i(\text{depth}(A_i)).$$

A system LK_d, or depth d sequent calculus, is a subsystem of LK allowing only formulas of depth at most d.

Exercise 8 (*)**.** The system LK_d proves all depth d tautologies.

Definition 9. The system ELK, or extended sequent calculus, is defined as LK, except is allows for any formula A to add the initial sequents ('extension sequents')

$$q \longrightarrow A \quad A \longrightarrow q,$$

where q is a propositional variable, called the extension variable, which was not used as an extension variable for another formula and does not appear in A.

Fact 10. For each $d \geq 0$, we have $LK_d \leq_p LK \leq_p ELK$, where $P \leq_p Q$ means that proofs of P can be transformed to proofs of Q without more than polynomial each in size.

Theorem 11 (Ajtai, early 1980's, first published 1988)**.** For each $d \geq 2$, the system LK_d does not have polynomial size proofs of the formula PHP_n.

Theorem 12 (Buss, 1987)**.** The system LK does have a polynomial size proofs of PHP_n.

Remark 13. The system LK_d, for any fixed d, is equivalent to a system called bounded-depth Frege (AC_0-Frege), the system LK is equivalent to a system called Frege (F), and ELK is equivalent to a system called extended Frege (EF).

Bounded arithmetic, propositional translations and Ajtai's argument

Definition 14. We say an L_{PA} formula φ is bounded if every quantifier is of the form $(\exists x \leq t(\overline{y}))(\dots)$ or $(\exists x) \leq s(\overline{y})$ and y. The set of all bounded formulas is denoted Δ_0.

Definition 15. Let R be a binary relational symbol and $L_{PA}(R) = L_{PA}(R)$. The theory $I\Delta_0(R)$ consists of Q and induction for all formulas in $\Delta_0(R)$, the bounded $L_{PA}(R)$.

Exercise 16. Show that

$$I\Delta_0(R) \vdash R(c,c) \to (\exists b \leq c)(R(b,b) \wedge (\forall a < b)(\neg R(a,a))),$$

or 'If $R(x,x)$ is non-empty, it has a smallest element.'

Definition 17 (Paris-Wilkie translation)**.** Let $\theta(a_1, \dots, a_k) \in \Delta_0(R)$ and let p_{ij} be a propositional variable for each $i, j \in \mathbb{N}$. For $(n_1, \dots, n_k) \in \mathbb{N}^k$ we define a propositional formula $\langle\theta\rangle_{(n_1,\dots,n_k)}$ by induction on the logical depth:

1. if θ is an atomic formula $s(\overline{n}) = t(\overline{n})$ or $s(\overline{n}) \leq t(\overline{n})$, then
$$\langle\theta\rangle_{\overline{n}} = \begin{cases} 1 & \theta(\overline{n}) \text{ is true} \\ 0 & \text{otherwise.} \end{cases}$$
2. if θ is an atomic formula $R(s(\overline{n}), t(\overline{n}))$, then
$$\langle\theta\rangle_{\overline{n}} = p_{s(\overline{n}),t(\overline{n})}$$
3. $\langle - \rangle_{\overline{n}}$ commutes with $\wedge$, $\vee$, $\neg$
4. if $\theta(\overline{a})$ is of the form $(\forall x \leq t(\overline{a}))\theta_0(\overline{a}, x)$, then
$$\langle\theta\rangle_{\overline{n}} = \bigwedge_{m \leq t(\overline{n})} \langle\theta_0\rangle_{(\overline{n},m)}$$
5. if $\theta(\overline{a})$ is of the form $(\exists x \leq t(\overline{a}))\theta_0(\overline{a}, x)$, then
$$\langle\theta\rangle_{\overline{n}} = \bigvee_{m \leq t(\overline{n})} \langle\theta_0\rangle_{(\overline{n},m)}.$$

Note that for a fixed θ and all $\overline{n}$ the size of $\langle\theta\rangle_{\overline{n}}$ is polynomial in $\overline{n}$ and the depth is constant.

Theorem 18. Assume that $\theta(x) \in \Delta_0(R)$ and that

$$I\Delta_0(R) \vdash (\forall x)\theta(x),$$

then there is a number d such that

$$LK_d \vdash_{poly(n)} \langle\theta\rangle_n.$$

Fact 19. Let F, P be binary relations and E unary. There are $\Delta_0(E, F, P)$ formulas

- $Fla_d(F)$ formalizing that F denotes a depth d DeMorgan formula,
- $Prf_d(P, F)$ formalizing that P is a valid LK_d proof of F which satisfies $Fla_d(F)$,
- $Sat_d(E, F)$ formalizing that E is a satisfying assignment to F,
- $Ref_d(E, F, P) \equiv (Prf_d(P, F) \to Sat_d(E, F))$, the formalization of the reflection principle for LK_d.

Then for every d, we have

$$I\Delta_0(E, F, P) \vdash Ref_d(E, F, P).$$

Definition 20. Let M be a non-standard model of true arithmetic, and let $n \in M \setminus \mathbb{N}$. Then $n^{\mathbb{N}} = \{i \in M; i < n^k; k \in \mathbb{N}\}$.

Theorem 21 (Ajtai's argument)**.** Let $\theta(x) \in \Delta_0(R)$, let M be a non-standard model of true arithmetic, let $n \in M \setminus \mathbb{N}$. Let τ be a set of relational symbols containing R, and let every $R' \in \tau \setminus \{R\}$ be interpreted by a relation $(R')^\alpha$ coded in M. If there is an interpretation of R, denoted R^α, such that

- $(n^{\mathbb{N}}, \tau^\alpha) \models I\Delta_0(\tau)$
- $(n^{\mathbb{N}}, \tau^\alpha) \models \neg\theta(n)$,

then $\langle\theta\rangle_n$ does not have polynomial size proofs in LK_d.

Theorem 22 (Ajtai)**.** For every non-standard model of true arithmetic M, and τ containing R, where each $R' \in \tau \setminus \{R\}$ is interpreted by elements of M as $(R')^\alpha$ there is a relation R^α such that

- $(n^{\mathbb{N}}, \tau^\alpha) \models I\Delta_0(\tau)$
- $(n^{\mathbb{N}}, \tau^\alpha) \models \neg PHP(n)$.

Exercise 23. Prove Theorem 11.

Remark 24. The theory $I\Delta_0(\tau)$ is a bit cumbersome to work with as the objects of our interest, the relations in τ, are not part of the model-theoretic universe. This can be fixed by introducing the theory V_1^0, which is two-sorted (sometimes called 'second order'): it has sorts for numbers and sets of numbers.

For every $\theta \in \Delta_0(R)$ we have

$$I\Delta_0(R) \vdash \theta(R) \iff V_1^0 \vdash (\forall X)\theta(X),$$

the theory V_1^0 contains a few axioms about the sets of numbers, bounded induction without set quantification and comprehension axiom which says that any set definable by a bounded formula without set quantification exists.

A stronger theory V_1^1, which allows comprehension for formulas existentially quantifying sets, then corresponds to polynomial size proofs of ELK in the same way V_1^0 (or $I\Delta_0(R)$) corresponds to polynomial size proofs of (all) LK_d. There is also a theory VNC^1 which corresponds to polynomial size proofs of LK.