Ajtai's argument

Theorem 1. 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

$$LK_d \vdash_{poly(k)} \langle\theta\rangle_k.$$

Fact 2. 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 3. 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 4 (Ajtai's argument)**.** Let $\theta(x) \in \Delta_0(R)$. If for every non-standard model M of true arithmetic, every $n \in M \setminus \mathbb{N}$, every τ set of relational symbols not containing R, where each $E \in \tau$ is interpreted by a relation E^I coded in M, there is an interpretation of R, denoted R^I, such that

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

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

Theorem 5 (Ajtai)**.** For every non-standard model of true arithmetic M, a non-standard $n \in M$, and τ not containing R, where each $E \in \tau$ is interpreted by elements of M as E^I there is a relation R^I such that

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

Exercise 6. Prove that $LK_d \nvdash_{poly} PHP_k$.

Remark 7. 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.