7. Sequent calculus and complexity theory

7.1. Gentzen's formalism of sequents

We now come to the other formalism introduced by Gentzen, namely the sequents calculus (the name, however, is due to Kleene). We want to introduce here the basic concepts and prove the most important result about it, namely cut-elimination. Actually we will not illustrate here the cut elimination for *pure logic*, for which we refer to Girard (1987) or Takeuti (1987), but rather a proof of the *free-cut elimination theorem*, according to which *some* cuts can be eliminated, and of *partial* cut-elimination, i.e. the elimination of cuts on formulas above a given logical complexity, in fact the only results available for *theories* (i.e. logic plus proper axioms and induction rule): we will see that for them *the full cut-elimination is not valid*). Takeuti (1987) only offers a sketch of the proof. The proof we propose was instead presented in Beckmann and Buss (2011) and involves the modification of the definition of anchored and free formulas, also with respect to an earlier version by the first of the two authors. To date, it does not appear in any manual, to our knowledge, and given the originality of the method employed, it seemed appropriate to refer to it. *Free-cut elimination* has important applications in computational complexity. In particular, Buss (1986) applies this result to obtain his "witnessing theorems"in *Bounded Arithmetic*, that is, the important result of characterization of functions computable in polynomial time that we will discuss in the last chapter: for this, we need only to be able to restrict cut formulas to lie in a given complexity class. Like the proof provided by the first author in Buss (1998) for pure logic, this too differs from the various proofs in the scientific literature, starting with Gentzen's, in that it is of the global kind, that is, it is not based on *local* transformations to a proof to reduce measures of complexity as the depth of cuts, the number of cuts, or the so-called rank of a cut. At the opposite here the depth or number of cuts are reduced by making *global* transformations to a proof.

Unlike the natural deduction by Gentzen-Prawitz, of which there are few variants in the literature (Fitch, sequential rules, generalized elimination rules ...) the the sequent calculus has a wide range of variations, which we will try in this section of illustrate and motivate. While in natural deduction and axiomatic systems rules apply to formulas, in the sequent calculus they apply to *assertions of derivability* of form:

$$\alpha_0, ..., \alpha_n \Longrightarrow \beta_0, ..., \beta_m$$

which must be read: "from $\alpha_0 \wedge ... \wedge \alpha_n$ it is derivable $\beta_0 \vee ... \vee \beta_m$". A sequent is therefore a contruction of the form:

$$\Gamma \Longrightarrow \Delta$$

where Γ, Δ can be, according to different versions, sets, sequences, or multisets (that is, sets that admit repetition, such as $\{A, A, B\}$, that as a set would be equivalent to $\{A, B\}$) of formulas; the choice of which data structure to prefer has one immediate consequences in the formulation of the rules. We use the longest arrow $\Longrightarrow$ to denote this derivability. We remark

Duccio Pianigiani, University of Siena, Italy, duccio.pianigiani@unisi.it, 0000-0001-9441-7226

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

Book References DOI 10.36253/979-12-215-0778-2.references

that the big arrow is a *metalinguistic* symbol. A sequent $\alpha_0, ..., \alpha_n \Longrightarrow \beta_0, ..., \beta_m$ has to be therefore intended as the formula $\alpha_0 \wedge ... \wedge \alpha_n \rightarrow \beta_0 \vee ... \vee \beta_m$, where:

(a) $\alpha_0, ..., \alpha_n \Longrightarrow$ must be read $\neg(\alpha_0 \wedge ... \wedge \alpha_n)$.

(b) $\Longrightarrow \beta_0, ..., \beta_m$ has to be read as $\beta_0 \vee ... \vee \beta_m$.

(c) "$\Longrightarrow$" has to be read as $\alpha \wedge \neg\alpha$; to prove the consistency of this calculus, therefore, means just to prove the unprovability of "$\Longrightarrow$".

(d) to prove a formula α means to prove the sequent $\Longrightarrow \alpha$.

(e) Unlike of natural deduction, this calculus has no elimination rules and introduction rules, but only introduction rules, right and left: the only one way to delete a connective or a quantifier, is to delete the entire formula where is contained, by means of a rule called CUT.

(f) The calculus is not subject to certainty typical asymmetries of natural deduction for full language, which we can find for example in the rule of elimination of $\vee$.

(g) Moerover it has a further collection of extremely important rules called structural rules; unlike the natural Gentzen-Prawitz deduction, this calculus has axioms.

Let us consider the propositional calculus PK defined in this way (see Buss (1998)). Suppose the sequents are made up of *sequences* of formulas.

Logical axioms $\alpha \Longrightarrow \alpha$ (where α is atomic).

Logical rules

$$\frac{\Gamma \Longrightarrow \Delta, \alpha}{\neg\alpha, \Gamma \Longrightarrow \Delta} \qquad \frac{\alpha, \Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \neg\alpha}$$

$$\frac{\Gamma \Longrightarrow \Delta, \alpha \quad \beta, \Gamma \Longrightarrow \Delta}{\alpha \rightarrow \beta, \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma, \alpha \Longrightarrow \Delta, \beta}{\Gamma \Longrightarrow \Delta, \alpha \rightarrow \beta}$$

$$\frac{\Gamma, \alpha, \beta \Longrightarrow \Delta}{\Gamma, \alpha \wedge \beta \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \alpha \quad \Gamma \Longrightarrow \Delta, \beta}{\Gamma \Longrightarrow \Delta, \alpha \wedge \beta}$$

$$\frac{\Gamma, \alpha \Longrightarrow \Delta \quad \beta, \Gamma \Longrightarrow \Delta}{\alpha \vee \beta, \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \alpha, \beta}{\Gamma \Longrightarrow \Delta, \alpha \vee \beta}$$

The reader who already knows Natural Deduction can think that left rules correspond to elimination rules and the right rules correspond to introduction rules.

To the logical rules, we must add the structural rules:

Exchange

$$\frac{\Gamma, \alpha, \beta, \Pi \Longrightarrow \Delta}{\Gamma, \beta, \alpha, \Pi \Longrightarrow \Delta} \qquad \frac{\Delta \Longrightarrow \Gamma, \alpha, \beta, \Pi}{\Delta \Longrightarrow \Gamma, \beta, \alpha, \Pi}$$

Contraction

$$\frac{\alpha, \alpha, \Gamma \Longrightarrow \Delta}{\alpha, \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \alpha, \alpha}{\Gamma \Longrightarrow \Delta, \alpha}$$

Weakening

$$\frac{\Gamma \Longrightarrow \Delta}{\alpha, \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta, \alpha}$$

Observe that if the calculus is formulated in terms of *sets*, then *exchange* and *contraction* are superfluous, since $\{A, A\} = \{A\}$ e $\{A, B\} = \{B, A\}$ are properties of sets; if on the contrary is formulated in terms of multisets $\{A, A\} \neq \{A\}$ and only the exchange is not necessary; lastly, if the axioms are formulated as: $\Theta \Longrightarrow \Psi$, where $\Theta \cap \Psi \neq \emptyset$ (e.g. $\alpha, \Gamma \Longrightarrow \alpha, \Sigma$), then the weakening rule is superfluous.

Lastly we have the (fundamental) rule of CUT:

$$\frac{\Gamma \Longrightarrow \Theta, \alpha \quad \alpha, \Gamma \Longrightarrow \Theta}{\Gamma \Longrightarrow \Theta}$$

The CUT rule can be intuitively interpreted in this way: divide the derivation of Θ from Γ into two *lemmas* which are subsequently reunited. A sequent calculus is *closed for cut*, if for any derivation there is another derivation of the same sequent, which does not make use of CUT. The sequences $\Gamma, \Delta, \Pi, \Theta...$ in the above rules are called *cedents*, whose formulas are called *side formulas*; in the sequent $\Gamma \Longrightarrow \Delta$, the sequence Γ is the *antecedent*, and Δ is the *consequent*. In the rules:

$$\frac{S_0 ... S_n}{S}$$

the sequents $S_0, ..., S_n$ are called *upper* sequents S is the *lower* sequent. In the conclusion of a rule, the formula that does not belong to cedents constitutes the *principal* formula (in axioms $\alpha \Longrightarrow \alpha$, both α are considered principal), while the formulas (not belonging to the cedents) of the premises, from which derives the principal formula, are called *active* (sometimes called *auxiliary* of the principal).

The first order calculus LK is obtained but adding to PK the following rules.

Universal $\forall : left$ and $\forall : right$ rules:

$$\frac{\phi(t), \Gamma \Longrightarrow \Delta}{\forall x \phi(x), \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \phi(y)}{\Gamma \Longrightarrow \Delta, \forall x \phi(x)}$$

Existential $\exists : left$ and $\exists : right$ rules:

$$\frac{\phi(y), \Gamma \Longrightarrow \Delta}{\exists x \phi(x), \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \phi(t)}{\Gamma \Longrightarrow \Delta, \exists x \phi(x)}$$

In $\forall : right$ and $\exists : left$ the *eigenvariable* $y \notin FVar(\Gamma, \Delta)$.

Definition 51. *Ancestors and descendents:*

(a) If ϕ is side and occours in a cedent Γ of an upper sequent, then the immediate descendent *of ϕ is the correspondent occurrence ϕ in the same position of the correspondent cedent Γ in the lower sequent.*

(b) In the exchange rule, say between ϕ and ψ, the immediate descendants of these ϕ and ψ, are still the ϕ and ψ in the lower sequent.

(c) If ϕ is active (auxiliary) in a rule that is not exchange or cut, then the immediate descendent is the principal formula.

(d) We say that ϕ is an immediate ancestor *of ψ if and only if ψ is an immediate descendent of ϕ. Formulas in the initial sequents and of a weakening have non immediate ancestors.*

(e) The cut formula has no descendants in an application of CUT.

(f) ϕ is a descendant *of ψ iff there is a chain of length ≥ 0 (reflexive and transitive closure) of immediate descendant from ψ to ϕ. Analogously we define the ancestor relation as the reflexive and transitive closure of the relation of immediate ancestor.*

(g) ϕ *is a* direct immediate descendant *of* ψ *(analogously* immediate direct ancestor*), iff it is an immediate descendant and* $\psi = \phi$.

We would like to briefly highlight the role and effect of the structural rules. Admitting the weakening rule, actually we admit in fact the *a fortiori* principle:

$$\dfrac{\dfrac{\dfrac{\alpha \Longrightarrow \alpha}{\alpha, \beta \Longrightarrow \alpha}}{\alpha \Longrightarrow (\beta \to \alpha)}}{\Longrightarrow \alpha \to (\beta \to \alpha)}$$

As well as, analogously, admitting the Contraction rule, we admit the law of absorption:

$$\dfrac{\dfrac{\alpha \Longrightarrow \alpha \quad \dfrac{\alpha \Longrightarrow \alpha \quad \beta \Longrightarrow \beta}{\alpha \to \beta, \alpha \Longrightarrow \beta}}{(\alpha \to (\alpha \to \beta)), \alpha, \alpha \Longrightarrow \to \beta}}{(\alpha \to (\alpha \to \beta)), \alpha \Longrightarrow \beta}}{\Longrightarrow (\alpha \to (\alpha \to \beta)) \to (\alpha \to \beta)}$$

Remember that these principles are *not* accepted in some non classical logic. For example the *a fortiori* is not accepted by the Relevant Logic, absorption is not accepted in the infinite-valent logics of Łukasiewicz etc. Therefore many formalizations in terms of sequent of these logics avoid some or all of the structural rules. This introduces to the topic of *substructural* logics (i.e. with limitation or absence of structural rules) and of Linear Logic. In the classical *propositional* calculus (unlike the intuitionist one), the contraction rule is actually redundant. Ketonen and Solovay (1981) showed instead that the classical *predicates* calculus without the contraction rule is decidable.

There are various reasons for formulating the rules as in PK, for example in this form they are invertible. A rule is called invertible in a sequent calculus system of a proof of its conclusion implies the existence of proofs of each of its premises. Conversely, to make those on quantifiers invertible, they must be formulated as follows:

Universal

$$\dfrac{\phi(t), \forall x \phi(x), \Gamma \Longrightarrow \Delta}{\forall x \phi(x), \Gamma \Longrightarrow \Delta} \qquad \dfrac{\Gamma \Longrightarrow \Delta, \phi(y)}{\Gamma \Longrightarrow \Delta, \forall x \phi(x)}$$

In the right rule, $y \notin FVar(\Gamma, \Delta)$ and if $y \neq x$, $y \notin FVar(\phi)$.

Existential

$$\dfrac{\phi(y), \Gamma \Longrightarrow \Delta}{\exists x \phi(x), \Gamma \Longrightarrow \Delta} \qquad \dfrac{\Gamma \Longrightarrow \Delta, \exists x \phi(x), \phi(t)}{\Gamma \Longrightarrow \Delta, \exists x \phi(x)}$$

In the left rule, $y \notin FVar(\Gamma, \Delta)$ e, se $y \neq x$, $y \notin FVar(\phi)$.

Note that in the rules above, the main formula has been repeated in the upper sequent, on the same side. The systems G3c and G3i invertible and closed for cut and contraction are essentially based on this idea, although in the intuitionistic case G3i the left-hand rule of implication will also have to undergo a similar modification (see Troelstra and Schwichtenberg (2000)).

Another distinction that needs to be made, which does not coincide with the previous one, is that between additive and multiplicative rules: in the presence of structural rules these two formulations are equivalent, but in their *absence* they introduce, on the contrary, connectives with distinct meaning. For example (see Girard, Lafont and Taylor (1989)), regarding

conjunction and disjunction, we have a pair of *multiplicative* connectives $\otimes$ (times) and $\wp$ (par) with rules:

$$\frac{\Gamma \Longrightarrow \Theta, \alpha \quad \Sigma \Longrightarrow \Pi, \beta}{\Gamma, \Sigma \Longrightarrow \Theta, \Pi, \alpha \otimes \beta} \qquad \frac{\Gamma, \alpha, \beta \Longrightarrow \Delta}{\Gamma, \alpha \otimes \beta \Longrightarrow \Delta}$$

$$\frac{\Gamma, \alpha \Longrightarrow \Theta \quad \Sigma, \beta \Longrightarrow \Pi}{\Gamma, \Sigma, \alpha \wp \beta \Longrightarrow \Theta, \Pi} \qquad \frac{\Gamma \Longrightarrow \Delta, \alpha, \beta}{\Gamma \Longrightarrow \Delta, \alpha \wp \beta}$$

and *additive* connectives & (and) e $\oplus$ (plus):

$$\frac{\Gamma \Longrightarrow \Theta, \alpha \quad \Gamma \Longrightarrow \Theta, \beta}{\Gamma \Longrightarrow \Theta, \alpha \& \beta} \qquad \frac{\Gamma, \alpha \Longrightarrow \Delta}{\Gamma, \alpha \& \beta \Longrightarrow \Delta} \qquad \frac{\Gamma, \beta \Longrightarrow \Delta}{\Gamma, \alpha \& \beta \Longrightarrow \Delta}$$

$$\frac{\Gamma, \alpha \Longrightarrow \Theta \quad \Gamma, \beta \Longrightarrow \Gamma}{\Gamma, \alpha \oplus \beta \Longrightarrow \Theta} \qquad \frac{\Gamma \Longrightarrow \Delta, \alpha}{\Gamma \Longrightarrow \Delta, \alpha \oplus \beta} \qquad \frac{\Gamma \Longrightarrow \Delta, \beta}{\Gamma \Longrightarrow \Delta, \alpha \oplus \beta}$$

In the presence of the structural rules, the two previous formulations are equivalent. In the presence of only the *Weakening*, $\otimes$ is stronger than &:

$$\frac{\dfrac{\dfrac{\alpha \Longrightarrow \alpha}{\alpha, \beta \Longrightarrow \alpha} \quad \dfrac{\beta \Longrightarrow \beta}{\alpha, \beta \Longrightarrow \beta}}{\alpha, \beta \Longrightarrow \alpha \& \beta}}{\alpha \otimes \beta \Longrightarrow \alpha \& \beta}$$

To show the equivalence we need *Contraction*[1].

Gentzen's original LK for classical logic is actually a little bit different from ours: also in that case sequents are sequences of formulas, axioms are of the form $\alpha \Longrightarrow \alpha$ (α atomic), all structural rules and CUT (in a moltiplicative form) are included, but the right rule for $\vee$ and left rule for $\wedge$ are in the *additive* version.

Sequent calculus for intuitionistic logic. The intuitionistic calculus LJ is obtained by imposing to LK a restriction on the form of sequents, namely that in $\Gamma \Longrightarrow \Delta$, the Δ is authorised to have at most oneformula. From the restriction on the shape of the sequents it follows automatically others on the form of the rules: for example *Exchange* right and *Contraction* right will be deleted and *Weakening* rigth will have the form:

$$\frac{\Gamma \Longrightarrow}{\Gamma \Longrightarrow \phi}$$

It should be noted that the additive intuitionist rules, in the presence of the permitted structural rules, are not equivalent to the corresponding multiplicatives, being implied by the latter, but not implying. The intuitionist structural rules allow to demonstrate the equivalence between multiplicative formulation and additive of the rules for the $\wedge$, but not for $\vee$. Ultimately, the calculs LJ has for $\vee$ the additive form and for $\rightarrow$ the multiplicative form.

Let's see a consequence of these restriction, considering a sequent $\Longrightarrow \alpha \vee \beta$ obtained without CUT: what is the last rule applied? It cannot be *Weakening*, because otherwise we would have previously had a derivation of $\Longrightarrow$, the empty sequence, i.e. a contradiction; but, as we shall see, this is not possible, since from the cut-elimination theorem it follows the consistency of the calculus, and in particular of LJ. It cannot be a right *Contraction* because otherwise we had $\Longrightarrow \alpha \vee \beta, \alpha \vee \beta$ as upper sequent, which is not an intuitionistic sequent. Then the

[1] Another important variant for the classical or for linear calculus which should be mentioned is the *one-side* version, based on the following argument: in a sequent $\alpha_0, ..., \alpha_n \Longrightarrow \beta_0, ..., \beta_m$ bringing all the formulas on the right (see the rules on negation) we obtain a sequent of the form: $\Longrightarrow \neg\alpha_0, ..., \neg\alpha_n \beta_0, ..., \beta_m$ that can be written simply as $\neg\alpha_0, ..., \neg\alpha_n, \beta_0, ..., \beta_m$. Negation cannot be a primitive symbol: rather, to each propositional variable p is associated its complement $\overline{p}$ and the inductively $\neg p = \overline{p}$,$\neg(p \wedge q) = (\neg p \vee \neg q)$ etc.

last ruel must be a right logical rule. It follows that in LJ, if $\Longrightarrow \alpha \vee \beta$ is derivable, then either $\Longrightarrow \alpha$, or $\Longrightarrow \beta$ is derivable. In particular it is not derivable $\Longrightarrow \alpha \vee \neg\alpha$: if α is atomic then we would have either $\Longrightarrow \alpha$, or $\Longrightarrow \neg\alpha$ but neither is, for α atomic. For the same reasons, if $\Longrightarrow \exists x\phi(x)$ is derivable in LJ, then $\Longrightarrow \phi(t)$ also is. A correspondence with natural deduction as in 74 is given by considering that proofs in LJ can be (not 1-1) translated in natural deduction derivations in which right rules correspond to introduction and left rules to elimination (see Girard, Lafont and Taylor (1989) pp. 43-49).

We finally arrive at the *Cut elimination.* The so called *Hauptsatz* is a weak normalization theorem, i.e. a *strategy* of normalization (for a discussion on strong normalization results see e.g. Urban and Bierman (2001)). Famous achievements due to Statman and Orevkov say that this algorithm for classical predicate calculus cannot be, in general, efficient. The methods of cut-elimination most frequently traceable in the scientific literature (with significant variants), are in general derived, either from the original one in Gentzen (1935), introduced with the aim of giving a consistency proof for Peano arithmetic (see e.g. Takeuti (1987)), or from Tait (1968). The *Hauptsatz* theorem for pure logic has important consequences, in first place the principle of *subformula*, where this notion is specified as follows:

Definition 52. *this is Gentzen's notion of a dottoformula:*

(a) if $\phi = p$, then the unique subformula of ϕ is p.

(b) If $\phi = \phi_0 \wedge \phi_1$ then the subformulas of ϕ are ϕ the subformulas of ϕ_0 and of ϕ_1.

(c) Analogously for $\phi_0 \vee \phi_1$, $\phi_0 \to \phi_1$.

(d) If $\phi = \neg\phi_0$, the subformulas of ϕ are ϕ and the subformulas of ϕ_0.

(e) If $\phi = \forall x\phi_0$, the subformulas of ϕ are ϕ and the subformulas of $\phi_0(t)$ for all terms t. Analogously for $\exists x\phi_0$.

As for the quantified formulas, notice that, since there are infinite variables, this formulas have infinite subformulas.

Corollary 21. (Principle of the subformula) *In a* cut-free *proof of $\Gamma \Longrightarrow \Delta$, all sequents consist of subformulas of formulas in Γ, Δ.*

Proof. Simply observe that, in the absence of *CUT*, in the proof in question will only need logical rules and structural rules; but in both cases, in the logical rules and in the structural ones, the upper sequents are made up of subformulas of the lower sequents. Remember that only the *CUT* rule eliminates formulas QED

However the cut-elimination theorem *does not hold* (in its general form) if there are specific axioms: a simple counterexample (see Girard (1987)) is the following. Let $\Longrightarrow \phi$ e $\Longrightarrow (\gamma \to \delta)$ sequents that represent proper axioms and consider the derivation:

$$\dfrac{\Longrightarrow \gamma \qquad \dfrac{\Longrightarrow (\gamma \to \delta) \qquad \dfrac{\gamma \Longrightarrow \gamma \quad \delta \Longrightarrow \delta}{\gamma, \gamma \to \delta \Longrightarrow \delta}}{\gamma \to \delta}}{\Longrightarrow \delta}$$

How to obtain a cut-free proof of $\Longrightarrow \delta$? However, there is one "partial" form of this result, also dating back to Gentzen, which we will state. To what extent is it possible to eliminate cuts in $\mathsf{LK} + \Psi$ proofs, where Ψ is a set of initial sequents closed under substitution? For instance, the first order logic with equality is obtained by adding the following sequents:

(a) $\Longrightarrow s = s$

(b) $s = t, t = r \Longrightarrow s = r$

(c) $s = t \Longrightarrow t = s$

(d) $s_0 = t_0, ..., s_k = t_k \Longrightarrow f(s_0, ..., s_k) = f(t_0, ..., t_k)$

(e) $s_0 = t_0, ..., s_k = t_k, P(s_0, ..., s_k) \Longrightarrow P(t_0, ..., t_k)$

The elementary axioms of arithmetic P^- can be expressd by sequents:

(a) $\Longrightarrow x + \overline{0} = x$

(b) $\Longrightarrow x + s(u) = S(x + u)$

(c) $\Longrightarrow x \cdot \overline{0} = \overline{0}$

(d) $\Longrightarrow x \cdot S(u) = x \cdot u + x$

(e) $x < 0 \Longrightarrow$

(f) $u < x \Longrightarrow u < S(x)$

(g) $u = x \Longrightarrow u < S(x)$

(h) $u < S(x) \Longrightarrow u = x, u < x$

(i) $\Longrightarrow u < x, u = x, x < u$

(j) $S(x) = 0 \Longrightarrow$

(k) $S(x) = S(u) \Longrightarrow x = u$

A set of sequents Ψ is *closed under substitution*, iff for all $\Gamma(x) \Longrightarrow \Delta(x)$ in Ψ and all terms t, also $\Gamma[t/x] \Longrightarrow \Delta[t/x]$ is in Ψ. The account offered in Buss (1998) of the free-cut elimination theorem proceeds as follows.

Definition 53. *Let π a proof $\mathsf{LK} + \Psi$; say that a formula of π is* anchored *at a sequent in Ψ, iff it is a direct descendant of a formula occurring in an initial sequent in Ψ. A cut inference is* anchored *iff at least one of the two occurrences of the cut formulas is anchored, and is* free *iff both of these occurrences of the cut formulas in the upper sequents are not anchored (i.e. are* free*). A proof is called* free-cut-free *if does not contain free cuts (i.e. all cuts are anchored).*

Theorem 107. *If Ψ is a set of sequents closed under substitution and there is a proof of $\Gamma \Longrightarrow \Delta$ in $\mathsf{LK} + \Psi$, then there exists a proof free-cut-free of the same sequent in $\mathsf{LK} + \Psi$.*

To conclude, in the applications of sequent calculus to formal arithmetic and to the fragments of arithmetic, it is customary to add an induction rule, that *in this form*:

$$\Phi - \mathsf{IND} = \frac{\phi(x), \Gamma \Longrightarrow \Delta, \phi(x+1)}{\phi(0), \Gamma \Longrightarrow \Delta, \phi(t)}$$

where $\phi \in \Phi$, for a class of formulas Φ, is equivalent to the induction axiom. Let us call $\phi(0)$ e $\phi(t)$ the *principal formulas* of this inference.

If $\mathsf{T} = \mathsf{LK} + \Psi + \Phi - \mathsf{IND}$ is an arithmetical theory formalized in sequent calculus (where Ψ are the specific axioms and both Ψ, Φ are closed under substitution), then an occurrence of a formula in a derivation in T is called *anchored* iff it is *direct descendant* of a formula occourring in a sequent of Ψ, *or a direct descendant of a principal formula of an induction.*

Theorem 108. *The following hold:*

(a) if $T = \mathsf{LK} + \Psi + \Phi - IND$ is a theory of formal arithmetic and Ψ, Φ are closed under substitution and $\Gamma \Longrightarrow \Delta$ follows from T, then exists a free-cut-free proof of the same sequent in T.

(b) If Φ, the class of formulas on which induction is allowed is closed under substitution and subformulas (e.g. $\Sigma_n \cup \Pi_n$) and all all sequents in Ψ is made of formulas from Φ and all formulas in $\Gamma \Longrightarrow \Delta$ are in Φ , then each formula occurring in the proof is in Φ.

7.2. Free-cut elimination: a more recent proof

What we briefly summarised was the version proposed in Buss (1998). We present here the detailed proof in Beckmann and Buss (2011) of the free-cut elimination theorem, according to which any provable sequent can be proved using only cuts in which at least one cut-formula was *anchored*. The aim of this paper was to correct and strengthen the previous upper bounds, after an inaccuracy was noted in the estimates of the size of free cut. This refinement actually involved a slight modification of the previous definition of *anchored* and *free* formulas, as well as the definition of the *depth* of a cut formula. In the above version, a formula was *anchored* if at least one of the places it is introduced is an anchor; cuts in which neither cut formula was anchored were called *free* and and it was shown that that any provable sequent is provable by a proof in which no cuts are free. In the most recent improvement we are showing, every place the formula is introduced is considered to be an anchor. A generic set $\Im$ of axioms or inference rules is actually added to which to anchor the cuts.

Definition 54. *A skeleton consists of a rule with k-hypothesis, for $k \geq 0$:*

$$\frac{\Psi_1, C_1 \Longrightarrow D_1, \Xi_1, ..., \Psi_k, C_k \Longrightarrow D_k, \Xi_k}{\Psi, C \Longrightarrow D, \Xi}$$

where cedents Ψ, Ξ contain the principal formulas and the cedents Ψ_i, Ξ_i contain the auxiliary formulas, C, C_i, D, D_i are metavariables for cedents that contain the side formulas. If $k = 0$, there are no upper sequents.

Moreover we have:

(a) side formulas indicators $s_1, ..., s_k \in \{0, 1\}$ indicating which hypothesis have side formulas.

(b) Lastly, we possibly have eigenvariables $a_1, ..., a_k$, that may appear each in exactly one upper sequent.

An *instance* of a skeleton is obtained as follows: let Γ, Δ be any cedents not containing *eigenvariables*; if $C = \Gamma$ and $D = \Delta$, then for each $i \leq k$, if $s_i = 1$, then $C_i = \Gamma$ and $D_i = \Delta$; if $s_i = 0$, then C_i, D_i are empty.

A set of inferences $\Im$ is *acceptable*, provided it is the union of all instances of some set of skeletons.

Some examples of acceptable sets of inferences are the following.

(a) Set of non logical axioms (with $k = 0$).

(b) *Induction*, for each $\phi(x)$ arithmetic (or belonging to a specific class as Σ_k), there is a skeleton with (necessarily!) $s_1 = 1$ and $k = 1$:

$$\frac{\phi(b), C_1 \Longrightarrow D_1, \phi(A(b))}{\phi(0), C \Longrightarrow D, \phi(t)}$$

(c) Negri-Von Plato quantifier -free axioms:

$$\frac{q_1, C_1 \Longrightarrow D_1, ..., q_k, C_k \Longrightarrow D_k}{p_1, ..., p_m, C \Longrightarrow D}$$

with q_i, p_j atomic.

(d) Logical rules (see below).

Moreover, the following complexity measures are adopted:

(a) Size of a proof $|\pi|$=total number of non structural inferences, without considering initial sequents.

(b) Height of a proof $h(\pi)$= maximum number of non-structural inferences on any branch , without considering initial sequents.

Ancestors. Let C, C' be two occurrences of the same formula in a proof π. We say that C' is an *immediate direct ancestor* of C, where C' appears in an upper sequent and C in the lower sequent of a logical or $\Im$ inference, if:

(a) C, C' occupy the same position in Γ, Δ of the respective sequents, or

(b) in contraction, they are occurrences of the contracted formula, or

(c) in exchange of ϕ, ψ occurrences C and C' are both ψ or both ϕ.

(d) Principal formulas of weakening, or of logical inferences, or of logical axioms, or formulas in Ψ, Ξ of $\Im$ do not have immediate direct ancestors.

The $\Im$-*depth* of an occurrence C of a formula is defined as follows:

(a) formulas in Ψ, Ξ of $\Im$ have $depth(C) = 0$.

(b) If C is in a logical axiom, $depth(C) = 1$.

(c) If C is in the lower sequent of a structural rule, or it is a side formula of a non structural rule, then:

$$depth(C) = max\{depth(C') | C' \ immediate \ direct \ ancestor \ of \ C\}$$

If a set is empty, then its maximum is defined as $-\infty$.

(d) If C is principal in a non $\Im$ rule and non structural rule, then:

$$depth(C) = 1 + max\{depth(C') | C' \ is \ auxiliary\}$$

(e) The depth of a CUT is the *minimum* of the depths of the cut formulas.

(f) The depth of a proof is the maximum of the depth of its CUT rules.

Anchored cuts. A CUT is *anchored*, if one occurrence C of its cut-formulas has $depth(C) = 0$. A CUT is *free* if either one occurrence of its cut formulas has depth=$-\infty$, or the cut formulas are atoms and one occurrence has depth=1, or it is not anchored.

Note that a *non free cut has depth* 0. A proof is *free cut-free*, if it has no *free cuts*: we are going to prove a *free-cut elimination* theorem.

Definition 55. *Let $\pi' \preccurlyeq \pi$ means that the proofs π, π' have the same endsequent, and each formula occurring in it has depth in π' less or equal than in π.*

Theorem 109. *For each proof π there is a proof π' of the same sequent with no depth $-\infty$ cuts, such that $|\pi'| \leq |\pi|$, and $h(\pi') \leq h(\pi)$ and the depth of π' is less or equal to the depth of π. Furthemore $\pi' \preccurlyeq \pi$.*

We prove a refined form of the theorem: remove an arbitrary set of formulas of depth $-\infty$ from the endsequent of π; then you can get a proof π' of what is left that has no cuts of depth $-\infty$ and such that $|\pi'| \leq |\pi|$ and $h(\pi') \leq h(\pi)$ and the depth of π' is less or equal of the depth of π and $\pi' \preccurlyeq \pi$.

Proof. Induction on $|\pi|$. Let us see the case in which the last rule is:

$$\frac{\Gamma \Longrightarrow \Delta, \alpha \quad \Gamma \Longrightarrow \Delta, \beta}{\Gamma \Longrightarrow \Delta, \alpha \wedge \beta}$$

Claim. Find a proof of $\Gamma' \Longrightarrow \Delta', (\alpha \wedge \beta)'$, the lower sequent of the above inference where some formulas of depth $-\infty$ has been removed and where $(\alpha \wedge \beta)'$ means that this formula has depth $-\infty$ and has been deleted, or is not among the formulas of this depth that have been deleted, or is just $\alpha \wedge \beta$ of depth $\neq -\infty$. QED

(a) In case $(\alpha \wedge \beta)'$, and this formula has depth $-\infty$ and has been deleted and we would give a proof of $\Gamma' \Longrightarrow \Delta'$. Since by convention $1 + (-\infty) = -\infty$, the formulas α and β in the upper sequents have depth $-\infty$. Just apply (IH) to the subproofs π_1 and π_2 of the upper sequents and from any of the resulting proofs you can get π_i' of $\Gamma' \Longrightarrow \Delta'$.

(b) In the other cases, just apply (IH) to the subproofs of the upper sequents to give a proof of $\Gamma' \Longrightarrow \Delta', \alpha \wedge \beta$

Note that in transformations 1. and 2. the depth of the formulas in the endsequent has not been increased. This follows from the definition of "depth" and by (IH).

Il the last rule is CUT:

$$\frac{\Gamma \Longrightarrow \Delta, \alpha \quad \alpha, \Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta}$$

By (IH) there are subproofs π_1', π_2' respectively of $\Gamma' \Longrightarrow \Delta', \alpha$ and $\alpha, \Gamma' \Longrightarrow \Delta'$ as required. In case in one of these two subproofs the formula α has depth $-\infty$, just apply once more (IH) to it and obtain a proof of $\Gamma' \Longrightarrow \Delta'$. Otherwise apply CUT to $\Gamma' \Longrightarrow \Delta', \alpha$ and $\alpha, \Gamma' \Longrightarrow \Delta'$ and note that the cut inference has depth $> -\infty$.

If the last rule is a $\Im$ rule, note that only the side formulas in that case may have depth $-\infty$. Hence just apply (IH).

If the last rule is structural, the proof is trivial.

Theorem 110. (Free-cut elimination) *Let π be a proof of depth $\leq d$ for $d \geq 0$. Then another proof π' exists of the same endsequent which contains no free cuts. Moreover:*

(a) $h(\pi') < 2^{h(\pi)+1}_{d+1}$.

(b) $|\pi'| < c^{2^{|\pi|+1}_{d+1}}$, *where c is the maximum of 2 and the maximum arity of $\Im$ inferences in π.*

where $2^k_0 = k$ and $2^k_{m+1} = 2^{2^k_m}$.

The theorem follows from this Lemma.

Lemma 35. *Suppose π ends with a free cut of depth $d \geq 0$ and all other free cuts above have depth $< d$. Then another proof π' exists of the same endsequent, such that all free cuts in π' have depth $< d$.*

Moreover:

(a) $h(\pi') \leq 2 \cdot h(\pi)$ *and* $\pi' \preccurlyeq \pi$.

(b) If the cut is not atomic $|\pi'| \leq |\pi|^2$; *otherwise* $|\pi'| \leq (c-1)|\pi|^2$.

Proof. By induction on the size $|\pi|$. Suppose π ends with the free cut inference:

$$\dfrac{\dfrac{\pi_1}{\Gamma \Longrightarrow \Delta, \alpha} \quad \dfrac{\pi_2}{\alpha, \Gamma \Longrightarrow \Delta}}{\Gamma \Longrightarrow \Delta}$$

where one occurrence of the cut-formula has depth d and the other has depth $\geq d$.

(a) If α is not atomic. We see the possible cases.

(a) $\alpha = \neg\beta$. Notice that, being $d \geq 0 > -\infty$, the formula not being atomic and the cut being free, this by definition means that the cut is actually *not anchored*, and this implies that for both cut formulas actually $d \geq 1$. Find all direct ancestors of $\neg\beta$ in π_1 that have no immediate direct ancestors (the points where this formula originates). These can be:

(i) The principal formula of a Weakening.

(ii) An $\Im$-inference.

(iii) A right rule:

$$\dfrac{\beta, \Pi \Longrightarrow \Lambda}{\Pi \Longrightarrow \Lambda, \neg\beta}$$

In case (iii), if $\neg\beta$ as a cut formula has depth d, in this inference has therefore depth $\leq d$ and β has depth $< d$.

This kind of inference will be replaced by:

$$\dfrac{\dfrac{\beta, \Pi \Longrightarrow \Lambda}{weak + exchange}}{\Pi, \beta \Longrightarrow \Lambda, \neg\beta}$$

Note that $\neg\beta$, being introduced by weakening, has here depth $-\infty$.

By means of structural rules the β in the antecedent of the lower sequent propagates as a side formula down in the proof, using weakening to add it when necessary, so that we get a proof π_1' of:

$$\Gamma, \beta \Longrightarrow \Delta, \neg\beta$$

where, after this transformation, direct ancestors of $\neg\beta$ can originate only from weakening (i) or $\Im-$inferences (ii), since logical axioms are atomic and therefore $\neg\beta$ cannot occur in a logical axiom. Hence in the final sequent of such a proof, by definition of "depth", $\neg\beta$ has depth ≤ 0.

(a) if $depth(\neg\beta) = -\infty$ in the endsequent of π_1', then use the first theorem to get a proof π_1'' of $\Gamma, \beta \Longrightarrow \Delta$.

(b) if $depth(\neg\beta) = 0$ in the endsequent of π_1', then obtain π_1'' as follows:

$$\dfrac{\dfrac{\pi_1'}{\Gamma, \beta \Longrightarrow \Delta, \neg\beta} \quad \dfrac{\neg\beta, \Gamma \Longrightarrow \Delta}{\neg\beta, \Gamma, \beta \Longrightarrow \Delta}}{\Gamma, \beta \Longrightarrow \Delta}$$

The cut formula in the right upper sequent has depth≥ 1 by the hypothesis of the theorem, whereas the left-hand occurrence has depth 0. Thus the cut has depth 0 and in anchored (not free!).

Now make a similar contruction on the right upper sequent of the initial cut inference, transforming π_2 in π_2'', a proof of $\Gamma \Longrightarrow \beta, \Delta$ and observe that if $\neg\beta$ had depth d in the endsequent of π_2, then β will have depth $< d$ in the endsequent of π_2''.

Hence we can cross π_1'' and π_2'' making a cut on β of depth $< d$ and obtaining the desired proof π' of $\Gamma \Longrightarrow \Delta$.

Now observe that:

(a) $h(\pi') = max\{h(\pi_1'') + 1, h(\pi_2'') + 1\}$
$\leq max\{h(\pi_1') + 2, h(\pi_2') + 2, h(\pi_1) + 2, h(\pi_2) + 2\}$
$\leq max\{h(\pi_1) + 2, h(\pi_1) + 2\} = h(\pi) + 1 < 2 \cdot h(\pi)$

(b) $|\pi'| \leq (|\pi_1'| + |\pi_2| + 1) + (|\pi_2'| + |\pi_1| + 1) + 1 \leq 2 \cdot |\pi_1| + 2 \cdot |\pi_2| + 1 < |\pi|^2$

Notice that $|\pi_i'| < |\pi_i|$, due to the removal of at least an introduction of the negation from π_i. From the construction it follow that $\pi' \preccurlyeq \pi$.

(b) $\alpha = \beta \vee \gamma$. How can this formula be generated in π_1 as a principal formula (i.e. as a first ancestor of a sequence of occurrences)? By a logical rule (i) (right introduction of $\vee$):

$$\frac{\Pi \Longrightarrow \Lambda, \beta, \gamma}{\Pi \Longrightarrow \Lambda, \beta \vee \gamma}$$

or by a $\Im-$inference (ii) or by a weakening (iii). First replace all the inferences of case (i.) by:

$$\frac{\dfrac{\Pi \Longrightarrow \Lambda, \beta, \gamma}{weakening + exchange}}{\Pi \Longrightarrow \beta, \gamma, \Lambda, \beta \vee \gamma}$$

and add structural rules to propagate β, γ down in the proof and obtain a proof π_1' of $\Gamma \Longrightarrow \beta, \gamma, \Delta, \beta \vee \gamma$.

Note that if $\beta \vee \gamma$ had depth d in the endsequent of π_1, then the occurrences of β, γ in the endsequent of π_1' have depth $< d$, while the depth of $\beta \vee \gamma$ in the endsequent of π_1' has depth ≤ 0 (i.e. 0 or $-\infty$). Now the depth of $\beta \vee \gamma$ in the endsequent of π_1' is 0 or $-\infty$:

(a) If the depth is $-\infty$ (case (iii.)), then use once more the first theorem to find a proof π_1'' of $\Gamma \Longrightarrow \beta, \gamma, \Delta$.

(b) If this depth is 0 (case ii.), form π_1'' as follows:

$$\frac{\dfrac{\pi_1'}{\Gamma \Longrightarrow \beta, \gamma, \Delta, \beta \vee \gamma} \quad \dfrac{\dfrac{\beta \vee \gamma, \Gamma \Longrightarrow \Delta}{structural\ rules}}{\beta \vee \gamma, \Gamma \Longrightarrow \beta, \gamma, \Delta}}{\Gamma \Longrightarrow \beta, \gamma, \Delta}$$

Note that cut has depth 0.

Now, let us consider π_2: once more, the inferences that originate the first direct ancestors of $\beta \vee \gamma$ in π_2 can be (i) a logical left-introduction of $\vee$, or (ii) an $\Im-$inference, or (iii) a weakening. In case (i) the upper sequents have the form $\beta, \Pi \Longrightarrow \Lambda$ and $\gamma, \Pi \Longrightarrow \Lambda$.

(a) Take the first kind of sequents and obtain by weakening $\beta \vee \gamma, \Pi, \beta \Longrightarrow \Lambda$, then from this, a proof π_2^B of $\beta \vee \gamma, \Gamma, \beta \Longrightarrow \Delta$.

(b) Perform the same transformation taking the second kind of sequents, obtaining a proof π_2^C of $\beta \vee \gamma, \Gamma, \gamma \Longrightarrow \Delta$.

(a) If $\beta \vee \gamma$ in the endsequent of π_2^B has depth 0, obtain $\pi_2'^B$ of $\Gamma, \beta \Longrightarrow \Delta$ by crossing it with π_1 making a cut of depth 0:

$$\dfrac{\dfrac{\dfrac{\Gamma \Longrightarrow \Delta, \beta \vee \gamma}{structural}}{\Gamma, \beta \Longrightarrow \Delta, \beta \vee \gamma} \quad \dfrac{\pi_2^B}{\beta \vee \gamma, \Gamma, \beta \Longrightarrow \Delta}}{\Gamma, \beta \Longrightarrow \Delta}$$

(b) If in the endsequent of π_2^B the formula $\beta \vee \gamma$ has depth $-\infty$, use the first theorem to get a proof $\pi_2'^B$ of $\Gamma, \beta \Longrightarrow \Delta$ with the claimed properties.

Do the same with π_2^C to obtain $\pi_2'^C$ of $\Gamma, \gamma \Longrightarrow \Delta$.

Now, if $\beta \vee \gamma$ in the endsequent of π_2 had depth d, then β has depth $< d$ in $\pi_2'^B$. Analogously with γ in $\pi_2'^C$.

Make therefore two cuts of depth $< d$:

$$\dfrac{\dfrac{\dfrac{\pi_1''}{\Gamma \Longrightarrow \beta, \gamma, \Delta} \quad \dfrac{\dfrac{\pi_2'^B}{\Gamma, \beta, \Longrightarrow \Delta}}{\Gamma, \beta, \Longrightarrow \Delta, \gamma}}{\Gamma \Longrightarrow \gamma, \Delta} \quad \dfrac{\pi_2'^C}{\Gamma, \gamma \Longrightarrow \Delta}}{\Gamma \Longrightarrow \Delta}$$

(Before the last cut, make some exchange). The following hold:

(a) $h(\pi') \leq max\{h(\pi') + 3, h(\pi_2) + 3, h(\pi_2^B) + 3, h(\pi_1) + 3, h(\pi_2^C) + 2\}$
$\leq max\{h(\pi_1) + 3, h(\pi_2) + 3\}$
$\leq h(\pi) + 2 \leq 2 \cdot h(\pi)$.

(b) $|\pi'| \leq |\pi_1'| + |\pi_2| + |\pi_2^B| + |\pi_2^C| + 2 \cdot |\pi_1| + 5$
$\leq (|\pi_1| - 1) + |\pi_2| + 2 \cdot (|\pi_2| - 1) + 2 \cdot |\pi_1| + 5$
$\leq 2 \cdot (|\pi_1| + |\pi_2|) + 2 < (|\pi_1| + |\pi_2| + 1)^2 = |\pi|^2$

(c) $\alpha = \forall x \beta(x)$. In π_1 once more the first ancestor of this formula can be originated by weakening (i.), or by a $\Im$–inference (ii.), or by a right introduction rule (iii.):

$$\dfrac{\Pi \Longrightarrow \Lambda, \beta(a)}{\Pi \Longrightarrow \Lambda, \forall x \beta(x)}$$

where a is an *eigenvariable* different from one inference to another. In case (iii.) take a fresh variable c and replace each of the above inferences with:

$$\dfrac{\Pi \Longrightarrow \Lambda, \beta(c)}{\Pi \Longrightarrow \beta(c), \Lambda, \forall x \beta(x)}$$

obtaining a proof π_1' of $\Gamma \Longrightarrow \beta(c), \Delta, \forall x \beta(x)$.

Get a proof π_1'' of $\Gamma \Longrightarrow \beta(c), \Delta$ as follows:

(a) If the formula $\forall x\beta(x)$ has depth $-\infty$ in the endsequent of π_1', then once more use the first theorem to obtain a proof π_1'' of $\Gamma \Longrightarrow \beta(c), \Delta$.

(b) If the formula $\forall x\beta(x)$ has depth 0 in the endsequent of π_1', then cross π_1' and π_2 making a depth 0 cut to form a proof π_1'' of this sequent.

$$\dfrac{\dfrac{\pi_1'}{\Gamma \Longrightarrow \beta(c), \Delta, \forall x\beta(x)} \quad \dfrac{\dfrac{\dfrac{\pi_2}{\forall x\beta(x), \Gamma \Longrightarrow \Delta}}{structural}}{\forall x\beta(x), \Gamma \Longrightarrow \beta(c), \Delta}}{\Gamma \Longrightarrow \beta(c), \Delta}$$

If the formula $\forall x\beta(x)$ had depth d in the endsequent of π_1, then $\beta(c)$ has depth $< d$ in the endsequent of π_1''.

(a) Now consider in π_2 the inferences that originate the direct ancestors of the cut formula: still can be weakening, or a $\Im$-inference of a left introduction rule:

$$\dfrac{\beta(t), \Pi \Longrightarrow \Lambda}{\forall x\beta(x), \Pi \Longrightarrow \Lambda}$$

Let us first consider the latter (left-introduction rule).

Replace these inferences with:

$$\dfrac{\dfrac{\dfrac{\pi_1''[t]}{\Gamma \Longrightarrow \beta(t), \Delta} \quad \beta(t), \Pi \Longrightarrow \Lambda}{\Pi, \Gamma \Longrightarrow \Delta, \Lambda}}{\forall x\beta(x), \Pi, \Gamma \Longrightarrow \Delta, \Lambda}$$

and from this (adding weak inferences as necessary) obtain a proof π_2' of $\forall x\beta(x), \Gamma \Longrightarrow \Delta$ where $\forall x\beta(x)$ has now depth ≤ 0. Note that the cut has depth $< d$. In case $\forall x\beta(x)$ has depth $-\infty$ we apply once more the first theorem; in case of depth $= 0$ make a cut (of depth 0) crossing π_1 and π_2'.

Check yourself that $h(\pi') \leq 2 \cdot h(\pi)$ and $|\pi'| < |\pi|^2$.

(d) $\alpha = atomic$, hence $d = 0$ or $d = 1$.In this case the point in which the first direct ancestor of the cut formula originates can be a weakening, a $\Im-$rule or an axiom $\alpha \Longrightarrow \alpha$. Build π_1' replacing occurrences of $\alpha \Longrightarrow \alpha$ which contain a first direct ancestor of the cut formula with:

$$\dfrac{\dfrac{\pi_2}{\alpha, \Gamma \Longrightarrow \Delta}}{\alpha, \Gamma \Longrightarrow \Delta, \alpha}$$

Note that α in the succedent has depth $-\infty$. So, at the end (with the help of structural rules) we get a proof π_1' of $\Gamma \Longrightarrow \Delta, \alpha$ with α in the endsequent of depth ≤ 0 and $\pi_1' \preccurlyeq \pi_1$. A proof π_2' of $\alpha, \Gamma \Longrightarrow \Delta$ is obtained specularly in the same way, again with α in the endsequent of depth ≤ 0 and $\pi_2' \preccurlyeq \pi_2$.

(a) If α has depth $-\infty$ in the endsequent either of π_1' or of π_2' then obtain from it a proof π' of $\Gamma \Longrightarrow \Delta$ by applying the first theorem.

(b) If α has depth 0 in both endsequents of π'_1 and π'_2, cross π'_1 and π'_2 and obtain π' making a cut on α. Note that this cut is *anchored*.

Check that $h(\pi') \leq 2 \cdot h(\pi)$. As or the size, $|\pi'| \leq (c-1) \cdot |\pi|^2$ follows from the fact that $(c-1) \cdot |\pi_i| + 1$ is a bound of the number of initial sequents of π_i. QED

Corollary 22. *Suppose π has depth $\leq d$ and $d \geq 0$. Then a proof π' exists with the same endsequent, in which all free cuts have depth $< d$ and $h(\pi') < 2^{h(\pi)+1}$ and $\pi' \preccurlyeq \pi$.*

Proof. Induction on $h(\pi)$. Let us define:

$$f(i) = \text{minimum number } z \text{ such that, if } h(\pi) \leq i, \text{ then } h(\pi') \leq z.$$

Notice that:

(a) $f(0) = 0$, because in this case there is no cut in π.

(b) If $i = h(\pi) = 1$, then:

i. if π does not contain *free cuts*, put $\pi' = \pi$.

ii. otherwise, since the height is 1, we can have only initial sequents, structural rules and *atomic* cuts (why atomic? Note that if the cut formula were introduced by weakening its *depth* would be $-\infty$ and if were a principal formula of a $\Im$-inference, the cut would be not free); hence by the previous theorem $h(\pi') < 2$, hence $f(1) = 1$.

3. If $i \geq 2$, suppose e.g. that π ends with a rule with two upper sequents whose proofs are π_1 and π_2. Apply (IH) to them and obtain π'_1 and π'_2 whose height is $\leq f(i-1)$, whose free cuts have depth $< d$ and such that $\pi'_1 \preccurlyeq \pi_1$ and $\pi'_2 \preccurlyeq \pi_2$. Form a new proof ξ replacing in π the subproofs π_1 and π_2 with π'_1 and π'_2:

i. If ξ does not end with a free cut, put $\pi' = \xi$. The height is $\leq f(i-1) + 1$

ii. otherwise, since $\pi'_j \preccurlyeq \pi_j$ $(j = 1, 2)$ the cut must have depth $\leq d$: if depth $< d$, then put $\pi' = \xi$; if depth $= d$, apply the previous theorem to ξ and obtain π'. The height is $\leq 2 \cdot f(i-1) + 2$.

By induction on i, prove that $f(i) < 2^{i+1}$.

QED

Now, iterating this result $d+1$ times, we obtain a proof of height $< 2^{h(\pi)+1}_{d+1}$, where every cut has depth < 0, namely $-\infty$. Hence apply once more the Theorem 109 to get a proof without free cuts and therefore Theorem 110 follows.

Corollary 23. *Let Φ be a class of formulas closed under substitution of terms and subformulas. Suppose that each $\Im-$inference has only formulas in the class Φ as principal formulas. Then for all proofs π, there is a proof π' of the same endsequent in which all cut formulas are in Φ.*

Proof. Note that logical inferences can be viewed as $\Im - inferences$. E.g. a right introduction inference of $\wedge$ can be seen an instance of a skeleton of this form:

$$\frac{C_1 \Longrightarrow D_1, \alpha \quad C_2 \Longrightarrow D_2, \beta}{C \Longrightarrow D, \alpha \wedge \beta}$$

Hence let us consider $\Im^+ = \Im - inferences$ plus logical inferences with the principal formulas in Φ plus all identities $\alpha \Longrightarrow \alpha$ with $\alpha \in \Phi$ atomic. The last theorem gives a π' with no free cuts with respect to $\Im^+$. If every $\Im^+$-inference has only formulas in Φ as principal formulas, then there is a proof π' of the same endsequent in which all cut formulas are *anchored*. Cuts in π' have depth 0, hence the cut formulas are occurrences of a principal formula in $\Im^+$, hence are in Φ. QED

An extremely powerful consequence of this corollary is the following:

(a) Suppose our acceptable inferences are the initial sequents corresponding to the non logical axioms of PA, the equality axioms and the induction rule restricted to Σ_k formulas (the fragment denoted $\mathsf{I\Sigma_k}$).

(b) Take $\Phi = \Sigma_k \cup \Pi_k$ and let π be a proof *free-cut-free* in $\mathsf{I\Sigma_k}$ of a sequent $\Gamma \Longrightarrow \Delta$ where Γ, Δ are made of formulas in Φ.

(c) Suppose by contradiction that there is a formula α occurring in π such that $\alpha \notin \Phi$. Hence, by the above corollary, α is not a cut formula, since all cut formulas in π are in Φ (notice that the principal formulas of the induction rules and of axioms are in $\Sigma_k \subseteq \Phi$).

(d) Therefore in π' the formula α has not been deleted and will occur in the final sequent as a side formula, or as a subformula (i.e. it occurs as an auxilary formula at some step). Contradiction: against the assumption that all formulas in $\Gamma \Longrightarrow \Delta$ were in Φ.

(e) Hence we conclude that in π occurs only formulas from Φ.

7.3. Bounded Arithmetic and Polynomial Time Computability

The philosophical motivation for the introduction of *Bounded Arithmetic* theories can perhaps be traced back to dissatisfaction with traditional finitism and intuitionist constructivism in constructive mathematics, not considered by some as a genuine alternative to realism: "finitism is the last refuge of platonism"(Nelson (1986), p. 10). In Parikh (1971), a pioneering work that sought to construct a system reflecting an "anthropomorphic point of view" in mathematics, it is proposed that numbers that are too large such as $10^{10^{10}}$ should be considered infinite and formal theories of arithmetic are proposed where exponentiation is not assumed to be defined over all numbers. This whole discussion is connected to the theme of feasibility and of the computational infeasibility of exponentiation that we have discussed in relation to the Church-Turing thesis.

There are two principal approaches to bounded arithmetic. The original approach involved theories such as $\mathsf{I\Delta_0}$ and $\mathsf{I\Delta_0} + \Omega_1$ (e.g. Cook and Nguyen (2010) is a handbook based on this approach). The first of these theories was introduced in Parikh (1971), where every Δ_0-formula defines what is called "a concrete predicate"; later, in Buss (1986), bounded theories such as S^i_2 and T^i_2, based on a broader language, have been introduced and extensively studied. One of the main features is their close connection to low-level computational complexity. The T^i_2 will be defined by restricting induction to Σ^b_i -formulas, where by induction we mean the usual one. For S^i_2, we need a different kind of induction schema. We will deal here mainly with the theories $\mathsf{S}^1_2, \mathsf{S}^2_2, \mathsf{S}^3_2$.... The idea behind this approach is to modify $\mathsf{I\Delta_0} + \Omega_1$ so that the definable functions in these theories are more directly related to the levels of the so-called *Polynomial Time Hierarchy*, instead of the *Linear Time Hierarchy*. Actually the union of

these theories $\bigcup_i \mathsf{S}^i_2$ is equivalent to the theory $\mathsf{I}\Delta_0 + \Omega_1$. All these theories are *predicative* in the sense of Nelson (1986), that is, interpretable in Robinson's Q. In particular, through an application of (partial) cut-elimination we will see that the Σ^b_1 definable functions of this extended language in the theory S^1_2 are the *polynomial time computable functions*.

Recall that $\Sigma^L_0 = \mathsf{LINTIME}$ are the languages decided in $c \cdot n$ time (for some c) and $\Sigma^L_{i+1} = \mathsf{NLINTIME}(\Sigma^{\mathsf{L}}_i)$ are the languages accepted in time $c \cdot n$ by a nondeterministic machine with oracle in Σ^L_i and finally $\mathsf{LTH} = \bigcup_i \Sigma^L_i$ is the so-called *Linear Time Hierarchy*. Note that LTH is a class of relations. We define a class of functions in terms of *function graph* i.e. the set of pairs $\langle x, y\rangle$ such that $f(x) = y$: a function f in computable in linear time iff this set belong to LTH. It is well known that $\mathsf{LTH} = \Delta^{\mathbb{N}}_0$, namely the relations $\Delta_0 - definable$ in the standard model.

Recall also that we say that a function f is Σ_1-*definable* in $\mathsf{I}\Delta_0$ iff there is a Σ_1-formula ϕ such that $\phi(\overline{n}, \overline{f(n)})$ is true for all n and the theory proves $\forall x \exists! y \phi(x, y)$. In this case it holds that this is true of f iff its graph is in LTH and there is a bounding term t of the language of the theory for existential quantifier, i.e. the theory actually proves $\forall x \exists! y \leq t\phi(x, y)$.

For many purposes, it is useful to extend $\mathsf{I}\Delta_0$ with the axiom:

$$\Omega_1 = \forall x \exists y (x^{|x|} = y)$$

where $|x|$=smallest integer bigger or equal to $log_2(x + 1)$=length of x in base two.

The theory $\mathsf{I}\Delta_0 + \Omega_1$ allow more flexible constructions, since the axiom Ω_1 just captures the polynomial increase of the lengths in such a way that definable functions of this theory satisfy the condition that $|f(x)| \leq p(|x|)$, for some polynomial p, instead of $|f(x)| \leq c \cdot |x|$ as in $\mathsf{I}\Delta_0$.

The function $x^{|x|}$ is superpolynomial and has a *polynomial growth rate*, i.e. if t is a term builded with functions $S, \cdot, +, x^{|x|}$, then a polynomial p_t exists such that $|t(x)| \leq p_t(|x|)$. Parikh's result that we are going to prove extend to $\mathsf{I}\Delta_0 + \Omega_1$ as well as to Buss's theories, and from this it follows that they does not prove the totality of exponential[2].

Parikh raised the question of whether exponentiation is necessary to carry out Gödel arithmetisation. The argument was as follows (here in Buss (1999) reconstruction). For instance, one wants the theory to be able to define the notion of substituting a term into a formula and prove the result is a formula. The following argument by Parikh, together with the difficulty in proving Löb's third derivability condition in this theory, led to believe that an 'intensional' type of arithmetization was not possible in $\mathsf{I}\Delta_0$. Actually, if the number of symbols of $\theta(x)$ is m and that of the term t is n, then the number of symbols of $\theta[t/x]$ is about $m \cdot n$. By using "efficient codings" we have that $\ulcorner \theta(x) \urcorner = 2^{O(m)}$ and $\ulcorner t \urcorner = 2^{O(n)}$, and therefore $\ulcorner \theta[t/x] \urcorner = 2^{O(m \cdot n)}$. But $\ulcorner \theta[t/x] \urcorner = 2^{O(m \cdot n)} \leq 2^{|\ulcorner \theta \urcorner| \cdot c \cdot n} \leq \ulcorner \theta(x) \urcorner^{O(n)}$ and since the number of symbols of a word whose code is x is bounded by $|x|$, lastly we have $\ulcorner \theta(x) \urcorner^{O(|\ulcorner t \urcorner|)}$. The conclusion is that the value of $\ulcorner \theta[t/x] \urcorner$ cannot be bounded by a polynomial of $\ulcorner t \urcorner$ and $\ulcorner \theta(x) \urcorner$. However, not all the power of the exponential function is required here: actually we need just the function $(x, y) \mapsto x^{|y|}$. This explain the axiom Ω_1.

Another motivation for the introduction of these extensions of $\mathsf{I}\Delta_0$ is related to the *intensional approach to arithmetization*. We have seen that every recursive function is numeralwise representable even in very weak theories such as R and Q: they can 'represent' all particular instances $f(n)$ of a recursive function f, but not prove general properties of the function. This in is in contrast to the approach to the arithmetization of syntax that Feferman (1960) called *intensional*. Here, when we define concepts such as "formula", "term", "substitution", "proof", "theorem", etc, we demand that the theory can prove general properties of these concepts,

[2] To get an idea of how much concrete number theory or combinatorics can be done in these theories, see for example Beame, Impagliazzo, Pitassi (1993) or Ajtai (1994) or D'Aquino (1992), Berarducci and D'Aquino (1995) and D'Aquino and Macintyre (2000).

which is not required in the case of arithmetisation based on the concept of representability. The intesional arithmetization can be carried out in S^1_2 as well as in $\mathsf{I}\Delta_0 + \Omega_1$ (see Buss (1986)). The above remarks about substitution suggest that an intensional arithmetization could hardly be done in $\mathsf{I}\Delta_0$, without resorting to the *shortening* technique discussed below (i.e. an intensional arithmetization of metamathematics can be given rather artificially already in Q by replacing "x is a proof"with "x is a proof in the initial segment J", as we explained when discussing the problem of Gödel's second theorem for Q).

Working in such weak theories generally entails the need to economise in the use of resources, to such an extent that Parikh (1971) stated as an open question the issue of whether the exponentiation function is required for the arithmetization of metamathematics in Gödel's incompleteness theorems. The way in which we code the syntax become relevant. We will refer to Wilkie and Paris (1987) for a careful Gödel coding such that, if n is the number of symbols of a formula θ:

(a) $n \leq |\ulcorner\theta\urcorner| \leq c \cdot n$, where $|x|$ is the base-two length of x, for some constant c. Hence also:

(b) $2^n \leq \ulcorner\theta\urcorner \leq 2^{d \cdot n}$, for some constant d.

We call *efficient* such a coding. Let us take two examples of how to economise:

(a) Speaking of Gödel's incompleteness results, coding sequences is an essential step. For coding sequences we used exponentiation, but this function is not total in $\mathsf{I}\Delta_0$. The coding of sequences e.g. in Hájek and Pudlák (1993) allows us to manipulate sequences provably in $\mathsf{I}\Delta_0$ and thereby define with a Δ_0 formula the graph of the function $x^y = z$, proving in $\mathsf{I}\Delta_0$ its main properties (except totality!).

To code a sequence of numbers in a more efficient way, they use a pair of numbers:

i. The first number will be the number determined by the concatenation of binary expansions of the numbers to be coded.

ii. The second one will be a binary code of the markers which determine beginnings and ends of the coded numbers.

In fact we code sequences of arbitrary $0-1$ words in such a way. Suppose we want to code a sequence of $0-1$ words:

$$0011, 101, 010$$

Then we take two numbers whose binary expansion is the following:

$$11101010, \quad 10001001001$$

The first one is the concatenation of the words above (where we have to omit the first two 0's) and the second one is a sequence of markers which determines the partition. If this pair is considered to be a code of *a sequence of numbers* then it will code $(3, 5, 2)$. This coding of finite sequences is used to define in $\mathsf{I}\Delta_0$ the exponential relation $x^y = z$ (however, it is not possible in this theory to show that such a z always exists!)[3].

(b) The second example concerns the efficient representation of numerals. We need to use in arithmetization the function $n \mapsto \ulcorner\overline{n}\urcorner$. Using efficient numerals and an efficient arithmetization, this transformation is p-time. Actually, to represent the number n by the numeral $S(S(...S(\overline{0})...))$ is problematic, when we don't have the exponentiation as a total function. The classical numerals $S^n(0)$ cannot be used, since their length (number

[3] The first Δ_0 definition of the graph of exponentiation, formalized in the theory $\mathsf{I}\Delta_0$ is due Gaifman and Dimitracopoulos (1982)

of symbols) is greater than n. Hence the Gödel number of this numeral will be of order $2^{c \cdot n}$, for a constant c. Hence the function $n \mapsto \ulcorner \overline{n} \urcorner$, sending a number to the code of its numeral will be exponential. At the opposite the length of the *efficient numerals* is bounded by a polynomial of $|n|$. Indeed, we think of the base two representation of n is $a_k a_{k-1} ... a_0$, where each a_i is 0 or 1, and we represent n as:

$$a_0 + 2(a_1 + 2(a_2 + ...(a_{k-1} + 2a_k)...))$$

Hence the Gödel number of the numeral of n is now of order $2^{c \cdot \log_2(n)}$.

Parikh proved that, although there exist formulas $\eta(x, y, z)$ having, provably in $\mathsf{I}\Delta_0$, the basic properties of exponentiation $x^y = z$, none of these formulas is such that $\mathsf{I}\Delta_0$ proves $\forall x \forall y \exists z\, \eta(x, y, z)$. The result follows from this theorem.

Theorem 111. *If $\theta(x, y)$ is* bounded *and $I\Delta_0 \vdash \forall x \exists y \theta(x, y)$, then exists a term t such that:*

$$I\Delta_0 \vdash \forall x \exists y < t\theta(x, y)$$

Proof. Recall that terms t in the language of PA are polynomials of the form $x^k + c$, which grow slower than the exponential function, and Parikh's theorem says that we can bound the value of Δ_0 definable functions in $\mathsf{I}\Delta_0$ only by a term in this language and therefore these functions *can increase the length of the input only linearly.* As the exponential relation $x^y = z$ actually has a Δ_0 definition, it follows that $\mathsf{I}\Delta_0$ cannot prove the totality of exponentiation.

An extremely laborious proof was given in Buss (1986) in sequent calculus; although more akin to the spirit of these readings, we prefer to report the semantic one contained in Hájek and Pudlák (1993) and Krajíček (1995), an elegant model-theoretic argument, using compactness. Suppose by contradiction that the premiss is true, but this conclusion is false. Therefore (for a new constant c) the following is consistent, for every t:

$$\mathsf{I}\Delta_0 + \forall y < t(c) \neg\theta(c, y)$$

Note that it is unprovable also any disjunction:

$$\bigvee_{i \leq k} \exists y < t_i(c)\theta(c, y)$$

(otherwise one could take $t = t_0 + t_1 + ... + t_k$ and $\exists y < t(c)\theta(c, y)$ would be provable, since each disjunct would imply this formula). Hence any finite subset of sets:

$$\Gamma_k = \mathsf{I}\Delta_0 + \forall y < t_0(c) \neg\theta(c, y) + ... + \forall y < t_k(c) \neg\theta(c, y)$$

is consistent. It follows by compactness that the set:

$$\Gamma = \mathsf{I}\Delta_0 + \{\forall y < t_i(c) \neg\theta(c, y) | t_i \textit{ is a term}\}$$

is consistent too (note that any finite subset of Γ is a subset of Γ_n, for some n). So, Γ has a model $\mathcal{M}$. Now consider an initial segment:

$$I = \{b \in \mathcal{M} | \mathcal{M} \models b < t(c),\ \textit{for some } t(x)\}$$

of this model, i.e. a subset closed downwards and by addition and product. It is well known that I remains a model of $\mathsf{I}\Delta_0$: actually $\mathsf{I}\Delta_0$ is a *bounded theory of arithmetic*, namely is axiomatized by bounded formulas, e.g. the induction principle can be formulated as follows:

$$\phi(\overline{0}) \wedge \forall x < z(\phi(x) \rightarrow \phi(x + 1)) \rightarrow \phi(z)$$

If $\psi(x)$ is a bounded formula and I an initial segment of a model $\mathcal{M}$ closed under addition and multiplication, an *absoluteness principle* holds, namely if $a \in I$, then $I \models \psi(a)$ iff $\mathcal{M} \models \psi(a)$. But:

$$I \models \exists x \forall y \neg \theta(x, y)$$

(contradiction).

Indeed, we have proved that $\mathsf{I}\Delta_0$ cannot prove the totality of such functions that eventually majorize all polynomials. QED

Corollary 24. *x^y is not provably total in $\mathsf{I}\Delta_0$.*

Remark 5. *Although Parikh's Theorem was originally established for this theory, it can be easily extended to Buss' theories $\mathsf{S}^{\mathsf{i}}_2$ (see Verbrugge (1993)).*

Here some key results. Points 2., 3. and 4. somehow support the argument of Nelson (1986) where Q is considered the reference theory from which to start, admitting only extensions that can be interpreted in it.

Theorem 112. *The following hold:*

(a) Q *is not intepretable in* R.

(b) S^1_2 *is intepretable in* Q.

(c) $\mathsf{I}\Delta_0 + \Omega_1$ *is intepretable in* Q.

(d) $I\Delta_0 + exp$ *is not intepretable in* Q .

(e) $I\Delta_0 + \neg exp$ *is intepretable in* Q.

(f) $\mathsf{I}\Delta_0 + \Omega_1$ *is intepretable in* $\mathsf{I}\Delta_0$.

(g) $I\Sigma_1$ *is not intepretable in* $I\Delta_0 + exp$.

where $exp = \forall x \exists y(2^x = y)$. We remark that the graphs of the functions 2^x and $x^{log(x)}$ are definable in $\mathsf{I}\Delta_0$ (which does *not* prove their totality) but we emphasize the difference between points 3. and 4.: although it has some induction, the theory $\mathsf{I}\Delta_0 + \Omega_1$ (as well as $\mathsf{I}\Delta_0$) is not too far from Q. The presence of exponentiation 2^x as a total function represents on the contrary, a sort of *impassable barrier* and determines a big jump in complexity. An evidence of the jump in complexity highlighted in Nelson (1986) is that by applying a technique called *shortening*, displayed in Solovay (1976) and involved in the results of interpretability or non-interpretability listed above, we can successively close an initial segment of a model of Q under each of the functions $2x, x^2, x^{|x|}, x^{|x|^{||x||}}$... However Paris and Dimitracopulos (1983) showed that it is *not always possible* to close also under exponentiation: there exist a model and an initial segment of it that cannot be restricted in such a away to be closed also under exponentiation. For this reason, we view $x^{log(x)}$ as being more akin to feasible polynomial growth rate functions than to the infeasible exponential function.

These theorems are long and complex, so here we report only one of the simplest cases, where however we see the aforementioned technique due to Solovay at work (see Ferreira G. and Ferreira F. (2013) and Hájek and Pudlák (1993), ch.V, section C for a complete account). Let us therefore consider a syntactical counterparts of initial segments we have seen in models of arithmetic.

Definition 56. *A formula $I(x)$ is* inductive *for a theory T, if this theory proves $I(\overline{0}) \wedge \forall x(I(x) \rightarrow I(Sx))$. It defines an* initial segment *of T, if moreover satisfies $I(x) \wedge y \leq x \rightarrow I(y)$. A formula $J(x)$ is a sub-initial segment of $I(x)$ in T, if the theory proves $J(x) \rightarrow I(x)$*[4].

[4] We point out that in much literature what we have called initial segment is called cut. Below, we have used another term to avoid misunderstandings.

Definition 57. *A theory* T *is locally intepretable in a theory* S *iff each finite part of* T *is intepretable in* S.

Let us add associativity and commutativity of $+, \cdot$ to Q, plus the following distributivity $x \cdot (y + z) = x \cdot y + x \cdot z$ and let us denote Q^+ the resulting arithmetical system. It is easily proved that if $\mathsf{T} \supset \mathsf{Q}^+$ and $I(x)$ is inductive in T, the there exists a subcut $J(x)$ of it. The central result is the following.

Theorem 113. (Solovay's shortening) *If* $\mathsf{T} \supset \mathsf{Q}^+$ *and* $I(x)$ *is inductive in* T*, then there exists a subcut* $J(x)$ *of it, closed under* $+, \cdot$.

Proof. We usw the tecnique of shortening, due to Solovay. Let:

(a) $J_0(x) = \forall y(I(y) \to I(y + x))$

(b) $J(x) = \forall y(J_0(y) \to J_0(y \cdot x))$

By using associativity of $+$ prove in Q^+ that $J_0(x)$ is closed under addition, i.e. if $J_0(x)$ and $J_0(y)$, then $J_0(y + x)$ and from this follows the closure under $+$ of $J(x)$ as well. With similar argument prove that $J(x)$ is closed under multiplication too.

We now show that $J(x)$ is an initial segment. We claim that $J(x) \wedge y \leq x \to J(y)$. We have to show that if $J_0(z)$, then $J_0(z \cdot y)$, that by definition is $J(y)$. Still by definition $J_0(z \cdot y)$ is $I(v) \to I(v + z \cdot y)$, for any v. Since $J(x)$ and $J_0(z)$, by definition of J we have $J_0(z \cdot x)$ and since $y \leq x$, there must be some w such that $y + w = x$ and there fore $J_0(z \cdot (y + w))$. Now we ude the distributivity axiom to obtain $J_0(z \cdot y + z \cdot w)$. But we had $I(v)$ and therefore, by definition of J_0 we have $I(v + (z \cdot y + z \cdot w))$. Since I is a cut and:

$$v + z \cdot y \leq (v + z \cdot y) + z \cdot w = v + (z \cdot y + z \cdot w)$$

we have $I(v + z \cdot y)$ and therefore $J_0(z \cdot y)$, as claimed.

QED

Theorem 114. *The theory* $\mathsf{I}\Delta_0$ *is locally intepretable in* Q^+.

Proof. Fix a finite number of formulas with only bounded quantifiers

$$\phi_0(x, p), ..., \phi_n(x, p)$$

and for each i, let:

$$I_i(x, p) = \phi_i(\overline{0}, p) \wedge \forall y \leq x(\phi_i(y, p) \to \phi_i(Sy, p)) \to \phi_i(x, p)$$

Then define $I(x) = \forall p(\bigwedge_{i \leq n} I_i(x, p))$. This is an inductive formula and by the previous theorem it can be shortened to a cut J closed under addition and multiplication and therefore to a "model" of Q^+. Moreover, since $J(x) \to I(x)$ and $I(x) \to I_i(x, p)$, the inductiion for every ϕ_i holds in J. QED

7.4. Cut-elimination and Polynomial time definable functions

We introduce now Buss' approach to bounded arithmetic and we show some importan application to the theory of computational complexity:

(a) The language af Buss's theory of Bounded Arithmetic is the following:

$$S, 0, +, \cdot, |x|, \lfloor \frac{1}{2}x \rfloor, \#, \leq$$

where $|x| = \lceil \log_2(x+1) \rceil$ =small $y \geq \log_2(x+1)$ is the length of the binary representation of x, $\lfloor \frac{1}{2}x \rfloor$ is the greatest integer less or equal to $\frac{1}{2}x$ and $x\#y$ means $2^{|x|\cdot|y|}$. We will use $\#, \cdot, \lfloor \frac{1}{2}x \rfloor$ to write terms of the form $2^{p(|x|)}$ where $p(x)$ is a polynomial.

(b) We actually "think" in base two: the operation $\lfloor \frac{1}{2}x \rfloor$ erases the last bit from the base two representation of x. Numerals ("dyadic numerals") are defined as follows:

$$\overline{2k+1} = \overline{2k} + S(\overline{0}), \quad \overline{2(k+1)} = S(S(\overline{0})) \cdot \overline{k+1}$$

Note that the length of $\overline{k}$ is of the order of $\log(k)$.

(a) We want to discuss here of a sequent calculus LKB for theories of bounded arithmetic. For these, we must first add the equality initial sequents and some rules for bounded quantifiers.

$$\frac{\phi(t), \Gamma \Longrightarrow \Delta}{t \leq s, \forall x \leq s\phi(x), \Gamma \Longrightarrow \Delta} \qquad \frac{b \leq s, \Gamma \Longrightarrow \Delta, \phi(b)}{\Gamma \Longrightarrow \Delta, \forall x \leq s\phi(x)}$$

$$\frac{b \leq s, \phi(b), \Gamma \Longrightarrow \Delta}{\exists x \leq s\phi(x), \Gamma \Longrightarrow \Delta} \qquad \frac{\Gamma \Longrightarrow \Delta, \phi(t)}{t \leq s, \Gamma \Longrightarrow \Delta, \exists x \leq s\phi(x)}$$

(b) If α is a BASIC axiom, then we add the initial sequent $\Longrightarrow \alpha$.

BASIC will be the set of basic axioms for these operators. A richer language corresponds to a higher number of axioms:

(a) $x \leq b \to a \leq S(b)$

(b) $a \neq S(a)$

(c) $0 \leq a$

(d) $a \leq b \wedge a \neq b \leftrightarrow S(a) \leq b$

(e) $a \neq 0 \to 2 \cdot a \neq 0$

(f) $a \leq b \vee b \leq a$

(g) $a \leq b \wedge b \leq a \to a = b$

(h) $a \leq b \wedge b \leq c \to a \leq c$

(i) $|0| = 0$

(j) $|S(0)| = S(0)$

(k) $a \neq 0 \to |2 \cdot a| = S(|a|) \wedge |S(2 \cdot a)| = S(|a|)$

(l) $a \leq b \to |a| \leq |b|$

(m) $|a\#b| = S(|a| \cdot |b|)$

(n) $|S(0) = 0\#a$

(o) $a \neq 0 \to 1\#(2{\cdot}a) = 2{\cdot}(1\#a) \wedge 1\#(S(2{\cdot}a)) = 2 \cdot (1\#a)$

(p) $a\#b = b\#a$

(q) $|a| = |b| \to a\#c = b\#c$

(r) $|a| = |b| + |c| \to a\#d = (b\#d) \cdot (c\#d)$

(s) $a \leq a + b$

(t) $a \leq b \wedge a \neq b \to S(2{\cdot}a) \leq 2{\cdot}b \wedge S(2{\cdot}a) \neq 2{\cdot}b$

(u) $a + b = b + a$

(v) $a + 0 = a$

(w) $a + S(b) = S(a + b)$

(x) $a + b \leq a + c \leftrightarrow b \leq c$

(y) $a \cdot b = b \cdot a$

(z) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

() $S(0) \leq a \to (a \cdot b \leq a \cdot c \leftrightarrow b \leq c)$

() $a \neq 0 \to |a| = S(|\lfloor \frac{1}{2}a \rfloor|)$

() $a = \lfloor \frac{1}{2}b \rfloor \leftrightarrow 2 \cdot a = b \vee S(2 \cdot a) = b$

We define now a hierarchy of bounded formulas of this language, analogous to the Arithmetical Hierarchy, but now we count the alternations of bounded quantifiers:

(a) The set $\Delta_0^b = \Sigma_0^b = \Pi_0^b$ is equal to the set of formulas in which all quantifiers are sharply bounded, i.e. of the form $\forall x \leq |t|$ or $\exists x \leq |t|$.

(b) For $i > 0$, the sets Σ_i^b and Π_i^b are inductively defined by the following conditions:

i. If α and β are Σ_i^b-formulas, then so are $\alpha \vee \beta$ and $\alpha \wedge \beta$.

ii. If α is a Π_i^b formula and β is a Σ_i^b-formula, then $\alpha \to \beta$ and $\neg\alpha$ are Σ_i^b-formulas.

iii. If α is a Π_i^b-formula, then α is a Σ_i^b-formula.

iv. If α is a Σ_i^b-formula and t is a term, then $(\forall x \leq |t|)\alpha$ is a Σ_i^b-formula.

v. If α is a Σ_i^b-formula and t is a term, then $(\forall x \leq t)\alpha$ is a Σ_i^b-formula.

vi. The four inductive conditions defining Π_i^b are dual.

The terms of this language define *functions of polynomial growth rate*. The theories T_2^i will be defined by adding to the BASIC axioms the standard induction INDrestricted to Σ_i^b-formulas. The theories S_2^i will be defined instead by adding the induction schema PIND:

$$\alpha(0) \wedge \forall x(\alpha(\lfloor \tfrac{1}{2}x \rfloor) \to \alpha(x)) \to \forall x \alpha(x)$$

restricted to Σ_i^b-formulas. We have that $\mathsf{S}_2 = \cup_i \mathsf{S}_2^i = \cup_i \mathsf{T}_2^i = \mathsf{T}_2$. Moreover

$$\mathsf{S}_2^1 \subseteq \mathsf{T}_2^1 \subseteq \mathsf{S}_2^2 \subseteq \mathsf{T}_2^2 \subseteq \mathsf{S}_2^3 \subseteq ...$$

but it is open whether they are distinct. Anyway T_2 (and therefore S_2) is equivalent to $\mathsf{I}\Delta_0 + \Omega_1$. The polynomial time computable functions can be inductively defined in a similar way to what we did for primitive recursive functions, that is, by means of axioms as follows:

(a) *Initial functions.*

i. The nullary constant function 0.
ii. The successor function $S(x)$.
iii. The doubling function $2x$.
iv. The conditional function $Cond(x, y, z)$=if $x = 0$ then y, else z.
v. The *projection* functions are polynomial time functions

(b) The *composition* of polynomial time functions is a polynomial time function.

(c) The function f defined by *limited iteration on notation* from g and h, polynomial time:

i. $f(0, x) = g(x)$
ii. $f(z, x) = h(z, x, f(\lfloor \frac{1}{2}z \rfloor, x))$ for $z > 0$ provided $|f(z, x)| \leq p(|z|, |x|)$ where $p(x)$ is a polynomial.

Following Buss we define in a rather unusual way the *Polynomial Time Hierarchy. Predicates* are here functions $0, 1$ (their characteristic functions). A predicate is polynomial time computable provided its characteristic function is polynomial time. We distinguish between *logarithmic* bounds $p(|x|)$ and *polynomial* bounds $2^{p(|x|)}$ to the quantifiers. Logarithmically bounded quantification corresponds to *sharply bounded* quantification. We denote P_0^p the smallest class containing the initial functions, closed under composition and logarithmically bounded quantifiers.

(a) $\Delta_0^p = \Sigma_0^p = \Pi_0^p$ are the predicates of P_0^p.

(b) Σ_i^p is the class of polynomially bounded predicates $R(x)$-definable by $R(x) = (\exists y \leq 2^{s(|x|)})(Q(x,y))$ for some polynomial $s(n)$ and Δ_i^p predicate Q

(c) Π_i^p is the dual class of their complements.

(d) $P_{i+1}^p$is the class of functions computable on a deterministic Turing machine in polynomial time with oracle in Σ_i^p.

(e) Δ_{i+1}^p is the class of predicates with characteristic function in $\Box_{i+1}^p$.

Hence $\mathsf{P} = \Delta_1^p$, $\mathsf{NP} = \Sigma_1^p$, $\mathsf{FP} = \Box_1^p$ and $co - \mathsf{NP} = \Pi_1^p$. The class of polynomial time functions is $\Box_1^p$, and the class of polynomial time predicates is Δ_1^p.

Definition 58. *A function f is Σ_i^b-* definable in a theory T*, if there is a formula $\phi \in \Sigma_i^b$ such that:*

(a) ϕ defines the graph of f,

(b) $\mathsf{T} \vdash \forall x \exists y \phi(x,y)$

(c) $\mathsf{T} \vdash \forall x \forall y \forall z(\phi(x,y) \wedge \phi(x,z) \rightarrow y = z)$

Definition 59. *A predicate $P(x)$ is Δ_i^b definable in T provided there are $\phi \in \Sigma_i^b$ and $\psi \in \Pi_i^b$ provably equivalent in T, that define $P(x)$.*

Definition 60. *A theory is said to be* bounded *if it is axiomatizable with a set of bounded formulas.*

In the previous discussion we used Parikh's theorem for all the theories of the hierarchy S_2^i. The syntactic proof in the sequent calculus contained in Buss (1986) is rather complex. However it can be achieved semantically in a simpler way along the same lines as in Verbrugge (1993).

Theorem 115. *If S_2^i proves $\forall x \exists y \theta(x,y)$, and θ is bounded, then $\forall x \exists y \leq t(x) \theta(x,y)$, for some term t.*

Proof. Suppose that this is not true. Then take:

$$\mathsf{S}_2^i \cup \{\forall y \leq \overbrace{c\#...\#c}^{k-times} \neg\theta(c,y) | k \in \omega\}$$

where c is a new constant and observe that this set is finitely satisfable. Hence by compactenss the whole set is satisfable, i.e. has a model, say $\mathcal{M}$ where a certain element a interprets c. Take the submodel $\mathcal{U}$ defined as:

$$\mathcal{U} = \{b \in \mathcal{M} | \exists k (b \leq \overbrace{c\#...\#c}^{k-times})\}$$

This model is closed under the operations $+, \cdot, S, \#, \lfloor \frac{1}{2} x \rfloor$ Note that the theory S_2^i can be axiomatized by Π_1 sentences. Actually we can write also the induction axiom as:

$$\forall y (\theta(\overline{0}) \wedge \forall x \leq y (\theta(\lfloor \tfrac{1}{2} x \rfloor) \rightarrow \theta(x)) \rightarrow \forall x \leq y \theta(x))$$

where $\theta \in \Sigma_i^b$. But Π_1 sentences are preserved "downward" hence this is a model of S_2^i too. On the other hand $\mathcal{U}$ does not verify $\exists y \theta(a,y)$, otherwise there would be a k and a $b \in \mathcal{M}$ such that:

(a) $b \leq \overbrace{c\#...\#c}^{k-times}$ and

(b) $\theta(a,b)$

against the hypothesis, and therefore $\mathsf{S}^{\mathsf{i}}_2 \nvdash \forall x \exists y \theta(x,y)$ (contradiction, against the assumption). QED

Some important facts.

(a) Every polynomial time function is Σ^b_1-definable in $\mathsf{S}^{\mathsf{i}}_2$.

(b) Every polynomial time predicate is Δ^b_1-definable in $\mathsf{S}^{\mathsf{i}}_2$.

(c) Every $\Box^p_i$ function is Σ^b_i-definable in $\mathsf{T}^{\mathsf{i}-1}_2$ and in $\mathsf{S}^{\mathsf{i}}_2$.

(d) Every Δ^p_i predicate is Δ^b_i-definable in $\mathsf{S}^{\mathsf{i}}_2$.

(e) A predicate is Σ^p_i if and only if there is a Σ^b_i-formula which defines it.

We are going to show the main result of Buss (1986), i.e. the inverse implications of these points, in particular:

(a) Every Σ^b_1-definable function in $\mathsf{S}^{\mathsf{i}}_2$ is polynomial time computable.

(b) Δ^b_1-definable predicate in $\mathsf{S}^{\mathsf{i}}_2$ is polynomial time computable.

Generalizations to other levels holds.

(a) To do this, first we must formulate the PIND induction as a rule:

$$\frac{\alpha(\lfloor \frac{1}{2} b \rfloor), \Gamma \Longrightarrow \Delta, \alpha(b)}{\alpha(\overline{0}), \Gamma \Longrightarrow \Delta, \alpha(t)}$$

where b occurs only as indicated.

(b) Axioms α are formalized as initial sequents $\Longrightarrow \alpha$

(c) In view of what we are about to say it must be emphasized that many functions needed for arithmetization of syntax are $\Sigma^b_1 - definable$ in S^1_2 (e.g. the coding of finite sequences, projections, concatenation of finite sequences) and many predicates are $\Delta^b_1 - definable$ in S^1_2 (e.g. $Seq(x)$, $Len(x)$).

Theorem 116. (Buss 1985) *Let $i \geq 1$ and let us suppose $\mathsf{S}^{\mathsf{i}}_2$ proves $\forall x \exists y \theta(x,y)$ where $\theta \in \Sigma^b_i$. Then there exists a term t, a formula ψ and a function $g \in \Box^p_i$ such that $\mathsf{S}^{\mathsf{i}}_2$ proves:*

(a) $\forall x \forall y (\psi(x,y) \rightarrow \theta(x,y))$

(b) $\forall x \forall y \forall z (\psi(x,y) \wedge \psi(x,z) \rightarrow y = z)$

(c) $\forall x \exists y \leq t \psi(x,y)$

(d) for all n it is true in the standard model $\psi(\overline{n}, \overline{g(n)})$

Corollary 25. *If g is Σ^b_i-definable in $\mathsf{S}^{\mathsf{i}}_2$, then $g \in \Box^p_i$.*

Buss's witnessing method. Although this theorem applies in its most general form for $i \geq 1$, in this exposition we can focus on the case where $i = 1$, in order to avoid introducing further details. Let therefore $\theta(c) \in \Sigma^b_i$-formula in prenex form. Then $Witness^i_\theta(w, c)$ (which is provably Δ^b_i in $\mathsf{S}^{\mathsf{i}}_2$) is defined inductively as follows:

(a) If $\theta \in \Pi^b_{i-1} \cup \Sigma^b_{i-1}$ then $Witness^i_\theta(w, c) \leftrightarrow \theta(c)$

(b) $Witness^i_\theta(w, c)$ distributes over $\vee$ and $\wedge$, e.g. w witnesses $\alpha \wedge \beta$ iff $(w)_1$ witnesses α *and* $(w)_2$ witnesses β.

(c) If $\theta \notin \Pi^b_{i-1} \cup \Sigma^b_{i-1}$ and has the form $\forall x \leq |s(c)|\psi(c, x)$, then $Witness^i_\theta(w, c)$ is the conjunction of:

i. $Seq(w) \wedge Len(w) = |s| + 1$
ii. $\forall x \leq |s(c)|Witness^i_{\psi(c,b)}((w)_{x+1}, c, x)$

(Hence $w = \langle w_0, ..., w_{|s|}\rangle$ witnesses the truth of θ iff each w_i witnesses $\psi(c, i)$).

(d) If $\theta \notin \Pi^b_{i-1} \cup \Sigma^b_{i-1}$ and has the form $\exists x \leq t(c)\psi(x, c)$, then $Witness^i_\theta(w, c)$ is the conjunction of:

i. $Seq(w) \wedge Len(w) = 2 \wedge (w)_1 \leq t$
ii. $Witness^i_{\psi(c,b)}((w)_2, c, (w)_1)$

(Hence $w = \langle n, v\rangle$, $n \leq t$ and v witnesses $\psi(c, n)$).

(e) In case of negated formulas not in $\Pi^b_{i-1} \cup \Sigma^b_{i-1}$ we internalize the negation in order to bring us back to the cases listed above.

Some properties. For all $\theta \in \Sigma^b_i$, the theory $\mathsf{S}^{\mathsf{i}}_2$ proves:

$$\exists w(Witness^i_\theta(w, c)) \leftrightarrow \theta(c)$$

In the following We use this notation. If $\Gamma = \langle A, B, C\rangle$ then $\bigwedge\Gamma = (A \wedge (B \wedge C))$ and $\bigvee\Gamma = (A \vee (B \vee C))$.

Theorem 117. (The main theorem) *Let us suppose* $\mathsf{S}^{\mathsf{i}}_2$ *proves* $\Gamma, \Pi \Longrightarrow \Lambda, \Delta$ *where* Γ, Δ *are composed by* Σ^b_i *formulas and* Π, Λ *are composed by* Π^b_i *formulas and* c *are all the variables of the sequent. Take* $G = \bigwedge\Gamma \wedge \bigwedge\{\neg\gamma | \gamma \in \Lambda\}$ *and* $H = \bigvee\Delta \vee \bigvee\{\neg\delta | \delta \in \Pi\}$. *Then there is a function* f *which is* $\Sigma^b_i - definable$ *in* $\mathsf{S}^{\mathsf{i}}_2$ *such that:*

(a) $f \in \Box^p_i$

(b) $\mathsf{S}^{\mathsf{i}}_2 \vdash Witness^i_G(w, c) \rightarrow Witness^i_H(f(w, c), c)$

Before proving this theorem, let us take a look of how we apply it. Suppose $\Gamma = \Pi = \Lambda = \emptyset$ and $\Delta = \exists y\theta(c, y)$. We apply Parikh's theorem to show $\Delta = \exists y \leq t\theta(c, y)$. By the main theorem there is a $\Sigma^b_i - definable$ function f that witnesses this formula. Take $\psi(x, y) \leftrightarrow y = (f(x))_1$ and notice that $g(x) = ((f(x))_1 \in \Box^p_i$.

*Proof of the Main Theorem.*By induction on the number of sequents in a free-cut free proof. Let us consider a proof of

$$\Gamma, \Pi \Longrightarrow \Lambda, \Delta$$

where for simplicity of exposition we assume $\Pi = \Lambda = \emptyset$. By the free-cut-free elimination theorem we can assume that, since Γ, Δ have all formulas in $\Sigma^b_i \cup \Pi^b_i$, the same holds for all formulas occurring in the proof. Since there are $\Sigma^b_i - \mathsf{PIND}$ inferences, all cut formulas will be in Σ^b_i. We will show here some relevant cases (the remaining cases as exercises).

(a) If $\Gamma \Longrightarrow \Delta$ is an initial sequent (BASIC axioms, logical axioms or equality axioms) these ar all composed by quantifier free formulas, hence by definition:

$$Witness^i_\theta(w,c) \leftrightarrow \theta(c)$$

and putting $f(n) = 0$ for all n this function satisfies the theorem.

(b) If the last inference has the form:

$$\frac{\alpha, \Theta \Longrightarrow \Delta}{\alpha \wedge \beta, \Theta \Longrightarrow \Delta}$$

Let D be $\alpha \wedge \bigwedge \Theta$ and E be $(\alpha \wedge \beta) \wedge \bigwedge \Theta$. By (IH) there is $g \in \Box^p_i$ which is Σ^b_i-definable in S^i_2 and this theory proves:

$$Witness^i_D(w,c) \rightarrow Witness^i_{\bigvee \Delta}(g(w,c),c)$$

Take $h(w) = \langle((w)_1)_1, (w)_2\rangle$ so that:

$$Witness^i_E(w,c) \rightarrow Witness^i_D(h(w),c)$$

and finally by putting $f(w,c) = g(h(w),c)$ we obtain:

$$Witness^i_E(w,c) \rightarrow Witness^i_{\bigvee \Delta}(f(w,c),c)$$

(c) If the last inference has the form:

$$\frac{\beta, \Theta \Longrightarrow \Delta \quad \gamma, \Theta \Longrightarrow \Delta}{\beta \vee \gamma, \Theta \Longrightarrow \Delta}$$

Let D be $\beta \wedge (\bigwedge \Theta)$ and E be $\gamma \wedge (\bigwedge \Theta)$ and F be $(\beta \vee \gamma) \wedge (\bigwedge \Theta)$. Apply (IH): hence there are $g, h \in \Box^p_i$ such that S^i_2 proves:

$$Witness^i_D(w,c) \rightarrow Witness^i_{\bigvee \Delta}(g(w,c),c)$$

$$Witness^i_E(w,c) \rightarrow Witness^i_{\bigvee \Delta}(h(w,c),c)$$

Let us define

$$f(w,c) = \begin{cases} g(\langle((w)_1)_1, (w)_2, c\rangle), & \text{if } Witness^i_\beta((w)_1)_1, c) \\ h(\langle((w)_1)_2, (w)_2\rangle, c) & \text{otherwise} \end{cases}$$

In other words, if w witnesses $(\beta \vee \gamma) \wedge (\bigwedge \Theta)$, then either $((w)_1)_1$ witnesses β or $((w)_1)_2$ witnesses γ, and $(w)_2$ witness $\bigwedge \Theta$. In the former case use g to find a witness of $\bigvee \Delta$; in the latter case use h. It follows:

$$Witness^i_F(w,c) \rightarrow Witness^i_{\bigvee \Delta}(f(w,c),c)$$

(d) If the last rule is:

$$\frac{a \leq t, \beta(a), \Theta \Longrightarrow \Delta}{\exists x \leq t \beta(x), \Theta \Longrightarrow \Delta}$$

(where a must not appear in the lower sequent) take for D the formula $a \leq t \wedge (\beta(a) \wedge \bigwedge \Theta)$ and E be $\exists x \leq t \beta(x) \wedge \bigwedge \Theta$. By (IH) there is a $g \in \Box^p_i$ such that:

$$Witness^i_D(w,c,a) \rightarrow Witness^i_{\bigvee \Delta}(g(w,c,a),c)$$

We consider two cases:

i. if $(\exists x \leq t\beta) \notin \Sigma^b_{i-1}$, then let $h(w) = \langle 0, \langle((w)_1)_2, (w)_2\rangle\rangle$, so that $Witness^i_E(w,c) \rightarrow Witness^i_D(h(w), c, ((w)_1)_1)$ so let $f(w,c) = g(h(w), c, ((w)_1)_1)$ and note that the theory proves:

$$Witness^i_E(w,c) \rightarrow Witness^i_{\bigvee \Delta}(f(w,c), c)$$

ii. if $(\exists x \leq t\beta) \in \Sigma^b_{i-1}$, then let $h(w) = \langle 0, \langle 0, (w)_2\rangle\rangle$ and $f(w,c) = g(h(w), c, (\mu x \leq t\beta(x))$

(e) If the last rule is

$$\frac{\Theta \Longrightarrow \beta(s), \Sigma}{s \leq t, \Theta \Longrightarrow \exists x \leq t\beta(x), \Sigma}$$

take D as $\beta(s) \vee (\bigvee \Sigma)$ and E be $s \leq t \wedge (\bigwedge \Theta)$ and F be $\exists x \leq t\beta(x) \vee (\bigvee \Sigma)$ and by (IH) we have:

$$Witness^i_{\bigwedge \Theta}(w,c) \rightarrow Witness^i_D(g(w,c), c)$$

But by definition we have $Witness^i_E(w,c) \rightarrow s \leq t \wedge Witness^i_{\bigwedge \Theta}((w)_2, c)$ so let $f(w,c) = \langle\langle s(c), (g((w)_2, c)_1\rangle, (g((w)_2.x)_2\rangle$ and note that:

$$Witness^i_E(w,c) \rightarrow Witness^i_F(f(w,c), c)$$

(f) Other logical rules are analized in a similar way (see Buss (1986)).

(g) If the last rule is a CUT:

$$\frac{\Gamma \Longrightarrow \Delta, \beta \quad \beta, \Gamma \Longrightarrow \Delta}{\Gamma \Longrightarrow \Delta}$$

Being the proof free-cut-free, β must be Σ^b_i. Take D be $\beta \vee (\bigvee \Delta)$ and E be $\beta \wedge (\bigwedge \Gamma)$, By (IH) there are $g, h \in \Box^p_i$ such that the theory proves:

$$Witness^i_{\bigwedge \Gamma}(w,c) \rightarrow Witness^i_D(g(w,c), c)$$

$$Witness^i_E(w,c) \rightarrow Witness^i_{\bigvee \Delta}(h(w,c), c)$$

Hence we define:

$$f(w,c) = \begin{cases} (g(w,c))_2 & \text{if } Witness^i_{\bigvee \Delta}((g(w,c))_2, c) \\ h(\langle (g(w,c))_1, w\rangle, c) & \text{otherwise} \end{cases}$$

Hence we obtain:

$$Witness^i_{\bigwedge \Gamma}(w,c) \rightarrow Witness^i_{\bigvee \Delta}(f(w,c), c)$$

(h) If the last rule is:

$$\frac{\beta(\lfloor \frac{1}{2} b \rfloor), \Theta \Longrightarrow \beta(b), \Sigma}{\beta(\overline{0}), \Theta \Longrightarrow \beta(t), \Sigma}$$

By (IH) if w witnesses $\beta(\lfloor \frac{1}{2} b \rfloor) \wedge \bigwedge \Theta$ there is $g \in \Box^p_i$ such that $g(w,b)$ witnesses $\beta(b) \vee \bigvee \Sigma$

Now let:

(a) $f(w,0) = \langle (w)_1, 0\rangle$; arguing as before, if w witnesses $\beta(\overline{0}) \wedge \bigwedge \Theta$, then $(w)_1$ witnesses $\beta(\overline{0})$ and therefore $\beta(\overline{0}) \vee \bigvee \Sigma$,

(b) Now let $f(w,b) = \langle X_0, X_1\rangle$, for $b > 0$, where:

i. $X_0 = g(\langle (f(w, \lfloor \frac{1}{2}b \rfloor)_1, (w)_2\rangle)_1$

ii. $X_1 = k((f(w, \lfloor \frac{1}{2}b \rfloor)_1, (w)_2)_2, (g(\langle f(w, \lfloor \frac{1}{2}b \rfloor, (w)_2\rangle)_2)$

and where:

$$k(v,w) = \begin{cases} v, & \text{if } Witness^i_{\bigvee \Sigma}(v,c) \\ w & \text{otherwise} \end{cases}$$

Note that if w witnesses $\beta(\overline{0}) \wedge \bigwedge \Theta$, then $f(w,b)$ witnesses $\beta(b) \vee \bigvee \Sigma$. The theory proves that:

(a) as we have seen, if w witnesses $\beta(\overline{0}) \wedge \bigwedge \Theta$, then $f(w,0)$ witnesses $\beta(0) \vee \bigvee \Sigma$.

(b) under the same condition, if $f(w, \lfloor \frac{1}{2}b \rfloor)$ witnesses $\beta(\lfloor \frac{1}{2}b \rfloor) \vee \bigvee \Sigma$, then $f(w,b)$ witnesses $\beta(b) \vee \bigvee \Sigma$.

(c) Hence by PIND we conclude that if w witnesses $\beta(\overline{0}) \wedge \bigwedge \Theta$, then $f(w,t)$ witnesses $\beta(t) \vee \bigvee \Sigma$.

To summarize:

(a) Buss's theorem says that if f is Σ^b_i-definable in $\mathsf{S}^{\mathsf{i}}_2$, then $f \in \Box^p_i$

(b) In case $i = 1$ we have that if f is Σ^b_1-definable in S^1_2, then f is polynomial time computable.

(c) Parson's theorem says that if f is Σ_1-definable in $I\Sigma_1$, then f is primitive recursive.

We remark that a proof of Parson's frequently mentioned theorem concerning the functions that can be defined in PRA can be obtained with Buss's method of the witness predicate too.

7.5. Further remarks and guide for further study

To conclude, let us make some proposals for further exploration of this topic. The literature on the weak fragments of arithmetic and their relation to computational complexity is endless and we therefore forego a priori the idea of giving a complete account of it, limiting ourselves to highlighting a few topics that we consider of particular importance, which can be approached with the tools we have introduced in the previous chapters.

A development worthy of consideration is the one who investigated what happens by narrowing the logical basis of theories. In this short presentation, we have dealt with theories based on classical logic: what can be said about intuitionist logic-based theories? *Intuitionistic Bounded Arithmetic* has been studied as well since Buss (1985): here a hierarchy of bounded formulas of the language of his theories is introduced, called $h - \Sigma^b_i$-formula (hereditarily Σ^b_i), i.e. those formulas that are Σ^b_i and whose subformulas are still Σ^b_i (for example, if $\phi \in \Pi^b_i$ and $\psi \in \Sigma^b_i$, then $\phi \to \psi \in \Sigma^b_i$, but ϕ is not). For each k, the theories $I - S^k_2$ are based on the $h - \Sigma^b_k$-induction schema (or rule) and for formulas in $h - \Sigma^b_k$ prove the excluded middle and the sability laws. Buss shows that if $\mathsf{I} - \mathsf{S}^{\mathsf{n}}_2 \vdash \forall x \exists y \phi(x,y)$, where ϕ is *arbitrarily complex* (note this difference with the classical case), then there exists a function $f \in \Box^P_n$, such that $\forall x \phi(x, f(x))$ is *true*. Actually, by a metod inspired ti Kleene's realisability, it is shown that the definable function f of $\mathsf{I} - \mathsf{S}^{\mathsf{n}}_2$ (i.e. those such that an arbitrarily complex formula ϕ exists such that $\phi(\overline{n}, \overline{f(n)})$ is true, for all n, and $\mathsf{I} - \mathsf{S}^{\mathsf{n}}_2 \vdash \forall x \exists! y \phi(x,y)$) are precisely those in $\Box^p_i$ (the class of functions computable in polynomial time with oracle in Σ^p_{i-1}, that coincides with

the class of predicates definable by a Σ^b_{i-1} formula). Further progress has been made in Cook and Urquhart (1993) and Harnik (1992).

We did not dwell on the theories T^i_2. However, a characterisation of the Σ^b_i-definable functions in T^{i-1}_2 is possible by proving that S^i_2 is $\forall\Sigma^b_i$-conservative on T^{i-1}_2 (where $\forall\Sigma^b_i$ means a universal quantifier followed by a Σ^b_i- formula). A different characterization of the Σ^b_1-definable (multivalued) functions of T^1_2 in terms of the so-called "polynomial local search problems" is given in Buss and Krajíček (1994). We only mention an important development, consisting in an application of the following well known result to these theories. Actually we consider an extension by definition of T^i_2, by adding symbols for all $\Box^p_{i+1}$ functions (which are Σ^b_{i+1}-definable in it) and the defining equations as axioms and obtain a kind of *Herbrand theorem.* Recall that a consequence of the cut elimination theorem for LK is that a cut free proof of a sequent $\Gamma \Longrightarrow \Delta$ where Γ, Δ are made of formulas in prenex normal form can be "divided" in two part. We define the *midsequent* as follows:

(a) If non quantifier rule occurs in the proof, then the midsequent is the last sequent.

(b) Otherwise, it is the topmost sequent which is a premiss of a quantifier rule (hence above there are only structural an propositional rules, and above only structural and quantifiers rules)

An application of this is the important *théorème fondamental* of Herbrand (1930). Let us consider a formula in prenex normal form, e.g. to fix the ideas:

$$\exists x \forall y \exists z \forall v \theta(x, y, z, v)$$

Let $f(x), g(x, y)$ new function symbols. Then for Herbrand's theorem that formula is provable in LK, iff there are terms $s_0, ..., s_n, t_0, ..., t_n$ such that the following:

$$\theta(s_0, f(s_0), t_0, g(s_0, t_0)) \vee ... \vee \theta(s_n, f(s_n), t_n, g(s_n, t_n))$$

is a propositional tautology (see Girard (1987) pp. 117-121 for a detailed proof). Variants of this have many applications to the problems we are discussing. A Herbrand-type theorem can be found in Krajíček, Pudlák, Takeuti (1991).

Theorem 118. *For $i \geq 1$, suppose $\phi(a, x, y)$ has the form $\exists \Pi^p_{i+1}$ and that T^i_2 proves $\exists x \forall y \phi(a, x, y)$. Then there are $\Box^p_{i+1}$-functions $f_0, ..., f_k$ such that T^i_2 proves:*

$$\phi(a, f_0(a), b_0) \vee \phi(a, f_1(a, b_0), b_1) \vee ... \vee \phi(a, f(a, b_0, .., b_{k-1}), b_k)$$

This research has important implications for an open problem: it is not known whether the hierarchy of theories of bounded arithmetic is proper, so we can hope that the connections between fragments of arithmetic and computational complexity that we have seen will also help us address the similar problem for the polynomial time hierarchy. The above result allows the following result to be deduced, due to Buss (1995), Krajíček, Pudlák, Takeuti (1991) and Zambella (1996).

Theorem 119. *If $\mathsf{T}^i_2 = \mathsf{S}^{i+1}_2$, then the polynomial time hierarchy collapses and this is provable in T^i_2.*

Last but not least, a natural continuation of the investigation around weak fragments of arithmetic leads one to consider *second-order* theories. The language of BASIC axioms is extended by adding second order variables $X^t, Y^s ...$ ranging over finite sets of numbers, where $t, s...$ are bounds to the value of the elements of the respective sets. We add also the membership relation $\in$, so that $x \in X^t$ is a new formula. The classes of formulas $\Sigma^{1,b}_i$

and $\Pi_i^{1,b}$ are introduced in analogy with the first order case counting the alternations of second-order quantifiers and not counting the alternations of first order quantifiers, where $\Sigma_0^{1,b}$ is the class of formulas with bounded first order quantifiers, but no unbounded quantifiers and no second-order quantifiers. The basic theory $\mathsf{I\Sigma_0^{1,b}}$ has the following axioms:

(a) BASIC axioms.

(b) $\forall X^t \forall Y^s \forall y \leq t + s(y \in X^t \leftrightarrow y \in Y^s) \rightarrow X^t = Y^s$ (extensionality).

(c) $\forall X^t \forall x \forall y (y \in X^t \rightarrow y \leq t(x))$.

(d) The scheme IND for $\Sigma_0^{1,b}$ formulas.

(e) $\mathsf{\Sigma_0^{1,b} - CA}$, i.e. the comprehension scheme:

$$\forall x \forall Y^x \forall y < x (y \in Y^x \leftrightarrow \theta(y))$$

(where $\theta \in \Sigma_0^{1,b}$).

The focus was mainly on these fragments, which have similarities with some fragments of the first order. We want to give an idea of what constitutes a key result linking the first- and second-order fragments, following Krajíček (1995) pp. 83-92. The second order family of fragments $\mathsf{V_1^i}$ actually had different presentations in different works. Each theory $\mathsf{V_1^i}$ is however equivalent to the above theory $\mathsf{I\Sigma_0^{1,b}}$ plus IND on all $\#-$free $\Sigma_i^{1,b}$ formulas. The family of fragments denoted $\mathsf{U_1^i}$ is obtained analogously but with PIND in place of IND. The families $\mathsf{U_2^i}$ and $\mathsf{V_2^i}$ are obtained in a similar manner, but admitting the respective induction schemes on $\Sigma_i^{1,b}$ formulas in the full language with $\#$. The strong analogy between first- order and second order fragments has the name of "RSUV isomorphism" and was highlighted by Takeuti (1993) and Razborov (1993). It is shown that there are translations $*, \circ$ between first-order and second-order languages such that:

(a) if $\phi \in \Sigma_\infty^{1,b}$, then $\phi^* \in \Sigma_\infty^b$

(b) if $\psi \in \Sigma_\infty^b$, then $\phi^\circ \in \Sigma_\infty^{1,b}$.

This translation fulfils the following conditions, linking fragments of the first and second order:

(a) if $S_2^i \vdash \psi$, then $V_1^i \vdash \psi^\circ$

(b) if $V_1^i \vdash \phi$, then $S_2^i \vdash \phi^*$

(c) $S_2^1 \vdash \psi \leftrightarrow (\psi^\circ)^*$

(d) $V_1^1 \vdash \phi \leftrightarrow (\phi^*)^\circ$.

The same relation subsist between $\mathsf{U_1^i}$ in place of $\mathsf{V_1^i}$ and R_2^i in place of S_2^i, where R_2^i is obtained from S_2^i replacing the PIND rule with the rule:

$$\frac{\Gamma, \phi(\lfloor \frac{1}{2} b \rfloor) \Longrightarrow \Delta, \phi(b)}{\Gamma, \phi(\overline{0}) \Longrightarrow \Delta, \phi(|t|)}$$

for $\phi \in \Sigma_i^b$ and adding the language the functions minus $\dot{-}$ and msf:

(a) $\mathsf{msf}(a, 0) = a$

(b) $\mathsf{msf}(a, i+1) = \lfloor \frac{1}{2}\mathsf{msf}(a, i) \rfloor$.

The fragments $\mathsf{R}^{\mathsf{i}}_3$ and $\mathsf{S}^{\mathsf{i}}_3$ include in the language the function $x\#_3 y = 2^{|x|\cdot|y|}$. The RSUV isomorphism extends to $\mathsf{S}^{\mathsf{i}}_3$ and $\mathsf{V}^{\mathsf{i}}_2$ as well as to $\mathsf{R}^{\mathsf{i}}_3$ and $\mathsf{U}^{\mathsf{i}}_2$. The main connection of these second-order fragments with computational complexity theory is condensed in this result:

(a) the $\Sigma^{1,b}_1$-definable functions of $\mathsf{U}^{\mathsf{1}}_2$ are the PSPACE-computable.

(b) the $\Sigma^{1,b}_1$-definable functions of $\mathsf{V}^{\mathsf{1}}_2$ are the EXPTIME-computable.

In other words, these theories have proof-theoretic strengths corresponding to polynomial space and exponential time computation. It is not known whether these two complexity classes coincide. Likewise, we know that $\mathsf{U}^{\mathsf{i}}_2 \subseteq \mathsf{V}^{\mathsf{i}}_2 \subseteq \mathsf{U}^{\mathsf{i+1}}_2$, but it is not known whether the theories $\mathsf{V}^{\mathsf{1}}_2$ and $\mathsf{U}^{\mathsf{1}}_2$ are different. See for instance Buss, Krajíček and Takeuti (1993) and Buss and Beckmann (2014) for further investigations and for improved witnessing theorems. Another interesting chapter (which we will not open for lack of space and to avoid excessive scattering) is that of the relationship with propositional systems and their complexity, of propositional proof systems corresponding to certain first-order and second-order bounded arithmetic theories, according to certain translations. We refer to Cook and Nguyen (2010), Buss (1997) and Krajíček (1995) for an extensive presentation.