Reprinted from

Samuel R. Buss   Philip J. Scott
Editors

Feasible Mathematics

A Mathematical Sciences Institute Workshop
Ithaca, New York, June 1989

1990

Birkhäuser
Boston · Basel · Berlin

On Bounded Σ_1^1 Polynomial Induction

JAN KRAJÍČEK[1] AND GAISI TAKEUTI

Abstract. We characterize the bounded first order consequences of theory U_2^1 in terms of a limited use of exponentiation, we construct a simulation of U_2^1 by the quantified propositional calculus, and we prove that U_2^1 is not conservative over $I\Delta_0$ and that it is stronger than a conservative $\Delta_1^{1,b}$–extension of S_2. As corollaries we obtain that U_2^1 is not conservative over TNC and that Σ_j^b–consequences of U_2^1 are finitely axiomatizable ($j \geq 2$).

We also show that $\overset{\circ}{U}{}_2^1$ plus a version of $\prod_1^{1,b}$–SEP is conservative over $U_2^1(BD)$ w.r.t. bounded formulas.

§0. INTRODUCTION

Bounded arithmetic $S_2(= T_2)$ and its second order version $U_2(= V_2)$ were introduced in Buss [1]. S_2 is conservative over $I\Delta_0 + \Omega_1$, cf. Paris–Wilkie [12]. These theories and their fragments S_2^i, T_2^i, U_2^i and V_2^i are closely related to various complexity classes and the separation problems for them are relevant to separation problems in complexity theory. For example, the collapse of S_2 implies the collapse of the polynomial hierarchy, cf. Krajíček–Pudlák–Takeuti [10], and $U_2^1 = V_2^1$ implies $PSPACE = EXPTIME$, cf. Buss [1].

In Clote–Takeuti [3] theory TNC (="theory for NC") was defined, as a subtheory of S_2^1. Again, $TNC = S_2^1$ implies $P = NC$.

The problems whether U_2^1 or V_2^1 are conservative over S_2 were posed in Buss [1]. In [8] it was shown that V_3^1 (in fact, V_2^1 + "f is total" for any reasonable f eventually majorizing all S_2–terms) is not $\prod_1^b$–conservative over S_2. Here we investigate the problem whether U_2^1 is conservative over S_2.

First we show a connection of quantified propositional calculus G to U_2^1 in the sense of Cook [4], Dowd [5] and Krajíček–Pudlák [9]. That is, we show that U_2^1 proves the reflection principles for G and that G simulates U_2^1–proofs of bounded first order formulas.

The connection of G and U_2^1 is not surprising as by Buss [1] U_2^1 is closely related to $PSPACE$ and by Dowd [5] G (or better, a calculus equivalent to G) is related to PSA ($PSPACE$–arithmetic), an equational theory with

[1] On leave from the Mathematical Institute on Prague

$PSPACE$–functions analogical to PV of Cook [4]. However, from this our simulation and results do not follow. This is because we want a propositional translation of a Σ^b_i–formula to have i blocks of the like quantifiers (i.e. to be Σ^q_i–propositional formula of [9]), but the quantifier complexity of a translation of equations in Dowd [5] grows with the length of the input and with the space bound.

The translation we use is the same as in Krajíček-Pudlák [9].

This gives the characterization of $\forall\Sigma^b_i$–consequences of U^1_2 as $S^1_2 + i$–$RFN(G)$, and hence entails finite axiomatizability of $\forall\Sigma^b_i(U^1_2)$. (It also allows to reduce the original question to a polynomial simulation problems of G_i versus G, similarly as in [9].)

We also characterize the bounded first order consequences of U^1_2, denoted $\Sigma^b_\infty(U^1_2)$, as $TNC + 1 - Exp$, in the manner of Krajíček [7, 8]. That is, we show that for $\varphi \in \Sigma^b_\infty : U^1_2 \vdash \varphi(a) \iff TNC \vdash$ "$2^{t(a)}$ exists" $\to \varphi(a)$, $t(a)$ some term. This gives that U^1_2 is not conservative over TNC, as $TNC + 1 -$ exp is stronger than TNC.

Then we construct a $\Delta^{1,b}_1$–extension of S_2 by adding $\Delta^{1,b}_1$–CA and $\Delta^{1,b}_1$–IND to $S_2(\alpha)$. This $\Delta^{1,b}_1$–extension is conservative over S_2. We show that U^1_2 is stronger than the $\Delta^{1,b}_1$–extension; in particular, U^1_2 can define the parity of the set $\{x \in \alpha | |x| = |a|\}$ while the later theory cannot–for this are used results of Håstad [6] and Yao [16] about the complexity of the parity function.

Finally we show that U^1_2 is not conservative over $I\Delta_0$. This is proved by showing that U^1_2 proves a form of consistency of $I\Delta_0$ unprovable in $I\Delta_0$. The consistency notion is that one studied in Takeuti [14] and Krajíček[7].

The paper is organized as follows. In §1 we recall the definitions of G, TNC and $TNC + 1$–exp. In §2 we show that $\overset{\circ}{U}{}^1_2$ is conservative over $U^1_2(BD)$ w.r.t. Σ^b_∞–formulas and in §§3, 4 we prove the reflection principles for G in U^1_2 and construct the simulation of U^1_2 by G; the corollaries are then derived in §5. In §6 we show the relation of $TNC + 1 - Exp$ and U^1_2 and finally in §§7, 8 we prove the non–conservativeness results of U^1_2 versus the $\Delta^{1,b}_1$–extension of S_2 and $I\Delta_0$ respectively.

We assume knowledge of Buss [1] and Krajíček-Pudlák [9]; knowledge of Takeuti [14] or Krajíček [7, 8] is useful.

§1. PRELIMINARIES

In this section we recall some notions and facts around the quantified propositional calculus and the definition of TNC to make the paper more self contained. The details and proofs can be found in Clote-Takeuti [3] and Krajíček-Pudlák [9] respectively.

Quantified propositional formulas are formed from atoms (called free atoms) p, $q, \ldots$, constants 0, 1, by usual connectives $\neg$, $\wedge$, $\vee$, $\supset$, and by quantification: if $A(p)$ is a formula then $\exists x \forall(x)$ and $\forall x A(x)$ are too (with the semantical meaning $A(0) \vee A(1)$ and $A(0) \wedge A(1)$ respectively). They are classified by their quantifier complexity to a hierarchy $\Sigma_i^q - \prod_i^q$, analogically with the arithmetic hierarchy.

Quantified propositional calculus G is a Gentzen–style propositional calculus allowing quantification of propositional variables and is formulated completely analogically with predicate calculus LK, cf. Takeuti [13].

Thus beside the usual structural rules (including the cut–rule) and the propositional rules there are the following right quantifier rules:

$$\forall \quad \text{right} \quad \frac{\Gamma \to \Delta, \quad A(p)}{\Gamma \to \Delta, \quad \forall x \forall(x)},$$

provided p does not occur in the lower sequent,

$$\exists \quad \text{right} \quad \frac{\Gamma \to \Delta, \quad A(B)}{\Gamma \to \Delta, \quad \exists x \forall(x)},$$

where B is any propositional formula, and the corresponding left rules.

Atoms x, $y, \ldots$ are called bounded and have never a free occurence in a formula.

Initial sequents of G has the form:

$$\begin{aligned} &p \to p, \\ &0 \to \\ &\quad \to 1. \end{aligned}$$

Proofs in calculus G are sequences of sequents, not necessarily trees.

To any bounded arithmetic formulas $A(a)$ (in the language of S_2) and any $m < \omega$ is assigned a propositional translation $[\![A]\!]^m(\bar{p})$ with free atoms $(p_1, \ldots, p_m) = \bar{p}$. The crucial property of the translation is that it represents $A(a)$ for a's of length $\leq m$. That is: if n has length $\leq m$ and $\epsilon_1, \ldots, \epsilon_m$ are its digits then $A(n)$ is true if $[\![A]\!]^m(p_j/\epsilon_j)$ is true.

A translation of equations was considered in Cook [4]. The idea is that any term defines a *PTIME*–function and thus its value can be computed by boolean circuits of polynomial size; these can be easily turned into propositional formulas. The translation of bounded quantifiers used in Krajíček-Pudlák [9] is based on the observation that in $A(n)$ the quantifiers range only over numbers of the length polynomial in the length of n and thus a single bounded quantifier can be translated by a polynomialy long block of the like propositional quantifiers. Sharply bounded quantifiers are translated by conjunctions resp. disjunctions of polynomial size.

There is certain ambiguity in this definition: as terms can denote numbers of length larger than m we should specify for each subformula B of A number m_B with respect to which the subformula is translated, cf. [9, the notion of bounding polynomial]. However, these numbers m_B can be chosen polynomial in m and sufficiently large such that the translation is correct, i.e. it reflects the truth of A. Their exact choice is not important.

The details of the definition can be found in [9]. We only mention four basic facts.

(a) If A is Σ_0^b then $[\![A]\!]^m$ can be written both as Σ_1^q and $\prod_1^q$ (and the equivalence is provable in G—*in* its fragment, in fact).

(b) If $A \in \Sigma_i^b$ then $[\![A]\!]^m$ is Σ_i^q, $i \geq 1$.

(c) The length of $[\![A]\!]^m$ (A fixed) is polynomial in m. In fact, the function constructing from 0^m the formula $[\![A]\!]^m$ is *PTIME* and definable—with its properties—in S_2^1.

The main property is the following simulation:

(d) If $T_2 \vdash A(a)$ then $[\![A]\!]^m$'s have G–proofs of polynomial size (in fact, definable in S_2^1).

A much more precise statement can be given relating fragments of G with fragments T_2^i, cf. Krajíček-Pudlák [9].

For $j \geq 1$ we have a $\forall\Sigma_j^b$-sentence formalizing:

$$\text{“if} \quad A \in \Sigma_j^q \quad \text{and} \quad G \vdash A \quad \text{then} \quad A \quad \text{is a tautology”.}$$

This sentence is denoted j–$RFN(G)$. For the formalization see [9]. We shall show that j–$RFN(G)$ is the strongest (over S_2^1) $\forall\Sigma_j^b$–sentence provable in U_2^1. From (d) it follows that j–$RFN(G)$ implies (over S_2^1) all $\forall\Sigma_j^b$–consequences of T_2.

Theory TNC was defined in Clote–Takeuti [3]. The language of the theory is the language of S_2 augmented by the function symbol truncate (x, i) := “the first i bits of x”. Using this function symbol we can define function bit(x, i) := “truncate (x, i) modulo 2”, i.e.“the i'th bit of x”.

Theory TNC is axiomatized by a finite number of basic axioms stressing the elementary propertis of the symbols in the language and by axioms:

Extensionality:

$$(|x| = |y| \wedge \forall i < |x|, \quad \mathrm{bit}(x,i) = \quad \mathrm{bit}(y,i)) \supset x = y.$$

Σ_1^b-L_2IND :

$$(A(0) \wedge \forall x, A(x) \supset A(x+1)) \supset \forall x A(||x||).$$

Formula A must be Σ_1^b. (This axiom was in [8] denoted Σ_1^b-$LLIND$).

$\prod_1^b$-SEP:

$$\begin{aligned}&(\forall t, A(t) \vee B(t)) \supset \forall x \exists y < 2(1\#x)\\ &\forall t < |x|, (A(t) \vee bit(y,t) = 0) \wedge (B(t) \vee bit(y,t) = 1).\end{aligned}$$

Here again formulas A, B have to be Σ_1^b.

The principal use of $\prod_1^b$-SEP in [3] is to derive a form of $\Delta_1^b - CA$:

$$(\forall t, A(t) \equiv B(t)) \supset \forall x \exists y < 2(1\#x) \forall t < |x|; \ A(t) \equiv (\mathrm{bit}(y,t) = 1),$$

where A is Σ_1^b and B is $\prod_1^b$. The extensionality axiom implies that the y above is unique.

A crucial fact about TNC is that it Σ_1^b-defines precisely NC-computable functions. For the details of the definition of TNC see Clote-Takeuti [3].

For R any system of bounded arithmetic we define the set of bounded first order formulas $R+1-Exp$, a particular case of the construction considered in Krajíček [7, 8].

A (bounded first order) formula $A(a)$ belongs to $R+1-Exp \iff$ there is a term $t(a)$ s.t.

$$R \vdash \text{“}2^{t(a)} \leq c\text{”} \rightarrow A(a),$$

where c is a free variable not occurring in A. The antecedent clearly stands for “$2^{t(a)}$ exists”.

Alternatively we can characterize $R+1-Exp$ model–theoretically as a $\prod_1$–theory of initial segments of models of R with elements bounded by some $|c|$, c an element of the model. That is, $A(a)$ is in $R+1-Exp \iff$ for any model $M \models R$ and any $I \subseteq_e M$ a substructure s.t. for each $m \in I$, $M \models$ “2^m exists”, it holds:

$$I \models \forall x A(x).$$

Pairs (I, M) are called in [8] 1–fold models of R and we shall use this terminology below.

§2. $\overset{\circ}{U}{}^1_2$ AND $U^1_2(BD)$

Although we talk in the whole paper about U^1_2 or $U^1_2(BD)$ we consider only second order variables for sets but not for functions (such subsystems are in Buss [1] named $\tilde{U}^1_2$ and $\tilde{U}^1_2(BD)$). The systems with function variables are (fully) conservative over the systems without them and the arguments are easier.

Lemma 2.0. *For any A a $\Sigma^{1,b}_1$–formula, $U^1_2(BD)$ proves:*

$$\exists\varphi^{|t|}\forall x \leq |t|; A(x) \equiv \varphi(x).$$

Proof: By $\Sigma^{1,b}_1$–$PIND$ prove that there is the maximal $k \leq |t| + 1$ s.t. there is $\varphi^{|t|}$ of cardinality k satisfying $\forall x \leq |t|$, $\varphi(x) \supset A(x)$.

For details see Takeuti [15]. ▮

Now let us consider a form of bounded $\prod^{1,b}_1$–SEP axiom:

$$(\forall t, \neg A(t) \vee \neg B(t)) \to \forall x\exists\varphi^x\forall t < x, (A(t) \supset \varphi^x(t)) \wedge (B(t) \supset \neg\varphi^x(t)),$$

where A and B are $\prod^{1,b}_1$–formulas.

Theorem 2.1. *$U^1_2(BD)$ proves the bounded $\prod^{1,b}_1$–SEP axioms.*

Proof: Take formula $C(a, b)$:

$$\forall s \leq b\exists\varphi^b\forall t \leq b, \quad (s \leq t \leq s + a \supset ((A(t) \supset \varphi^b(t)) \wedge (B(t) \supset \neg\varphi^b(t)))).$$

Obviously $U^1_2(BD)$ proves the sequent

$$(\forall t, \neg A(t) \vee \neg B(t)), \quad C(\lfloor \frac{a}{2} \rfloor, b) \to C(a, b).$$

By $\Sigma^{1,b}_1$–$PIND$ it follows then:

$$(\forall t, \neg\, A(t) \vee \neg\, B(t)), \quad C(0, b) \to C(b, b).$$

As $C(0, b)$ is trivially provable (or instance of Lemma 2.0 for t = 0–a.s. parameters are allowed), the axiom of bounded $\prod^{1,b}_1$–SEP follows. ▮

THEOREM 2.2. *$\overset{\circ\,1}{U}_2$ is conservative over $U^1_2(BD)$ w.r.t. first order bounded formulas.*

PROOF: We give a simple model–theoretic argument; an effective procedure constructing a $U^1_2(BD)$–proof from a $\overset{\circ\,1}{U}_2$–proof of a first order bounded formulas can be given following the similar argument about V^1_2 in [15].

Assume $U^1_2(BD) \vdash A(a)$, where A is a first order bounded formula. Thus there is a model $\mathcal{M} = (M, X)$ of $U^1_2(BD)$ and $m \in M$ such that:

$$(M, X) \models_{\neg} A(m).$$

Moreover, by compactness we may assume that for some $c \in M$,

$$M \models t(m) < c$$

is true for all terms t.

Then define $M' = (M', X')$ by:

$$M' = \{n \in M| \quad \text{for some term} \quad t : M \models n \leq t(m)\},$$
$$X' = \{\alpha^c \cap M' | \alpha^c \in X\}.$$

We claim that $\mathcal{M}'$ as a model of $\overset{\circ\,1}{U}_2$. It is obvious that

$$\mathcal{M}' \models S_2(\alpha) + \Delta^{1,b}_0 - CA.$$

Observe that for any bounded formula $B(a)$ there is a term t s.t. $B(a) \equiv B^t(a)$ where $B^t(a)$ arises from $B(a)$ replacing all set variables α, φ by α^t resp. by φ^t.

By Theorem 2.1, $\mathcal{M} \models$ bounded $\prod^{1,b}_1 - SEP$. Applying bounded $\prod^{1,b}_1 - SEP$ to formulas $B(a)$, $C(a) \in \prod^{1,b}_1$ s.t. $\mathcal{M} \models \forall x,\ B(x) \equiv_{\neg} C(x)$ gives an instance of bounded $\Delta^{1,b}_1 - CA$:

$$\mathcal{M} \models \exists \varphi^c \forall x \leq c;\ x \in \varphi^c \equiv B(x).$$

By the observation above for $\psi = \varphi^c \cap M'$:

$$\mathcal{M}' \models \forall x;\ x \in \psi \equiv B(x).$$

Finally $\mathcal{M}' \models \sum^{1,b}_1 - PIND$ follows (again using the above observation) from

$$\mathcal{M} \models \sum_1^{1,b} -PIND.$$

The theorem then follows, as obviously

$$M' \models \neg A(m)$$

holds too. ∎

In the next sections we shall freely pass from $\overset{\circ}{U}{}_2^1$ to $U_2^1(BD)$ when talking about first order bounded consequences.

§3. REFLECTION PRINCIPLES FOR G IN U_2^1.

Here we show that all reflection principles $i - RFN(G)$ are provable in U_2^1. This is because U_2^1 can $\Sigma_1^{1,b}$–define true quantified propositional formulas.

THEOREM 3.0. *For all* $i < \omega$,

$$U_2^1 \vdash i - RFN(G).$$

PROOF: The set of true quantified propositional formulas is in PSPACE and so it is $\Sigma_1^{1,b}$–definable. A particular $\Sigma_1^{1,b}$–definition is constructed as follows.

Let $f(A)$ be a polynomial time function which assigns to a quantified propositional formula A one of its prenex forms; such function is $\sum_1^b$-definable in S_2^1 by induction on the logical complexity of A using few prenex operations. Then define:

$Tr(A, \tau) \rightleftharpoons$ "$\exists$ Skolem functions for $f(A)$ witnessing the existential quantifiers for any truth evaluation of the universally quantified atoms, where free atoms of $f(A)$ are evaluated by τ."
Skolem functions are coded by a set, the details of the definition are obvious.

Tr satisfies Tarski's conditions, this is easily verifed by induction on the logical complexity of A (i.e. by $\Sigma_1^{1,b} - PIND$).

As $Tr(A, \tau) \equiv \neg Tr(\neg A, \tau)$ is U_2^1–provable formula Tr is, in fact, $\Delta_1^{1,b}$ w.r.t. U_2^1.

Assume now that d is a G–proof, i.e. a sequence of sequents $d = S_1, \ldots, S_r$. Then by induction on i we prove:

$$\neg Tr(S_r, \eta) \to [(\exists j \leq r - i \exists \tau \in \{0,1\}^*, \quad \neg Tr(S_j, \tau)) \vee$$
$$\vee (\exists j \leq r, \ S_j \quad \text{is initial} \quad \wedge \exists \tau, \quad \neg Tr(S_j, \tau))].$$

As S_1 must be initial, taking $i := r - 1$ gives:

$$\neg Tr(S_r, \eta) \to \exists S_j \quad \text{initial} \quad \exists \tau, \quad \neg Tr(S_j, \tau).$$

Since all initial sequents are tautological, S_r must be true for all evaluations η.

Finally, if $S_r \subseteq \Sigma_i^q$ then $Tr(S_r, \eta) \rightarrow SSat_i(S_r, \eta)$, where $SSat_i(S_r, \eta)$ is Δ_{i+1}^b—truth definition for Σ_i^q–sequents used in [9]. ∎

(Observe that the above proof works also if D is a G–proof coded by a set instead by a number. That is, D is a set $\{< 1, S_1 >, \ldots, < r, S_r >\}$ coding "proof" $S_1, \ldots, S_r$. Not every proof coded by a set can be coded by a number,as exponentiation is not total in U_2^1 (cf. §6).)

§4. THE SIMULATION OF U_2^1 BY G.

The aim of this section is to prove the following simulation theorem, a result in the line of simulation of PV by EF in Cook [4] and of T_2^i by G_i in Krajíček-Pudlák [9].

THEOREM 4.0. *Let $A(a)$ be first order bounded formula and assume that*

$$U_2^1 \vdash A(a).$$

Then for each $m < \omega$ there is a G-proof d_m of $[\![A]\!]^m$ whose length is polynomial in m. Moreover, this is provable in S_2^1:

$$S_2^1 \vdash \forall y, \quad G \vdash [\![A]\!]^{|y|} \quad ∎$$

We shall prove a stronger statement (Theorem 4.1) whose immediate corollary Theorem 4.0 is. In Buss [1] a witnessing theorem for U_2^1–proofs of $\sum_1^{1,b}$–formulas is proved where the second order existential quantifiers are witnessed by $PSPACE$–functionals. Theorem 4.1 is a propositional version of this theorem.

We shall work with $U_2^1(BD)$ rather than U_2^1 itself (allowed by Theorem 2.2) and to simplify the argument we shall assume that all $\sum_1^{1,b}(BD)$–formulas are of the form:

$$\exists \varphi^t A(\bar{a}, \bar{\alpha}^r, \varphi^t),$$

where A is $\sum_0^{1,b}(BD)$. This can be achieved by introducing to the language a functional coding finite sequences of sets:

$$n \in (i, \alpha) \iff \langle i, n \rangle \in \alpha,$$

and relevant axioms to $BASIC$ implying (with $PIND$) $\sum_1^{1,b}$–replacement.

We shall also use a propositional translation of $\sum_0^{1,b}(BD)$–formulas for which we make the following convention: a translation $\llbracket A(a,\alpha)\rrbracket^m$ of $A(a,\alpha)$ is constructed as in the first order case, just atomic formulas $\alpha(x)$ are translated $\llbracket\alpha\rrbracket(q_1,\dots,q_n)$. Here $\llbracket\alpha\rrbracket$ is a new metavariable for quantified propositional formulas. Such metavariables shall never occur in a G–proof; they are introduced only as a convenient notation. For example, $\llbracket A(a,\alpha/B)\rrbracket$ is $\llbracket A(a,\alpha)\rrbracket(\llbracket\alpha\rrbracket/\llbracket B\rrbracket)$.

There is certain ambiguity in this definition as n (the number of atoms) in the metavariable $\llbracket\alpha\rrbracket$ is not explicitly specified. This is treated as in §1: n is larger than the length of any value of a term occurring in α when evaluating the formula on inputs of length $\leq m$.

Now we can state the theorem.

Theorem 4.1. *Let* $\exists\phi^t A(a,\alpha^s,\phi^t)$ *and* $\exists\varphi^r B(a,\alpha^s,\varphi^r)$ *be* $\sum_1^{1,b}(BD)$–*formulas,* A *and* B $\sum_0^{1,b}(BD)$–*formulas, and assume:*

$$U_2^1(BD)\vdash\exists\phi^t A(a,\alpha^s,\phi^t)\rightarrow\exists\varphi^r B(a,\alpha^s,\varphi^r).$$

Then for each m *there is a quantified propositional formula with metavariables*

$$W_m(\llbracket\alpha^s\rrbracket,\llbracket\phi^t\rrbracket)$$

such that for any quantified propositional formulas C,D *it holds:*

$$\begin{aligned}G\vdash{}&\llbracket A\rrbracket^m(\bar p,\llbracket\alpha^s\rrbracket/C,\llbracket\phi^t\rrbracket/D)\\&\rightarrow\llbracket B\rrbracket^m(\bar p,\llbracket\alpha^s\rrbracket/C,\llbracket\varphi^r\rrbracket/W_m(\llbracket\alpha^s\rrbracket/C,\llbracket\phi^t\rrbracket/D)).\end{aligned}$$

Moreover, this is provable in S_2^1 :

$$S_2^1\vdash\forall y\exists W_{|y|}\forall C,D;$$

$$\begin{aligned}G\vdash{}&\llbracket A\rrbracket^{|y|}(\bar p,\llbracket\alpha^s\rrbracket/C,\llbracket\phi^t\rrbracket/D)\\&\rightarrow\llbracket B\rrbracket^{|y|}(\bar p,\llbracket\alpha^s\rrbracket/C,\llbracket\varphi^r\rrbracket/W_{|y|}(\llbracket\alpha^s\rrbracket/C,\llbracket\phi^t\rrbracket/D).\end{aligned}$$

Here C *and* D *are assumed to have the appropriate number of atoms and* W_m *may contain atoms* $\bar p$ *too.*

Proof: Fix m. To simplify the reading of formulas we shall write $\llbracket\ \rrbracket$ instead of $\llbracket\ \rrbracket^m$ and we shall not explicitly write superscript bounds in predicate variables.

Let d be a $U_2^1(BD)$ proof of:

$$\exists\phi A(a,\alpha,\phi) \to \exists\varphi B(a,\alpha,\varphi).$$

By cut–elimination (cf. [1]) and the discussion above we may assume that all sequents in d have the form:

$$\exists\phi_i A_i(a,\bar{b},\alpha,\bar{\beta},\phi_i),\ldots,\Gamma \to \Delta,\ldots,\exists\varphi_j B_j(a,\bar{b},\alpha,\bar{\beta},\varphi_j),$$

where Γ,Δ are cedents of $\sum_0^{1,b}(BD)$–formulas and $A_i,\ldots,B_j,\ldots$ are $\sum_0^{1,b}(BD)$ too ($\bar{b}$ and $\bar{\beta}$ will be omitted further).

By induction on the number of inferences above the sequent we construct propositional formulas with metavariables

$$W^j(\llbracket\alpha\rrbracket,\overline{\llbracket\beta\rrbracket},\ldots,\llbracket\phi_i\rrbracket,\ldots$$

and show that for any $C,\ldots,D_i,\ldots$ G proves:

$$\ldots,\llbracket A_i\rrbracket(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots),\ldots,\llbracket\Gamma\rrbracket \to$$

$$\llbracket\Delta\rrbracket,\ldots,\llbracket B_j\rrbracket(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\varphi_j\rrbracket/W_j(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)).$$

(Here $\llbracket\Gamma\rrbracket$ resp. $\llbracket\Delta\rrbracket$ denotes the cedent of translations of formulas in Γ resp. in Δ.) Formulas W^j will be called witnessing formulas.

Moreover, to be able to formalize the construction in S_2^1 we have to show that the length of W^j is polynomial in m and that the length of the G–proofs is polynomial in m, $|C|$ and $|D_i|$'s.

We proceed by considering several cases according to the type of the last inference.

(a) $\underline{\wedge : \text{right}}$. The principal formula

$$E(a,\alpha) \wedge F(a,\alpha)$$

must be $\sum_0^{1,b}(BD)$ and belongs to Δ. Let $\overline{W}^j$ resp. $\overline{\overline{W}}^j$ be the witnessing formulas already constructed for the upper sequents of the inference containing E resp. F. Then define:

$$W^j \rightleftharpoons \llbracket E \wedge F\rrbracket \vee (\llbracket\neg E \wedge F\rrbracket \wedge \overline{W}^j) \vee (\llbracket\neg F\rrbracket \wedge \overline{\overline{W}}^j.$$

It is obvious that the sequent is correctly witnessed but we have to show that all its instances have actually polynomial G–proofs, as it is required.

The G–proof considers three cases

(i) $\llbracket E \wedge F\rrbracket(\llbracket\alpha\rrbracket/C)$ is true,

(ii) $(\llbracket\neg E \wedge F\rrbracket(\llbracket\alpha\rrbracket/C)$ is true,

(iii) $(\llbracket\neg F\rrbracket(\llbracket\alpha\rrbracket/C)$ is true.

The formula in (i) is itself in the succedent and so there is nothing to prove.

In the second case first show:

$$(1) \qquad W^j(\llbracket\alpha\rrbracket/C, \quad ,\llbracket\phi_i\rrbracket/D_i, \qquad \equiv \overline{W}^j(\llbracket\alpha\rrbracket/C, \quad ,\llbracket\phi_i\rrbracket/D_i,$$

and then:

$$(2) \qquad \begin{aligned} &\llbracket B_j\rrbracket(\llbracket\alpha\rrbracket/C,\ldots\llbracket\varphi_j\rrbracket/W^j(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)) \\ &\quad \equiv \llbracket B_j\rrbracket(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\varphi_j\rrbracket/\overline{W}^j(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)). \end{aligned}$$

(1) is proved from the definition of W^j and (2) is proved by induction on the logical complexity of B_j using proofs of the same for subformulas of B_j and (1).

The third case is handled similarly. Then by cuts these three cases are joined into a proof of the required instance.

(b) contraction : right. The non-trivial case is only when two occurrences of a proper $\sum_1^{1,b}(BD)$–formula are contracted:

$$\frac{\rightarrow \quad , \exists\varphi B(a,\alpha,\varphi), \exists\varphi B(a,\alpha,\varphi),}{\rightarrow}$$

Let $\overline{W}$ resp. $\overline{\overline{W}}$ be the two witnessing formulas corresponding to the two occurrences of the formula in the upper sequent. Then define:

$$W \rightleftharpoons (\llbracket B\rrbracket(\llbracket\alpha\rrbracket, \llbracket\varphi\rrbracket/\overline{W}) \supset \overline{W}) \wedge (\neg\llbracket B\rrbracket(\llbracket\alpha\rrbracket, \llbracket\varphi\rrbracket/\overline{W}) \supset \overline{\overline{W}}).$$

A G–proof of an instance is constructed as above considering two cases whether $\llbracket B\rrbracket(\llbracket\alpha\rrbracket/C, \llbracket\varphi\rrbracket/\overline{W}(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots))$ is resp. is not true. Then $W(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)$ is either equivalent to $\overline{W}(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)$ or to $\overline{\overline{W}}(\llbracket\alpha\rrbracket/C,\ldots,\llbracket\phi_i\rrbracket/D_i,\ldots)$ and the proof is completed as before.

(c) $\exists$: right, $\sum_0^{1,b}(BD) - CR$. This inference has the form:

$$\frac{\rightarrow \ldots, B(a,\alpha,\varphi/E(a,\alpha)),}{\rightarrow}$$

where E is $\sum_0^{1,b}(BD)$. Simply put:

$$W \rightleftharpoons \llbracket E\rrbracket(\llbracket\alpha\rrbracket).$$

(d) $\sum_1^{1,b}$-PIND. Consider two cases when the induction formula is resp. is not $\sum_0^{1,b}(BD)$.

The first case is an instance of the translation of first order induction and by [9] is provable in G, cf. property (d) of $[\![\ ]\!]$ in §1.

In the second case assume the induction is:

$$\frac{\ldots, \exists\phi E(\lfloor \frac{b}{2} \rfloor, \alpha, \phi) \rightarrow \exists\varphi E(b, \alpha, \varphi), \ldots}{\ldots, \exists\phi E(0, \alpha, \phi) \rightarrow \exists\varphi E(t, \alpha, \varphi), \ldots}$$

and let $\overline{W}(a, b, \alpha, \ldots, \phi_i, \ldots, \phi)$ be the witnessing formula constructed for the upper sequent.

Define terms t_k, $k = n$, $n-1, \ldots, 0$ by: $t_n := t$, $t_k := \lfloor \frac{t_{k+1}}{2} \rfloor$. Observe $t_0 = 0$. Here again n is the maximal length of value of t when parameters have length $\leq m$. Then put:

$$W^{(1)} \rightleftharpoons \overline{W}(a, b/t_1, \alpha, \phi_i, \phi)$$

and

$$W^{(k+1)} \rightleftharpoons \overline{W}(a, b/t_{k+1}, \alpha, \phi_i, \phi/W^{(k)}),$$

for $k < n$, and

$$W \rightleftharpoons W^{(n)}.$$

It is easily seen that $W^{(k)}$ witnesses implication:

$$\exists\phi E(0, \alpha, \phi) \rightarrow \exists\varphi E(t_k, \alpha, \varphi),$$

and hence W has the required properties. A G–proof verifying this is constructed by joining by cuts n G–proofs verifying correctness of instances for the upper sequent with b and ϕ being respectively t_1 and ϕ, t_2 and $W^{(1)}, \ldots, t_n$ and $W^{(n-1)}$. As n is polynomial in m we have only to verify that W is polynomial in m. However, we must be careful here: if ϕ has at least two occurrences in $\overline{W}$ then the length of $W^{(k)}$ grows exponentially in k and so W would not have the length polynomial in m. Hence before the construction we have to put first $\overline{W}$ into G–equivalent form with only one occurrence of ϕ, following some standard trick, cf. [11].

The remaining rules are analogical or dual (or trivial) to the rules treated above and we skip the details.

The construction of the witnessing formulas as well as of the required G–proofs is effective with polynomial bounds and so is readily formalized in S_2^1.

Finally, let us note that the witnessing formulas can be chosen fairly uniformly as quantified boolean formulas coding computations of oracle *PSPACE* machines, cf. [11]. This would, however, require more detailed construction. ▮

§5. COROLLARIES TO THE SIMULATION

THEOREM 5.0. *For $i \geq 2$, the set of Σ^b_i–consequences of U^1_2 is axiomatized by $S^1_2 + i\text{–}RFN(G)$. Thus the set of first order bounded consequences of U^1_2 is axiomatized by $S^1_2 + \{i - RFN(G) | i < \omega\}$.*

PROOF: The second part of the statement follows from the first part.

Formula $i - RFN(G)$ is Σ^b_i, cf. §1, and by Theorem 3.0 provable in U^1_2. Let A(a) be a Σ^b_i consequences of U^1_2; then by Theorem 4.0:

$$S^1_2 \vdash \forall y; G \ \vdash [\![A]\!]^{|y|}.$$

By the reflection principle then

$$S^1_2 \vdash \ i - RFN(G) \supset \text{“}\forall y; [\![A]\!]^{|y|} \in TAUT\text{”}.$$

But by Krajíček-Pudlák [9],

$$S^1_2 \vdash \text{“}[\![A]\!]^{|y|} \in TAUT\text{”} \to \forall x, |x| \leq |y| \supset A(x).$$

Putting this together we get:

$$S^1_2 + i - RFN(G) \vdash \ A(a).$$

This proves the theorem. ▮

COROLLARY 5.1. *For each $i \geq 2$, the set of Σ^b_i–consequences of U^1_2 is finitely axiomatizable.* ▮

§6. U^1_2 AND TNC

In Krajíček [8] it was shown that the set of bounded first order consequences of V^i_2, denoted $\Sigma^b_\infty(V^i_2)$, is exactly $S^i_2 + 1 - Exp$. Also it was observed that $\Sigma^b_\infty(\overset{\circ}{U}{}^1_2)$ proves

$$\Sigma^b_1 - L_2IND + 1 - Exp,$$

(and analogically for $i > 1$. Rule L_2IND is in [8] denoted $LLIND$.) Here we show that $\Sigma^b_\infty(U^1_2)$ is precisely $TNC + 1 - Exp$ and, in general, $\Sigma^b_\infty(U^i_2)$ is

$$TNC + \Sigma^b_i - L_2IND + 1 - Exp.$$

Theorem 6.0. *For $i \geq 1$ it holds: the set of bounded first order consequencs of U_2^i is precisely*

$$TNC + \Sigma_i^b - L_2IND + 1 - Exp.$$

Proof: The proof is analogical to the proof of Thm 2.5 in [8]. We recall the idea of the proof and then discuss only steps needed for the extension of the proof from [8] to our case. The idea is the following.

Having (M, X) a model of $\overset{\circ}{U}{}_2^1$ we define a model M' of TNC: the elements of M' are pairs (α, a), $\alpha \in X$, $a \in M$. We think about (α, a) as coding number $\Sigma\{2^i | i < a, \alpha(i)\}$. With this interpretation in mind it is easy to define in the obvious way operations on M' (for these definitions one needs bounded $\Delta_1^{1,b} - CA$). As an element $a \in M$ can be identified with the pair $(\alpha_a, |a|)$, where α_a is the set $\{i | bit(a, i) = 1\}$, M is naturally identified with an initial segment of M'. Pair (M, M') then forms a 1-fold model of TNC.

On the other side, having a 1–fold model (I, M) of TNC we define X as the class of all bounded subsets of I coded in M. That is:

$$X = \{\alpha \subseteq I | \alpha \quad \text{bounded}, \quad \alpha = \{i | bit(a, i) = 1\}, \quad \text{for some} \quad a \in M\}.$$

Then $(I, X) \models \overset{\circ}{U}{}_2^1 \ (BD)$. An easy compactness argument, together with Theorem 2.2, then establishes the result.

In [8] it was shown that model M' satisfies $\Sigma_1^b - L_2IND$. As extensionality is obvious it remains to observe that

$$M' \models \prod\limits_{1}^{b} -SEP.$$

This follows — via the construction of M' in [8] — from:

$$(M, X) \models \quad \text{bounded} \quad \prod\limits_{1}^{1,b} -SEP,$$

which is true by Theorem 2.1.

On the other side, $(I, X) \models \overset{\circ}{U}{}_2^1 \ (BD)$ follows immediately: for example $\Delta_1^{1,b} - CA$ follows from TNC proving a weak form of $\Delta_1^b - CA$:

$$(\forall t, A(t) \equiv_\neg B(t)) \to \exists y \forall t < |x| (A(t) \equiv (bit(y, t) = 1)),$$

where A, B are Σ_1^b-formulas, cf. Clote-Takeuti [3].

Cases for $i > 1$ are completely analogical. ∎

COROLLARY 6.1. *U_2^1 is not $\prod_1^b$–conservative over TNC.*

PROOF: As $TNC + 1 - Exp$ is $\Sigma_\infty^b(U_2^1)$, in particular:

$$TNC + 1 - Exp \vdash S_2.$$

Thus:

$$TNC + Exp = S_2 + Exp.$$

It is well-known that $S_2 + Exp$ is not $\prod_1^b$–conservative over S_2, cf. Paris-Wilkie [12], and hence $TNC + Exp$ is not $\prod_1^b$–conservative over $TNC \subseteq S_2$. As $TNC + (k+1) - Exp = (TNC + k - Exp) + 1 - Exp$ and $TNC + Exp = \cup_k TNC + k - Exp$, this immediately implies that $TNC + 1 - Exp$ is not $\prod_1^b$–conservative over TNC and hence neither is U_2^1. ∎

§7. U_2^1 AND A $\Delta_1^{1,b}$ EXTENSION OF T_2.

We are not able to show that U_2^1 is not conservative over S_2. In this section we at least show that it is stronger than a $\Delta_1^{1,b}$–extension of S_2; The formula we constructed to separate U_2^1 from the $\Delta_1^{1,b}$–extension is of second order.

The class of the formulas without any second order quantifiers is denoted $\Delta_0^{1,b}$. The $\Delta_0^{1,b}$ extension of S_2 is obtained from S_2 by introducing the following initial sequents and inferences.

(1) $s_1 = t_1, \ldots, s_n = t_n, \alpha(s_1, \ldots, s_n) \rightarrow \alpha(t_1, \ldots, t_n)$

(2) $\dfrac{F(\{x_1, \ldots, x_n\}A(x_1, \ldots, x_n)), \Gamma \rightarrow \Delta}{\forall\phi F(\phi), \Gamma \rightarrow \Delta}$

$$\frac{\Gamma \rightarrow \Delta, F(\{x_1, \ldots, x_n\}A(x_1, \ldots, x_n))}{\Gamma \rightarrow \Delta, \exists\phi F(\phi)}$$

where $A(a_1, \ldots, a_n)$ is a $\Delta_0^{1,b}$–formula.

$$\frac{|\Gamma \rightarrow \Delta, F(\alpha)}{\Gamma \rightarrow \Delta, \forall\phi f(\phi)} \qquad \frac{F(\alpha), \Gamma \rightarrow \Delta}{\exists\phi F(\phi), \Gamma \rightarrow \Delta}$$

where α satisfies the eigenvariable condition i.e. α does not occur in the lower sequent.

(3) $\Delta_0^{1,b} - PIND$

$$\frac{A([\frac{1}{2}a]), \Gamma \rightarrow \Delta, A(a)}{A(0), \Gamma \rightarrow A(t)}$$

where a satisfies the eigenvariable condition and $A(a)$ is a $\Delta_0^{1,b}$–formula. The $\Delta_0^{1,b}$–extension of T_2 is obtained from T_2 by introducing (1), (2) and the following inference:

(4) $\Delta_0^{1,b} - IND$

$$\frac{A(a), \Gamma \rightarrow \Delta, A(S(a))}{A(0), \Gamma \rightarrow \Delta, A(t)}$$

where a satisfies the eigenvariable condition and $A(a)$ is a $\Delta_0^{1,b}$–formula.

The $\Delta_1^{1,b}$–extension of S_2 is obtained from S_2 by introducing (1), (2'), and (3'), where (2') and (3') are obtained from (2) and (3) respectively by replacing $\Delta_0^{1,b}$ by $\Delta_1^{1,b}$ with respect to S_2. (3') is called the $\Delta_1^{1,b}$–$PIND$.

Analogically, the $\Delta_1^{1,b}$–extension of T_2 is obtained from T_2 by introducing (1), (2'), and (4'), where (4') is obtained from (4) by replacing $\Delta_0^{1,b}$ by $\Delta_1^{1,b}$ with respect to T_2. (4') is called the $\Delta_1^{1,b}$–IND.

Lemma 7.1. *Let $F(\phi) \in \Delta_0^{1,b}$ and $\rightarrow \exists\phi F(\phi)$ be provable in the $\Delta_0^{1,b}$ extension of S_2 (or T_2). Then there exists a sequent of the form*

$$\exists \vec{u}^1 \leq \vec{t}^1 \; F(\{x\}A_1(x, \vec{u} \qquad\qquad \vee \exists \vec{u}^n \leq \vec{t}^n \; F \quad x\}A_n(x, \vec{u}^n)),$$

here A_1 $\qquad$ A_n are in $\Delta_0^{1,b}$ which is also provable in S_2 (or T_2,

Proof: If $\rightarrow \exists\phi F(\phi)$ is provable, there exists a free cut free proof P of $\exists\phi F(\phi)$. Without loss of generality, we assume that P satisfies the following conditions.

(1) P is in a free variable normal form.

(2) Let $\vec{c}$ be a sequence of all parameter variables in P and $\vec{b}$ be an enumeration of all other variables in P satisfying the condition that if the elimination inference for b_i is below the elimination inference for b_j then $i < j$. There exists an assignment $t_i(\vec{c})$ for b_i satisfying the following conditions.

(i) $t_i(\vec{c})$ is a term in the language of S_2.

(ii) If the elimination inference of b_i is

$$\frac{A(\lfloor b_i/2 \rfloor), \Gamma \rightarrow \Delta, A(b_i)}{A(0), \quad \rightarrow \Delta, A(t(b_1,}$$

or

$$\frac{b_i \leq t(b_1, \ldots, b_{i-1}, \vec{c}), A(b_i),] \qquad \Delta}{\exists x \leq t(b_1, \ldots, b_i, \vec{c}) A(x), \Gamma \qquad \Delta}$$

or

$$\frac{b_i \le t(b_1,\dots,b_{i-1},\vec{c}),\Gamma \to \Delta, A(b_i)}{\Gamma \to \Delta, \forall x \le t(b_1,\dots,b_{i-1},\vec{c})A(x)}$$

then $a_1 \le t_1(\vec{c}),\dots,a_{i-1} \le t_{i-1}(\vec{c}) \to t(a_1,\dots,a_{i-1},\vec{c}) \le t_i(\vec{c})$ is provable without using logical inferences, induction, or any free variables other than $a_1,\dots,a_{i-1}$ and $\vec{c}$.

Let $\Gamma \to \Delta$ be a sequent in P. Let $b_1,\dots,b_n$, $\vec{c}$ be all free variables in $\Gamma \to \Delta$ and below $\Gamma \to \Delta$. Then we transform P to P' by replacing $\Gamma \to \Delta$ by $b_1 \le t_1(\vec{c}),\dots,b_n \le t_n(\vec{c})$, $\Gamma \to \Delta'$, where Δ' is obtained by transforming:

$$\frac{\Gamma \to \Delta_0, F(\{x\}A(x,b_1,\dots,b_n))}{\Gamma \to \Delta_0, \exists\phi F(\phi)}$$

to:

$$\frac{b_1 \le t_1(\vec{c}),\dots,b_n \le t_n(\vec{c}),\Gamma \to \Delta_0', F(\{x\}A(x,b_1,\dots,b_n))}{b_1 \le t_1(\vec{c}),\dots,b_n \le t_n(\vec{c}),\Gamma \to \Delta_0', \exists\,\vec{u} \le \vec{t}\ (\vec{c})F(\{x\}A(x,\vec{u}))}.$$

The provable sequent we are looking for is easily obtained from this proof P'. (See also Proposition 16.7 and Proposition 16.9 in [13]). ▮

LEMMA 7.2. *Let A be a $\Delta_1^{1,b}$-formula with respect to the $\Delta_0^{1,b}$-extension of S_2 (or T_2). Then there exists a $\Delta_0^{1,b}$-formula B such that $A \longleftrightarrow B$ is provable in $\Delta_0^{1,b}$-extension of S_2 (or T_2).*

PROOF: We treat only the case that A is $\forall\phi F(\phi)$, $\forall\phi F(\phi) \longleftrightarrow \exists\psi G(\psi)$ is provable in the system, and $F(\phi)$ and $G(\psi)$ are $\Delta_0^{1,b}$-formulas. Then by Lemma 7.1, there exist $\Delta_0^{1,b}$-formulas $A_1,\dots,A_n$, $B_1,\dots,B_n$ such that

$$\forall\,\vec{u}^{\,1} \le \vec{t}^{\,1}\ F(\{x\}A_1(x,\vec{u}^{\,1})) \wedge \cdots \wedge \forall\,\vec{u}^{\,n} \le \vec{t}^{\,n}\ F(\{x\}A_n(x,n\,\vec{u}^{\,n}))$$
$$\longrightarrow \exists\,\vec{v}^{\,1} \le \vec{s}^{\,1}\ G(\{x\}B_1(x,\vec{v}^{\,1})) \vee \cdots \vee \exists\,\vec{v}^{\,m} \le \vec{s}^{\,m}\ G(\{x\}B_m(x,\vec{v}^{\,m})).$$

Since $\exists\psi G(\psi) \to \forall\phi F(\phi)$ is provable in the system,

$$\exists\,\vec{v}^{\,1} \le \vec{s}^{\,1}\ G(\{x\}B_1(x,\vec{v}^{\,1})) \vee \cdots \vee \exists\,\vec{v}^{\,m} \le \vec{s}^{\,m}\ G(\{x\}B_m(x,\vec{v}^{\,m})),$$
$$\exists\psi G(\psi),$$
$$\forall\phi F(\phi),$$

and

$$\forall\,\vec{u}^{\,1} \le \vec{t}^{\,1}\ F(\{x\}A_1(x,\vec{u}^{\,1})) \wedge \cdots \wedge \forall\,\vec{u}^{\,n} \le \vec{t}^{\,n}\ F(\{x\}A_n(x,\vec{v}^{\,n}))$$

are equivalent. Obviously the first formula and the last formula are $\Delta_0^{1,b}$-formulas. ▮

COROLLARY 7.3. *The systems: the $\Delta_0^{1,b}$–extension of S_2, the $\Delta_0^{1,b}$–extension of T_2, the $\Delta_1^{1,b}$–extension of S_2, and the $\Delta_1^{1,b}$–extension of T_2 are equivalent.*

PROOF: This immediately follows from Lemma 7.2 since $S_2(\alpha)$ and $T_2(\alpha)$ are the same systems. ▮

COROLLARY 7.4. *The $\Delta_1^{1,b}$–extension of S_2 is a conservative extension of S_2.*

PROOF: This immediately follows from Corollary 7.3 since the $\Delta_0^{1,b}$ –extension of S_2 is conservative over S_2. (See also Corollary 16.3 in **13**). ▮

Now we shall work in U_2^1. We include sequents (1) above among initial sequents of U_2^1. Define formulas $F(a,\alpha,\beta)$ and $G(a,k,\alpha,\beta)$ as follows.

$$F(a,\alpha,\beta) \iff \forall x \leq 2a((|x| = |a| \supset (\beta(x) \leftrightarrow \alpha(x)))$$

$$\wedge(|x| < |a| \supset (\beta(x) \leftrightarrow (\beta(2x) \wedge \neg\beta(2x+1)) \vee (\neg\beta(2x) \wedge \beta(2x+1))).$$

$$G(a,k,\alpha,\beta) \iff \forall x \leq 2a(|a| - k \leq |x| \supset ((|x| = |a| \supset (\beta(x) \leftrightarrow \alpha(x)))$$

$$\wedge(|x| < |a| \supset (\beta(x) \leftrightarrow (\beta(2x) \wedge \neg\beta(2x+1)) \vee (\neg\beta(2x) \wedge \beta(2x+1))))).$$

Observe that if $F(a,\alpha,\beta)$ is true then $\beta(1)$ resp. $\neg\beta(1)$ is equivalent to the fact that the parity of the set $\{x \| x| = |a| \ \& \ \alpha(x)\}$ is odd resp. is even.

LEMMA 7.5. $U_2^1 \vdash \exists\beta F(a,\alpha,\beta)$.

PROOF: This is easily shown by *LIND* on k applied to $\exists\beta G(a,k,\alpha,\beta)$. ▮

LEMMA 7.6. $U_2^1 \vdash F(a,\alpha,\beta), F(a,\alpha,\gamma), |b| \leq |a|, \beta(b) \rightarrow \gamma(b)$.

PROOF: This is easily shown by *LIND* on k applied to $\forall x \leq 2a(|a| \dot{-} k \leq |x| \supset (\beta(x) \longleftrightarrow \gamma(x)))$. ▮

LEMMA 7.7. $U_2^1 \vdash \exists\beta(F(a,\alpha,\beta) \wedge \beta(1)) \longleftrightarrow \forall\beta(F(a,\alpha,\beta) \supset \beta(1))$. ▮

THEOREM 7.8. *$\forall\alpha(\exists\beta(F(a,\alpha,\beta) \wedge \beta(1)) \longleftrightarrow \forall\beta(F(a,\alpha,\beta) \supset \beta(1)))$ is provable in U_2^1 but not provable in the $\Delta_1^{1,b}$–extension of S_2.*

PROOF: Suppose $\forall\alpha(\exists\beta(F(a,\alpha,\beta) \wedge \beta(1)) \longleftrightarrow \forall\beta(F(a,\alpha,\beta) \supset \beta(1)))$ is provable in the $\Delta_1^{1,b}$–extension of S_2. Then $\exists\beta(F(a,\alpha,\beta) \wedge \beta(1)) \longleftrightarrow \forall\beta(F(a,\alpha,\beta) \supset \beta(1))$ is provable in the $\Delta_0^{1,b}$–extenesion of S_2. So $\exists\beta(F(a,\alpha,\beta)\wedge\beta(1))$ is equivalent to a $\Delta_0^{1,b}$–formula. This is a contradiction since
$\exists\beta(F(a,\alpha,\beta) \wedge \beta(1))$ expresses the parity of α and the parity cannot be expressed by a $\Delta_0^{1,b}$–formula as follows from A. Yao [16], cf. J. Håstad [6] for a proof. ∎

REMARK: In the proof of the theorem # is not used. Therefore

$$\forall\alpha(\exists\beta(F(a,\alpha,\beta) \wedge \beta(1)) \longleftrightarrow \forall\beta(F(a,\alpha,\beta) \supset \beta(1)))$$

is also provable in U_1^1.

§8. U_2^1 versus $I\Delta_0$

We shall separate U_2^1 and $I\Delta_0$ by showing that a consistency statement unprovable in $I\Delta_0$ is provable in U_2^1. We assume that $I\Delta_0$ is formulated in a sequential formalism with IND–rule instead of IND–axioms, cf. [1, Theory T_1] or [7].

We shall use a notion of normal consistency from in [14], for its variants see [7, 8,15]. For details of the definition see the references, we only sketch the idea here.

Normal Proofs in $I\Delta_0$ are proofs containing only bounded formulas and which are in a free variable normal form. If $b_1, \dots, b_k$ are all non–parametrical free variables then if the elimination rule of b_j occurs below the elimination rule of b_i, then $j < i$. The normal proof is augmented by a list of terms $t_1(\bar{a}), \dots, t_k(\bar{a})$ where $\bar{a}$ are the parametrical free variables.

The elimination rule of b_i is either IND, $\exists \leq$ left or $\forall \leq$ right. Moreover, if the elimination inference of b_i is

$$\frac{A(b_i), \Gamma \rightarrow \Delta, A(b_i + 1)}{A(0), \Gamma \rightarrow \Delta, A(s(\bar{a}, b_1, \dots, b_{i-1}))}$$

or

$$\frac{b_i \leq s(\bar{a}, b_1, \dots, b_{i-1}), A(b_i), \Gamma \rightarrow \Delta}{\exists x \leq s(\bar{a}, b_1, \dots, b_{i-1}) A(x), \Gamma \rightarrow \Delta}$$

or

$$\frac{b_i \leq s(\bar{a}, b_1, \dots, b_{i-1}), \Gamma \rightarrow \Delta, A(b_i)}{\Gamma \rightarrow \Delta, \forall x \leq s(\bar{a}, b_1, \dots, b_{i-1}) A(x)},$$

then $x_1 \leq t_1(\bar{a}), \ldots, x_{i-1} \leq t_{i-1}(\bar{a})$ implies $s(\bar{a}, x_1, \ldots, x_{i-1}) \leq t_i(\bar{a})$ and this implication is provable without induction or quantifier rules. These supplementary proofs are also required.

Thus the normal proof is a bounded proof augmented by a list of terms and supplementary proofs with the above properties.

Normal consistency of $I\Delta_0$ asserts that the empty sequent is not normally provable.

THEOREM 8.1. $U_2^1 \vdash N\ Con(I\Delta_0)$

PROOF: The proof is rather sketchy as the material is elaborated in [**14, 7,8,15**] and the details can be found there. The idea is that one can find in U_2^1 a $\Delta_1^{1,b}$–partial truth definition for formulas occurring in a normal $I\Delta_0$–proof and thus prove its soundness.

For any #–free term t, the value of t on $\bar{c}$, $val(\ t\ , \bar{c})$, satisfies the inequality: $val(\ t\ , \bar{c}) \leq \max(\bar{c}, 2)^{|\ t\ |}$, and can be defined in S_2^1.

Let D be a normal $I\Delta_0$–proof with $\bar{a}$ parametrical variables. To check the truth value of the end–sequent for given $\bar{a}$ following the derivation D, one has to know the truth–values of the sequents in D only for $b_i \leq t_i(\bar{a})$, where t_i are the terms guaranteed by D. If D is a proof of a contradiction its end-sequent does not contain any variables and so t_i are closed. Hence it is sufficient to construct a partial truth definition for bounded formulas $A(\bar{b})$ occurring in D *s.t.* : $A\ \leq m$, $\max(\bar{b}) \leq n$ and quantifier complexity of $A \leq k$. Obviously: $m \leq D$, $n \leq \max_i\ (\mathrm{val}(t_i)) \leq 2^{|D|} \leq D$ and $k \leq |D|$.

Let $Tr(\gamma, m, n, k)$ be formula

$$\begin{aligned}
&\forall\ A\ \leq m \forall \bar{b} \leq n, \quad [\text{“}q\text{–complexity of } \ A \leq k\text{”}] \supset \\
&\supset [(A\ q\text{–free} \quad \supset (\gamma(\ A\ , \bar{b}) \equiv T(\ A\ , \bar{b})))\wedge \\
&\wedge (\ A\ \ = (\ Qx \leq sB(x)\ \ \supset \\
&\supset (\gamma(\ A\ , \bar{b}) \equiv (Qx \leq \mathrm{val}(S, \bar{b})\gamma(\ B(x)\ , \bar{b} * x))))\wedge
\end{aligned}$$

$$\wedge \cdots\cdot \text{ and clauses for Tarski conditions for } \ \wedge, \vee, \neg \text{ and } \ \supset \cdots\cdot\ ],$$

where T is a truth definition for quantifier free formulas.

Thus we only need to prove that there is a unique γ satisfying $Tr(\gamma, m, n, k)$ for m, $n \leq D$ and $k \leq |D|$. This is easily proved by $\sum_1^{1,b}$–$LIND$ on k.

Having such γ the soundness of D is easily verified. ▮

$I\Delta_0$ does not prove its own normal consistency, this is proved by a technique based on length–of–proof considerations completely analogical to [**7, 8**], cf. also [**14, 15**]. Thus we have the following statement.

THEOREM 8.2. *U^1_2 is not conservative over $I\Delta_0$.* ∎

Let us mention another possible argument giving Thm. 8.1. In [15], a transformation of $I\Delta_0$–proofs to S^0_2–proofs is described. In particular, in S^1_2 we can from $N\ Con(S^0_2)$ derive $N\ Con(I\Delta_0)$. As (by [14]) $\overset{\circ}{U}{}^1_2 \vdash N\ Con(S^0_2)$, $U^1_2 \vdash N\ Con(I\Delta_0)$ follows using also Theorem 2.2.

In Krajíček [8] it was shown that V^1_3 (and weaker theories of the form V^1_2 + "f is total", cf. [8]) is not conservative over S_2. Using the results of §§2, 6 here it is possible to obtain the same result for U^1_3 too.

REFERENCES

[1]. S. Buss, "Bounded Arithmetic," Bibliopolis, Napoli, 1986.

[2]. S. Buss, *Axiomatizations and Conservation Results for Fragments of Bounded Arithmetic.* to appear Contemporary Mathematics AMS, Proc. of Workshop in Logic and Computation, (1987).

[3]. P. Clote–G. Takeuti, *Bounded Arithmetic for NC, Alog TIME, L and NL typescript.*

[4]. S. Cook, *Feasibly Constructive Proofs and the Propositional Calculus,* Proc. 7th Annual ACM Symp. Th. of Comp..

[5]. M. Dowd, *Propositional Representation of Arithmetic Proofs,* 10th STOC (1978), 246–252, San Diego.

[6]. J. Håstad, "Computational Limitations of Small-Depth Circuits," MIT Press, Cambridge, Massachusetts, Mass., 1987.

[7]. J. Krajíček, *$\prod_1$–conservativeness in Systems of Bounded Arithmetic.* Submitted.

[8]. J. Krajíček, *Exponentiation and Second Order Bounded Arithmetic,* Annals of Pure and Applied Logic (1989). To appear.

[9]. J. Krajíček–P. Pudlák, *Quantified Propositional Calculus and Fragments of bounded Arithmetic,* Zeitschr. f. Math. Logik (1988). To appear.

[10]. J. Krajíček–P. Pudlák–G. Takeuti, *Bounded Arithmetic and the Polynomial Hierarchy,* Annals of Pure and Applied Logic (1989). To appear.

[11]. A. Meyer–L. Stockmeyer, *The Equivalence Problem for Regular Expressions with Squaring Requires Exponential Time,* Proc. 13th IEEE Symp. on Switching and Automato Th. (1973), 125–129.

[12]. J. Paris–A. Wilkie, *On the Scheme of Induction for Bounded Arithmetic Formulas,* Annals of Pure and Applied Logic **35(3)** (1987), 205–303.

[13]. G. Takeuti, "Proof Theory," North Holland, 1975. Second edition (1987).

[14]. G. Takeuti, *Bounded Arithmetic and Truth Definition,* Annals of Pure and Applied Logic **39(1)** (1988), 75–104.

[15]. G. Takeuti,, *S^i_3 and $\overset{\circ}{V}{}^i_2$ (BD).* Archive for Mathematical Logic (1990). To appear.

[16]. A. Yao, *Separating the Polynomial–Time Hierarchy by Oracles Proceedings,* 26th Annual IEEE Symposium on Foundations of Computer Science (1985), 1–10.

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, Illinois 61801, U.S.A.