A CONSERVATION RESULT CONCERNING BOUNDED THEORIES AND THE COLLECTION AXIOM

Samuel R. Buss
Mathematical Sciences Research Institute
Berkeley, California

August 1985

Abstract.

We present two proofs, one proof-theoretic and one model-theoretic, showing that adding the $B\Sigma_1^0$-collection axioms to any bounded first-order theory R of arithmetic yields an extension which is $\forall\Sigma_1^0$-conservative over R.

Preliminaries.

A theory of arithmetic R contains the non-logic symbols 0, S, +, $\cdot$, and $\leq$. R may contain further non-logical symbols; in particular, S_2 is a theory of arithmetic [1]. We shall say that R is sufficient if and only if R proves

---

Research supported in part by NSF Grant DMS 85-11465
1980 *Mathematics Subject Classification.* 03C30, 03B99.
Key words and phrases. Bounded Arithmetic, collection axioms, cut elimination, resplendency.

(a) $\leqslant$ is a linear ordering.

(b) For every term $t(\vec{x})$, there is a term σ_t such that

$$R \vdash x_1 \leqslant y_1 \wedge \ldots \wedge x_k \leqslant y_k \longrightarrow t(\vec{x}) \leqslant \sigma_t(\vec{y}).$$

Of course, the usual bounded theories of arithmetic, for example $I\Delta_0$ or S_2^i, are sufficient, Indeed letting σ_t be t suffices for these theories. Although Theorem 1 below holds for second order bounded theories of arithmetic such as U_2^i and V_2^i, we shall only discuss first order theories in this paper. From now on, R is pressumed to be a first order theory.

The syntax of first order logic is enlarged to include <u>bounded quantifiers</u> of the forms $(\forall x \leqslant t)$ and $(\exists x \leqslant t)$ where t is any term not containing x. In [1] it is shown how Gentzen's sequent calculus LK may be enlarged to incorporate bounded quantifiers. A formula is <u>bounded</u> if and only if it contains no unbounded (i.e., usual) quantifiers. A theory R of arithmetic is <u>bounded</u> if and only if R is axiomatized by a set of bounded formulae.

The class of Σ_1^0-formulae is defined to contain those formulae in which each unbounded quantifier is either existential and in the scope of an even number of negations or universal and in the scope of an odd number of negations. Note that our definition of Σ_1^0 is slightly broader than the set of Σ_1 formulae defined by Paris and Kirby [4]. The $B\Sigma_1^0$-<u>collection axioms</u> are

$$(\forall x \leqslant a)(\exists y)A(x,y) \longrightarrow (\exists z)(\forall x \leqslant a)(\exists y \leqslant z)A(x,y)$$

where A is any Σ_1^0-formula [4]. Note that A may contain additional free variables as parameters. The $B\Sigma_1^0$-collection axioms are equivalent to the $B\Sigma_1$-collection axioms of Paris and Kirby [4] since $B\Sigma_1$-collection can prove that every Σ_1^0 formula is equivalent to a Σ_1-formula. The class $\forall\Sigma_1^0$ of formulae is the set of sentences which are universal

closures of Σ^0_1-formulae.

The object of this paper is to prove:

Theorem 1. Let R be a bounded, sufficient theory of arithmetic. Then R+BΣ^0_1 is $\forall\Sigma^0_1$-conservative over R (in other words, every $\forall\Sigma^0_1$-consequence of R+BΣ^0_1 is a theorem of R).

It has been known for some time that $I\Delta_0$+BΣ^0_1 is Π^0_2-conservative over $I\Delta_0$. However, the proof of this by Paris [3] does not extend readily to prove Theorem 1. This author first discovered the proof-theoretic proof of Theorem 1 after Alex Wilkie brought Paris' theorem to his attention. Later, a result of J.P. Ressayre [5] prompted the author's discovery of a model-theoretic proof based on resplendency.

Both proofs are presented below and they are independent and self-contained; so the reader should feel free to read only the one which he or she prefers.

The Proof-Theoretic Proof

We shall work with the sequent calculus LKB, which is Gentzen's system LK enlarged to include bounded quantifiers (see chapter 4 of [1]). In addition to the inferences of LKB we allow inferences given by the BΣ^0_1-collection rule:

$$\frac{\Gamma \longrightarrow (\forall x\leqslant t)(\exists y)A(x,y),\Delta}{\Gamma \longrightarrow (\exists z)(\forall x\leqslant t)(\exists y\leqslant z)A(x,y),\Delta}$$

where Γ and Δ denote arbitrary cedents of formulae and A must be a Σ^0_1-formula.

Lemma 2. The BΣ^0_1-collection axiom and the BΣ^0_1-collection rule are equivalent.

Proof. This is obvious. ■

A proof P of the sequent calculus LKB plus BΣ^0_1-collection is a tree of sequents

$\Gamma \longrightarrow \Delta$ where Γ and Δ are lists of formulae. Each node in the proof tree must be a valid inference. The lowest sequent, or root, of P is called the endsequent or the conclusion of P. The leaves, or highest sequents, of P are the initial sequents of P. When A is an occurrence of a formula in an upper sequent of an inference of P, the successor of A is defined to be the formula in the lower sequent of the same inference which corresponds to A. Except when A is the principal formula of a cut (modus ponens) inference A always has a unique successor. If A_{i+1} is a successor of A_i for all $i < k$ then A_k is defined to be a descendant of A_0. If in addition A_0 and A_k are occurrences of the same formula then A_k is a direct descendant of A_0.

We modify the definition [1] of a free cut somewhat to account for the new collection rules.

Definition. A cut is free if and only if neither of the following hold:

(1) one of the principal formulae of the cut is a direct descendant of a formula in an initial sequent (i.e., in an axiom),

(2) one of the principal formulae of the cut is a direct descendant of the principal formula of a $B\Sigma_1^0$-collection inference.

Lemma 3. Let R be any first order theory. The free cut elimination theorem holds for $R+B\Sigma_1^0$. Namely, if P is an $(R+B\Sigma_1^0)$-proof, then there is a free-cut free $(R+B\Sigma_1^0)$-proof P^* with the same conclusion as P so that the principal formulae of collection inference in P^* are instances of the principal formulae of collection inferences of P.

The proof of Lemma 3 follows the usual proof of the cut-elimination theorem (see Takeuti [6]).

Lemma 4. Let R be a bounded, sufficient theory of arithmetic and suppose $A \in \Sigma_1^0$ and $R \vdash A$. Further suppose A contains a subformula of the form $(\exists x)B$. That is to say, $A = C((\exists x)B)$ where $C(\alpha)$ contains only a single instance of the second order variable α. Then there is a term t such that

$$R \vdash C((\exists x \leq t)B).$$

Proof (outline). This is a corollary to a theorem of Parikh [2]. For our purposes, it is useful to see that Lemma 4 can be proved by the method of proof of Theorem 4.11 of [1]. This proof consists of three parts: first, by cut elimination, there is a cut free R-proof of A. Second, it can be shown that in this cut free proof all of the free variables can be explicitly bounded; that is to say, for each free variable b_i there is a term u_i such that b_i is restricted to be less than u_i and further the only variables of u_i are the free variables of A. Finally, it is easy to see that whenever an unbounded existential quantifier is introduced, it can be explicitly bounded by a term involving only the free variables of A. The reader should refer to [1] for complete details. (Actually, the proof is easier here than for theorem 4.11 of [1] since there are no induction inferences in R.) Note that the proof depends strongly on R being both bounded and sufficient. ■

Lemma 4 can be strengthened to apply to theories with $B\Sigma_1^0$-collection; this is the content of Lemma 5.

Lemma 5. Let R be a bounded, sufficient theory of arithmetic and suppose $A \in \Sigma_1^0$ and $R+B\Sigma_1^0 \vdash A$. Further suppose $A = C((\exists x)B)$ where $C(a)$ contains only a single instance of a. In addition assume that there is a free-cut free $(R+B\Sigma_1^0)$-proof P of A so that the occurrence of A in the endsequent of P is not a descendant of the principal formula of any collection inference in P. Then there is a term t and a free-cut free $(R+B\Sigma_1^0)$-proof P^* of $C((\exists x \leq t)B)$ such that P^* and P have the same number of collection inferences.

Proof. Since A is not a descendant of the principal formula of a collection inference, the construction used in the proof of Lemma 4 still applies. ■

If R is any theory and P is a $(R+B\Sigma_1^0)$-proof, we say that P is **good** if and only if for every cut inference in P either its principal formula is bounded or one of its principal formulae is a direct descendant of the principal formula of a $B\Sigma_1^0$-collection inference.

Since R is a bounded theory, every direct descendant of a formula in an initial sequent is bounded; hence every free cut free proof is good.

We define some further syntactic properties of a sequent calculus proof P. An inference branch of P is a sequence of inferences $I_1,\ldots,I_k$ such that every upper sequent of I_1 is an initial sequent of P, the lower sequent of I_k is the endsequent of P, and for $1\leqslant j<k$, the lower sequent of I_j is an upper sequent of I_{j+1}. If B is an inference branch of P and I is an inference of P then I is to the left of B if and only if I is not in B and I is on the left side of B in the proof tree P. It is important for this definition that upper sequents of inferences are always ordered in the usual fashion (as in [1] or Takeuti [6]). If I and J are inferences, then I is to the left of J if and only if I is to the left of every inference branch containing J.

We are now ready to prove the main lemma for Theorem 1.

Lemma 6. Let R be any bounded and sufficient theory of arithmetic. Suppose P is a good $(R+B\Sigma^0_1)$-proof of a Σ^0_1-formula A. Then $R\vdash A$.

Proof. The proof is by induction on the number c of uses of the $B\Sigma^0_1$ collection rule in P. For c=0, this is trivial. So suppose $c\geqslant 1$. Let I be the unique collection inference of P such that no other collection inference is above or to the left of I. So I is of the form

$$\frac{\Gamma \longrightarrow (\forall x\leqslant t)(\exists y)C(x,y),\Delta}{\Gamma \longrightarrow (\exists z)(\forall x\leqslant t)(\exists y\leqslant z)C(x,y),\Delta}$$

Let Q be the subproof of P which has I as its root.

We claim that every formula in Γ is a Π^0_1-formula and every formula in Δ is a Σ^0_1-formula. If not; let $B \notin \Sigma^0_1$ and $B \in \Delta$, or $B \notin \Pi^0_1$ and $B \in \Gamma$. Since no descendant of B can appear in the endsequent of P and no descendant of B can be the principal formula of a $B\Sigma^0_1$-collection inference and since P is good, it must be the case that some descendant E of B is a Σ^0_1-formula in the antecedent of a sequent and is removed by a cut inference and the formula against which E is cut must be a direct descendant of the principal formula of a collection inference. But this is impossible since

there is no collection inference to the left of I and the claim is established.

Since Q is an R-proof except for its last inference, it now follows by Lemma 4 that there is term s so that R proves

$$\Gamma \longrightarrow (\forall x \leqslant t)(\exists y \leqslant s(x))C(x,y),\Delta$$

By the sufficiency of R and by Lemma 3, there is a good R-proof Q* which has final inference:

$$\frac{\Gamma \longrightarrow (\forall x \leqslant t)(\exists y \leqslant \sigma_s(t))C(x,y),\Delta}{\Gamma \longrightarrow (\exists z)(\forall x \leqslant t)(\exists y \leqslant z)C(x,y),\Delta}$$

Replace the subproof Q of P by Q* to form the proof P*. If P* is good, we are done since P* has one less collection inference than P. So suppose P* is not good. Then there is subproof of P* of the form

$$\frac{\begin{array}{cc} Q_1 & Q_2 \\ \Pi \longrightarrow D,\Lambda & \Pi, D \longrightarrow \Lambda \end{array}}{\Pi \longrightarrow \Lambda}$$

where Q* is a subproof of Q_1, $D \in \Sigma_1^0$ and D is a direct descendant of the principal formula of the last inference of Q*. Since Q_1 has fewer than c $B\Sigma_1^0$-collection inferences and by the induction hypothesis, there is an R-proof Q_1^* of $\Pi \longrightarrow D,\Lambda$.

Let the unbounded quantifiers of D be $(Q_1x_1),\ldots,(Q_kx_k)$ where, of course, existential (respectively, universal) quantifiers occur positively (negatively) in A. An argument similar to the one above establishes that $\Pi \subset \Pi_1^0$ and $\Lambda \subset \Sigma_1^0$. Thus k applications of Lemma 4 show that there are terms $t_1,\ldots,t_k$ and a good R-proof Q_3 with endsequent

$$\Pi \longrightarrow D^*,\Lambda$$

where D* is obtained from D by replacing each unbounded quantifier (Q_ix_i) by the bounded quantifier $(Q_ix_i \leqslant t_i)$.

It is easy to modify Q_2 to obtain a proof Q_4 with endsequent $\Pi, D^* \longrightarrow \Lambda$ so that Q_2 and Q_4 have the same number of collection inferences and so that Q_4 is also good.

Finally, we replace the subproofs Q_1 and Q_2 of P^* by Q_3 and Q_4 and obtain a good proof with the same endsequent as P and with fewer collection inferences than P. Applying the induction hypothesis yields an R-proof of A. ■

Theorem 1 is now proved, since if $R+B\Sigma_1^0$ proves the universal closure of a Σ_1^0-formula A then, by Lemma 3 (cut elimination), there is a good proof of A, and hence, by Lemma 6, there is an R-proof of A.

The Model-Theoretic Proof

We next present a second, model-theoretic proof of Theorem 1.

Let R be any bounded, sufficient model of arithmetic. If M is a model of R, then the $\leqslant$ relation gives a linear ordering on R. A subset I of M is an initial segment of M if and only if for all $b \in I$, $c \in M$, $c \leqslant b$ implies $c \in I$. We say that I is closed under all operations if and only if for every sequence $\vec{c}$ of elements of I and every term t, $t(\vec{c}) \in I$.

Definition. Let $M \models R$. The language $\mathcal{L}(M)$ is the language of R enlarged to include a constant symbol for each element of M. If A is any formula and $b \in M$, then $A^{\leqslant b}$ is formed from A by changing each unbounded quantifier $(\forall x)$ or $(\exists y)$ to the bounded quantifier $(\forall x \leqslant b)$ or $(\exists y \leqslant b)$. So $A^{\leqslant b}$ is an $\mathcal{L}(M)$-formula. When z is a variable not occurring in A, $A^{\leqslant z}$ is defined similarly.

Lemma 7. If $M \models R$, I is an initial segment of M closed under all operations, $b \in I$ and A is a Σ_1^0-formula in the language $\mathcal{L}(M)$, then

(a) $I \models R$

(b) If $b<c$ and $M \models A^{\leqslant b}$ then $M \models A^{\leqslant c}$

(c) If $M \models A^{\leqslant b}$ and every constant symbol in A denotes an element in I, then $I \models A$

(d) If $I \models A$ and $c \in M \setminus I$ then $M \models A^{\leq c}$

Proof. (a) follows from the fact that R is a bounded theory. (b)-(d) are easily proved by induction on the complexity of the Σ_1^0-formula A. ■

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let $A(x_1,\ldots,x_r)$ be a Σ_1^0-formula with free variables as indicated such that $(\forall \vec{x})A(\vec{x})$ is not a theorem of R. There exists a countable, recursively saturated model M of $R+\sim A(c_1,\ldots,c_r)$ where $c_1,\ldots,c_r$ are new constant symbols. Since M is countable and recursively saturated, it is also resplendent.

Let $m_0,m_1,m_2,\ldots$ enumerate the universe of M and let $\theta_0,\theta_1,\theta_2,\ldots$ enumerate the Σ_1^0-formulae in the language $\mathcal{L}(M)$ with a single free variable x. So $\theta_i = \theta_i(x,\vec{n}_i)$ where $\vec{n}_i$ is a vector of elements of M. We shall define a sequence of models $M_0,M_1,M_2,\ldots$ and a sequence of elements $a_0,a_1,a_2,\ldots$ so that

(1) M_{i+1} is an initial segment of M_i closed under all operations;

(2) $a_i \in M_i$;

(3) $a_{i+1} \geq a_i$;

(4) and each M_i is recursively saturated and hence resplendent.

Begin by defining $a_0 = \max(c_1,\ldots,c_r)$ and $M_0 = M$.

Now suppose a_k and M_k have been defined. Let $i = \beta(1,k)$ and $j = \beta(2,k)$ where β is the Godel sequence coding function. Consider the element $m_i \in M$ and the formula $\theta_j(x,\vec{n}_j)$. There are three cases:

Case (1) $m_i \notin M_k$ or $\vec{n}_j \notin M_k$ or $M_k \models \sim(\forall x \leq m_i)\theta_j(x)$. Set $M_{k+1} = M_k$ and $a_{k+1}=a_k$.

Case (2) $M_k \models (\forall x \leq m_i)\theta_j(x)$ and there is a $b \in M_k$ such that

$$M_k \models (\forall x \leq m_i)\theta_j^{\leq b}(x).$$

In this case, let $M_{k+1} = M_k$ and let a_{k+1} be the maximum of a_k and b.

Case (3) Neither of the above cases holds. Let I be the initial segment of M_k defined by

$$I = \{b \in M_k: b \leq t(a_k) \text{ for some term } t\}.$$

By the recursive saturation of M_k, $I \neq M_k$ (except in the degenerate case where M_k has a maximum element). Also, I is closed under all operations and $a_k \in I$. Hence

$M_k \models$ ($\exists$ predicate Q)(Q is a proper initial segment, containing a_k and is closed under all operations).

Namely, choose Q to be I. By the resplendency of M_k, there is a (different) predicate Q_k so that all of the above properties hold and so that the expanded structure $(M_k, Q_k, \ldots)$ is resplendent.

By Lemma 7(d) and since Case 2 did not hold,

$$Q_k \models \sim(\forall x \leq m_i)\theta_j(x, \vec{n}_j).$$

Now define $a_{k+1} = a_k$ and $M_{k+1} = Q_k$.

This completes the definition of $M_0, M_1, M_2, \ldots$

Let M_ω be defined by

$$M_\omega = \bigcap_{i=0}^{\infty} M_i.$$

We claim that $M_\omega \models R+B\Sigma_1^0$ and yet $M_\omega \models \sim A(\vec{c})$. This suffices to prove Theorem 1 since it implies that $R+B\Sigma_1^0$ does not prove $(\forall \vec{x})A(\vec{x})$. Since M_ω is an initial segment of M and M_ω is closed under all operations, Lemma 7(a) implies $M_\omega \models R$. In addition since $A \in \Sigma_1^0$, $M_\omega \models \sim A(\vec{c})$.

An arbitrary instance of a $B\Sigma_1^0$-collection axiom over M_ω is of the form

$$(\forall x \leq m_i)(\exists y)\varphi(x,y,\vec{n}) \longrightarrow (\exists z)(\forall x \leq m_i)(\exists y \leq z)\varphi(x,y,\vec{n})$$

where $m_i, \vec{n} \in M_\omega$ and $\varphi \in \Sigma_1^0$. Let j be such that $\theta_j(x,\vec{n}_j)$ is $(\exists y)\varphi(x,y,\vec{n})$. It will suffice to show that

$$M_\omega \models (\forall x \leq m_i)\theta_j(x,\vec{n}_j) \longrightarrow (\exists z)(\forall x \leq m_i)\theta_j^{\leq z}(x,\vec{n}_j).$$

Let $k = \langle i,j \rangle$, so $\beta(1,k) = i$ and $\beta(2,k) = j$. Examine the way in which M_{k+1} was defined. If M_{k+1} was defined by case (1) or case (3), then $(\forall x \leq m_i)\theta_j(x,\vec{n}_j)$ is false in M_{k+1}. Since M_ω is an initial segment of M_{k+1} closed under all operations and since $\theta_j \in \Sigma_1^0$,

$$M_\omega \models \sim(\forall x \leq m_i)\theta_j(x,\vec{n}_j).$$

If M_{k+1} was defined via case (2), then

$$M_{k+1} \models (\forall x \leq m_i)\theta_j^{\leq a_{k+1}}(x,\vec{n}_j).$$

Since $a_{k+1} \in M_\omega$ and $\theta_j^{\leq a_{k+1}}$ is bounded,

$$M_\omega \models (\exists z)(\forall x \leq m_i)\theta_j^{\leq z}(x,\vec{n}_j).$$

Q.E.D. ■

REFERENCES

[1] S.R. Buss, Bounded Arithmetic, Ph.D. dissertation, Princeton University 1985.

[2] R. Parikh, "Existence and feasibility in arithmetic", Journal of Symbolic Logic, 36(1971), 494-508.

[3] J.B. Paris, "Some conservation results for fragments of arithmetic", in Model Theory and Arithmetic, Lecture notes in Mathematics #890, Springer-Verlag, 1980, pp.251-262.

[4] J.B. Paris and L.A.S. Kirby, "Σ_n-collection schemes in arithmetic", in Logic Colloquium '77, North-Holland, 1978, pp.199-209.

[5] J.P. Ressayre, "A conservation result for systems of Bounded Arithmetic", handwritten notes, 1985.

[6] G. Takeuti, Proof Theory, North-Holland, 1975.