The Arithmetic Hierarchy, Parikh's Theorem and Related Matters

Juliette Kennedy

April 25, 2007

1 The Arithmetic Hierarchy

Our language or signature is $\langle +, \cdot, <, 0, {}' \rangle$, denoted $\mathcal{L}_{PA}$. PA^- is the theory of the positive part of discretely ordered rings in this language, consisting of e.g. the commutative, associate and distributive laws, the recursion equations for addition and multiplication, and ordering axioms. (See [2] page 16 for the exact definition of PA^-.) The arithmetic hierarchy is a family of formula classes within PA and is defined as follows:

- The Δ_0 ($= \Sigma_0 = \Pi_0$) formulas consist of atomic formulas closed under Boolean connectives and bounded quantifiers, i.e. quantifiers of the form $\exists \vec{x} < t$ and $\forall \vec{x} < t$, where t is any $\mathcal{L}_{PA}$-term.
- Σ_{n+1} formulas are those of the form $\exists \vec{x} \phi(\vec{x}, \vec{y})$, where ϕ is Π_n,
- Π_{n+1} formulas are those of the form $\forall \vec{x} \phi(\vec{x}, \vec{y})$, where ϕ is ,
- A formula is Δ_n if it is provably (in PA) equivalent to both a Σ_n formula and a Π_n formula.

A corresponding hierarchy of theories within PA is defined by restricting the induction axiom to a fixed level of the arithmetic hierarchy. Specifically we define $I\Sigma_n$ as PA^- together with the induction schema for Σ_n formulas; $I\Pi_n$ and $I\Delta_n$ are defined similarly.

The first fact which we observe is that the arithmetic hierarchy is *strict*. (Note: this does not imply that the $I\Sigma_n$ hierarchy is also strict. It may not be! But see below.):

Theorem 1 *There is an $\mathcal{L}_{PA}$ formula $\Psi(x)$ which is Π_n but not provably equivalent to a Σ_n formula, and an $\mathcal{L}_{PA}$ formula $\Theta(x)$ which is Σ_n but not provably equivalent to a Π_n formula.*

Proof There is a truth definition for Σ_n formulas in Σ_n, i.e. for each n there is a Σ_n formula $Sat_{\Sigma_n}(x, y)$ such that for all $\mathcal{L}_{PA}$ formulas $\phi(x)$, which are Σ_n,

$$I\Sigma_n \vdash \forall z[Sat_{\Sigma_n}(\ulcorner \phi(y) \urcorner, z) \leftrightarrow \phi(z)].$$

It is alot of work to write this down, but the idea is simple: just formalize the Tarski truth conditions. To show that the definition has all the properties you want it to have, you use induction on n. (See section 9.3 of [2] for the details.) But now we are almost done, for let $\phi(x) = \neg Sat_{\Sigma_n}(x, x)$. We claim that $\phi(x)$ is (up to equivalence) Π_n but not Σ_n. Why? Suppose it is Σ_n. Then we could apply Sat_{Σ_n} to ϕ to obtain

$$Sat_{\Sigma_n}(\ulcorner \phi(x) \urcorner, \ulcorner \phi(x) \urcorner) \leftrightarrow \neg Sat_{\Sigma_n}(\ulcorner \phi(x) \urcorner, \ulcorner \phi(x) \urcorner).$$

The other half of the claim follows similarly, i.e. this time let $\phi(x) = \neg Sat_{\Pi_n}(x, x)$ and apply $Sat_{\Pi_n}(x, x)$ to obtain a contradiction. □

Recall that we defined the theory $I\Sigma_n$ as PA^- together with the schema

$$[\phi(0, \vec{y}) \wedge \forall x(\phi(x, \vec{y}) \rightarrow \phi(x + 1, \vec{y}))] \rightarrow \forall x \phi(x, \vec{y}),$$

where ϕ is a Σ_n formula; $I\Pi_n$ was defined similarly.

Theorem 2 *The theories $I\Sigma_n$ and $I\Pi_n$ are equivalent.*

Proof We prove the "left to right" direction by induction on n. The case $n = 0$ is trivial. So suppose $n > 0$ and ϕ is a Π_n formula. We work model theoretically; that is we fix a model M of $I\Sigma_n$ and suppose that

$$M \models [\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x + 1))] \wedge \neg\phi(a),$$

for some a in M (suppressing parameters in ϕ). We claim that M must satisfy the following Σ_n formula:

$$\forall z(z \leq a \rightarrow \neg\phi(a - z)).$$

Note that we are done if we can prove the claim, as then since $a \leq a$, we must have $\neg\phi(0)$. But this is a contradiction and therefore we must have $M \models \forall x \phi(x)$.

We prove the claim by induction on z. The case $z = 0$ is true, since we already have $\neg\phi(a)$. Now suppose $u \leq a \rightarrow \neg\phi(a - u)$ for all $u \leq z_0$, and suppose $z_0 + 1$ is $\leq a$. Then z_0 is $\leq a$ and therefore by the induction hypothesis (and Modus Tollens) we must have $\neg\phi(a - (z_0 + 1))$. By Σ_n induction we now have $\forall z(z \leq a \rightarrow \neg\phi(a - z))$. The right to left direction is proved similarly. □

Have we proved that the $I\Sigma_n$ hierarchy does not collapse? Not yet. As was mentioned in class, one way to do this is to show that the consistency statement for $I\Sigma_n$ is provable in $I\Sigma_{n+1}$, for all $n \geq 0$. (For a hint how to do this, see [2] page 140, exercise 10.8.) Then recall that for no n do we have $I\Sigma_n \vdash Con(I\Sigma_n)$.

We mentioned that certain special principles such as the Pigeon Hole Principle, the principle that there are infinitely many primes, and others, generate interesting subsystems of PA. (See [2], [3] and [1] for more details, on this and other points from the lecture.) One such principle is *Collection* or *Coll*, which resembles the replacement axiom from ZF set theory:

Definition $B\Sigma_n$ is the theory $I\Delta_0$ together with the following axiom scheme (suppressing extra parameters as usual, for the sake of readability):

$$\forall u[(\forall x \leq u \exists y \phi(x,y)) \rightarrow (\exists v \forall x \leq u \exists y \leq v \phi(x,y))],\ \phi \in \Sigma_n.$$

Coll is the axiom scheme "for all n, $B\Sigma_n$."

The following is an interesting fact about the collection scheme:

Theorem 3 *$B\Sigma_{n+1}$ is between $I\Sigma_{n+1}$ and $I\Sigma_n$, i.e. $I\Sigma_{n+1} \rightarrow B\Sigma_{n+1} \rightarrow I\Sigma_n$. Moreover, the implications are all strict.*

Proof Strictness is shown by model theoretic methods. (See e.g. [3]. Note that this gives another proof that the $I\Sigma_n$ hierarchy is strict.)

We first prove that $B\Sigma_{n+1} \rightarrow I\Sigma_n$, by induction on n. (Here and in the remainder of the proof, the "$\rightarrow$" in e.g. $I\Sigma_{n+1} \rightarrow B\Sigma_{n+1}$ denotes semantic implication, i.e. any model of $I\Sigma_{n+1}$ is a model of $B\Sigma_{n+1}$.) The case $n = 0$ is trivial. Now suppose $n > 0$ and $\phi(x) = \exists z \psi(x,z)$, where $\psi \in \Pi_{n-1}$. We assume

$$\phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x+1)).$$

We wish to show $\forall x \phi(x)$. As before we work model theoretically. Accordingly let $M \models B\Sigma_{n+1}$ and let $a \in M$. We wish to show $\forall x \leq a \phi(x)$. (For then we are done, since a was an arbitrary element of M.) Note that

$$\begin{aligned} M \models \forall x(\phi(x) \rightarrow \phi(x+1)) \quad &\rightarrow \quad \forall x \leq a(\phi(x) \rightarrow \phi(x+1)) \\ &\rightarrow \quad \forall x \leq a(\exists z \psi(x,z) \rightarrow \exists z \psi(x+1,z)) \\ &\rightarrow \quad \forall x \leq a(\exists z \psi(x,z) \rightarrow \exists w \psi(x+1,w)) \\ &\rightarrow \quad \forall x \leq a \exists w \forall z(\psi(x,z) \rightarrow \psi(x+1,w)). \end{aligned}$$

Note that the subformula $\forall z(\psi(x,z) \rightarrow \psi(x+1,w))$ is Π_n and therefore by $B\Sigma_{n+1}$ we get

$$\exists v \forall x \leq a \exists w \leq v \forall z(\psi(x,z) \rightarrow \psi(x+1,w)).$$

Choose b in M to witness this last formula:

$$\forall x \leq a \exists w \leq b \forall z(\psi(x,z) \rightarrow \psi(x+1,w)). \tag{1}$$

Without loss of generality, b can be chosen so that $M \models \exists w \leq b\psi(0,z)$. (Why? because we already have $\phi(0)$.) We now claim that

$$M \models \forall x \leq a \exists w \leq b\psi(x,w).$$

We prove this by Π_{n-1}-induction on x (which we have by the induction hypothesis). Case $x = 0$ is true, by choice of b. Now assume the claim holds for $x \leq a$ (so $\exists w \leq b\psi(x,w)$ holds in M) and assume $x+1 \leq a$. We wish to show that $M \models \exists w \leq b\psi(x+1,w)$. Choose $c \in M$ to witness $\exists w \leq b\psi(x,w)$ i.e. $\psi(x,c)$. By (1) we must have $\exists w \leq b\psi(x+1,w)$. But then we are done, since then we have $M \models \forall x \leq a \exists w \leq b\psi(x,w)$, or $M \models \forall x \leq a \exists w\psi(x,w)$, or $M \models \forall x \exists w\psi(x,w)$ or finally $\forall x\phi(x)$, as a was arbitrary.

The proof in the other direction, that is to prove that $I\Sigma_{n+1} \rightarrow B\Sigma_{n+1}$, also uses induction on n and is left as an exercise. Note that for the case $n = 0$ it is enough to show that $I\Sigma_1 \rightarrow B\Sigma_0$, for trivially $B\Sigma_0 \rightarrow B\Sigma_1$. (The extra existential quantifier can be "peeled off" so to speak.) □

Note that this theorem gives the following nice characterization of Peano:

Corollary 4 *$I\Delta_0$+ Coll is equivalent to PA.*

2 Parikh's Theorem and Related Matters

We will now prove a few theorems about the theory $I\Delta_0$, a very interesting subtheory of Peano. Of the principles we mentioned before, which generate other interesting subtheories of Peano, we know for example that $I\Delta_0 + exp \vdash PHP$, where "*exp*" is the axiom stating that the exponential function is provably total, and "PHP" is the Pigeon Hole Principle. We also know that $I\Delta_0 + exp$ proves that there are infinitely many primes; it also proves the $MRDP$ theorem, i.e. the theorem stating that Σ_1 formulas are Diophantine, that is, definable using only existential quantifiers with a polynomial equation matrix. There are many interesting open questions concerning how weak a theory can be and still prove certain of these principles, e.g. the exact complexity of PHP is to date not known.

By the way, why do we need to add the axiom "exp" to $I\Delta_0$? Are the two theories $I\Delta_0$ and $I\Delta_0$+exp really different? The answer is: Yes! Parikh's Theorem states that the exponential function is not provably total in $I\Delta_0$. (Though expontiation *is* Δ_0 definable, by a result of Bennett (see [2]).) This means that there are lots of interesting models of this theory, namely models in which exponentiation fails to be a total function.

Another interesting, if not astonishing, fact about $I\Delta_0$ is the following: the Gödel Incompleteness Theorems generalize to $I\Delta_0$, so that $I\Delta_0$ does not prove (or refute for that matter) its own consistency statement $Con(I\Delta_0)$. This is interesting but in itself perhaps not surprising. But in fact $I\Delta_0$ cannot even prove $Con(Q)$ and in fact even $I\Delta_0 + exp$ does not prove $Con(Q)$. (See [4].) This is very surprising in light of the fact that Q is much weaker than $I\Delta_0$ in that it has no induction scheme.

Before proving Parikh's Theorem, we need the following

Definition Let M be a model of a theory extending PA^-. We say that a subset I of M is a *cut* in M, denoted $I \subseteq_e M$, if it is closed downwards, i.e. $x \in I \rightarrow \forall y \leq x(y \in I)$, and closed under the successor function, i.e. $x \in I \rightarrow (x+1) \in I$.

We also need the following lemma:

Lemma 5 *Let $M \models I\Delta_0$ and let I be a cut in M which is closed under $+$ and $\cdot$. Then $I \models I\Delta_0$.*

Proof We first show that under our assumption $I \preceq_{\Delta_0} M$, that is to say, I is a Δ_0 elementary substructure of M.

The proof is by induction on the complexity of ϕ, defined to be the number of connectives and quantifiers occurring in ϕ. The case $n = 0$ is clear, as for all $\vec{a} \in I$,

$$I \models \phi(\vec{a}) \text{ iff } M \models \phi(\vec{a}),$$

if ϕ is atomic. Now suppose $\phi(\vec{x}) = \psi_1(\vec{x}) \wedge \psi_2(\vec{x})$, and the induction hypothesis holds for each conjunct. Then if $\vec{a} \in I$, $M \models \phi(\vec{a})$ iff $M \models \psi_i(\vec{a})$, for $i = 1, 2$, iff $I \models \psi_i(\vec{a})$, for $i = 1, 2$ (by the induction hypothesis), iff $I \models \phi(\vec{a})$. Conjunction and negation work similarly.

Now suppose ϕ is $\forall y \leq t(\vec{x})\psi(\vec{x}, y)$ and again $\vec{a} \in I$. Then by assumption $t(\vec{a}) \in I$, since I is closed under addition and multiplication. We claim that

$$\{b \in I | I \models b < t(\vec{a})\} = \{b \in M | M \models b < t(\vec{a})\},$$

and leave it to you to prove the claim. (It's easy!) But then

$$I \models \phi(\vec{a}) \text{ iff}$$

$$\text{for all } b \in I \text{ such that } b < t(\vec{a}),\ I \models \psi(\vec{a}, b), \text{ iff}$$

$$\text{for all } b \in M \text{ such that } b < t(\vec{a}),\ M \models \psi(\vec{a}, b),$$

by what you have just shown and by the induction hypothesis. But then $M \models \phi(\vec{a})$ and we are done.

We now claim that I is itself a model of $I\Delta_0$. For suppose not. Then for some $a \in I$, and for some Δ_0 formula ϕ,

$$I \models \phi(0) \wedge \forall x(\phi(x) \rightarrow \phi(x+1)) \wedge \neg\phi(a).$$

Now

$$I \models (z \leq a \wedge \phi(z)) \rightarrow (z \leq a \wedge \phi(z+1)),$$

or

$$I \models \forall z \leq a(\phi(z) \rightarrow \phi(z+1)),$$

and therefore, since $I \preceq_{\Delta_0} M$,

$$M \models \forall z \leq a(\phi(z) \rightarrow \phi(z+1)).$$

Since $M \models I\Delta_0$ we must have that $M \models \forall z \leq a\phi(z)$. But then $M \models \phi(a)$ and therefore $I \models \phi(a)$, a contradiction. So I is a model of $I\Delta_0$ and we are done. $\square$

We are now ready to prove Parikh's Theorem:

Theorem 6 *Let $\theta(\vec{x}, y)$ be a Δ_0 formula and suppose $I\Delta_0 \vdash \forall\vec{x}\exists y\theta(\vec{x}, y)$. Then for some term $t(\vec{x})$, $I\Delta_0 \vdash \forall\vec{x}\exists y < t(\vec{x})\theta(\vec{x}, y)$.*

Proof Suppose $I\Delta_0 \vdash \forall\vec{x}\exists y\theta(\vec{x}, y)$ but for no term $t(\vec{x})$ do we have $I\Delta_0 \vdash \forall\vec{x}\exists y < t(\vec{x})\theta(\vec{x}, y)$. We adjoin new constants $c_1, \ldots c_n$ to $\mathcal{L}_{PA}$, where n is the arity of the vector $\vec{x}$, and we consider the theory T defined

$$T = I\Delta_0 + \{\forall y \leq t(\vec{c})\neg\theta(\vec{c}, y) | t \text{ any } \mathcal{L}_{PA} \text{ term}\}.$$

We claim that T is consistent and leave it to you to prove the claim. (It's easy!) We now let $M \models T$ and let $I \subseteq M$ be defined as $b \in I \leftrightarrow b \in M$ and $M \models b < t(\vec{c})$, for some $\mathcal{L}_{PA}$ term t. (Note that I use the same symbol $\vec{c}$ both for the tuple of constants c_i and for their interpretation in M.) I is a cut in M; moreover I is closed under addition and multiplication. Therefore by the above lemma $I \models I\Delta_0$ and thus $I \models \forall\vec{x}\exists y\theta(\vec{x}, y)$. Let $b \in I$ be such that $I \models \theta(\vec{c}, b)$. Let $t(\vec{c})$ be a term such that $I \models b \leq t(\vec{c})$. Note that $I \models T$ (because $I \preceq_{\Delta_0} M$) and therefore $I \models \forall y \leq t(\vec{c})\neg\theta(\vec{c}, y)$. But this is a contradiction and so we are done. $\square$

We mention just one application of Parikh's theorem:

Theorem 7 *Suppose* $I\Sigma_0 + \Omega_1 \vdash MRDP$. *Then* $NP = co - NP$.

Proof (Sketch. For the details see p.261 of [1].) The problem of solving $ax^2 + by = c$ in the positive integers is well known to be an NP-complete problem (with input a, b, c). Therefore deciding

$$\phi(a, b, c) = \forall x, y \leq c(ax^2 + by \neq c)$$

is co-NP-complete. We wish to show that under our assumption that $I\Sigma_0 + \Omega_1 \vdash MRDP$, this problem is in NP. By our assumption

$$I\Sigma_0 + \Omega_1 \vdash \forall u, v, w[\phi(u, v, w) \leftrightarrow \exists \vec{z}\psi(u, v, w, \vec{z})],$$

where ψ is a polynomial equation. Hence

$$I\Sigma_0 + \Omega_1 \vdash \forall u, v, w\exists \vec{z}[\phi(u, v, w) \rightarrow \psi(u, v, w, \vec{z})],$$

Now by the discussion on p. 273 of [1] Parikh's theorem holds in $I\Sigma_0 + \Omega_1$. Therefore the existential quantifier "$\exists \vec{z}$" in the above is bounded by a polynomial $p(u, v, w)$ (by Parikh's theorem) and therefore we have

$$I\Sigma_0 + \Omega_1 \vdash \forall u, v, w\exists \vec{z} \leq p(u, v, w)[\phi(u, v, w) \rightarrow \psi(u, v, w, \vec{z})].$$

That is,

$$I\Sigma_0 + \Omega_1 \vdash \forall u, v, w[\phi(u, v, w) \leftrightarrow \exists \vec{z} \leq p(u, v, w)\psi(u, v, w, \vec{z})].$$

But $\exists \vec{z} \leq p(u, v, w)\psi(u, v, w, \vec{z})]$ is NP in u, v, w. That is, to check whether such $\vec{z}$ exists we need only guess $\vec{z}$ for which $\vec{z} \leq p(u, v, w)$, and this is NP.

References

[1] Hájek, Petr; Pudlák, Pavel. Metamathematics of first-order arithmetic. Second printing. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1998.

[2] Richard Kaye. Models of Peano Arithmetic. Oxford Logic Guides, 15. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1991, 74, 1974.

[3] Jan Krajicek. Bounded arithmetic, propositional logic, and complexity theory. Encyclopedia of Mathematics and its Applications, 60. Cambridge University Press, Cambridge, 1995.

[4] Paris, J.B.; Wilkie, A.J. On the Scheme of induction for Bounded Arithmetic Formulas. Annals of pure and applied logic 35, 1987.