Bounded Arithmetic S_2 – part II

Recall L_{PA} is the language $0, 1, +, \cdot, <$ and PA^- is the theory in L_{PA} axiomatizing positive parts of discreetly-ordered rings. The axioms are as follows.

PA^-

- $\forall x, y, z\, ((x + y) + z = x + (y + z))$
- $\forall x, y\, (x + y) = (y + x)$
- $\forall x, y, z\, ((x \cdot y) \cdot z = x \cdot (y \cdot z))$
- $\forall x, y\, (x \cdot y) = (y \cdot x)$
- $\forall x, y, z\, (x \cdot (y + z)) = x \cdot y + x \cdot z$
- $\forall x\, ((x + 0 = x) \wedge (x \cdot 0 = 0))$
- $\forall x\, (x \cdot 1 = x)$
- $\forall x, y, z\, ((x < y \wedge y < z) \to x < z)$
- $\forall x\, \neg x < x$
- $\forall x, y\, (x < y \vee x = y \vee y < x)$
- $\forall x, y, z\, (x < y \to x + z < y + z)$
- $\forall x, y, z\, (0 < z \wedge x < y \to x \cdot z < y \cdot z)$
- $\forall x, y\, (x < y \to \exists z\, x + z = y)$
- $0 < 1 \wedge \forall x\, (x > 0 \to x \geq 1)$
- $\forall x\, (x \geq 0)$

Below $\mathbb{N}$ is the standard model interpreting L_{PA} symbols in the usual way. Of course, $\mathbb{N}$ models PA^-.

As a first step we expand L_{PA} by an additional unary function symbol $\lfloor \frac{x}{2} \rfloor$ together with the axiom

- $\forall x, y\, (x = \lfloor \frac{y}{2} \rfloor \leftrightarrow (2 \cdot x = y \vee 2 \cdot x + 1 = y))$

Exercise 1. Show that there is a unique interpretation of $\lfloor \frac{x}{2} \rfloor$ in $\mathbb{N}$ satisfying the above axiom.

From now on $\mathbb{N}$ is assumed to interpret $\lfloor \frac{x}{2} \rfloor$, as well.

As a second step, we add a unary function symbol $|x|$ together with the following axioms

- $|0| = 0$
- $|1| = 1$
- $\forall x, y\, (x < y \to |x| < |y|)$
- $\forall x\, (x \neq 0 \to (|2 \cdot x| = |x| + 1 \wedge |2 \cdot x + 1| = |x| + 1))$
- $\forall x\, (x \neq 0 \to |x| = |\lfloor \frac{x}{2} \rfloor| + 1)$

Exercise 2. Show that there is a unique interpretation of $|x|$ in $\mathbb{N}$ satisfying the above axioms.

From now on $\mathbb{N}$ is assumed to interpret $|x|$, as well.
Finally, we add a binary function symbol $x\#y$ with the following axioms

- $\forall x\, (0\#x = 1)$
- $\forall x, y\, (x\#y = y\#x)$
- $\forall x\, (1\#(2 \cdot x) = 2 \cdot (1\#x) \wedge 1\#(2 \cdot x + 1) = 2 \cdot (1\#x))$
- $\forall x, y\, (|x\#y| = |x| \cdot |y| + 1)$
- $\forall x, y, z\, (|x| = |y| \to x\#z = y\#z)$
- $\forall x, y, z, w\, (|x| = |y| + |z| \to x\#w = (y\#w) \cdot (z\#w))$

Exercise 3. Show that there is a unique interpretation of $x\#y$ in $\mathbb{N}$ satisfying the above axioms.

The motivation behind $x\#y$ is the following simple but very important observation.

Exercise 4. Let x, y be numbers representing binary strings in the standard way. Then, the bit-length of y is poly-size bounded in the bit-length of x if and only if y as a number is bounded by a term resulting from applying $\#$ to x iteratively.

Concretely

$$|y| < |x|^c \iff y < x\# \cdots \#x$$

with c a fixed constant and $\#$ applied exactly c-times.

From now on $\mathbb{N}$ is assumed to interpret $x\#y$, as well.

Remark 5. * It is possible to solve Exercises 1 and 2 with $\mathbb{N}$ being replaced by an arbitrary $I\Delta_0$ model $\mathbb{M}$.

Exercise 3 is a bit tricky. First of all one needs to be sure that the operation $x\#y$ is even definable by a Δ_0-formula. This is true, although not trivial, i.e. there is a Δ_0-formula $\varphi(x, y, z)$ so that in $\mathbb{N}$ $\forall x, y, z\, (x\#y = z \leftrightarrow \varphi(x, y, z))$.

By choosing $\varphi(x, y, z)$ well enough, one can show that $I\Delta_0$ does indeed prove the uniqueness of the interpretation of $x\#y$.

However, $I\Delta_0$ is not able to prove $\forall x, y \exists z \varphi(x, y, z)$ and so there exist models of $I\Delta_0$ where $x\#y$ can only be interpreted as a *partial* operation.

The language L_{PA} with newly introduced symbols is denoted as L_{S_2} and the corresponding theory is called $BASIC$.

The notion of a bounded L_{S_2}-formula is defined in the same way as before and so we can overload Δ_0. Finally, the overloaded $I\Delta_0$ is denoted as S_2.

Remark 6. * The number 2 in S_2 indicates the presence of # in the language. The theory without such a symbol is called S_1, while at the same time, it is possible to iteratively define $\#_k$ symbols (the usual # here is $\#_2$). Such operations are all super-polynomial (quasi-polynomial and faster) but are still not as fast as the exponential function.

Fact 7. Theorem of Parikh still applies in the current context, i.e. for any Δ_0-formula $\varphi(x, y)$

$$S_2 \vdash \forall x \exists y \varphi(x, y) \implies S_2 \vdash \forall x \exists y \leq t(x) \varphi(x, y),$$

with $t(x)$ - an L_{S_2}-term, i.e. a quasi-polynomial.

Exercise 8. What kind of deterministic/non-deterministic witnessing do we get for the theory S_2 and Δ_0-definable total relation $P(x, y)$? Compare it to the witnessing for $I\Delta_0$.