Euler's $\varphi$-function in the context of $I\Delta_0$

Marc Jumelet

Department of Philosophy, Utrecht University, Heidelberglaan 8, NL-3584 CS Utrecht, The Netherlands (e-mail: Marc.Jumelet@phil.ruu.nl)

Received May 20, 1994

Abstract. It is demonstrated that we can represent Euler's $\varphi$-function by means of a $\Delta_0$-formula in such a way that the theory $I\Delta_0$ proves the recursion equations that are characteristic for this function.

1 Introduction

The theory $I\Delta_0$, that is, the theory of arithmetic which has as its axioms those that define the properties of a discretely ordered semiring as well as induction axioms for those formulas that contain bounded quantifiers only, has been the object of study for a variety of mathematical aspects. It has been studied for its mathematical strength, its metamathematical properties (often with the addition of axioms that ascertain the totality of certain rapidly growing functions to make reasoning about objects of metamathematical character possible) and its purely syntactical abilities, notably, as a proof system. In the following we will treat a problem concerning the possibility of defining a classical number theoretical function.

It is known for quite a long time already that a $\Delta_0$-definition for the exponentiation function exists, in the sense that we have a $\Delta_0$-formula $EXP(x, y, z)$ such that the formulas $EXP(0, S0, z), \forall x, y_1, y_2 EXP(x, y_1, z) \land EXP(x, y_2, z) \rightarrow y_1 = y_2$ as well as the formula that articulates the specific recursion property of exponentiation, that is $\forall x, y EXP(x, y, z) \rightarrow EXP(Sx, y, z)$, become provable in $I\Delta_0$. It is due to this result that the theory $I\Delta_0$ can handle finite sequences by means of binary coding. This kind of coding can be used for syntactical purposes such as the construction of a proof predicate, a truth predicate, or any other type of syntactical object, or the construction of predicates that represent the counting of certain sets that are themselves described by $\Delta_0$-formulas. As to the last case, the picture that is emerging about the possibility to find formulas that represent the
counting of $\Delta_0$-sets, gives rise to the idea that either these sets should be very small in the sense that for every number $n$, the amount of elements smaller than that number is in logarithmic proportion with respect to that number (in order to make sure that a formula that "counts" by constructing the code of a bijection between the subset of $n$ of elements that satisfy the $\Delta_0$-predicate under consideration and the ordinal that represents the size of this subset does not necessarily use values for codes that might become too large, see Paris and Wilkie [5]), or they should be described by means of very simple $\Delta_0$-formulas, expressing rather trivial properties.

Traditionally, coding syntax was performed by means of a different kind of coding, the one that is based on the Chinese Remainder Theorem. It is rather hard to judge in general under which circumstances we should prefer binary coding to number theoretical coding like the one in which the Chinese Remainder Theorem is used as a coding device.

2 Result

We will present here a $\Delta_0$-definition of a well-known function that can most easily be computed with the help of the Chinese Remainder Theorem, whereas a computation of its values by means of a binary coding procedure alone might be a lot more complicated. The function we will describe is Euler's $\varphi$-function that assigns to a number $n \in \mathbb{N}$ the cardinality of the set $\{m < n \mid \gcd(n, m) = 1\}$.

We will prove the following theorem:

**Theorem 2.1.** There is a $\Delta_0$-formula $\varphi(x, y)$ such that $\mathbb{I} \Delta_0$ proves the following clauses that articulate the recursion equations for Euler's $\varphi$-function:

i. "$\varphi(x, y)$ defines a total function for argument $x$";

ii. "$\varphi(0, 0)$ and $\varphi(1, 1)$ hold";

iii. "for all $m, p$ if $p$ is a prime divisor of $m$ and $r$ is such that $r.p = m$, then, if not $p^2|m$ and $\varphi(r, s)$ holds, this will imply $\varphi(m, (p - 1).s)$ and if $p^2|m$, then $\varphi(m, p.s)$ holds".

These are recursion equations that we have to verify to be sure that the constructed formula $\varphi(x, y)$ behaves the way it should inside the theory $\mathbb{I} \Delta_0$. Note that we immediately get that $\mathbb{I} \Delta_0$ proves for all prime numbers $p > 1$: $\varphi(p, p - 1)$. As we said above, we will construct the formula $\varphi(x, y)$ by means of the Chinese Remainder Theorem.

We remark that the definition for Euler's $\varphi$-function presented here uses roughly the same ingredients as the ones that are used to produce definitions of the graph of the factorial function in D'Aquino [1]. The difference is, that, in the case of Euler's $\varphi$-function we get more or less everything; not just the definition, but also a proof of the recursion equations as well as its totality in $\mathbb{I} \Delta_0$.

Intuitively, the construction is as follows. Let a number $x$ be given. Let furthermore