Report on
ANEW PROOF OF EUCLID'S ALGORITHM
by ANDRZEJ SALWICKI

The paper argues that the usual proofs of Euclid's algorithm are not satisfactory because they study the computations of the algorithm and not the algorithm itself and they assume the computations are done in the usual natural numbers and implicitly assume semantical properties of the standard model of the natural numbers.

The paper proposes a proof of Euclid's algorithm done in the framework of Algorithmic Logic, using only axioms and inference rules of algorithmic logic. In my opinion the (clever) trick is to use enough axioms and rules to force the semantical properties of the standard model of the natural numbers to be provable from these axioms and rules. In particular, programming constructs (assignments, conditionals and WHILE loops) are included in axioms.

I think the result could be written in a more reader friendly way. Of course the reader can refer to your very nice on-line book MS87 for all notations and details, but it would be more convenient to state some more intuitions about the syntax and semantics in the paper so that the paper is self contained, and one does not have to refer to the book MS87 to check details. Also please say before hand that you will give all axioms and rules of AL in appendix B.

GENERAL COMMENTS

Please say from the beginning that you will state your axioms and rules in the Appendix... As it is now, when reading the paper for instance on page 11 middle, one does not know whether the introduction of $\exists$ has been stated as a rule.

Please be more precise in your deductions (e.g., page 15 line 5 "finally we can add the quantifiers..." Using WHICH rule ?): it will help the reader.

I am not sure whether it is interesting to have Presburger : because you show non provability in Peano which subsumes Presburger. I would just delete Presburger, or explain why it is interesting to keep both.

Is there a link between table 1 and figure 1 ?

Did you experiment and try to run your proof on a theorem prover or proof checker ?

Appendix A was not clear to me: 1) Exactly why and where does the (H) property fail for this non standard class ? i.e., if easy can you say which axiom of AL fails for this model. 2) Please explain in detail why computation of $E(x,z)$ is infinite as this is the point that gives power to your paper, showing that in this non standard model of Peano Arithmetic, Euclid's algorithm does not terminate, hence proof of correctness is false. If this example can be explained simply, without specifying the class, it would be worth stating it earlier in the paper, to motivate the reader.

There are in the paper some sequences of Lemmata without proofs (5.9–5.11, 5.12–5.17, 5.20–5.23) : each of these sequences could be grouped in a single lemma.

It seems to me that what you pinpoint is the fact that, implicitly, the proofs of Euclid's algorithm use the fact that there there is no infinite descending chain in the natural numbers which is not a first order property but a second order property. You can express this second order property in algorithmic logic (which is thus a higher order logic). If I am true, on page 23, it would be clearer to say "no infinite descending chain" (or well-foundedness) rather than "regression principle".

Is there any containment relation between AL and second order logic ?

TYPOS AND MINOR COMMENTS

I.e, should be written i.e., and c.f. should be written cf.

Pressburger $\Longrightarrow$ Presburger

Abstract: either say where is (H) or do not say where is correctness formula

the sentence *For these and other reasons the proofs go beyond the elementary Peanos theory.* is not clear; I would either delete "other reasons" or explain what the reasons are.

algorithm of Euclid E. $\Longrightarrow$ Euclid's algorithm.

- page 1: every of known proofs $\Longrightarrow$ every one of known proofs
- page 2: wortwhile $\Longrightarrow$ worthwhille
- page 3: The section 5 gives a flavour of such theory $\Longrightarrow$ Section 5 gives a flavour of such a theory

theories od numbers $\Longrightarrow$ theories of numbers
algorithm of Euclid $\Longrightarrow$ Euclid's algorithm
play important $\Longrightarrow$ play an important
as the aim their proof or an counterexample $\Longrightarrow$ as aim their proof or a counterexample
In the algorithmics $\Longrightarrow$ In algorithmics
Cn that satisfies axioms $\Longrightarrow$ Cn that satisfies the axioms
thes set proposed $\Longrightarrow$ the set proposed
the proof of correctness of $\Longrightarrow$ the correctness proof of
The Euclid's algorithm $\Longrightarrow$ Euclid's algorithm

- page 4: in standard model. One has assume that the algorithm works in standard $\Longrightarrow$ in the standard model. One has to assume that the algorithm works in the standard
proof itself lead correctly $\Longrightarrow$ proof itself led correctly

- page 5: State right away where the general axioms and rules of AL will be given
The alfabets are similar. $\Longrightarrow$ The alphabets are similar.
give example of $\mathcal{F}_{AL}$ formula which is not $\mathcal{F}_{FOL}$ formula

- page 6: if γ thenK else M fi $\Longrightarrow$ if γ then K else M fi
in several places: expresion $\Longrightarrow$ expression

- page 7: Please could you make more precise the notations: I guessed K, M always means programs, α, β logical formulas ? Please explain meaning of $\bigcup$ and $\bigcap$.
in several places: expresion $\Longrightarrow$ expression
$\cup$ Kα i $\cap$ Kα ??? what is the "i" in midlle of formula?
It would be nice to explain the intuition of the formulas of AL: if I understood right, something like $K\alpha$ means that after executing K, formula α holds (just before formal definition of semantics)
otherwise i.e. if the computation of K loops $\Longrightarrow$ otherwise (could it not happen that the result of the computation is not defined even when there is no loop, for instance deadlock ?)
just before section 3 delete "def.! "

- page 8: Is the non standard model for $\mathcal{T}h_2$ the same one as for $\mathcal{T}h_1$: if so I do not see the point in introducing $\mathcal{T}h_1$.

- page 9: title of section 5: Algorithmic theory of standard natural numbers. If I understood correctly, the clever trick in your proof is that axioms of theory exclude non-standard models; if true this should be pointed out.

axioms (A) (P) (O) : I have a problem with these axioms, on the right of the = sign, are "algorithmic terms" of the form either Kw or $K(w)$. Such terms have not been defined. One more question: is there a difference between Kw and $K(w)$?

addition, predecessor, subtraction +, P, $\dot{-}$ $\Longrightarrow$ addition, predecessor, subtraction (respectively +, P, $\dot{-}$)

properties thet $\Longrightarrow$ properties that

proofs of these properties $\Longrightarrow$ proofs of those properties

• page 10: modus ponens $\Longrightarrow$ modus ponens (axiom (S) and previous line.) However I have a small problem here : the universal quantifier in (S) is gone

Lemma 5.2 and in the sequel : please make precise the meaning of $\bigcup$ and $\bigcap$

I do not understand how you apply axiom Ax_{16} and I had to guess the meaning of $\{y := s(y)\}^i$

• page 11: withe the $\Longrightarrow$ with the

Now, we can introduce the existential $\Longrightarrow$ Now, by rule R_6 we can introduce the existential

• page 12: is a teorem $\Longrightarrow$ is a theorem

the formula on line 3 is hard to read, and I did not understand 1) how you apply rule $R2$ to this formula (i.e. why formula $\{x := 0\}$**true** holds, and 2) what is connection (if any) between rule R_2 which stated in Appendix B page 26 and rule (R2) which is stated here. Could you please explain more please, and if rules R_2 and (R2) are different, why is rule (R2) not stated in the axioms and rules Appendix B.

(c.f.13) $\Longrightarrow$ (cf. formula (13))

• page 14: two assignment instruction, $\Longrightarrow$ two assignment instructions,

line 5, could you please say which rule you apply to add quantifiers

the application of axion Ax_{21} of while instruction to transform a **while** into a combination of **if...then...else** + **while** is not clear tot me.

the axiom Ax_{21} of while instruction to obtain $\Longrightarrow$ the axioms Ax_{21} and Ax_{20} to obtain line -6 : I have a problem with the equivalence: on the left side of $\Leftrightarrow$ is a formula, and on the right is a term. may be last w to be replaced by $(z = w)$?

line -5: from the properties of while instruction : please make more precise, which properties of while you use.

- page 15: formula on line -7 : the formula with $\wedge$ and $\vee$ is hard to read: please could you put parentheses, or state the priority rules about $\wedge$ and $\vee$. This occurs also else where in the text, please clarify all such occurrences.

  is a theorem of AL,too. $\Longrightarrow$ follows from axiom Ax_6.

- page 16: $x < y$ i $y < x$. ?what is the "i" in midlle of formula?

  line 3, the footnote number 2 after y looks like y^2 which is somehow unfortunate.

  We are recalling $\Longrightarrow$ We first recall

  The succession of 3 Lemmas 5.9 to 5.11 could be grouped in a single Lemma

- page 17: The succession of 6 Lemmas 5.12 to 5.17 could be grouped in a single Lemma

- page 18: Another remark: please explain why it is so.

- page 21: the following program has all computations finite $\Longrightarrow$ all computations of the following program are finite

- page 23: would be better to rename *regression principle* into *no infinite descending chain* which is more usual for natural numbers.

  prone ot leading $\Longrightarrow$ prone or leading ??

- page 24: in everydays work $\Longrightarrow$ in everyday work

  execution of the Euclid's algorithm $\Longrightarrow$ execution of Euclid's algorithm

- page 25: non=negative rational $\Longrightarrow$ nonnegative rational

  the algorithm of Euclides $\Longrightarrow$ Euclid's algorithm

- page 26: you might recall that rule R_1 is modus ponens (as you use the terminology modus ponens in the paper)

- Appendix B : why do you need so many axioms for propositional logic ? (this question is not relevant to the paper subject though)