JOURNAL OF FORMALIZED MATHEMATICS
Volume 5, Released 1993, Published 2003
Inst. of Computer Science, Univ. of Białystok

Euclid's Algorithm

Andrzej Trybulec
Warsaw University
Białystok

Yatsuka Nakamura
Shinshu University
Nagano

Summary. The main goal of the paper is to prove the correctness of the Euclid's algorithm for **SCM**. We define the Euclid's algorithm and describe the natural semantics of it. Eventually we prove that the Euclid's algorithm computes the Euclid's function. Let us observe that the Euclid's function is defined as a function mapping finite partial states to finite partial states of **SCM** rather than pairs of integers to integers.

MML Identifier: `AMI_4`.

WWW: `http://mizar.org/JFM/Vol5/ami_4.html`

The articles [8], [7], [9], [2], [3], [11], [1], [4], [12], [5], [13], [6], and [10] provide the notation and terminology for this paper.

1. Preliminaries

One can prove the following propositions:

(1) For all integers i, j such that $i \geq 0$ and $j \geq 0$ holds $i \div j \geq 0$.

(2) For all integers i, j such that $i \geq 0$ and $j > 0$ holds $|i| \bmod |j| = i \bmod j$ and $|i| \div |j| = i \div j$.

In the sequel i, k are natural numbers.

The scheme *Euklides'* deals with a unary functor $\mathcal{F}$ yielding a natural number, a unary functor $\mathcal{G}$ yielding a natural number, a natural number $\mathcal{A}$, and a natural number $\mathcal{B}$, and states that:

There exists k such that $\mathcal{F}(k) = \gcd(\mathcal{A}, \mathcal{B})$ and $\mathcal{G}(k) = 0$

provided the parameters have the following properties:

- $0 < \mathcal{B}$,
- $\mathcal{B} < \mathcal{A}$,
- $\mathcal{F}(0) = \mathcal{A}$,
- $\mathcal{G}(0) = \mathcal{B}$, and
- For every k such that $\mathcal{G}(k) > 0$ holds $\mathcal{F}(k+1) = \mathcal{G}(k)$ and $\mathcal{G}(k+1) = \mathcal{F}(k) \bmod \mathcal{G}(k)$.

2. Euclid's Algorithm

The Euclid's algorithm is a programmed finite partial state of **SCM** and is defined by:

(Def. 1) The Euclid's algorithm $= (\mathbf{i}_0 \dot{\longmapsto} (\mathbf{d}_2 := \mathbf{d}_1)) +\cdot ((\mathbf{i}_1 \dot{\longmapsto} \mathrm{Divide}(\mathbf{d}_0, \mathbf{d}_1)) +\cdot ((\mathbf{i}_2 \dot{\longmapsto} (\mathbf{d}_0 := \mathbf{d}_2)) +\cdot ((\mathbf{i}_3 \dot{\longmapsto} (\mathbf{if}\ \mathbf{d}_1 > 0\ \mathbf{goto}\ \mathbf{i}_0)) +\cdot (\mathbf{i}_4 \dot{\longmapsto} \mathbf{halt}_{\mathbf{SCM}}))))$.

One can prove the following proposition

(4)[1] dom(the Euclid's algorithm) $= \{\mathbf{i}_0, \mathbf{i}_1, \mathbf{i}_2, \mathbf{i}_3, \mathbf{i}_4\}$.

3. The Natural Semantics of the Euclid's Algorithm

The following propositions are true:

(5) Let s be a state of **SCM**. Suppose the Euclid's algorithm $\subseteq s$. Let given k. Suppose $\mathbf{IC}_{(\mathrm{Computation}(s))(k)} = \mathbf{i}_0$. Then $\mathbf{IC}_{(\mathrm{Computation}(s))(k+1)} = \mathbf{i}_1$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_0) = (\mathrm{Computation}(s))(k)(\mathbf{d}_0)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_1) = (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_2) = (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$.

(6) Let s be a state of **SCM**. Suppose the Euclid's algorithm $\subseteq s$. Let given k. Suppose $\mathbf{IC}_{(\mathrm{Computation}(s))(k)} = \mathbf{i}_1$. Then $\mathbf{IC}_{(\mathrm{Computation}(s))(k+1)} = \mathbf{i}_2$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_0) = (\mathrm{Computation}(s))(k)(\mathbf{d}_0) \div (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_1) = (\mathrm{Computation}(s))(k)(\mathbf{d}_0) \bmod (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_2) = (\mathrm{Computation}(s))(k)(\mathbf{d}_2)$.

(7) Let s be a state of **SCM**. Suppose the Euclid's algorithm $\subseteq s$. Let given k. Suppose $\mathbf{IC}_{(\mathrm{Computation}(s))(k)} = \mathbf{i}_2$. Then $\mathbf{IC}_{(\mathrm{Computation}(s))(k+1)} = \mathbf{i}_3$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_0) = (\mathrm{Computation}(s))(k)(\mathbf{d}_2)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_1) = (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$ and $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_2) = (\mathrm{Computation}(s))(k)(\mathbf{d}_2)$.

(8) Let s be a state of **SCM**. Suppose the Euclid's algorithm $\subseteq s$. Let given k. Suppose $\mathbf{IC}_{(\mathrm{Computation}(s))(k)} = \mathbf{i}_3$. Then

(i) if $(\mathrm{Computation}(s))(k)(\mathbf{d}_1) > 0$, then $\mathbf{IC}_{(\mathrm{Computation}(s))(k+1)} = \mathbf{i}_0$,

(ii) if $(\mathrm{Computation}(s))(k)(\mathbf{d}_1) \leq 0$, then $\mathbf{IC}_{(\mathrm{Computation}(s))(k+1)} = \mathbf{i}_4$,

(iii) $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_0) = (\mathrm{Computation}(s))(k)(\mathbf{d}_0)$, and

(iv) $(\mathrm{Computation}(s))(k+1)(\mathbf{d}_1) = (\mathrm{Computation}(s))(k)(\mathbf{d}_1)$.

(9) For every state s of **SCM** such that the Euclid's algorithm $\subseteq s$ and for all k, i such that $\mathbf{IC}_{(\mathrm{Computation}(s))(k)} = \mathbf{i}_4$ holds $(\mathrm{Computation}(s))(k+i) = (\mathrm{Computation}(s))(k)$.

(10) Let s be a state of **SCM**. Suppose s starts at $\mathbf{i}_0$ and the Euclid's algorithm $\subseteq s$. Let x, y be integers. If $s(\mathbf{d}_0) = x$ and $s(\mathbf{d}_1) = y$ and $x > 0$ and $y > 0$, then $(\mathrm{Result}(s))(\mathbf{d}_0) = x \gcd y$.

The Euclid's function is a partial function from FinPartSt(**SCM**) to FinPartSt(**SCM**) and is defined by the condition (Def. 2).

(Def. 2) Let p, q be finite partial states of **SCM**. Then $\langle p, q\rangle \in$ the Euclid's function if and only if there exist integers x, y such that $x > 0$ and $y > 0$ and $p = [\mathbf{d}_0 \longmapsto x, \mathbf{d}_1 \longmapsto y]$ and $q = \mathbf{d}_0 \dot{\longmapsto} (x \gcd y)$.

One can prove the following propositions:

(11) Let p be a set. Then $p \in$ dom(the Euclid's function) if and only if there exist integers x, y such that $x > 0$ and $y > 0$ and $p = [\mathbf{d}_0 \longmapsto x, \mathbf{d}_1 \longmapsto y]$.

(12) For all integers i, j such that $i > 0$ and $j > 0$ holds (the Euclid's function)$([\mathbf{d}_0 \longmapsto i, \mathbf{d}_1 \longmapsto j]) = \mathbf{d}_0 \dot{\longmapsto} (i \gcd j)$.

(13) Start-At$(\mathbf{i}_0)$+·(the Euclid's algorithm) computes the Euclid's function.

[1] The proposition (3) has been removed.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[3] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[4] Czesław Byliński. A classical first order language. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/cqc_lang.html.

[5] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

[6] Yatsuka Nakamura and Andrzej Trybulec. A mathematical model of CPU. *Journal of Formalized Mathematics*, 4, 1992. http://mizar.org/JFM/Vol4/ami_1.html.

[7] Andrzej Trybulec. Enumerated sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/enumset1.html.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[9] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[10] Andrzej Trybulec and Yatsuka Nakamura. Some remarks on the simple concrete model of computer. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/ami_3.html.

[11] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_1.html.

[12] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_1.html.

[13] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

Received October 8, 1993

Published January 2, 2004