FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 163–170, 2018
DOI: 10.2478/forma-2018-0014

DE GRUYTER OPEN
degruyter.com/view/j/forma

Partial Correctness of GCD Algorithm

Ievgen Ivanov
Taras Shevchenko National University
Kyiv, Ukraine

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Mykola Nikitchenko
Taras Shevchenko National University
Kyiv, Ukraine

Summary. Poprosze

MSC: 03B35 68T99

Keywords:

MML identifier: NOMIN_4, version: 8.1.08 5.52.1328

From now on v denotes an object, V, A denote sets, and f denotes a SCBinominativeFunction of V, A.

Let us consider A. We say that A is complex-containing if and only if

(Def. 1) $\mathbb{C} \subseteq A$.

One can check that there exists a set which is complex-containing and every set which is complex-containing is also non empty.

The scheme *BinPredToFunEx* deals with sets $\mathcal{X}$, $\mathcal{Y}$ and a binary predicate $\mathcal{P}$ and states that

(Sch. 1) There exists a function f from $\mathcal{X} \times \mathcal{Y}$ into *Boolean* such that for every objects x, y such that x, $y \in \mathcal{Y}$ holds if $\mathcal{P}[x, y]$, then $f(x, y) = \mathit{true}$ and if $\mathcal{P}[x, y]$, then $f(x, y) = \mathit{false}$.

The scheme *BinPredToFunUnique* deals with sets $\mathcal{X}$, $\mathcal{Y}$ and a binary predicate $\mathcal{P}$ and states that

(Sch. 2) For every functions f, g from $\mathcal{X} \times \mathcal{Y}$ into *Boolean* such that for every objects x, y such that x, $y \in \mathcal{Y}$ holds if $\mathcal{P}[x, y]$, then $f(x, y) = \mathit{true}$ and if $\mathcal{P}[x, y]$, then $f(x, y) = \mathit{false}$ and for every objects x, y such that x, $y \in \mathcal{Y}$

ISSN 1426–2630(Print), 1898-9934(Online)

holds if $\mathcal{P}[x, y]$, then $g(x, y) = \mathit{true}$ and if $\mathcal{P}[x, y]$, then $g(x, y) = \mathit{false}$ holds $f = g$.

The scheme *Lambda2Unique* deals with sets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ and a binary functor $\mathcal{F}$ yielding an object and states that

(Sch. 3) For every functions f, g from $\mathcal{X} \times \mathcal{Y}$ into $\mathcal{Z}$ such that for every objects x, y such that x, $y \in \mathcal{Y}$ holds $f(x, y) = \mathcal{F}(x, y)$ and for every objects x, y such that x, $y \in \mathcal{Y}$ holds $g(x, y) = \mathcal{F}(x, y)$ holds $f = g$.

Let us consider V and A. The functor nonatomicsND(V, A) yielding a set is defined by the term

(Def. 2) the set of all d where d is a non-atomic nominative data of V and A.

Now we state the propositions:

(1) Let us consider an object d. Suppose $d \in \mathrm{nonatomicsND}(V, A)$. Then d is a non-atomic nominative data of V and A.

(2) $\emptyset \in \mathrm{nonatomicsND}(V, A)$.

Let us consider V and A. Let us note that $\mathrm{nonatomicsND}(V, A)$ is non empty and functional.

We say that A is-without-nonatomicND-wrt V if and only if

(Def. 3) A misses $\mathrm{nonatomicsND}(V, A)$.

Now we state the propositions:

(3) If A is-without-nonatomicND-wrt V, then for every non-atomic nominative data d of V and A, $d \notin A$.

(4) Suppose A is-without-nonatomicND-wrt V and $v \in V$. Let us consider a non-atomic nominative data d_1 of V and A, and a nominative data d_2 with simple names from V and complex values from A. Then $\mathrm{dom}\, d_1 \nabla_a^v d_2 = \{v\} \cup \mathrm{dom}\, d_1$. The theorem is a consequence of (3).

(5) Suppose A is-without-nonatomicND-wrt V. Let us consider a non-atomic nominative data d of V and A. Suppose $v \in V$ and $d \in \mathrm{dom}\, f$. Then $\mathrm{dom}((\text{SC-assignment}(f, v))(d)) = \mathrm{dom}\, d \cup \{v\}$. The theorem is a consequence of (3).

In the sequel d denotes a nominative data with simple names from V and complex values from A.

Now we state the proposition:

(6) Let us consider a non-atomic nominative data d_1 of V and A. Suppose $v \in V$ and A is-without-nonatomicND-wrt V. Then $d_1 \nabla_a^v d \in \mathrm{dom}\, v \Rightarrow_a$. The theorem is a consequence of (4).

From now on a, b, c, x, y, z denote elements of V and p, q, r, s denote SCPartialNominativePredicates of V, A.

Let us consider V, A, d, and a. We say that a is an ext real on d if and only if

(Def. 4) $(a \Rightarrow_a)(d)$ is extended real.

We say that a is a complex on d if and only if

(Def. 5) $(a \Rightarrow_a)(d)$ is complex.

We say that a is a value on d if and only if

(Def. 6) $(a \Rightarrow_a)(d) \in A$.

Now we state the propositions:

(7) If A is complex-containing and for every d, a is a complex on d, then for every d, a is a value on d.

(8) If for every d, a is a value on d, then $\operatorname{rng} a \Rightarrow_a \subseteq A$.

(9) If for every d, a is a value on d and for every d, b is a value on d, then $\operatorname{rng}\langle a \Rightarrow_a, b \Rightarrow_a\rangle \subseteq A \times A$. The theorem is a consequence of (8).

Let us consider V and A. Let a, b be elements of V and p be a function from $A \times A$ into *Boolean*. The functor lift-binary-pred(p, a, b) yielding a SCPartialNominativePredicate of V, A is defined by the term

(Def. 7) $p \cdot \langle a \Rightarrow_a, b \Rightarrow_a\rangle$.

Let o_1 be a function from $A \times A$ into A. The functor lift-binary-op(o_1, a, b) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 8) $o_1 \cdot \langle a \Rightarrow_a, b \Rightarrow_a\rangle$.

The functor Equality(A) yielding a function from $A \times A$ into *Boolean* is defined by

(Def. 9) for every objects a, b such that $a, b \in A$ holds if $a = b$, then $it(a, b) = \mathit{true}$ and if $a \neq b$, then $it(a, b) = \mathit{false}$.

Let us consider V. Let x, y be elements of V. The functor Equality(A, x, y) yielding a SCPartialNominativePredicate of V, A is defined by the term

(Def. 10) lift-binary-pred(Equality$(A), x, y)$.

Let x, y be objects. We say that x less-pred y if and only if

(Def. 11) there exist extended reals x_1, y_1 such that $x_1 = x$ and $y_1 = y$ and $x_1 < y_1$.

Observe that the predicate is irreflexive and asymmetric.

Now we state the proposition:

(10) Let us consider extended reals x, y. Suppose not x less-pred y. Then

(i) y less-pred x, or

(ii) $x = y$.

Let us consider A. The functor less(A) yielding a function from $A \times A$ into *Boolean* is defined by

(Def. 12) for every objects x, y such that x, $y \in A$ holds if x less-pred y, then $it(x, y) = true$ and if not x less-pred y, then $it(x, y) = false$.

Let us consider V. Let x, y be elements of V. The functor less(A, x, y) yielding a SCPartialNominativePredicate of V, A is defined by the term

(Def. 13) lift-binary-pred(less(A), x, y).

Now we state the propositions:

(11) Suppose for every d, a is a value on d and for every d, b is a value on d. Then $\operatorname{dom}\text{Equality}(A, a, b) = \operatorname{dom} a \Rightarrow_a \cap \operatorname{dom} b \Rightarrow_a$. The theorem is a consequence of (9).

(12) Suppose for every d, a is a value on d and for every d, b is a value on d. Then $\operatorname{dom}\text{less}(A, a, b) = \operatorname{dom} a \Rightarrow_a \cap \operatorname{dom} b \Rightarrow_a$. The theorem is a consequence of (9).

(13) Suppose for every d, a is a value on d and for every d, b is a value on d and for every d, a is an ext real on d and for every d, b is an ext real on d. Then $\neg\,\text{Equality}(A, a, b) = \text{less}(A, a, b) \vee \text{less}(A, b, a)$.

PROOF: Set $e = \text{Equality}(A, a, b)$. Set $p = \neg e$. Set $q = \text{less}(A, a, b)$. Set $r = \text{less}(A, b, a)$. Set $o = q \vee r$. Set $D_1 = a \Rightarrow_a$. Set $D_2 = b \Rightarrow_a$. $\operatorname{dom} e = \operatorname{dom} D_1 \cap \operatorname{dom} D_2$. $\operatorname{dom} q = \operatorname{dom} D_1 \cap \operatorname{dom} D_2$. $\operatorname{dom} r = \operatorname{dom} D_1 \cap \operatorname{dom} D_2$. $\operatorname{dom} p = \operatorname{dom} o$ by [**?** , (8)], [1, (13)], (10), (12). Consider d_3 being a non-atomic nominative data of V and A such that $x = d_3$ and $a \in \operatorname{dom} d_3$. $x \in \operatorname{dom} q$ and $x \in \operatorname{dom} r$. □

(14) Suppose for every d, a is a value on d and for every d, b is a value on d and a is an ext real on d and b is an ext real on d and $d \in \operatorname{dom} \neg\,\text{Equality}(A, a, b)$ and $(\neg\,\text{Equality}(A, a, b))(d) = true$. Then

(i) $d \in \operatorname{dom}\text{less}(A, a, b)$ and $(\text{less}(A, a, b))(d) = true$, or

(ii) $d \in \operatorname{dom}\text{less}(A, b, a)$ and $(\text{less}(A, b, a))(d) = true$.

The theorem is a consequence of (10) and (12).

Let x, y be objects. Assume x is a complex number and y is a complex number. The functor $x'(y)$ yielding a complex number is defined by

(Def. 14) there exist complex numbers x_1, y_1 such that $x_1 = x$ and $y_1 = y$ and $it = x_1 - y_1$.

Let us consider A. Assume A is complex-containing. The functor $\square \setminus_A \square$ yielding a function from $A \times A$ into A is defined by

(Def. 15) for every objects x, y such that x, $y \in A$ holds $it(x, y) = x'(y)$.

Let us consider V. Let x, y be elements of V. The functor $\mathrm{diff}_y(A, x)$ yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 16) lift-binary-op$(\square \setminus_A \square, x, y)$.

Let us consider a and b. The functor gcd-conditional-step(V, A, a, b) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 17) PP-IF$(\mathrm{less}(A, b, a), \text{SC-assignment}(\mathrm{diff}_b(A, a), a), \mathrm{PPid}(\mathrm{ND}_{\mathrm{SC}}(V, A)))$.

The functor gcd-loop-body(V, A, a, b) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 18) PP-composition(gcd-conditional-step(V, A, a, b), gcd-conditional-step(V, A, b, a)).

The functor gcd-main-loop(V, A, a, b) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 19) PP-while$(\neg \mathrm{Equality}(A, a, b)$, gcd-loop-body$(V, A, a, b))$.

Let us consider x and y. The functor gcd-var-init(V, A, a, b, x, y) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 20) PP-composition$(\text{SC-assignment}(x \Rightarrow_a, a), \text{SC-assignment}(y \Rightarrow_a, b))$.

The functor gcd-main-part(V, A, a, b, x, y) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 21) PP-composition(gcd-var-init(V, A, a, b, x, y), gcd-main-loop(V, A, a, b)).

Let us consider z. The functor gcd-program(V, A, a, b, x, y, z) yielding a SCBinominativeFunction of V, A is defined by the term

(Def. 22) PP-composition(gcd-main-part(V, A, a, b, x, y), SC-assignment$(a \Rightarrow_a, z)$).

From now on x_0, y_0 denote natural numbers.

Let us consider V, A, x, y, x_0, and y_0. Let d be an object. We say that valid-gcd-input-predV, A, x, y, x_0, y_0, d if and only if

(Def. 23) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and x, $y \in \mathrm{dom}\, d_1$ and $d_1(x) = x_0$ and $d_1(y) = y_0$.

The functor valid-gcd-input(V, A, x, y, x_0, y_0) yielding a SCPartialNominativePredicate of V, A is defined by

(Def. 24) $\mathrm{dom}\, it = \mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \mathrm{dom}\, it$ holds if valid-gcd-input-predV, A, x, y, x_0, y_0, d, then $it(d) = \mathit{true}$ and if not valid-gcd-input-pred V, A, x, y, x_0, y_0, d, then $it(d) = \mathit{false}$.

One can verify that valid-gcd-input(V, A, x, y, x_0, y_0) is total.

Let us consider z. Let d be an object. We say that valid-gcd-output-predV, A, z, x_0, y_0, d if and only if

(Def. 25) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and $z \in \mathrm{dom}\, d_1$ and $d_1(z) = \gcd(x_0, y_0)$.

The functor valid-gcd-output(V, A, z, x_0, y_0) yielding a SCPartialNominativePredicate of V, A is defined by

(Def. 26) dom *it* = {d, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom} z \Rightarrow_a$} and for every object d such that $d \in \operatorname{dom}$ *it* holds if valid-gcd-output-predV, A, z, x_0, y_0, d, then $it(d) =$ *true* and if not valid-gcd-output-pred V, A, z, x_0, y_0, d, then $it(d) =$ *false*.

Let us consider a and b. Let d be an object. We say that gcd-inv-predV, A, a, b, x_0, y_0, d if and only if

(Def. 27) there exists a non-atomic nominative data d_1 of V and A such that $d = d_1$ and a, $b \in \operatorname{dom} d_1$ and there exist natural numbers x, y such that $x = d_1(a)$ and $y = d_1(b)$ and $\gcd(x, y) = \gcd(x_0, y_0)$.

The functor gcd-inv(V, A, a, b, x_0, y_0) yielding a SCPartialNominativePredicate of V, A is defined by

(Def. 28) dom *it* = $\mathrm{ND}_{\mathrm{SC}}(V, A)$ and for every object d such that $d \in \operatorname{dom}$ *it* holds if gcd-inv-predV, A, a, b, x_0, y_0, d, then $it(d) =$ *true* and if not gcd-inv-pred V, A, a, b, x_0, y_0, d, then $it(d) =$ *false*.

Let us note that gcd-inv(V, A, a, b, x_0, y_0) is total.

Now we state the propositions:

(15) $\langle$PP-inversion(SC-Psuperpos$(p, x \Rightarrow_a, a)$), SC-assignment$(x \Rightarrow_a, a), p\rangle$ is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

(16) Suppose V is not empty and $A$is-without-nonatomicND-wrt V and $a \neq b$ and $a \neq y$. Then $\langle$valid-gcd-input(V, A, x, y, x_0, y_0), gcd-var-init(V, A, a, b, x, y), gcd-inv$(V, A, a, b, x_0, y_0)\rangle$ is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $D_3 = x \Rightarrow_a$. Set $D_4 = y \Rightarrow_a$. Set $p =$ gcd-inv(V, A, a, b, x_0, y_0). Set $Q =$ SC-Psuperpos(p, D_4, b). Set $P =$ SC-Psuperpos(Q, D_3, a). Set $G =$ SC-assignment(D_4, b). Set $I =$ valid-gcd-input(V, A, x, y, x_0, y_0). $\langle$PP-inversion($G, p\rangle$ is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. $I \mid\mid = P$ by [**?** , (9)], (3), [3, (64)], [2, (2)]. □

(17) Suppose V is not empty and $A$is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \mathrm{less}(A, b, a) \wedge$ gcd-inv(V, A, a, b, x_0, y_0), SC-assignment$(\mathrm{diff}_b(A, a), a)$, gcd-inv$(V, A, a, b, x_0, y_0)\rangle$ is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $i =$ gcd-inv(V, A, a, b, x_0, y_0). Set $l = \mathrm{less}(A, b, a)$. Set $D = \mathrm{diff}_b(A, a)$. Set $f =$ SC-assignment(D, a). Set $p = l \wedge i$. For every d such that $d \in \operatorname{dom} p$ and $p(d) =$ *true* and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} i$ holds $i(f(d)) =$ *true* by [4, (23)], [5, (25), (26)], [**?** , (9), (10)]. □

(18) Suppose V is not empty and $A$is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for

every d, b is a complex on d. Then $\langle \text{less}(A,a,b) \wedge \text{gcd-inv}(V,A,a,b,x_0,y_0)$, $\text{SC-assignment}(\text{diff}_a(A,b),b), \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. PROOF: Set $i = \text{gcd-inv}(V,A,a,b,x_0,y_0)$. Set $l = \text{less}(A,a,b)$. Set $D = \text{diff}_a(A,b)$. Set $f = \text{SC-assignment}(D,b)$. Set $p = l \wedge i$. For every d such that $d \in \text{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \text{dom}\, f$ and $f(d) \in \text{dom}\, i$ holds $i(f(d)) = \mathit{true}$ by [4, (23)], [5, (25), (26)], [**?** , (9), (10)]. □

(19) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{gcd-inv}(V,A,a,b,x_0,y_0), \text{gcd-conditional-step}(V,A,a,b), \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (17).

(20) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{gcd-inv}(V,A,a,b,x_0,y_0), \text{gcd-conditional-step}(V,A,b,a), \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (18).

(21) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{gcd-inv}(V,A,a,b,x_0,y_0), \text{gcd-loop-body}(V,A,a,b), \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (19) and (20).

(22) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{PP-inversion}(\text{gcd-inv}(V,A,a,b,x_0,y_0)), \text{gcd-loop-body}(V,A,a,b), \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (20).

(23) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{gcd-inv}(V,A,a,b,x_0,y_0), \text{gcd-main-loop}(V,A,a,b), \text{Equality}(A,a,b) \wedge \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (21) and (22).

(24) Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and $a \neq y$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \text{valid-gcd-input}(V,A,x,y,x_0,y_0), \text{gcd-main-part}(V,A,a,b,x,y), \text{Equality}(A,a,b) \wedge \text{gcd-inv}(V,A,a,b,x_0,y_0)\rangle$ is a SFHT of $\text{ND}_{\text{SC}}(V,A)$. The theorem is a consequence of (16) and (23).

(25) Suppose V is not empty and A is-without-nonatomicND-wrt V and for every d, a is a value on d and for every d, b is a value on d. Then $\langle \text{Equality}(A,a,b) \wedge \text{gcd-inv}(V,A,a,b,x_0,y_0), \text{SC-assignment}(a \Rightarrow_a, z), \text{valid-gcd-outpu}$

is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

PROOF: Set $D_1 = a \Rightarrow_a$. Set $q = \mathrm{Equality}(A, a, b) \wedge \mathrm{gcd\text{-}inv}(V, A, a, b, x_0, y_0)$. Set $r = \mathrm{valid\text{-}gcd\text{-}output}(V, A, z, x_0, y_0)$. Set $s_3 = \mathrm{SC\text{-}Psuperpos}(r, D_1, z)$. $q \mid\mid = s_3$ by [3, (39)], [**?** , (16)], (11), [4, (19)]. □

Now we state the proposition:

(26) PARTIAL CORRECTNESS OF GCD ALGORITHM:

Suppose V is not empty and A is-without-nonatomicND-wrt V and $a \neq b$ and $a \neq y$ and A is complex-containing and for every d, a is a complex on d and for every d, b is a complex on d. Then $\langle \mathrm{valid\text{-}gcd\text{-}input}(V, A, x, y, x_0, y_0), \mathrm{gcd\text{-}program}(V, A, a, b, x, y, z), \mathrm{valid\text{-}gcd\text{-}output}(V, A, z, x_0, y_0) \rangle$ is a SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (7), (24), (25), and (11).

REFERENCES

[1] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[2] Czesław Byliński. Graphs of functions. *Formalized Mathematics*, 1(**1**):169–173, 1990.

[3] Ievgen Ivanov, Mykola Nikitchenko, Andrii Kryvolap, and Artur Korniłowicz. Simple-named complex-valued nominative data – definition and basic operations. *Formalized Mathematics*, 25(**3**):205–216, 2017. doi:10.1515/forma-2017-0020.

[4] Artur Korniłowicz, Ievgen Ivanov, and Mykola Nikitchenko. Kleene algebra of partial predicates. *Formalized Mathematics*, 26(**1**):11–20, 2018. doi:10.2478/forma-2018-0002.

[5] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**): 73–83, 1990.

Received June 29, 2018