JOURNAL OF FORMALIZED MATHEMATICS
Volume 15, Released 2003, Published 2003
Inst. of Computer Science, Univ. of Białystok

Correctness of Non Overwriting Programs. Part I

Yatsuka Nakamura
Shinshu University
Nagano

Summary. Non overwriting program is a program where each variable used in it is written only just one time, but the control variables used for for-statement are exceptional. Contrarily, variables are allowed to be read many times. There are other restriction for non overwriting program. For statements, only the followings are allowed: substituting-statement, if-else-statement, for-statement(with break and without break), function(correct one)-call - statement and return-statement. Grammars of non overwriting program is like one of C-language. For type of variables, 'int','real","char" and "float" can be used, and and array of them can also be used. For operation, "+", "-" and "*" are used for a type int, "+","-","*" and "/" are used for a type float. User can also define structures like in C. Non overwriting program can be translated to (predicative) logic formula in definition part to define functions. If a new function is correctly defined, a corresponding program is correct, if it does not use arrays. If it uses arrays, area check is necessary in the following theorem. Semantic correctness is shown by some theorems following the definition. These theorems must tie up the result of the program and mathematical concepts introduced before. Correctness is proven function-wise. We must use only correctness-proven functions to define a new function(to write a new program as a form of a function). Here, we present two program of division function of two natural numbers and of two integers. An algorithm is checked for each case, by proving correctness of the definitions. We also do an area check of index of arrays used in one of the programs.

MML Identifier: `PRGCOR_1`.

WWW: `http://mizar.org/JFM/Vol15/prgcor_1.html`

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

One can prove the following propositions:

(1) For all natural numbers n, m, k holds $(n+k) -' (m+k) = n -' m$.

(2) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k \geq k$ holds $(n \bmod 2 \cdot k) - k = n \bmod k$ and $(n \bmod k) + k = n \bmod 2 \cdot k$.

(3) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k \geq k$ holds $n \div k = (n \div 2 \cdot k) \cdot 2 + 1$.

(4) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k < k$ holds $n \bmod 2 \cdot k = n \bmod k$.

(5) For all natural numbers n, k such that $k > 0$ and $n \bmod 2 \cdot k < k$ holds $n \div k = (n \div 2 \cdot k) \cdot 2$.

Let C be a set, let f be a partial function from C to $\mathbb{Z}$, and let x be a set. Observe that $f(x)$ is integer.

The following two propositions are true:

© Association of Mizar Users

(6) Let m, n be natural numbers. Suppose $m > 0$. Then there exists a natural number i such that for every natural number k_2 such that $k_2 < i$ holds $m \cdot 2^{k_2} \leq n$ and $m \cdot 2^i > n$.

(7) For every integer i and for every finite sequence f such that $1 \leq i$ and $i \leq \operatorname{len} f$ holds $i \in \operatorname{dom} f$.

Let n, m be integers. Let us assume that $n \geq 0$ and $m > 0$. The functor $\operatorname{Idiv1Prg}(n,m)$ yields an integer and is defined by the condition (Def. 1).

(Def. 1) There exist finite sequences s_1, s_2, p_1 of elements of $\mathbb{Z}$ such that

(i) $\operatorname{len} s_1 = n+1$,

(ii) $\operatorname{len} s_2 = n+1$,

(iii) $\operatorname{len} p_1 = n+1$,

(iv) if $n < m$, then $\operatorname{Idiv1Prg}(n,m) = 0$, and

(v) if $n \not< m$, then $s_1(1) = m$ and there exists an integer i such that $1 \leq i$ and $i \leq n$ and for every integer k such that $1 \leq k$ and $k < i$ holds $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $p_1(i+1) = 0$ and $s_2(i+1) = n$ and for every integer j such that $1 \leq j$ and $j \leq i$ holds if $s_2((i+1)-(j-1)) \geq s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2+1$ and if $s_2((i+1)-(j-1)) \not\geq s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $\operatorname{Idiv1Prg}(n,m) = p_1(1)$.

One can prove the following propositions:

(8) Let n, m be integers. Suppose $n \geq 0$ and $m > 0$. Let s_1, s_2, p_1 be finite sequences of elements of $\mathbb{Z}$ and i be an integer. Suppose that

(i) $\operatorname{len} s_1 = n+1$,

(ii) $\operatorname{len} s_2 = n+1$,

(iii) $\operatorname{len} p_1 = n+1$, and

(iv) if $n \not< m$, then $s_1(1) = m$ and $1 \leq i$ and $i \leq n$ and for every integer k such that $1 \leq k$ and $k < i$ holds $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $p_1(i+1) = 0$ and $s_2(i+1) = n$ and for every integer j such that $1 \leq j$ and $j \leq i$ holds if $s_2((i+1)-(j-1)) \geq s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2+1$ and if $s_2((i+1)-(j-1)) \not\geq s_1((i+1)-j)$, then $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $\operatorname{Idiv1Prg}(n,m) = p_1(1)$.

Then

(v) $\operatorname{len} s_1 = n+1$,

(vi) $\operatorname{len} s_2 = n+1$,

(vii) $\operatorname{len} p_1 = n+1$,

(viii) if $n < m$, then $\operatorname{Idiv1Prg}(n,m) = 0$, and

(ix) if $n \not< m$, then $1 \in \operatorname{dom} s_1$ and $s_1(1) = m$ and $1 \leq i$ and $i \leq n$ and for every integer k such that $1 \leq k$ and $k < i$ holds $k+1 \in \operatorname{dom} s_1$ and $k \in \operatorname{dom} s_1$ and $s_1(k+1) = s_1(k) \cdot 2$ and $s_1(k+1) \not> n$ and $i+1 \in \operatorname{dom} s_1$ and $i \in \operatorname{dom} s_1$ and $s_1(i+1) = s_1(i) \cdot 2$ and $s_1(i+1) > n$ and $i+1 \in \operatorname{dom} p_1$ and $p_1(i+1) = 0$ and $i+1 \in \operatorname{dom} s_2$ and $s_2(i+1) = n$ and for every integer j such that $1 \leq j$ and $j \leq i$ holds $(i+1)-(j-1) \in \operatorname{dom} s_2$ and $(i+1)-j \in \operatorname{dom} s_1$ and if $s_2((i+1)-(j-1)) \geq s_1((i+1)-j)$, then $(i+1)-j \in \operatorname{dom} s_2$ and $(i+1)-j \in \operatorname{dom} s_1$ and $s_2((i+1)-j) = s_2((i+1)-(j-1)) - s_1((i+1)-j)$ and $(i+1)-j \in \operatorname{dom} p_1$ and $(i+1)-(j-1) \in \operatorname{dom} p_1$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2+1$ and if $s_2((i+1)-(j-1)) \not\geq s_1((i+1)-j)$, then $(i+1)-j \in \operatorname{dom} s_2$ and $(i+1)-(j-1) \in \operatorname{dom} s_2$ and $s_2((i+1)-j) = s_2((i+1)-(j-1))$ and $(i+1)-j \in \operatorname{dom} p_1$ and $(i+1)-(j-1) \in \operatorname{dom} p_1$ and $p_1((i+1)-j) = p_1((i+1)-(j-1)) \cdot 2$ and $1 \in \operatorname{dom} p_1$ and $\operatorname{Idiv1Prg}(n,m) = p_1(1)$.

(9) For all natural numbers n, m such that $m > 0$ holds $\mathrm{Idiv1Prg}((n$ **qua** integer$),(m$ **qua** integer$)) = n \div m$.

(10) For all integers n, m such that $n \geq 0$ and $m > 0$ holds $\mathrm{Idiv1Prg}(n,m) = n \div m$.

(11) Let n, m be integers and n_2, m_2 be natural numbers. Then

(i) if $m = 0$ and $n_2 = n$ and $m_2 = m$, then $n \div m = 0$ and $n_2 \div m_2 = 0$,

(ii) if $n \geq 0$ and $m > 0$ and $n_2 = n$ and $m_2 = m$, then $n \div m = n_2 \div m_2$,

(iii) if $n \geq 0$ and $m < 0$ and $n_2 = n$ and $m_2 = -m$, then if $m_2 \cdot (n_2 \div m_2) = n_2$, then $n \div m = -(n_2 \div m_2)$ and if $m_2 \cdot (n_2 \div m_2) \neq n_2$, then $n \div m = -(n_2 \div m_2) - 1$,

(iv) if $n < 0$ and $m > 0$ and $n_2 = -n$ and $m_2 = m$, then if $m_2 \cdot (n_2 \div m_2) = n_2$, then $n \div m = -(n_2 \div m_2)$ and if $m_2 \cdot (n_2 \div m_2) \neq n_2$, then $n \div m = -(n_2 \div m_2) - 1$, and

(v) if $n < 0$ and $m < 0$ and $n_2 = -n$ and $m_2 = -m$, then $n \div m = n_2 \div m_2$.

Let n, m be integers. The functor $\mathrm{IdivPrg}(n,m)$ yields an integer and is defined by the condition (Def. 2).

(Def. 2) There exists an integer i such that

(i) if $m = 0$, then $\mathrm{IdivPrg}(n,m) = 0$, and

(ii) if $m \neq 0$, then if $n \geq 0$ and $m > 0$, then $\mathrm{IdivPrg}(n,m) = \mathrm{Idiv1Prg}(n,m)$ and if $n \not\geq 0$ or $m \not> 0$, then if $n \geq 0$ and $m < 0$, then $i = \mathrm{Idiv1Prg}(n,-m)$ and if $(-m) \cdot i = n$, then $\mathrm{IdivPrg}(n,m) = -i$ and if $(-m) \cdot i \neq n$, then $\mathrm{IdivPrg}(n,m) = -i - 1$ and if $n \not\geq 0$ or $m \not< 0$, then if $n < 0$ and $m > 0$, then $i = \mathrm{Idiv1Prg}(-n,m)$ and if $m \cdot i = -n$, then $\mathrm{IdivPrg}(n,m) = -i$ and if $m \cdot i \neq -n$, then $\mathrm{IdivPrg}(n,m) = -i - 1$ and if $n \not< 0$ or $m \not> 0$, then $\mathrm{IdivPrg}(n,m) = \mathrm{Idiv1Prg}(-n,-m)$.

One can prove the following proposition

(12) For all integers n, m holds $\mathrm{IdivPrg}(n,m) = n \div m$.

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] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

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

[4] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Journal of Formalized Mathematics*, 10, 1998. http://mizar.org/JFM/Vol10/euler_2.html.

[5] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/binarith.html.

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

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

[8] Edmund Woronowicz. Relations defined on sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relset_1.html.

Received December 5, 2003

Published January 2, 2004