FORMALIZED MATHEMATICS
Volume 12, Number 1, 2004
University 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 restrictions for the non overwriting program. For statements, only the following are allowed: "substituting-statement", "if-else-statement", "for-statement" (with break and without break), function (correct one) – "call-statement" and "return-statement". Grammar of non overwriting program is like the one of the C-language. For type of variables, "int", "real", "char" and "float" can be used, 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 programs 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 perform an area check of the index of arrays used in one of the programs.

MML Identifier: PRGCOR_1.

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

One can prove the following propositions:

ISSN 1426–2630

(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 $n \bmod 2 \cdot k \geqslant k$ 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 $n \bmod 2 \cdot k \geqslant k$ 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. One can verify that $f(x)$ is integer.

Next we state two propositions:

(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 $m \cdot 2^{k_2} \leqslant n$ and $m \cdot 2^i > n$.

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

Let n, m be integers. Let us assume that $n \geqslant 0$ 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 $1 \leqslant i$ and $i \leqslant n$ and for every integer k such that $1 \leqslant k$ 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 $1 \leqslant j$ and $j \leqslant i$ holds if $s_2((i+1)-(j-1)) \geqslant s_1((i+1)-j)$, 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 $s_2((i + 1) - (j - 1)) \not\geqslant s_1((i + 1) - j)$, 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 $\operatorname{Idiv1Prg}(n, m) = p_1(1)$.

Next we state four propositions:

(8) Let n, m be integers. Suppose $n \geqslant 0$ 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 $1 \leqslant i$ and $i \leqslant n$ and for every integer k such that $1 \leqslant k$ 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 $1 \leqslant j$ and $j \leqslant i$ holds if $s_2((i+1)-(j-1)) \geqslant s_1((i+1)-j)$, 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 $s_2((i+1)-(j-1)) \not\geqslant s_1((i+1)-j)$, 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 $\mathrm{Idiv1Prg}(n, m) = p_1(1)$.

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 $\mathrm{Idiv1Prg}(n, m) = 0$, and

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

(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 $n \geqslant 0$ 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 $n \geqslant 0$ and $m > 0$ and $n_2 = n$ and $m_2 = m$, then $n \div m = n_2 \div m_2$,

(iii) if $n \geqslant 0$ 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 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 IdivPrg$(n, m) = 0$, and

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

The following proposition is true

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

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

[4] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[5] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[6] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[7] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[8] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received December 5, 2003