FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 91–100, 2018
DOI: 10.2478/forma-2018-0008

sciendo
https://www.sciendo.com/

Parity as a Property of Integers

Rafał Ziobro
Department of Carbohydrate Technology
University of Agriculture
Krakow, Poland

Summary. Even and odd numbers appear early in history of mathematics [9], as they serve to describe the property of objects easily noticeable by human eye [7]. Although the use of parity allowed to discover irrational numbers [6], there is a common opinion that this property is "not rich enough to become the main content focus of any particular research" [9].

On the other hand, due to the use of decimal system, divisibility by 2 is often regarded as the property of the last digit of a number (similarly to divisibility by 5, but not to divisibility by any other primes), which probably restricts its use for any advanced purposes.

The article aims to extend the definition of parity towards its notion in binary representation of integers, thus making an alternative to the articles grouped in [5], [4], and [3] branches, formalized in Mizar [1], [2].

MSC: 11A51 03B35 68T99

Keywords: divisibility; binary representation

MML identifier: `NEWTON05`, version: `8.1.08 5.52.1328`

Let a be an integer. One can check that $a \bmod a$ is zero and $a \bmod 2$ is natural.

Let a, b be integers. Observe that $\gcd(a \cdot b, |a|)$ reduces to $|a|$.

Let a be an odd natural number. Note that $a \bmod 2$ is non zero.

Let a be an even integer. One can check that $a \bmod 2$ is zero.

Note that $a + 1 \bmod 2$ reduces to 1.

Let a, b be real numbers. Let us observe that $\max(a, b) - \min(a, b)$ is non negative.

Let a be a natural number and b be a non zero natural number. Note that $a \bmod (a + b)$ reduces to a. One can check that $a \operatorname{div}(a + b)$ is zero.

Let a be a non trivial natural number. Let us observe that a-count(1) is zero and a-count(-1) is zero.

Let b be a natural number. One can check that a-count(a^b) reduces to b and a-count$(-a^b)$ reduces to b.

Now we state the proposition:

(1) Let us consider integers a, b. If $a \mid b$, then $\frac{b}{a}$ is integer.

Note that there exists an even integer which is non zero and every natural number which is non zero and trivial is also odd and there exists an odd natural number which is non trivial.

Let a be an integer and b be an even integer. One can verify that $\operatorname{lcm}(a, b)$ is even.

Let a, b be odd integers. Let us observe that $\operatorname{lcm}(a, b)$ is odd.

Let a, b be integers. Observe that $\frac{a+b}{\gcd(a,b)}$ is integer and $\frac{a-b}{\gcd(a,b)}$ is integer.

Let us consider real numbers a, b. Now we state the propositions:

(2) (i) $|a + b| = |a| + |b|$, or

(ii) $|a - b| = |a| + |b|$.

(3) (i) $||a| - |b|| = |a + b|$, or

(ii) $||a| - |b|| = |a - b|$.

(4) $||a| - |b|| = |a + b|$ if and only if $|a - b| = |a| + |b|$.

(5) $|a + b| = |a| + |b|$ if and only if $|a - b| = ||a| - |b||$. The theorem is a consequence of (4).

(6) Let us consider non zero real numbers a, b. Then $||a| - |b|| = |a + b|$ and $|a - b| = |a| + |b|$ if and only if it is not true that $||a| - |b|| = |a - b|$ and $|a + b| = |a| + |b|$.

Proof: $||a| - |b|| = |a + b|$ iff $|a - b| = |a| + |b|$. $||a| - |b|| = |a - b|$ iff $|a + b| = |a| + |b|$. $|a + b| = |a| + |b|$ iff $|a - b| \neq |a| + |b|$. □

Let us consider positive real numbers a, b and a natural number n. Now we state the propositions:

(7) $\min(a^n, b^n) = (\min(a, b))^n$.

(8) $\max(a^n, b^n) = (\max(a, b))^n$.

Let us consider a non zero natural number a and natural numbers m, n. Now we state the propositions:

(9) $\min(a^n, a^m) = a^{\min(n,m)}$.

(10) $\max(a^n, a^m) = a^{\max(n,m)}$.

(11) Let us consider natural numbers a, b. Then $a \bmod b \leqslant a$.

Let us consider a natural number a and non zero natural numbers b, c. Now we state the propositions:

(12) $(a \bmod c) + (b \bmod c) \geqslant a + b \bmod c$. The theorem is a consequence of (11).

(13) $(a \bmod c) \cdot (b \bmod c) \geqslant a \cdot b \bmod c$. The theorem is a consequence of (11).

Let us consider a natural number a and non zero natural numbers b, n. Now we state the propositions:

(14) $(a \bmod b)^n \geqslant a^n \bmod b$. The theorem is a consequence of (11).

(15) If $a \bmod b = 1$, then $a^n \bmod b = 1$.

(16) Let us consider natural numbers a, b, and a non zero natural number c. Then $(a \bmod c) \cdot (b \bmod c) < c$ if and only if $a \cdot b \bmod c = (a \bmod c) \cdot (b \bmod c)$.

(17) Let us consider natural numbers a, b, c. Suppose $(a \bmod c) \cdot (b \bmod c) = c$. Then $a \cdot b \bmod c = 0$.

(18) Let us consider natural numbers a, b, and a non zero natural number c. Suppose $(a \bmod c) \cdot (b \bmod c) \geqslant c$. Then $a \bmod c > 1$.

(19) Let us consider integers a, b, and a non zero natural number c. Then

(i) if $a + b \bmod c = b \bmod c$, then $a \bmod c = 0$, and

(ii) if $a + b \bmod c \neq b \bmod c$, then $a \bmod c > 0$.

Proof: If $a + b \bmod c = b \bmod c$, then $a \bmod c = 0$ by [8, (7)]. □

(20) Let us consider a natural number a, and non zero natural numbers b, c. Suppose $a \cdot b \bmod c = b$. Then $a \cdot (\gcd(b, c)) \bmod c = \gcd(b, c)$.

(21) Let us consider integers a, b. Then $a \equiv b \pmod{\gcd(a, b)}$.

Let us consider odd, a square integers k, l. Now we state the propositions:

(22) $k - l \bmod 8 = 0$.

(23) $k + l \bmod 8 = 2$. The theorem is a consequence of (22).

Let a be an integer. The functor parity(a) yielding a trivial natural number is defined by the term

(Def. 1) $a \bmod 2$.

Note that the functor parity(a) yields a trivial natural number and is defined by the term

(Def. 2) $2 - (\gcd(a, 2))$.

Let a be an even integer. Let us observe that parity(a) is zero.

Let a be an odd integer. One can check that parity(a) is non zero.

Let a be an integer. The functor Parity(a) yielding a natural number is defined by the term

(Def. 3) $\begin{cases} 0, & \textbf{if } a = 0, \\ 2^{2\text{-count}(a)}, & \textbf{otherwise}. \end{cases}$

Let a be a non zero integer. Observe that Parity(a) is non zero.

Let a be a non zero, even integer. One can verify that Parity(a) is non trivial and Parity(a) is even.

Let a be an even integer. Observe that Parity(a) is even and Parity$(a+1)$ is odd.

Let a be an odd integer. Note that Parity(a) is trivial.

Let n be a natural number. Observe that Parity(2^n) reduces to 2^n.

Note that Parity(1) reduces to 1 and Parity(2) reduces to 2.

Now we state the propositions:

(24) Let us consider an integer a. Then $\mathrm{Parity}(a) \mid a$.

(25) Let us consider integers a, b. Then $\mathrm{Parity}(a \cdot b) = (\mathrm{Parity}(a)) \cdot (\mathrm{Parity}(b))$.

Let a be an integer. The functor Oddity(a) yielding an integer is defined by the term

(Def. 4) $\frac{a}{\mathrm{Parity}(a)}$.

Now we state the proposition:

(26) Let us consider a non zero integer a. Then $\frac{a}{\mathrm{Parity}(a)} = a \operatorname{div} \mathrm{Parity}(a)$.
The theorem is a consequence of (24).

Let a be an integer. One can check that $(\mathrm{Parity}(a)) \cdot (\mathrm{Oddity}(a))$ reduces to a and Parity(Parity(a)) reduces to Parity(a) and Oddity(Oddity(a)) reduces to Oddity(a). Observe that Parity(Oddity(a)) is trivial and $a + \mathrm{Parity}(a)$ is even and $a - \mathrm{Parity}(a)$ is even and $\frac{a}{\mathrm{Parity}(a)}$ is integer.

Now we state the propositions:

(27) Let us consider a non zero integer a. Then $\mathrm{Oddity}(\mathrm{Parity}(a)) = 1$.

(28) Let us consider integers a, b. Then $\mathrm{Oddity}(a \cdot b) = (\mathrm{Oddity}(a)) \cdot (\mathrm{Oddity}(b))$.
The theorem is a consequence of (25).

Let a be a non zero integer. Observe that $\frac{a}{\mathrm{Parity}(a)}$ is odd and $a \operatorname{div} \mathrm{Parity}(a)$ is odd.

Now we state the proposition:

(29) Let us consider integers a, b. Then

(i) $\mathrm{Parity}(a) \mid \mathrm{Parity}(b)$, or

(ii) $\mathrm{Parity}(b) \mid \mathrm{Parity}(a)$.

Let us consider non zero integers a, b. Now we state the propositions:

(30) $\mathrm{Parity}(a) \mid \mathrm{Parity}(b)$ if and only if $\mathrm{Parity}(b) \geqslant \mathrm{Parity}(a)$.
PROOF: If $\mathrm{Parity}(b) \geqslant \mathrm{Parity}(a)$, then $\mathrm{Parity}(a) \mid \mathrm{Parity}(b)$. □

(31) If $\mathrm{Parity}(a) > \mathrm{Parity}(b)$, then $2 \cdot (\mathrm{Parity}(b)) \mid \mathrm{Parity}(a)$.

Let us consider an integer a. Now we state the propositions:

(32) $\mathrm{Parity}(a) = \mathrm{Parity}(-a)$.

(33) $\mathrm{Parity}(a) = \mathrm{Parity}(|a|)$. The theorem is a consequence of (32).

(34) $\mathrm{Parity}(a) \leqslant |a|$. The theorem is a consequence of (24) and (33).

(35) Let us consider integers a, b. If a and b are relatively prime, then a is odd or b is odd.

Let us consider odd integers a, b. Now we state the propositions:

(36) If $|a| \neq |b|$, then $\min(\mathrm{Parity}(a-b), \mathrm{Parity}(a+b)) = 2$. The theorem is a consequence of (33), (9), (2), and (4).

(37) $\min(\mathrm{Parity}(a-b), \mathrm{Parity}(a+b)) \leqslant 2$. The theorem is a consequence of (3), (33), and (36).

(38) Let us consider integers a, b. Suppose a and b are relatively prime. Then $\min(\mathrm{Parity}(a-b), \mathrm{Parity}(a+b)) \leqslant 2$. The theorem is a consequence of (35) and (37).

(39) Let us consider non zero integers a, b, and a non trivial natural number c. Then $c\text{-count}(\gcd(a,b)) = \min(c\text{-count}(a), c\text{-count}(b))$.

(40) Let us consider non zero integers a, b.
Then $\mathrm{Parity}(\gcd(a,b)) = \min(\mathrm{Parity}(a), \mathrm{Parity}(b))$. The theorem is a consequence of (39) and (9).

(41) Let us consider integers a, b. Then $\gcd(\mathrm{Parity}(a), \mathrm{Parity}(b)) = \mathrm{Parity}(\gcd(a,b))$. The theorem is a consequence of (33), (29), and (40).

(42) Let us consider a natural number a. Then $\mathrm{Parity}(2 \cdot a) = 2 \cdot (\mathrm{Parity}(a))$. The theorem is a consequence of (25).

(43) Let us consider integers a, b. Then $\mathrm{lcm}(\mathrm{Parity}(a), \mathrm{Parity}(b)) = \mathrm{Parity}(\mathrm{lcm}(a,b))$. The theorem is a consequence of (25), (33), and (41).

(44) Let us consider non zero integers a, b.
Then $\mathrm{Parity}(\mathrm{lcm}(a,b)) = \max(\mathrm{Parity}(a), \mathrm{Parity}(b))$. The theorem is a consequence of (41), (40), and (43).

(45) Let us consider integers a, b. Then $\mathrm{Parity}(a+b) = (\mathrm{Parity}(\gcd(a,b))) \cdot (\mathrm{Parity}(\frac{a+b}{\gcd(a,b)}))$. The theorem is a consequence of (25).

(46) Let us consider an integer a, and a natural number n. Then $\mathrm{Parity}(a^n) = (\mathrm{Parity}(a))^n$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \mathrm{Parity}(a^{\$_1}) = (\mathrm{Parity}(a))^{\$_1}$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural number x, $\mathcal{P}[x]$. □

(47) Let us consider non zero integers a, b, and a natural number n. Then $\min(\mathrm{Parity}(a^n), \mathrm{Parity}(b^n)) = (\min(\mathrm{Parity}(a), \mathrm{Parity}(b)))^n$. The theorem is a consequence of (40) and (46).

Let a be an odd integer. We identify $\mathrm{parity}(a)$ with $\mathrm{Parity}(a)$. We identify $\mathrm{Parity}(a)$ with $\mathrm{parity}(a)$. Let us observe that $a^{\mathrm{parity}(a)}$ reduces to a.

Let a be an even integer. Let us observe that $a^{\mathrm{parity}(a)}$ is trivial and non zero.

Let a be an integer. One can check that $\mathrm{parity}(\mathrm{parity}(a))$ reduces to $\mathrm{parity}(a)$ and $\mathrm{Parity}(\mathrm{parity}(a))$ reduces to $\mathrm{parity}(a)$.

Now we state the proposition:

(48) Let us consider an integer a. Then

- (i) a is even iff $\mathrm{parity}(a)$ is even, and
- (ii) $\mathrm{parity}(a)$ is even iff $\mathrm{Parity}(a)$ is even.

Let a be an integer. Note that $\mathrm{parity}(a) + \mathrm{Parity}(a)$ is even and $\mathrm{Parity}(a) - \mathrm{parity}(a)$ is even and $\mathrm{Parity}(a) - \mathrm{parity}(a)$ is natural and $a + \mathrm{parity}(a)$ is even and $a - \mathrm{parity}(a)$ is even.

Let us consider an integer a. Now we state the propositions:

(49) $\mathrm{parity}(\mathrm{Parity}(a)) = \mathrm{parity}(a)$.

(50) $\mathrm{parity}(a) = \mathrm{parity}(-a)$.

Let us consider integers a, b. Now we state the propositions:

(51) $\mathrm{parity}(a - b) = |\,\mathrm{parity}(a) - \mathrm{parity}(b)|$.

(52) $\mathrm{parity}(a + b) = \mathrm{parity}(\mathrm{parity}(a) + \mathrm{parity}(b))$.

(53) $\mathrm{parity}(a + b) = \mathrm{parity}(a - b)$. The theorem is a consequence of (50).

(54) $\mathrm{parity}(a + b) = |\,\mathrm{parity}(a) - \mathrm{parity}(b)|$. The theorem is a consequence of (53) and (51).

(55) Let us consider natural numbers a, b. Then

- (i) if $\mathrm{parity}(a + b) = \mathrm{parity}(b)$, then $\mathrm{parity}(a) = 0$, and
- (ii) if $\mathrm{parity}(a + b) \neq \mathrm{parity}(b)$, then $\mathrm{parity}(a) = 1$.

The theorem is a consequence of (19).

Let us consider integers a, b. Now we state the propositions:

(56)
- (i) $\mathrm{parity}(a + b) = \mathrm{parity}(a) + \mathrm{parity}(b) - 2 \cdot (\mathrm{parity}(a)) \cdot (\mathrm{parity}(b))$, and
- (ii) $\mathrm{parity}(a) - \mathrm{parity}(b) = \mathrm{parity}(a + b) - 2 \cdot (\mathrm{parity}(a + b)) \cdot (\mathrm{parity}(b))$, and
- (iii) $\mathrm{parity}(a) - \mathrm{parity}(b) = 2 \cdot (\mathrm{parity}(a)) \cdot (\mathrm{parity}(a + b)) - \mathrm{parity}(a + b)$.

(57) $a + b$ is even if and only if $\mathrm{parity}(a) = \mathrm{parity}(b)$. The theorem is a consequence of (54).

(58) $\mathrm{parity}(a \cdot b) = (\mathrm{parity}(a)) \cdot (\mathrm{parity}(b))$.

(59) $\mathrm{parity}(\mathrm{lcm}(a, b)) = \mathrm{parity}(a \cdot b)$.

(60) $\mathrm{parity}(\mathrm{gcd}(a, b)) = \max(\mathrm{parity}(a), \mathrm{parity}(b))$.

(61) $\mathrm{parity}(a \cdot b) = \min(\mathrm{parity}(a), \mathrm{parity}(b))$.

(62) Let us consider an integer a, and a non zero natural number n. Then $\mathrm{parity}(a^n) = \mathrm{parity}(a)$.

(63) Let us consider non zero integers a, b. Suppose $\mathrm{Parity}(a+b) \geqslant \mathrm{Parity}(a) + \mathrm{Parity}(b)$. Then $\mathrm{Parity}(a) = \mathrm{Parity}(b)$.

(64) Let us consider integers a, b. Suppose $\mathrm{Parity}(a + b) > \mathrm{Parity}(a) + \mathrm{Parity}(b)$. Then $\mathrm{Parity}(a) = \mathrm{Parity}(b)$. The theorem is a consequence of (63).

(65) Let us consider odd integers a, b, and an odd natural number m. Then $\mathrm{Parity}(a^m + b^m) = \mathrm{Parity}(a + b)$.

(66) Let us consider odd integers a, b, and an even natural number m. Then $\mathrm{Parity}(a^m + b^m) = 2$.

Let us consider non zero integers a, b. Now we state the propositions:

(67) If $a+b \neq 0$, then if $\mathrm{Parity}(a) = \mathrm{Parity}(b)$, then $\mathrm{Parity}(a+b) \geqslant \mathrm{Parity}(a) + \mathrm{Parity}(b)$.

(68) $\mathrm{Parity}(a + b) = \mathrm{Parity}(b)$ if and only if $\mathrm{Parity}(a) > \mathrm{Parity}(b)$. The theorem is a consequence of (67).

(69) Let us consider non zero natural numbers a, b. Suppose $\mathrm{Parity}(a + b) < \mathrm{Parity}(a) + \mathrm{Parity}(b)$. Then $\mathrm{Parity}(a+b) = \min(\mathrm{Parity}(a), \mathrm{Parity}(b))$. The theorem is a consequence of (67).

(70) Let us consider non zero integers a, b. Suppose $a+b \neq 0$. If $\mathrm{Parity}(a+b) = \mathrm{Parity}(a)$, then $\mathrm{Parity}(a) < \mathrm{Parity}(b)$. The theorem is a consequence of (67).

Let us consider an integer a. Now we state the propositions:

(71) (i) $\mathrm{Parity}(a + \mathrm{Parity}(a)) = (\mathrm{Parity}(\mathrm{Oddity}(a) + 1)) \cdot (\mathrm{Parity}(a))$, and

(ii) $\mathrm{Parity}(a - \mathrm{Parity}(a)) = (\mathrm{Parity}(\mathrm{Oddity}(a) - 1)) \cdot (\mathrm{Parity}(a))$.

The theorem is a consequence of (25).

(72) (i) $2 \cdot (\mathrm{Parity}(a)) \mid \mathrm{Parity}(a + \mathrm{Parity}(a))$, and

(ii) $2 \cdot (\mathrm{Parity}(a)) \mid \mathrm{Parity}(a - \mathrm{Parity}(a))$.

The theorem is a consequence of (71).

(73) Let us consider integers a, b. Suppose $\mathrm{Parity}(a) = \mathrm{Parity}(b)$. Then $\mathrm{Parity}(a + b) = \mathrm{Parity}(a + \mathrm{Parity}(a) + (b - \mathrm{Parity}(b)))$.

Let us consider a natural number a. Now we state the propositions:

(74) $\mathrm{Parity}(a + \mathrm{Parity}(a)) \geqslant 2 \cdot (\mathrm{Parity}(a))$. The theorem is a consequence of (72).

(75) (i) $\mathrm{Parity}(a - \mathrm{Parity}(a)) \geqslant 2 \cdot (\mathrm{Parity}(a))$, or

(ii) $a = \mathrm{Parity}(a)$.

The theorem is a consequence of (71).

Let us consider odd integers a, b. Now we state the propositions:

(76) $\mathrm{Parity}(a+b) \neq \mathrm{Parity}(a-b)$. The theorem is a consequence of (25).

(77) If $\mathrm{Parity}(a+1) = \mathrm{Parity}(b-1)$, then $a \neq b$. The theorem is a consequence of (76).

(78) Let us consider an odd natural number a, and a non trivial, odd natural number b. Then

(i) $\mathrm{Parity}(a+b) = \min(\mathrm{Parity}(a+1), \mathrm{Parity}(b-1))$, or

(ii) $\mathrm{Parity}(a+b) \geqslant 2 \cdot (\mathrm{Parity}(a+1))$.

The theorem is a consequence of (67).

Let us consider non zero integers a, b. Now we state the propositions:

(79) If $\mathrm{Parity}(a) > \mathrm{Parity}(b)$, then $a \operatorname{div} \mathrm{Parity}(b)$ is even. The theorem is a consequence of (31) and (24).

(80) $\mathrm{Parity}(a) > \mathrm{Parity}(b)$ if and only if $\mathrm{Parity}(a) \operatorname{div} \mathrm{Parity}(b)$ is non zero and even. The theorem is a consequence of (31).

(81) Let us consider an odd natural number a. Then $\mathrm{Parity}(a-1) = 2 \cdot (\mathrm{Parity}(a \operatorname{div} 2))$. The theorem is a consequence of (25).

(82) Let us consider non zero integers a, b. Then

(i) $\min(\mathrm{Parity}(a), \mathrm{Parity}(b)) \mid a$, and

(ii) $\min(\mathrm{Parity}(a), \mathrm{Parity}(b)) \mid b$.

The theorem is a consequence of (30) and (24).

Let a, b be non zero integers. Note that $\frac{a+b}{\min(\mathrm{Parity}(a),\mathrm{Parity}(b))}$ is integer.

Let p be a non square integer and n be an odd natural number. Let us note that p^n is non square.

Let a be an integer and n be an even natural number. Let us note that a^n is a square.

Let p be a prime natural number and a be a non zero, a square integer. Let us observe that p-count(a) is even.

Let a be an odd integer. Note that $2 \cdot a$ is non square.

Let a be square integer. One can check that $\mathrm{Parity}(a)$ is a square and $\mathrm{Oddity}(a)$ is a square.

Let a be a non zero, a square integer. One can check that 2-count(a) is even.

Now we state the propositions:

(83) Let us consider non negative real numbers a, b. Then $\max(a, b) - \min(a, b) = |a-b|$.

(84) Let us consider an even integer a. If $4 \nmid a$, then a is not square.

Proof: $2 \nmid \frac{a}{2}$ by [10, (2)]. □

(85) Let us consider odd integers a, b. If $a - b$ is a square, then $a + b$ is not a square. The theorem is a consequence of (2), (5), (83), (84), and (4).

Let us consider non zero integers a, b. Now we state the propositions:

(86) $\mathrm{Parity}(a+b) = (\min(\mathrm{Parity}(a), \mathrm{Parity}(b)))\cdot(\mathrm{Parity}(\frac{a+b}{\min(\mathrm{Parity}(a),\mathrm{Parity}(b))}))$. The theorem is a consequence of (30) and (25).

(87) (i) $\mathrm{Parity}(a)$ and $\mathrm{Oddity}(b)$ are relatively prime, and

(ii) $\gcd(\mathrm{Parity}(a), \mathrm{Oddity}(b)) = 1$.

(88) Let us consider an integer a. Then $|\,\mathrm{Oddity}(a)| = \mathrm{Oddity}(|a|)$. The theorem is a consequence of (33).

(89) Let us consider integers a, b. Then $\gcd(\mathrm{Oddity}(a), \mathrm{Oddity}(b)) = \mathrm{Oddity}(\gcd(a, b))$. The theorem is a consequence of (87), (28), (41), (27), and (88).

(90) Let us consider non zero integers a, b. Then $\gcd(a, b) = (\gcd(\mathrm{Parity}(a), \mathrm{Parity}(b))) \cdot (\gcd(\mathrm{Oddity}(a), \mathrm{Oddity}(b)))$. The theorem is a consequence of (87).

(91) Let us consider an odd natural number a. Then $\mathrm{Parity}(a + 1) = 2$ if and only if $\mathrm{parity}(a \operatorname{div} 2) = 0$. The theorem is a consequence of (78), (76), and (25).

(92) Let us consider an even integer a. Then $a \operatorname{div} 2 = a + 1 \operatorname{div} 2$.

(93) Let us consider integers a, b. Then $a + b = 2 \cdot ((a \operatorname{div} 2) + (b \operatorname{div} 2)) + \mathrm{parity}(a) + \mathrm{parity}(b)$.

Let us consider odd integers a, b. Now we state the propositions:

(94) $\mathrm{Parity}(a + b) = 2 \cdot (\mathrm{Parity}((a \operatorname{div} 2) + (b \operatorname{div} 2) + 1))$. The theorem is a consequence of (93) and (25).

(95) $\mathrm{Parity}(a + b) = 2$ if and only if $\mathrm{parity}(a \operatorname{div} 2) = \mathrm{parity}(b \operatorname{div} 2)$. The theorem is a consequence of (94) and (57).

Let us consider non zero integers a, b. Now we state the propositions:

(96) $\mathrm{Parity}(a + b) = \mathrm{Parity}(a) + \mathrm{Parity}(b)$ if and only if $\mathrm{Parity}(a) = \mathrm{Parity}(b)$ and $\mathrm{parity}(\mathrm{Oddity}(a) \operatorname{div} 2) = \mathrm{parity}(\mathrm{Oddity}(b) \operatorname{div} 2)$. The theorem is a consequence of (63), (25), and (95).

(97) Suppose $a+b \neq 0$ and $\mathrm{Parity}(a) = \mathrm{Parity}(b)$ and $\mathrm{parity}(\mathrm{Oddity}(a) \operatorname{div} 2) \neq \mathrm{parity}(\mathrm{Oddity}(b) \operatorname{div} 2)$. Then $\mathrm{Parity}(a + b) > \mathrm{Parity}(a) + \mathrm{Parity}(b)$. The theorem is a consequence of (67) and (96).

Acknowledgement: Ad Maiorem Dei Gloriam

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Yoshinori Fujisawa and Yasushi Fuwa. Definitions of radix-2^k signed-digit number and its adder algorithm. *Formalized Mathematics*, 9(**1**):71–75, 2001.

[4] Adam Naumowicz. On the representation of natural numbers in positional numeral systems. *Formalized Mathematics*, 14(**4**):221–223, 2006. doi:10.2478/v10037-006-0025-9.

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

[6] Lucio Russo and Silvio Levy (translator). *The forgotten revolution: how science was born in 300 BC and why it had to be reborn.* Springer Science & Business Media, 2013.

[7] Walter Warwick Sawyer. *Vision in elementary mathematics.* Courier Corporation, 2003.

[8] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**):247–252, 2008. doi:10.2478/v10037-008-0029-8.

[9] Rina Zazkis. Odds and ends of odds and evens: An inquiry into students' understanding of even and odd numbers. *Educational Studies in Mathematics*, 36(1):73–89, Jun 1998. doi:10.1023/A:1003149901409.

[10] Rafał Ziobro. Fermat's Little Theorem via divisibility of Newton's binomial. *Formalized Mathematics*, 23(**3**):215–229, 2015. doi:10.1515/forma-2015-0018.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 101–124, 2018
DOI: 10.2478/forma-2018-0009

sciendo
https://www.sciendo.com/

About Supergraphs. Part I

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. Drawing a finite graph is usually done by a finite sequence of the following three operations.

1. Draw a vertex of the graph.
2. Draw an edge between two vertices of the graph.
3. Draw an edge starting from a vertex of the graph and immediately draw a vertex at the other end of it.

By this procedure any finite graph can be constructed. This property of graphs is so obvious that the author of this article has yet to find a reference where it is mentioned explicitly. In introductionary books (like [10], [5], [9]) as well as in advanced ones (like [4]), after the initial definition of graphs the examples are usually given by graphical representations rather than explicit set theoretic descriptions, assuming a mutual understanding how the representation is to be translated into a description fitting the definition. However, Mizar [2], [3] does not possess this innate ability of humans to translate pictures into graphs. Therefore, if one wants to create graphs in Mizar without directly providing a set theoretic description (i.e. using the `createGraph` functor), a rigorous approach to the constructing operations is required.

In this paper supergraphs are defined as an inverse mode to subgraphs as given in [8]. The three graph construction operations are defined as modes extending `Supergraph` similar to how the various remove operations were introduced as submodes of `Subgraph` in [8]. Many theorems are proven that describe how graph properties are transferred to special supergraphs. In particular, to prove that disconnected graphs cannot become connected by adding an edge between two vertices that lie in the same component, the theory of replacing a part of a walk with another walk is introduced in the preliminaries.

MSC: 05C76 03B35 68T99

Keywords: supergraph; graph operations

MML identifier: GLIB_006, version: 8.1.08 5.52.1328

[1] mailto: skoch02@students.uni-mainz.de

1. General Preliminaries

Let us consider an even integer n and an odd integer m. Now we state the propositions:

(1) If $n \leqslant m$, then $n+1 \leqslant m$.

(2) If $m \leqslant n$, then $m+1 \leqslant n$.

(3) Let us consider natural numbers i, j. If $i > i -' 1 + j$, then $j = 0$.

(4) Let us consider finite sequences f, g, and a natural number i. Suppose $i \leqslant \operatorname{len} f$ and $\operatorname{mid}(f, i, i -' 1 + \operatorname{len} g) = g$. Then $i -' 1 + \operatorname{len} g \leqslant \operatorname{len} f$. The theorem is a consequence of (3).

Let us consider a finite sequence p and a natural number n. Now we state the propositions:

(5) If $n \in \operatorname{dom} p$ and $n+1 \leqslant \operatorname{len} p$, then $\operatorname{mid}(p, n, n+1) = \langle p(n), p(n+1) \rangle$.

(6) If $n \in \operatorname{dom} p$ and $n+2 \leqslant \operatorname{len} p$, then $\operatorname{mid}(p, n, n+2) = \langle p(n), p(n+1), p(n+2) \rangle$. The theorem is a consequence of (5).

(7) Let us consider a non empty set D, finite sequences f, g of elements of D, and a natural number n. Suppose g is a substring of f. Then

(i) $\operatorname{len} g = 0$, or

(ii) $1 \leqslant n -' 1 + \operatorname{len} g \leqslant \operatorname{len} f$ and $n \leqslant n -' 1 + \operatorname{len} g$.

The theorem is a consequence of (4).

Let D be a non empty set, f, g be finite sequences of elements of D, and n be a natural number. We say that g is an odd substring of f not starting before n if and only if

(Def. 1) if $\operatorname{len} g > 0$, then there exists an odd natural number i such that $n \leqslant i \leqslant \operatorname{len} f$ and $\operatorname{mid}(f, i, i -' 1 + \operatorname{len} g) = g$.

We say that g is an even substring of f not starting before n if and only if

(Def. 2) if $\operatorname{len} g > 0$, then there exists an even natural number i such that $n \leqslant i \leqslant \operatorname{len} f$ and $\operatorname{mid}(f, i, i -' 1 + \operatorname{len} g) = g$.

Let us consider a non empty set D, finite sequences f, g of elements of D, and a natural number n. Now we state the propositions:

(8) If g is an odd substring of f not starting before n, then g is a substring of f.

(9) If g is an even substring of f not starting before n, then g is a substring of f.

(10) Let us consider a non empty set D, finite sequences f, g of elements of D, and natural numbers n, m. Suppose $m \geqslant n$. Then

(i) if g is an odd substring of f not starting before m, then g is an odd substring of f not starting before n, and

(ii) if g is an even substring of f not starting before m, then g is an even substring of f not starting before n.

(11) Let us consider a non empty set D, and a finite sequence f of elements of D. If $1 \leqslant \operatorname{len} f$, then f is an odd substring of f not starting before 0.

(12) Let us consider a non empty set D, finite sequences f, g of elements of D, and an even element n of $\mathbb{N}$. Suppose g is an odd substring of f not starting before n. Then g is an odd substring of f not starting before $n+1$.

(13) Let us consider a non empty set D, finite sequences f, g of elements of D, and an odd element n of $\mathbb{N}$. Suppose g is an even substring of f not starting before n. Then g is an even substring of f not starting before $n+1$.

(14) Let us consider a non empty set D, and finite sequences f, g of elements of D. Suppose g is an odd substring of f not starting before 0. Then g is an odd substring of f not starting before 1. The theorem is a consequence of (12).

2. Graph Preliminaries

Let G be a non-directed-multi graph. Observe that every subgraph of G is non-directed-multi.

(15) Every graph is a subgraph of G induced by the vertices of G.

(16) Let us consider graphs G_1, G_3, sets V, E, and a subgraph G_2 of G_1 induced by V and E. If $G_2 \approx G_3$, then G_3 is a subgraph of G_1 induced by V and E.

(17) Let us consider a graph G, a set X, and objects e, y. Suppose e joins a vertex from X and a vertex from $\{y\}$ in G. Then there exists an object x such that

(i) $x \in X$, and

(ii) e joins x and y in G.

(18) Let us consider a graph G, and a set X. Suppose $X \cap$ (the vertices of G) $= \emptyset$. Then

(i) G.edgesInto$(X) = \emptyset$, and

(ii) G.edgesOutOf$(X) = \emptyset$, and

(iii) G.edgesInOut$(X) = \emptyset$, and

(iv) G.edgesBetween$(X) = \emptyset$.

PROOF: G.edgesInto$(X) = \emptyset$. G.edgesOutOf$(X) = \emptyset$. □

Let us consider a graph G, sets X_1, X_2, and an object y. Now we state the propositions:

(19) If X_1 misses X_2, then G.edgesBetween$(X_1, \{y\})$ misses G.edgesBetween $(X_2, \{y\})$. The theorem is a consequence of (17).

(20) G.edgesBetween$(X_1 \cup X_2, \{y\}) =$ G.edgesBetween$(X_1, \{y\}) \cup G$.edgesBetween$(X_2, \{y\})$.
PROOF: Set $E_1 = G$.edgesBetween$(X_1, \{y\})$. Set $E_2 = G$.edgesBetween$(X_2, \{y\})$. For every object e such that $e \in G$.edgesBetween$(X_1 \cup X_2, \{y\})$ holds $e \in E_1 \cup E_2$. □

(21) Let us consider a trivial graph G. Then there exists a vertex v of G such that

(i) the vertices of $G = \{v\}$, and

(ii) the source of $G =$ (the edges of G) $\longmapsto v$, and

(iii) the target of $G =$ (the edges of G) $\longmapsto v$.

PROOF: Consider v being a vertex of G such that the vertices of $G = \{v\}$. For every object e such that $e \in$ dom(the source of G) holds (the source of G)$(e) = v$. For every object e such that $e \in$ dom(the target of G) holds (the target of G)$(e) = v$. □

Let G be a graph. Let us note that every walk of G which is closed, trail-like, and non trivial is also circuit-like and every walk of G which is closed, path-like, and non trivial is also cycle-like.

Let us consider graphs G_1, G_2, a walk W_1 of G_1, and a walk W_2 of G_2. Now we state the propositions:

(22) If $W_1 = W_2$, then if W_1 is trail-like, then W_2 is trail-like.

(23) If $W_1 = W_2$, then if W_1 is path-like, then W_2 is path-like. The theorem is a consequence of (22).

(24) If $W_1 = W_2$, then if W_1 is cycle-like, then W_2 is cycle-like. The theorem is a consequence of (23).

(25) If $W_1 = W_2$, then if W_1 is vertex-distinct, then W_2 is vertex-distinct.

(26) Let us consider a graph G, a walk W of G, and a vertex v of G. If $v \in W$.vertices(), then G.walkOf(v) is a substring of W.

(27) Let us consider a graph G, a walk W of G, and an odd element n of $\mathbb{N}$. Suppose $n + 2 \leqslant \operatorname{len} W$. Then G.walkOf$(W(n), W(n+1), W(n+2))$ is an odd substring of W not starting before 0. The theorem is a consequence of (6).

Let us consider a graph G, a walk W of G, and objects u, e, v. Now we state the propositions:

(28) Suppose e joins u and v in G and $e \in W$.edges(). Then

(i) G.walkOf(u, e, v) is an odd substring of W not starting before 0, or

(ii) G.walkOf(v, e, u) is an odd substring of W not starting before 0.

The theorem is a consequence of (27).

(29) If e joins u and v in G and G.walkOf(u, e, v) is an odd substring of W not starting before 0, then $e \in W$.edges() and u, $v \in W$.vertices(). The theorem is a consequence of (14), (8), and (7).

Let G be a graph and W_1, W_2 be walks of G.

The functor W_1.findFirstVertex(W_2) yielding an odd element of $\mathbb{N}$ is defined by

(Def. 3) (i) *it* $\leqslant \operatorname{len} W_1$ and there exists an even natural number k such that *it* $= k + 1$ and for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(k + n) = W_2(n)$ and for every even natural number l such that for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(l + n) = W_2(n)$ holds $k \leqslant l$, **if** W_2 is an odd substring of W_1 not starting before 0,

(ii) *it* $= \operatorname{len} W_1$, **otherwise**.

The functor W_1.findLastVertex(W_2) yielding an odd element of $\mathbb{N}$ is defined by

(Def. 4) (i) *it* $\leqslant \operatorname{len} W_1$ and there exists an even natural number k such that *it* $= k + \operatorname{len} W_2$ and for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(k + n) = W_2(n)$ and for every even natural number l such that for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(l + n) = W_2(n)$ holds $k \leqslant l$, **if** W_2 is an odd substring of W_1 not starting before 0,

(ii) *it* $= \operatorname{len} W_1$, **otherwise**.

Let us consider a graph G and walks W_1, W_2 of G. Now we state the propositions:

(30) Suppose W_2 is an odd substring of W_1 not starting before 0. Then

(i) $W_1(W_1$.findFirstVertex$(W_2)) = W_2$.first(), and

(ii) $W_1(W_1$.findLastVertex$(W_2)) = W_2$.last().

(31) Suppose W_2 is an odd substring of W_1 not starting before 0. Then

(i) $1 \leqslant W_1$.findFirstVertex$(W_2) \leqslant \operatorname{len} W_1$, and

(ii) $1 \leqslant W_1$.findLastVertex$(W_2) \leqslant \operatorname{len} W_1$.

(32) Let us consider a graph G, and a walk W of G. Then

(i) $1 = W.\mathrm{findFirstVertex}(W)$, and

(ii) $W.\mathrm{findLastVertex}(W) = \mathrm{len}\, W$.

The theorem is a consequence of (11).

(33) Let us consider a graph G, and walks W_1, W_2 of G. Suppose W_2 is an odd substring of W_1 not starting before 0. Then $W_1.\mathrm{findFirstVertex}(W_2) \leqslant W_1.\mathrm{findLastVertex}(W_2)$.

Let G be a graph and W_1, W_2, W_3 be walks of G. The functor $W_1.\mathrm{replaceWith}(W_2, W_3)$ yielding a walk of G is defined by the term

$$\text{(Def. 5)} \quad \begin{cases} ((W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{append}(W_3)).\mathrm{append}((W_1.\mathrm{cut} \\ \quad (W_1.\mathrm{findLastVertex}(W_2), \mathrm{len}\, W_1))), \\ \textbf{if } W_2 \text{ is an odd substring of } W_1 \text{ not starting before 0 and } W_2.\mathrm{first}() \\ \quad = W_3.\mathrm{first}() \text{ and } W_2.\mathrm{last}() = W_3.\mathrm{last}(), W_1, \\ \textbf{otherwise}. \end{cases}$$

Let W_1, W_3 be walks of G and e be an object.

The functor $W_1.\mathrm{replaceEdgeWith}(e, W_3)$ yielding a walk of G is defined by the term

$$\text{(Def. 6)} \quad \begin{cases} W_1.\mathrm{replaceWith}(G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}()), W_3), \\ \textbf{if } e \text{ joins } W_3.\mathrm{first}() \text{ and } W_3.\mathrm{last}() \text{ in } G \text{ and } G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, \\ \quad W_3.\mathrm{last}()) \text{ is an odd substring of } W_1 \text{ not starting before } 0, W_1, \\ \textbf{otherwise}. \end{cases}$$

Let W_1, W_2 be walks of G. The functor $W_1.\mathrm{replaceWithEdge}(W_2, e)$ yielding a walk of G is defined by the term

$$\text{(Def. 7)} \quad \begin{cases} W_1.\mathrm{replaceWith}(W_2, G.\mathrm{walkOf}(W_2.\mathrm{first}(), e, W_2.\mathrm{last}())), \\ \textbf{if } W_2 \text{ is an odd substring of } W_1 \text{ not starting before 0 and } e \text{ joins} \\ \quad W_2.\mathrm{first}() \text{ and } W_2.\mathrm{last}() \text{ in } G, W_1, \\ \textbf{otherwise}. \end{cases}$$

Let us consider a graph G and walks W_1, W_2, W_3 of G. Now we state the propositions:

(34) Suppose W_2 is an odd substring of W_1 not starting before 0 and $W_2.\mathrm{first}() = W_3.\mathrm{first}()$ and $W_2.\mathrm{last}() = W_3.\mathrm{last}()$. Then

(i) $(W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{first}() = W_1.\mathrm{first}()$, and

(ii) $(W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{last}() = W_3.\mathrm{first}()$, and

(iii) $((W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{append}(W_3)).\mathrm{first}() = W_1.\mathrm{first}()$, and

(iv) $((W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{append}(W_3)).\mathrm{last}() = W_3.\mathrm{last}()$, and

(v) $(W_1.\mathrm{cut}(W_1.\mathrm{findLastVertex}(W_2), \mathrm{len}\, W_1)).\mathrm{first}() = W_3.\mathrm{last}()$, and

(vi) $(W_1.\mathrm{cut}(W_1.\mathrm{findLastVertex}(W_2), \mathrm{len}\, W_1)).\mathrm{last}() = W_1.\mathrm{last}()$.

The theorem is a consequence of (31) and (30).

(35) (i) $W_1.\mathrm{first}() = (W_1.\mathrm{replaceWith}(W_2, W_3)).\mathrm{first}()$, and

(ii) $W_1.\mathrm{last}() = (W_1.\mathrm{replaceWith}(W_2, W_3)).\mathrm{last}()$.

The theorem is a consequence of (34).

(36) Suppose W_2 is an odd substring of W_1 not starting before 0 and $W_2.\mathrm{first}() = W_3.\mathrm{first}()$ and $W_2.\mathrm{last}() = W_3.\mathrm{last}()$. Then $(W_1.\mathrm{replaceWith}(W_2, W_3)).\mathrm{vertices}() = ((W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{vertices}() \cup W_3.\mathrm{vertices}()) \cup (W_1.\mathrm{cut}(W_1.\mathrm{findLastVertex}(W_2), \mathrm{len}\, W_1)).\mathrm{vertices}()$. The theorem is a consequence of (34).

(37) Suppose W_2 is an odd substring of W_1 not starting before 0 and $W_2.\mathrm{first}() = W_3.\mathrm{first}()$ and $W_2.\mathrm{last}() = W_3.\mathrm{last}()$. Then $(W_1.\mathrm{replaceWith}(W_2, W_3)).\mathrm{edges}() = ((W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(W_2))).\mathrm{edges}() \cup W_3.\mathrm{edges}()) \cup (W_1.\mathrm{cut}(W_1.\mathrm{findLastVertex}(W_2), \mathrm{len}\, W_1)).\mathrm{edges}()$. The theorem is a consequence of (34).

(38) Let us consider a graph G, walks W_1, W_3 of G, and an object e. Suppose e joins $W_3.\mathrm{first}()$ and $W_3.\mathrm{last}()$ in G and $G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}())$ is an odd substring of W_1 not starting before 0.

Then $e \in (W_1.\mathrm{replaceEdgeWith}(e, W_3)).\mathrm{edges}()$ if and only if $e \in (W_1.\mathrm{cut}(1, W_1.\mathrm{findFirstVertex}(G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}())))).\mathrm{edges}()$ or $e \in W_3.\mathrm{edges}()$ or $e \in (W_1.\mathrm{cut}(W_1.\mathrm{findLastVertex}(G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}())), \mathrm{len}\, W_1)).\mathrm{edges}()$. The theorem is a consequence of (37).

(39) Let us consider a graph G, walks W_1, W_3 of G, and an object e. Suppose e joins $W_3.\mathrm{first}()$ and $W_3.\mathrm{last}()$ in G and $e \notin W_3.\mathrm{edges}()$ and $G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}())$ is an odd substring of W_1 not starting before 0 and for every even natural numbers n, m such that n, $m \in \mathrm{dom}\, W_1$ and $W_1(n) = e$ and $W_1(m) = e$ holds $n = m$.

Then $e \notin (W_1.\mathrm{replaceEdgeWith}(e, W_3)).\mathrm{edges}()$.

Proof: Set $W_2 = G.\mathrm{walkOf}(W_3.\mathrm{first}(), e, W_3.\mathrm{last}())$. W_2 is an odd substring of W_1 not starting before 1. Define $\mathcal{P}[\text{natural number}] \equiv \$_1$ is odd and $1 \leqslant \$_1 \leqslant \mathrm{len}\, W_1$ and $\mathrm{mid}(W_1, \$_1, \$_1 -' 1 + \mathrm{len}\, W_2) = W_2$. Consider i being a natural number such that $\mathcal{P}[i]$ and for every natural number n such that $\mathcal{P}[n]$ holds $i \leqslant n$. Set $j = i -' 1 + \mathrm{len}\, W_2$. W_2 is a substring of W_1. $1 \leqslant j \leqslant \mathrm{len}\, W_1$ and $i \leqslant j$. Set $n_1 = i + 1$. Reconsider $k = i - 1$ as an even natural number. For every natural number n such that $1 \leqslant n \leqslant \mathrm{len}\, W_2$ holds $W_1(k + n) = W_2(n)$. For every even natural number l such that for every natural number n such that $1 \leqslant n \leqslant \mathrm{len}\, W_2$ holds $W_1(l + n) = W_2(n)$ holds $k \leqslant l$. $i \leqslant \mathrm{len}\, W_1$ and there exists an even natural number k such that $i = k + 1$ and for every natural number n

such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(k+n) = W_2(n)$ and for every even natural number l such that for every natural number n such that $1 \leqslant n \leqslant \operatorname{len} W_2$ holds $W_1(l+n) = W_2(n)$ holds $k \leqslant l$. W_1.findFirstVertex(W_2) $<$ n_1. $n_1 \in \operatorname{dom} W_1$. $e \notin$ (W_1.cut(1, W_1.findFirstVertex(W_2))).edges(). $e \notin$ (W_1.cut(W_1.findLastVertex(W_2), len W_1)).edges() by [1, (4)], [6, (99)]. □

(40) Let us consider a graph G, a trail T_1 of G, a walk W_3 of G, and an object e. Suppose e joins W_3.first() and W_3.last() in G and $e \notin W_3$.edges() and G.walkOf(W_3.first(), e, W_3.last()) is an odd substring of T_1 not starting before 0. Then $e \notin$ (T_1.replaceEdgeWith(e, W_3)).edges().

Proof: For every even natural numbers n, m such that n, $m \in \operatorname{dom} T_1$ and $T_1(n) = e$ and $T_1(m) = e$ holds $n = m$. □

(41) Let us consider a graph G, and walks W_1, W_2 of G. Suppose W_1.first() = W_2.first() and W_1.last() = W_2.last(). Then W_1.replaceWith(W_1, W_2) = W_2. The theorem is a consequence of (11), (32), and (31).

(42) Let us consider a graph G, walks W_1, W_3 of G, and an object e. Suppose e joins W_3.first() and W_3.last() in G and G.walkOf(W_3.first(), e, W_3.last()) is an odd substring of W_1 not starting before 0. Then there exists a walk W_2 of G such that W_1.replaceEdgeWith(e, W_3) = W_1.replaceWith(W_2, W_3).

(43) Let us consider a graph G, walks W_1, W_2 of G, and an object e. Suppose W_2 is an odd substring of W_1 not starting before 0 and e joins W_2.first() and W_2.last() in G. Then there exists a walk W_3 of G such that W_1.replaceWithEdge(W_2, e) = W_1.replaceWith(W_2, W_3).

(44) Let us consider a graph G, walks W_1, W_3 of G, and an object e. Then

(i) W_1.first() = (W_1.replaceEdgeWith(e, W_3)).first(), and

(ii) W_1.last() = (W_1.replaceEdgeWith(e, W_3)).last().

The theorem is a consequence of (42) and (35).

(45) Let us consider a graph G, walks W_1, W_2 of G, and an object e. Then

(i) W_1.first() = (W_1.replaceWithEdge(W_2, e)).first(), and

(ii) W_1.last() = (W_1.replaceWithEdge(W_2, e)).last().

The theorem is a consequence of (43) and (35).

(46) Let us consider a graph G, walks W_1, W_2, W_3 of G, and objects u, v. Then W_1 is walk from u to v if and only if W_1.replaceWith(W_2, W_3) is walk from u to v. The theorem is a consequence of (35).

(47) Let us consider a graph G, walks W_1, W_3 of G, and objects e, u, v. Then W_1 is walk from u to v if and only if W_1.replaceEdgeWith(e, W_3) is walk from u to v. The theorem is a consequence of (42) and (46).

(48) Let us consider a graph G, walks W_1, W_2 of G, and objects e, u, v. Then W_1 is walk from u to v if and only if W_1.replaceWithEdge(W_2, e) is walk from u to v. The theorem is a consequence of (43) and (46).

(49) Let us consider a graph G, and vertices v_1, v_2 of G. Suppose v_1 is isolated and $v_1 \neq v_2$. Then $v_2 \notin G$.reachableFrom(v_1).

(50) Let us consider a graph G, and vertices v_1, v_2 of G.
If $v_1 \in G$.reachableFrom(v_2), then $v_2 \in G$.reachableFrom(v_1).

(51) Let us consider a graph G, and a vertex v of G. If v is isolated, then $\{v\} = G$.reachableFrom(v).

Proof: For every object x, $x \in \{v\}$ iff $x \in G$.reachableFrom(v) by [7, (9)], (49). □

(52) Let us consider a graph G, a vertex v of G, and a subgraph C of G induced by $\{v\}$. If v is isolated, then C is a component of G. The theorem is a consequence of (51).

(53) Let us consider a non trivial graph G_1, a vertex v of G_1, and a subgraph G_2 of G_1 with vertex v removed. Suppose v is isolated. Then

(i) G_1.componentSet() $= G_2$.componentSet() $\cup \{\{v\}\}$, and

(ii) G_1.numComponents() $= G_2$.numComponents() $+ 1$.

Proof: For every object V, $V \in G_1$.componentSet() iff $V \in G_2$ .componentSet() $\cup \{\{v\}\}$. $\{v\} \notin G_2$.componentSet() by [8, (47)]. □

Let G be a graph. Let us observe that every vertex of G which is isolated is also non cut-vertex.

Now we state the propositions:

(54) Let us consider a graph G_1, a subgraph G_2 of G_1, a walk W_1 of G_1, and a walk W_2 of G_2. If $W_1 = W_2$, then W_1 is cycle-like iff W_2 is cycle-like.

(55) Let us consider a connected graph G_1, and a component G_2 of G_1. Then $G_1 \approx G_2$.

Observe that every graph which is complete is also connected and there exists a graph which is non non-directed-multi, non non-multi, non loopless, non directed-simple, non simple, non acyclic, and non finite.

From now on G denotes a graph.

Let us consider G. The functor G.endVertices() yielding a subset of the vertices of G is defined by

(Def. 8) for every object v, $v \in it$ iff there exists a vertex w of G such that $v = w$ and w is endvertex.

Now we state the proposition:

(56) Let us consider a vertex v of G. Then $v \in G$.endVertices() if and only if v is endvertex.

3. Supergraphs

Let us consider G.

A supergraph of G is a graph defined by

(Def. 9) the vertices of $G \subseteq$ the vertices of *it* and the edges of $G \subseteq$ the edges of *it* and for every set e such that $e \in$ the edges of G holds (the source of $G)(e) =$ (the source of $it)(e)$ and (the target of $G)(e) =$ (the target of $it)(e)$.

Let us consider graphs G_1, G_2. Now we state the propositions:

(57) G_2 is a subgraph of G_1 if and only if G_1 is a supergraph of G_2.

(58) G_2 is subgraph of G_1 and supergraph of G_1 if and only if $G_1 \approx G_2$. The theorem is a consequence of (57).

(59) G_1 is a supergraph of G_2 and G_2 is a supergraph of G_1 if and only if $G_1 \approx G_2$. The theorem is a consequence of (57).

(60) G_1 is a supergraph of G_2 if and only if $G_2 \subseteq G_1$. The theorem is a consequence of (57).

(61) G is a supergraph of G.

(62) Let us consider a graph G_3, and a supergraph G_2 of G_3. Then every supergraph of G_2 is a supergraph of G_3. The theorem is a consequence of (57).

In the sequel G_2 denotes a graph and G_1 denotes a supergraph of G_2.

(63) Let us consider graphs G_1, G_2. Suppose the vertices of $G_2 \subseteq$ the vertices of G_1 and the source of $G_2 \subseteq$ the source of G_1 and the target of $G_2 \subseteq$ the target of G_1. Then G_1 is a supergraph of G_2.

Let us consider G_2 and G_1. Now we state the propositions:

(64) (i) the source of $G_2 \subseteq$ the source of G_1, and

(ii) the target of $G_2 \subseteq$ the target of G_1.

(65) Suppose the vertices of $G_2 =$ the vertices of G_1 and the edges of $G_2 =$ the edges of G_1. Then $G_1 \approx G_2$. The theorem is a consequence of (64).

(66) Let us consider graphs G_1, G_2. Suppose the vertices of $G_2 =$ the vertices of G_1 and the edges of $G_2 =$ the edges of G_1 and the source of $G_2 \subseteq$ the source of G_1 and the target of $G_2 \subseteq$ the target of G_1. Then $G_1 \approx G_2$. The theorem is a consequence of (63) and (65).

(67) Let us consider a set x. Then

(i) if $x \in$ the vertices of G_2, then $x \in$ the vertices of G_1, and

(ii) if $x \in$ the edges of G_2, then $x \in$ the edges of G_1.

The theorem is a consequence of (57).

Let us consider G_2 and G_1. Now we state the propositions:

(68) Every vertex of G_2 is a vertex of G_1.

(69) (i) the source of G_2 = (the source of G_1)$\restriction$(the edges of G_2), and

(ii) the target of G_2 = (the target of G_1)$\restriction$(the edges of G_2).

The theorem is a consequence of (57).

(70) Let us consider sets x, y, and an object e. Then

(i) if e joins x and y in G_2, then e joins x and y in G_1, and

(ii) if e joins x to y in G_2, then e joins x to y in G_1, and

(iii) if e joins a vertex from x and a vertex from y in G_2, then e joins a vertex from x and a vertex from y in G_1, and

(iv) if e joins a vertex from x to a vertex from y in G_2, then e joins a vertex from x to a vertex from y in G_1.

The theorem is a consequence of (57).

Let us consider G_2, G_1, and objects e, v_1, v_2. Now we state the propositions:

(71) If e joins v_1 to v_2 in G_1, then e joins v_1 to v_2 in G_2 or $e \notin$ the edges of G_2.

(72) If e joins v_1 and v_2 in G_1, then e joins v_1 and v_2 in G_2 or $e \notin$ the edges of G_2. The theorem is a consequence of (71).

Let G be a finite graph. Observe that there exists a supergraph of G which is finite.

Now we state the propositions:

(73) (i) G_2.order() $\subseteq G_1$.order(), and

(ii) G_2.size() $\subseteq G_1$.size().

(74) Let us consider a finite graph G_2, and a finite supergraph G_1 of G_2. Then

(i) G_2.order() $\leqslant G_1$.order(), and

(ii) G_2.size() $\leqslant G_1$.size().

The theorem is a consequence of (57).

(75) Every walk of G_2 is a walk of G_1. The theorem is a consequence of (57).

(76) Let us consider a walk W_2 of G_2, and a walk W_1 of G_1. Suppose $W_1 = W_2$. Then

(i) W_1 is closed iff W_2 is closed, and

(ii) W_1 is directed iff W_2 is directed, and

(iii) W_1 is trivial iff W_2 is trivial, and

(iv) W_1 is trail-like iff W_2 is trail-like, and

(v) W_1 is path-like iff W_2 is path-like, and

(vi) W_1 is vertex-distinct iff W_2 is vertex-distinct, and

(vii) W_1 is cycle-like iff W_2 is cycle-like.

The theorem is a consequence of (57) and (54).

Let G be a non trivial graph. Note that every supergraph of G is non trivial.

Let G be a non non-directed-multi graph. Observe that every supergraph of G is non non-directed-multi.

Let G be a non non-multi graph. One can verify that every supergraph of G is non non-multi.

Let G be a non loopless graph. Let us note that every supergraph of G is non loopless.

Let G be a non directed-simple graph. Observe that every supergraph of G is non directed-simple.

Let G be a non simple graph. One can check that every supergraph of G is non simple.

Let G be a non acyclic graph. One can verify that every supergraph of G is non acyclic.

Every supergraph of a non finite graph G is non finite.

In the sequel V denotes a set. Let us consider G and V.

A supergraph of G extended by the vertices from V is a supergraph of G defined by

(Def. 10) the vertices of it = (the vertices of G)$\cup V$ and the edges of it = the edges of G and the source of it = the source of G and the target of it = the target of G.

Now we state the propositions:

(77) Let us consider supergraphs G_1, G_2 of G extended by the vertices from V. Then $G_1 \approx G_2$.

(78) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then $G_1 \approx G_2$ if and only if $V \subseteq$ the vertices of G_2.

(79) Let us consider graphs G_1, G_2, and a set V. Suppose $G_1 \approx G_2$ and $V \subseteq$ the vertices of G_2. Then G_1 is a supergraph of G_2 extended by the vertices from V. The theorem is a consequence of (59).

(80) Let us consider a supergraph G_1 of G extended by the vertices from V. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by the vertices from V. The theorem is a consequence of (58) and (62).

(81) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_1.edgesBetween(the vertices of G_2) = the edges of G_1.

Proof: Set E_1 = the edges of G_1. Set V_2 = the vertices of G_2. For every object e, $e \in E_1$ iff $e \in G_1$.edgesInto(V_2) $\cap$ G_1.edgesOutOf(V_2). □

(82) Let us consider a graph G_3, sets V_1, V_2, and a supergraph G_2 of G_3 extended by the vertices from V_2. Then every supergraph of G_2 extended by the vertices from V_1 is a supergraph of G_3 extended by the vertices from $V_1 \cup V_2$. The theorem is a consequence of (62).

(83) Let us consider a graph G_3, sets V_1, V_2, and a supergraph G_1 of G_3 extended by the vertices from $V_1 \cup V_2$. Then there exists a supergraph G_2 of G_3 extended by the vertices from V_2 such that G_1 is a supergraph of G_2 extended by the vertices from V_1.

(84) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_2 is a subgraph of G_1 induced by the vertices of G_2. The theorem is a consequence of (57) and (81).

(85) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, and objects x, y, e. Then e joins x to y in G_1 if and only if e joins x to y in G_2.

(86) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, and an object v. If $v \in V$, then v is a vertex of G_1.

(87) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, and objects x, y, e. Then e joins x and y in G_1 if and only if e joins x and y in G_2. The theorem is a consequence of (85).

(88) Let us consider a supergraph G_1 of G_2 extended by the vertices from V, and a vertex v of G_1. Suppose $v \in V \setminus$ (the vertices of G_2). Then v is isolated and non cut-vertex.

Proof: v.edgesInOut() $= \emptyset$. □

(89) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Suppose $V \setminus$ (the vertices of G_2) $\neq \emptyset$. Then G_1 is non trivial, non connected, non tree-like, and non complete.

Proof: Consider v_1 being an object such that $v_1 \in V \setminus$ (the vertices of G_2). $\overline{\overline{\alpha}} \neq 1$, where α is the vertices of G_1. v_1 is isolated. □

Let G be a non-directed-multi graph and V be a set. Note that every supergraph of G extended by the vertices from V is non-directed-multi.

Let G be a non-multi graph. One can verify that every supergraph of G extended by the vertices from V is non-multi.

Let G be a loopless graph. Observe that every supergraph of G extended by the vertices from V is loopless.

Let G be a directed-simple graph. Let us note that every supergraph of G extended by the vertices from V is directed-simple.

Let G be a simple graph. Let us note that every supergraph of G extended by the vertices from V is simple.

Let us consider G_2, V, a supergraph G_1 of G_2 extended by the vertices from V, and a walk W of G_1. Now we state the propositions:

(90) (i) W.vertices() misses $V \setminus$ (the vertices of G_2), or

(ii) W is trivial.

The theorem is a consequence of (85).

(91) If W.vertices() misses $V \setminus$ (the vertices of G_2), then W is a walk of G_2. The theorem is a consequence of (57).

Let G be an acyclic graph and V be a set. Let us note that every supergraph of G extended by the vertices from V is acyclic.

(92) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then G_2 is chordal if and only if G_1 is chordal.

PROOF: If G_2 is chordal, then G_1 is chordal. G_2 is a subgraph of G_1 induced by the vertices of G_2. □

Let G be a chordal graph and V be a set. Let us observe that every supergraph of G extended by the vertices from V is chordal.

From now on v denotes an object.

Let us consider G and v.

A supergraph of G extended by v is a supergraph of G extended by the vertices from $\{v\}$.

Let us consider G_2, v, and a supergraph G_1 of G_2 extended by v. Now we state the propositions:

(93) $G_1 \approx G_2$ if and only if $v \in$ the vertices of G_2.

(94) v is a vertex of G_1. The theorem is a consequence of (86).

Let us consider G. One can verify that every supergraph of G extended by the vertices of G is non trivial, non connected, and non complete and there exists a graph which is non trivial, non connected, and non complete.

Let G be a non connected graph and V be a set. Note that every supergraph of G extended by the vertices from V is non connected.

Now we state the propositions:

(95) Let us consider a supergraph G_1 of G_2 extended by the vertices from V. Then

(i) G_1.size() $= G_2$.size(), and

(ii) G_1.order() $= G_2$.order() $+ \overline{\overline{V \setminus \alpha}}$,

where α is the vertices of G_2.

(96) Let us consider a finite graph G_2, a finite set V, and a supergraph G_1 of G_2 extended by the vertices from V. Then G_1.order() $= G_2$.order() $+$ $\overline{\overline{V \setminus \alpha}}$, where α is the vertices of G_2.

(97) Let us consider a graph G_2, an object v, and a supergraph G_1 of G_2 extended by v. Suppose $v \notin$ the vertices of G_2. Then G_1.order() $= G_2$.order() $+ 1$. The theorem is a consequence of (95).

(98) Let us consider a finite graph G_2, an object v, and a supergraph G_1 of G_2 extended by v. Suppose $v \notin$ the vertices of G_2. Then G_1.order() $=$ G_2.order() $+ 1$. The theorem is a consequence of (96).

Let G be a finite graph and V be a finite set. Note that every supergraph of G extended by the vertices from V is finite.

Let v be an object. Note that every supergraph of G extended by v is finite.

Let G be a graph and V be a non finite set. Note that every supergraph of G extended by the vertices from V is non finite.

Let us consider G. Let v_1, e, v_2 be objects.

A supergraph of G extended by e between vertices v_1 and v_2 is a supergraph of G defined by

(Def. 11) (i) the vertices of *it* $=$ the vertices of G and the edges of *it* $=$ (the edges of G) $\cup \{e\}$ and the source of *it* $=$ (the source of G)$+\cdot(e \overset{.}{\longmapsto} v_1)$ and the target of *it* $=$ (the target of G)$+\cdot(e \overset{.}{\longmapsto} v_2)$, **if** v_1, $v_2 \in$ the vertices of G and $e \notin$ the edges of G,

(ii) *it* $\approx G$, **otherwise**.

Now we state the propositions:

(99) Let us consider objects v_1, e, v_2, and supergraphs G_1, G_2 of G extended by e between vertices v_1 and v_2. Then $G_1 \approx G_2$.

(100) Let us consider vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Then $G_1 \approx G_2$ if and only if $e \in$ the edges of G_2.

(101) Let us consider objects v_1, e, v_2, and a supergraph G_1 of G extended by e between vertices v_1 and v_2. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by e between vertices v_1 and v_2. The theorem is a consequence of (58) and (62).

Let us consider G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Now we state the propositions:

(102) The vertices of $G_1 =$ the vertices of G_2.

(103) G_1.edgesBetween(the vertices of G_2) $=$ the edges of G_1. The theorem is a consequence of (102).

(104) Every vertex of G_1 is a vertex of G_2.

(105) If $e \notin$ the edges of G_2, then e joins v_1 to v_2 in G_1.

Let us consider G_2, vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, and objects e_1, w_1, w_2. Now we state the propositions:

(106) Suppose $e \notin$ the edges of G_2. Then if e_1 joins w_1 and w_2 in G_1 and $e_1 \notin$ the edges of G_2, then $e_1 = e$.

(107) Suppose $e \notin$ the edges of G_2. Then suppose e_1 joins w_1 and w_2 in G_1 and $e_1 \notin$ the edges of G_2. Then

(i) $w_1 = v_1$ and $w_2 = v_2$, or

(ii) $w_1 = v_2$ and $w_2 = v_1$.

The theorem is a consequence of (106) and (105).

(108) Let us consider vertices v_1, v_2 of G_2, a set e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_2. Then G_2 is a subgraph of G_1 with edge e removed. The theorem is a consequence of (57).

(109) Let us consider vertices v_1, v_2 of G_2, an object e, a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2, and a walk W of G_1. Suppose if $e \in W$.edges(), then $e \in$ the edges of G_2. Then W is a walk of G_2. The theorem is a consequence of (57).

Let G be a trivial graph and v_1, e, v_2 be objects. Let us note that every supergraph of G extended by e between vertices v_1 and v_2 is trivial.

Let G be a connected graph. Let us note that every supergraph of G extended by e between vertices v_1 and v_2 is connected.

Let G be a complete graph. Note that every supergraph of G extended by e between vertices v_1 and v_2 is complete.

Now we state the propositions:

(110) Let us consider vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_2. Then

(i) G_1.order() $= G_2$.order(), and

(ii) G_1.size() $= G_2$.size() $+ 1$.

(111) Let us consider a finite graph G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_2. Then G_1.size() $= G_2$.size() $+ 1$.

Let G be a finite graph and v_1, e, v_2 be objects. Observe that every supergraph of G extended by e between vertices v_1 and v_2 is finite.

(112) Let us consider vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. If G_2 is loopless and $v_1 \neq v_2$, then G_1 is loopless. The theorem is a consequence of (105).

(113) Let us consider a vertex v of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v and v. Suppose G_2 is not loopless or $e \notin$ the edges of G_2. Then G_1 is not loopless. The theorem is a consequence of (105).

Let us consider G. Let v be a vertex of G. Let us note that every supergraph of G extended by the edges of G between vertices v and v is non loopless.

Let us consider G_2, vertices v_1, v_2 of G_2, an object e, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Now we state the propositions:

(114) If G_2 is non-directed-multi and there exists no object e_3 such that e_3 joins v_1 to v_2 in G_2, then G_1 is non-directed-multi. The theorem is a consequence of (71) and (105).

(115) Suppose $e \notin$ the edges of G_2 and there exists an object e_2 such that e_2 joins v_1 to v_2 in G_2. Then G_1 is not non-directed-multi. The theorem is a consequence of (105) and (70).

(116) If G_2 is non-multi and v_1 and v_2 are not adjacent, then G_1 is non-multi. The theorem is a consequence of (72) and (105).

(117) If $e \notin$ the edges of G_2 and v_1 and v_2 are adjacent, then G_1 is not non-multi.

Proof: There exist objects e_1, e_2, u_1, u_2 such that e_1 joins u_1 and u_2 in G_1 and e_2 joins u_1 and u_2 in G_1 and $e_1 \neq e_2$. □

(118) If G_2 is acyclic and $v_2 \notin G_2$.reachableFrom(v_1), then G_1 is acyclic. The theorem is a consequence of (57), (54), and (105).

(119) If $e \notin$ the edges of G_2 and $v_2 \in G_2$.reachableFrom(v_1), then G_1 is not acyclic. The theorem is a consequence of (75), (105), and (113).

(120) If G_2 is not connected and $v_2 \in G_2$.reachableFrom(v_1), then G_1 is not connected. The theorem is a consequence of (68), (109), (27), (105), (75), (47), and (40).

(121) Suppose $e \notin$ the edges of G_2 and for every vertices v_3, v_4 of G_2 such that v_3 and v_4 are not adjacent holds $v_3 = v_4$ or $v_1 = v_3$ and $v_2 = v_4$ or $v_1 = v_4$ and $v_2 = v_3$. Then G_1 is complete.

Proof: For every vertices u_1, u_2 of G_1 such that $u_1 \neq u_2$ holds u_1 and u_2 are adjacent. □

(122) If G_2 is not complete and v_1 and v_2 are adjacent, then G_1 is not complete. The theorem is a consequence of (68), (72), and (105).

Let us consider G. Let v_1, e, v_2 be objects.

A supergraph of G extended by v_1, v_2 and e between them is a supergraph of G defined by

(Def. 12) (i) the vertices of *it* = (the vertices of G) $\cup$ $\{v_2\}$ and the edges of *it* = (the edges of G) $\cup$ $\{e\}$ and the source of *it* = (the source of G)$+\cdot(e\overset{.}{\longmapsto}v_1)$ and the target of *it* = (the target of G)$+\cdot(e\overset{.}{\longmapsto}v_2)$, **if** $v_1 \in$ the vertices of G and $v_2 \notin$ the vertices of G and $e \notin$ the edges of G,

(ii) the vertices of *it* = (the vertices of G) $\cup$ $\{v_1\}$ and the edges of *it* = (the edges of G) $\cup$ $\{e\}$ and the source of *it* = (the source of G)$+\cdot(e\overset{.}{\longmapsto}v_1)$ and the target of *it* = (the target of G)$+\cdot(e\overset{.}{\longmapsto}v_2)$, **if** $v_1 \notin$ the vertices of G and $v_2 \in$ the vertices of G and $e \notin$ the edges of G,

(iii) *it* $\approx G$, **otherwise**.

Let v_1 be a vertex of G and e, v_2 be objects.

One can check that a supergraph of G extended by v_1, v_2 and e between them can equivalently be formulated as follows:

(Def. 13) (i) the vertices of *it* = (the vertices of G) $\cup$ $\{v_2\}$ and the edges of *it* = (the edges of G) $\cup$ $\{e\}$ and the source of *it* = (the source of G)$+\cdot(e\overset{.}{\longmapsto}v_1)$ and the target of *it* = (the target of G)$+\cdot(e\overset{.}{\longmapsto}v_2)$, **if** $v_2 \notin$ the vertices of G and $e \notin$ the edges of G,

(ii) *it* $\approx G$, **otherwise**.

Let v_1, e be objects and v_2 be a vertex of G.

Let us note that a supergraph of G extended by v_1, v_2 and e between them can equivalently be formulated as follows:

(Def. 14) (i) the vertices of *it* = (the vertices of G) $\cup$ $\{v_1\}$ and the edges of *it* = (the edges of G) $\cup$ $\{e\}$ and the source of *it* = (the source of G)$+\cdot(e\overset{.}{\longmapsto}v_1)$ and the target of *it* = (the target of G)$+\cdot(e\overset{.}{\longmapsto}v_2)$, **if** $v_1 \notin$ the vertices of G and $e \notin$ the edges of G,

(ii) *it* $\approx G$, **otherwise**.

Now we state the propositions:

(123) Let us consider objects v_1, e, v_2, and supergraphs G_1, G_2 of G extended by v_1, v_2 and e between them. Then $G_1 \approx G_2$.

(124) Let us consider objects v_1, e, v_2, and a supergraph G_1 of G extended by v_1, v_2 and e between them. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by v_1, v_2 and e between them. The theorem is a consequence of (58) and (62).

(125) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2. Then there exists a supergraph G_3 of G_2 extended by v_2 such that G_1 is a supergraph of G_3 extended by e between vertices v_1 and v_2. The theorem is a consequence of (94).

(126) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2. Then there exists a supergraph G_3 of G_2 extended by v_1 such that G_1 is a supergraph of G_3 extended by e between vertices v_1 and v_2. The theorem is a consequence of (94).

(127) Let us consider a graph G_3, a vertex v_1 of G_3, objects e, v_2, a supergraph G_2 of G_3 extended by v_2, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_3 and $v_2 \notin$ the vertices of G_3. Then G_1 is a supergraph of G_3 extended by v_1, v_2 and e between them. The theorem is a consequence of (62), (68), and (94).

(128) Let us consider a graph G_3, objects v_1, e, a vertex v_2 of G_3, a supergraph G_2 of G_3 extended by v_1, and a supergraph G_1 of G_2 extended by e between vertices v_1 and v_2. Suppose $e \notin$ the edges of G_3 and $v_1 \notin$ the vertices of G_3. Then G_1 is a supergraph of G_3 extended by v_1, v_2 and e between them. The theorem is a consequence of (62), (68), and (94).

(129) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_2 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then v_2 is a vertex of G_1.

(130) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_1 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then v_1 is a vertex of G_1.

(131) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_2 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then

(i) e joins v_1 to v_2 in G_1, and

(ii) e joins v_1 and v_2 in G_1.

(132) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_1 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then

(i) e joins v_1 to v_2 in G_1, and

(ii) e joins v_1 and v_2 in G_1.

(133) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_2 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Let us consider objects e_1, w. If $w \neq v_1$ or $e_1 \neq e$, then e_1 does not join w and v_2 in G_1. The theorem is a consequence of (72) and (131).

(134) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_1 \notin$ the vertices of

G_2 and $e \notin$ the edges of G_2. Let us consider objects e_1, w. If $w \neq v_2$ or $e_1 \neq e$, then e_1 does not join v_1 and w in G_1. The theorem is a consequence of (72) and (132).

Let us consider G_2, objects v_1, e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Now we state the propositions:

(135) G_1.edgesBetween(the vertices of G_2) = the edges of G_2. The theorem is a consequence of (131), (70), and (132).

(136) G_2 is a subgraph of G_1 induced by the vertices of G_2. The theorem is a consequence of (57), (135), (15), and (16).

(137) Let us consider a vertex v_1 of G_2, an object e, a set v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2. Then G_2 is a subgraph of G_1 with vertex v_2 removed. The theorem is a consequence of (136).

(138) Let us consider a set v_1, an object e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2. Then G_2 is a subgraph of G_1 with vertex v_1 removed. The theorem is a consequence of (136).

(139) Let us consider a non trivial graph G, a vertex v_1 of G, objects e, v_2, a supergraph G_1 of G extended by v_1, v_2 and e between them, a subgraph G_2 of G_1 with vertex v_1 removed, and a subgraph G_3 of G with vertex v_1 removed. Suppose $e \notin$ the edges of G and $v_2 \notin$ the vertices of G. Then G_2 is a supergraph of G_3 extended by v_2.

PROOF: v_1 is a vertex of G_1 and $v_1 \neq v_2$. For every object e_1, $e_1 \in G_1$.edgesBetween((the vertices of $G_1) \setminus \{v_1\}$) iff $e_1 \in G$.edgesBetween((the vertices of $G) \setminus \{v_1\}$). For every object e_1 such that $e_1 \in$ dom(the source of G_2) holds (the source of $G_2)(e_1)$ = (the source of $G_3)(e_1)$. For every object e_1 such that $e_1 \in$ dom(the target of G_2) holds (the target of $G_2)(e_1)$ = (the target of $G_3)(e_1)$. □

(140) Let us consider a non trivial graph G, objects v_1, e, a vertex v_2 of G, a supergraph G_1 of G extended by v_1, v_2 and e between them, a subgraph G_2 of G_1 with vertex v_2 removed, and a subgraph G_3 of G with vertex v_2 removed. Suppose $e \notin$ the edges of G and $v_1 \notin$ the vertices of G. Then G_2 is a supergraph of G_3 extended by v_1.

PROOF: v_2 is a vertex of G_1 and $v_1 \neq v_2$. For every object e_1, $e_1 \in G_1$.edgesBetween((the vertices of $G_1) \setminus \{v_2\}$) iff $e_1 \in G$.edgesBetween((the vertices of $G) \setminus \{v_2\}$). For every object e_1 such that $e_1 \in$ dom(the source of G_2) holds (the source of $G_2)(e_1)$ = (the source of $G_3)(e_1)$. For every object e_1 such that $e_1 \in$ dom(the target of G_2) holds (the target of $G_2)(e_1)$ = (the target of $G_3)(e_1)$. □

(141) Let us consider a vertex v_1 of G_2, objects e, v_2, a supergraph G_1 of G_2 extended by v_1, v_2 and e between them, and a vertex w of G_1. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2 and $w = v_2$. Then w is endvertex.

Proof: There exists an object e_1 such that w.edgesInOut() $= \{e_1\}$ and e_1 does not join w and w in G_1. □

(142) Let us consider objects v_1, e, a vertex v_2 of G_2, a supergraph G_1 of G_2 extended by v_1, v_2 and e between them, and a vertex w of G_1. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2 and $w = v_1$. Then w is endvertex.

Proof: There exists an object e_1 such that w.edgesInOut() $= \{e_1\}$ and e_1 does not join w and w in G_1. □

(143) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_2 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then G_1 is not trivial. The theorem is a consequence of (125) and (89).

(144) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $v_1 \notin$ the vertices of G_2 and $e \notin$ the edges of G_2. Then G_1 is not trivial. The theorem is a consequence of (126) and (89).

Let G be a graph and v be a vertex of G. Let us note that every supergraph of G extended by v, the vertices of G and the edges of G between them is non trivial and every supergraph of G extended by the vertices of G, v and the edges of G between them is non trivial.

Let G be a trivial graph. Note that every supergraph of G extended by v, the vertices of G and the edges of G between them is complete and every supergraph of G extended by the vertices of G, v and the edges of G between them is complete.

Let G be a loopless graph and v_1, e, v_2 be objects. One can verify that every supergraph of G extended by v_1, v_2 and e between them is loopless.

Let G be a non-directed-multi graph. One can check that every supergraph of G extended by v_1, v_2 and e between them is non-directed-multi.

Let G be a non-multi graph. One can check that every supergraph of G extended by v_1, v_2 and e between them is non-multi.

Let G be a directed-simple graph. One can check that every supergraph of G extended by v_1, v_2 and e between them is directed-simple.

Let G be a simple graph. One can check that every supergraph of G extended by v_1, v_2 and e between them is simple.

Now we state the propositions:

(145) Let us consider a vertex v_1 of G_2, objects e, v_2, a supergraph G_1 of G_2 extended by v_1, v_2 and e between them, and a walk W of G_1. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2 and ($e \notin W$.edges() and W is not trivial or $v_2 \notin W$.vertices()). Then W is a walk of G_2. The theorem is a consequence of (125), (68), (94), (108), (90), (91), (137), (129), and (143).

(146) Let us consider objects v_1, e, a vertex v_2 of G_2, a supergraph G_1 of G_2 extended by v_1, v_2 and e between them, and a walk W of G_1. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2 and ($e \notin W$.edges() and W is not trivial or $v_1 \notin W$.vertices()). Then W is a walk of G_2. The theorem is a consequence of (126), (68), (94), (108), (90), (91), (138), (130), and (144).

(147) Let us consider objects v_1, e, v_2, a supergraph G_1 of G_2 extended by v_1, v_2 and e between them, and a trail T of G_1. Suppose $e \notin$ the edges of G_2 and T.first(), T.last() $\in$ the vertices of G_2. Then $e \notin T$.edges(). The theorem is a consequence of (129), (141), (145), (130), (142), and (146).

Let G be a connected graph and v_1, e, v_2 be objects. Let us observe that every supergraph of G extended by v_1, v_2 and e between them is connected.

Let G be a non connected graph. One can check that every supergraph of G extended by v_1, v_2 and e between them is non connected.

Let G be an acyclic graph. Note that every supergraph of G extended by v_1, v_2 and e between them is acyclic.

Let G be a tree-like graph. One can verify that every supergraph of G extended by v_1, v_2 and e between them is tree-like.

Now we state the propositions:

(148) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2 and G_2 is not trivial. Then G_1 is not complete.
PROOF: There exist vertices u, v of G_1 such that $u \neq v$ and u and v are not adjacent. □

(149) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2 and G_2 is not trivial. Then G_1 is not complete.
PROOF: There exist vertices u, v of G_1 such that $u \neq v$ and u and v are not adjacent. □

Let G be a non complete graph and v_1, e, v_2 be objects. Observe that every supergraph of G extended by v_1, v_2 and e between them is non complete.

Let v be a vertex of G. Observe that every supergraph of G extended by v, the vertices of G and the edges of G between them is non complete and every supergraph of G extended by the vertices of G, v and the edges of G between them is non complete.

Now we state the propositions:

(150) Let us consider a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2. Then

(i) G_1.order() $= G_2$.order() $+ 1$, and

(ii) G_1.size() $= G_2$.size() $+ 1$.

(151) Let us consider objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2. Then

(i) G_1.order() $= G_2$.order() $+ 1$, and

(ii) G_1.size() $= G_2$.size() $+ 1$.

(152) Let us consider a finite graph G_2, a vertex v_1 of G_2, objects e, v_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_2 \notin$ the vertices of G_2. Then

(i) G_1.order() $= G_2$.order() $+ 1$, and

(ii) G_1.size() $= G_2$.size() $+ 1$.

(153) Let us consider a finite graph G_2, objects v_1, e, a vertex v_2 of G_2, and a supergraph G_1 of G_2 extended by v_1, v_2 and e between them. Suppose $e \notin$ the edges of G_2 and $v_1 \notin$ the vertices of G_2. Then

(i) G_1.order() $= G_2$.order() $+ 1$, and

(ii) G_1.size() $= G_2$.size() $+ 1$.

Let G be a finite graph and v_1, e, v_2 be objects. One can verify that every supergraph of G extended by v_1, v_2 and e between them is finite.

References

[1] Jesse Alama. Euler's polyhedron formula. *Formalized Mathematics*, 16(**1**):7–17, 2008. doi:10.2478/v10037-008-0002-6.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] Lowell W. Beineke and Robin J. Wilson, editors. *Selected Topics in Graph Theory.* Academic Press, London, 1978. ISBN 0-12-086250-6.

[5] John Adrian Bondy and U. S. R. Murty. *Graph Theory.* Graduate Texts in Mathematics, 244. Springer, New York, 2008. ISBN 978-1-84628-969-9.

[6] Gilbert Lee. Walks in graphs. *Formalized Mathematics*, 13(**2**):253–269, 2005.

[7] Gilbert Lee. Trees and graph components. *Formalized Mathematics*, 13(**2**):271–277, 2005.

[8] Gilbert Lee and Piotr Rudnicki. Alternative graph structures. *Formalized Mathematics*, 13(**2**):235–252, 2005.

[9] Klaus Wagner. *Graphentheorie.* B.I-Hochschultaschenbücher; 248. Bibliograph. Inst., Mannheim, 1970. ISBN 3-411-00248-4.

[10] Robin James Wilson. *Introduction to Graph Theory.* Oliver & Boyd, Edinburgh, 1972. ISBN 0-05-002534-1.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 125–140, 2018
DOI: 10.2478/forma-2018-0010

sciendo
https://www.sciendo.com/

About Supergraphs. Part II

Sebastian Koch
Johannes Gutenberg University
Mainz, Germany[1]

Summary. In the previous article [5] supergraphs and several specializations to formalize the process of drawing graphs were introduced. In this paper another such operation is formalized in Mizar [1], [2]: drawing a vertex and then immediately drawing edges connecting this vertex with a subset of the other vertices of the graph. In case the new vertex is joined with all vertices of a given graph G, this is known as the join of G and the trivial loopless graph K_1. While the join of two graphs is known and found in standard literature (like [9], [4], [8] and [3]), the operation discribed in this article is not.

Alongside the new operation a mode to reverse the directions of a subset of the edges of a graph is introduced. When all edge directions of a graph are reversed, this is commonly known as the converse of a (directed) graph.

MSC: 05C76 03B35 68T99

Keywords: supergraph; graph operations

MML identifier: GLIB_007, version: 8.1.08 5.52.1328

1. Reversing Edge Directions

From now on G, G_2 denote graphs, V, E denote sets, and v denotes an object. Let us consider G and E.

A graph given by reversing directions of the edges E of G is a graph defined by

(Def. 1) (i) the vertices of it = the vertices of G and the edges of it = the edges of G and the source of it = (the source of G)$+\cdot$(the target of G)$\restriction E$ and the target of it = (the target of G)$+\cdot$(the source of G)$\restriction E$, **if** $E \subseteq$ the edges of G,

[1] mailto: skoch02@students.uni-mainz.de

(ii) $it \approx G$, **otherwise**.

A graph given by reversing directions of the edges of G is a graph given by reversing directions of the edges of G of G. Now we state the propositions:

(1) Let us consider graphs G_1, G_2 given by reversing directions of the edges E of G. Then $G_1 \approx G_2$.

(2) Let us consider a graph G_1 given by reversing directions of the edges E of G. Suppose $G_1 \approx G_2$. Then G_2 is a graph given by reversing directions of the edges E of G.

Let us consider G_2, E, and a graph G_1 given by reversing directions of the edges E of G_2. Now we state the propositions:

(3) G_2 is a graph given by reversing directions of the edges E of G_1.

(4) (i) the vertices of G_1 = the vertices of G_2, and

(ii) the edges of G_1 = the edges of G_2.

(5) Let us consider a graph G_1 given by reversing directions of the edges of G_2. Then G_2 is a graph given by reversing directions of the edges of G_1. The theorem is a consequence of (4) and (3).

(6) Let us consider a trivial graph G_2, a set E, and a graph G_1. Then $G_1 \approx G_2$ if and only if G_1 is a graph given by reversing directions of the edges E of G_2.

Let us consider G_2, E, a graph G_1 given by reversing directions of the edges E of G_2, and objects v_1, e, v_2. Now we state the propositions:

(7) If $E \subseteq$ the edges of G_2 and $e \in E$, then e joins v_1 to v_2 in G_2 iff e joins v_2 to v_1 in G_1. The theorem is a consequence of (3) and (4).

(8) If $E \subseteq$ the edges of G_2 and $e \notin E$, then e joins v_1 to v_2 in G_2 iff e joins v_1 to v_2 in G_1. The theorem is a consequence of (3) and (4).

(9) e joins v_1 and v_2 in G_2 if and only if e joins v_1 and v_2 in G_1. The theorem is a consequence of (3).

(10) Let us consider a graph G_1 given by reversing directions of the edges E of G_2. Then v is a vertex of G_1 if and only if v is a vertex of G_2.

Let us consider G_2, E, V, and a graph G_1 given by reversing directions of the edges E of G_2. Now we state the propositions:

(11) G_1.edgesBetween(V) = G_2.edgesBetween(V).

PROOF:

For every object e, $e \in G_1$.edgesBetween(V) iff $e \in G_2$.edgesBetween(V). □

(12) G_1.edgesInOut(V) = G_2.edgesInOut(V).

PROOF: For every object e, $e \in G_1$.edgesInOut(V) iff $e \in G_2$.edgesInOut(V). □

(13) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a vertex v_1 of G_1, and a vertex v_2 of G_2. If $v_1 = v_2$, then v_1.edgesInOut() $=$ v_2.edgesInOut(). The theorem is a consequence of (12).

Let us consider G_2, E, and a graph G_1 given by reversing directions of the edges E of G_2. Now we state the propositions:

(14) Every walk of G_2 is a walk of G_1. The theorem is a consequence of (4) and (9).

(15) Every walk of G_1 is a walk of G_2. The theorem is a consequence of (3) and (14).

(16) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a walk W_2 of G_2, and a walk W_1 of G_1. Suppose $E \subseteq$ the edges of G_2 and $W_1 = W_2$ and W_2.edges() $\subseteq E$. Then W_1 is directed if and only if W_2.reverse() is directed.

PROOF: For every odd element n of $\mathbb{N}$ such that $n < \operatorname{len} W_1$ holds $W_1(n+1)$ joins $W_1(n)$ to $W_1(n+2)$ in G_1 by [6, (1)], [7, (12)]. □

(17) Let us consider a graph G_1 given by reversing directions of the edges of G_2, a walk W_2 of G_2, and a walk W_1 of G_1. Suppose $W_1 = W_2$. Then W_1 is directed if and only if W_2.reverse() is directed. The theorem is a consequence of (16).

(18) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a walk W_2 of G_2, and a walk W_1 of G_1. If $W_1 = W_2$, then W_1 is chordal iff W_2 is chordal. The theorem is a consequence of (3).

(19) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, and objects v_1, v_2. Then there exists a walk W_1 of G_1 such that W_1 is walk from v_1 to v_2 if and only if there exists a walk W_2 of G_2 such that W_2 is walk from v_1 to v_2. The theorem is a consequence of (15) and (14).

(20) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a vertex v_1 of G_1, and a vertex v_2 of G_2. If $v_1 = v_2$, then G_1.reachableFrom(v_1) $=$ G_2.reachableFrom(v_2). The theorem is a consequence of (19).

(21) Let us consider a graph G_1 given by reversing directions of the edges E of G_2. Then

(i) G_1.componentSet() $=$ G_2.componentSet(), and

(ii) G_1.numComponents() $=$ G_2.numComponents().

The theorem is a consequence of (10) and (20).

Let G be a trivial graph and E be a set. Observe that every graph given by reversing directions of the edges E of G is trivial.

Let G be a non trivial graph. Let us observe that every graph given by reversing directions of the edges E of G is non trivial.

Now we state the propositions:

(22) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a set v, and a subgraph G_3 of G_1 with vertex v removed. Then every subgraph of G_2 with vertex v removed is a graph given by reversing directions of the edges $E \setminus G_1.\mathrm{edgesInOut}(\{v\})$ of G_3. The theorem is a consequence of (11), (2), (3), and (6).

(23) Let us consider a graph G_1 given by reversing directions of the edges E of G_2, a vertex v_1 of G_1, and a vertex v_2 of G_2. Suppose $v_1 = v_2$. Then

(i) v_1 is isolated iff v_2 is isolated, and

(ii) v_1 is endvertex iff v_2 is endvertex, and

(iii) v_1 is cut-vertex iff v_2 is cut-vertex.

The theorem is a consequence of (3).

Let us consider G_2, E, and a graph G_1 given by reversing directions of the edges E of G_2. Now we state the propositions:

(24) (i) $G_1.\mathrm{order}() = G_2.\mathrm{order}()$, and

(ii) $G_1.\mathrm{size}() = G_2.\mathrm{size}()$.

The theorem is a consequence of (4).

(25) Suppose $E \subseteq$ the edges of G_2 and G_2 is non-directed-multi and for every objects e_1, e_2, v_1, v_2 such that e_1 joins v_1 and v_2 in G_2 and e_2 joins v_1 and v_2 in G_2 holds e_1, $e_2 \in E$ or $e_1 \notin E$ and $e_2 \notin E$. Then G_1 is non-directed-multi.

PROOF: For every objects e_1, e_2, v_1, v_2 such that e_1 joins v_1 to v_2 in G_1 and e_2 joins v_1 to v_2 in G_1 holds $e_1 = e_2$. □

Let G be a non-directed-multi graph. Let us note that every graph given by reversing directions of the edges of G is non-directed-multi.

Let G be a non non-directed-multi graph. Observe that every graph given by reversing directions of the edges of G is non non-directed-multi.

Let G be a non-multi graph and E be a set. One can verify that every graph given by reversing directions of the edges E of G is non-multi.

Let G be a non non-multi graph. Let us note that every graph given by reversing directions of the edges E of G is non non-multi.

Let G be a loopless graph. One can check that every graph given by reversing directions of the edges E of G is loopless.

Let G be a non loopless graph. One can check that every graph given by reversing directions of the edges E of G is non loopless.

Let G be a connected graph. Let us observe that every graph given by reversing directions of the edges E of G is connected.

Let G be a non connected graph. Observe that every graph given by reversing directions of the edges E of G is non connected.

Let G be an acyclic graph. Note that every graph given by reversing directions of the edges E of G is acyclic.

Let G be a non acyclic graph. One can verify that every graph given by reversing directions of the edges E of G is non acyclic.

Let G be a complete graph. Observe that every graph given by reversing directions of the edges E of G is complete.

Let G be a non complete graph. Observe that every graph given by reversing directions of the edges E of G is non complete.

Let G be a chordal graph. Note that every graph given by reversing directions of the edges E of G is chordal.

Let G be a finite graph. Let us note that every graph given by reversing directions of the edges E of G is finite.

Let G be a non finite graph. One can verify that every graph given by reversing directions of the edges E of G is non finite.

Now we state the propositions:

(26) Let us consider a graph G_1 given by reversing directions of the edges of G_2. Then

(i) the source of $G_1 =$ the target of G_2, and

(ii) the target of $G_1 =$ the source of G_2.

(27) Let us consider a graph G_1 given by reversing directions of the edges of G_2, and objects v_1, e, v_2. Then e joins v_1 to v_2 in G_2 if and only if e joins v_2 to v_1 in G_1. The theorem is a consequence of (26).

2. Adding a Vertex and Several Edges to a Graph

Let us consider G, v, and V.

A supergraph of G extended by vertex v and edges from v to V of G is a supergraph of G defined by

(Def. 2) (i) the vertices of $it =$ (the vertices of G) $\cup \{v\}$ and the edges of $it =$ (the edges of G) $\cup$ ($V \longmapsto$ (the edges of G)) and the source of $it =$ (the source of G)$+\cdot$(($V \longmapsto$ (the edges of G)) $\longmapsto v$) and the target of $it =$ (the target of G)$+\cdot\pi_1(V \boxtimes \{$the edges of $G\})$, **if** $V \subseteq$ the vertices of G and $v \notin$ the vertices of G,

(ii) $it \approx G$, **otherwise**.

A supergraph of G extended by vertex v and edges from V of G to v is a supergraph of G defined by

(Def. 3) (i) the vertices of it = (the vertices of G) $\cup$ $\{v\}$ and the edges of it = (the edges of G) $\cup$ ($V \longmapsto$ (the edges of G)) and the source of it = (the source of G)$+\cdot\pi_1$($V \boxtimes$ {the edges of G}) and the target of it = (the target of G)$+\cdot$(($V \longmapsto$ (the edges of G)) $\longmapsto v$), **if** $V \subseteq$ the vertices of G and $v \notin$ the vertices of G,

(ii) $it \approx G$, **otherwise**.

A supergraph of G extended by vertex v and edges from v to the vertices of G is a supergraph of G extended by vertex v and edges from v to the vertices of G of G.

A supergraph of G extended by vertex v and edges from the vertices of G to v is a supergraph of G extended by vertex v and edges from the vertices of G of G to v. Now we state the propositions:

(28) Let us consider supergraphs G_1, G_2 of G extended by vertex v and edges from v to V of G. Then $G_1 \approx G_2$.

(29) Let us consider supergraphs G_1, G_2 of G extended by vertex v and edges from V of G to v. Then $G_1 \approx G_2$.

(30) Let us consider a supergraph G_1 of G extended by vertex v and edges from v to V of G. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by vertex v and edges from v to V of G.

(31) Let us consider a supergraph G_1 of G extended by vertex v and edges from V of G to v. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by vertex v and edges from V of G to v.

(32) Let us consider a supergraph G_1 of G extended by vertex v and edges from v to V of G, and a supergraph G_2 of G extended by vertex v and edges from V of G to v. Then

(i) the vertices of G_1 = the vertices of G_2, and

(ii) the edges of G_1 = the edges of G_2.

(33) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from v to V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_1.edgesOutOf($\{v\}$) = $V \longmapsto$ (the edges of G_2).

Proof: For every object e, $e \in G_1$.edgesOutOf($\{v\}$) iff $e \in V \longmapsto$ (the edges of G_2). □

(34) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from V of G_2 to v. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_1.edgesInto($\{v\}$) = $V \longmapsto$ (the edges of G_2).

Proof: For every object e, $e \in G_1$.edgesInto($\{v\}$) iff $e \in V \longmapsto$ (the edges of G_2). □

(35) Let us consider a supergraph G_1 of G extended by vertex v and edges from v to V of G, and a supergraph G_2 of G extended by vertex v and edges from V of G to v. Suppose $V \subseteq$ the vertices of G and $v \notin$ the vertices of G. Then

(i) G_2 is a graph given by reversing directions of the edges G_1.edgesOutOf($\{v\}$) of G_1, and

(ii) G_1 is a graph given by reversing directions of the edges G_2.edgesInto($\{v\}$) of G_2.

The theorem is a consequence of (33) and (34).

(36) Let us consider a supergraph G_1 of G extended by vertex v and edges from v to V of G, a supergraph G_2 of G extended by vertex v and edges from V of G to v, and objects v_1, e, v_2. Then e joins v_1 and v_2 in G_1 if and only if e joins v_1 and v_2 in G_2. The theorem is a consequence of (35) and (9).

(37) Let us consider a supergraph G_1 of G extended by vertex v and edges from v to V of G, a supergraph G_2 of G extended by vertex v and edges from V of G to v, and an object w. Then w is a vertex of G_1 if and only if w is a vertex of G_2.

(38) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from v to V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Let us consider objects e_1, u. Then

(i) e_1 does not join u to v in G_1, and

(ii) if $u \notin V$, then e_1 does not join v to u in G_1, and

(iii) for every object e_2 such that e_1 joins v to u in G_1 and e_2 joins v to u in G_1 holds $e_1 = e_2$.

Proof: e_1 does not join u to v in G_1. If $u \notin V$, then e_1 does not join v to u in G_1. $e_1 \notin$ the edges of G_2 and $e_2 \notin$ the edges of G_2. Consider x_1, y_1 being objects such that $x_1 \in V$ and $y_1 \in$ {the edges of G_2} and $e_1 = \langle x_1, y_1 \rangle$. Consider x_2, y_2 being objects such that $x_2 \in V$ and $y_2 \in$ {the edges of G_2} and $e_2 = \langle x_2, y_2 \rangle$. □

(39) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from V of G_2 to v. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Let us consider objects e_1, u. Then

(i) e_1 does not join v to u in G_1, and

(ii) if $u \notin V$, then e_1 does not join u to v in G_1, and

(iii) for every object e_2 such that e_1 joins u to v in G_1 and e_2 joins u to v in G_1 holds $e_1 = e_2$.

Proof: e_1 does not join v to u in G_1. If $u \notin V$, then e_1 does not join u to v in G_1. $e_1 \notin$ the edges of G_2 and $e_2 \notin$ the edges of G_2. Consider x_1, y_1 being objects such that $x_1 \in V$ and $y_1 \in \{$the edges of $G_2\}$ and $e_1 = \langle x_1, y_1\rangle$. Consider x_2, y_2 being objects such that $x_2 \in V$ and $y_2 \in \{$the edges of $G_2\}$ and $e_2 = \langle x_2, y_2\rangle$. □

(40) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from v to V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Let us consider objects e, v_1, v_2. Suppose $v_1 \neq v$. If e joins v_1 to v_2 in G_1, then e joins v_1 to v_2 in G_2.
Proof: $e \in$ the edges of G_2. □

(41) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from V of G_2 to v. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Let us consider objects e, v_1, v_2. Suppose $v_2 \neq v$. If e joins v_1 to v_2 in G_1, then e joins v_1 to v_2 in G_2.
Proof: $e \in$ the edges of G_2. □

(42) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from v to V of G_2, and an object v_1. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and $v_1 \in V$. Then $\langle v_1$, the edges of $G_2\rangle$ joins v to v_1 in G_1.

(43) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges from V of G_2 to v, and an object v_1. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and $v_1 \in V$. Then $\langle v_1$, the edges of $G_2\rangle$ joins v_1 to v in G_1.

Let us consider G, v, V, a supergraph G_1 of G extended by vertex v and edges from v to V of G, and a supergraph G_2 of G extended by vertex v and edges from V of G to v. Now we state the propositions:

(44) Every walk of G_1 is a walk of G_2. The theorem is a consequence of (35) and (14).

(45) Every walk of G_2 is a walk of G_1. The theorem is a consequence of (35) and (14).

Let us consider G, v, and V.

A supergraph of G extended by vertex v and edges between v and V of G is a supergraph of G defined by

(Def. 4) (i) the vertices of *it* = (the vertices of G) $\cup \{v\}$ and for every object e, e does not join v and v in *it* and for every object v_1, if $v_1 \notin V$, then e does not join v_1 and v in *it* and for every object v_2 such that $v_1 \neq v$

and $v_2 \neq v$ and e joins v_1 to v_2 in *it* holds e joins v_1 to v_2 in G and there exists a set E such that $\overline{\overline{V}} = \overline{\overline{E}}$ and E misses the edges of G and the edges of *it* $=$ (the edges of G) $\cup\, E$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in *it* and for every object e_2 such that e_2 joins v_1 and v in *it* holds $e_1 = e_2$, **if** $V \subseteq$ the vertices of G and $v \notin$ the vertices of G,

(ii) *it* $\approx G$, **otherwise**.

A supergraph of G extended by vertex v and edges between v and the vertices of G is a supergraph of G extended by vertex v and edges between v and the vertices of G of G.

One can verify that a supergraph of G extended by vertex v and edges from v to V of G is a supergraph of G extended by vertex v and edges between v and V of G.

Note that a supergraph of G extended by vertex v and edges from V of G to v is a supergraph of G extended by vertex v and edges between v and V of G. Now we state the propositions:

(46) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and $\emptyset$ of G_2. Then the edges of $G_2 =$ the edges of G_1.

(47) Let us consider a non empty set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then the edges of $G_1 \neq \emptyset$.

(48) Let us consider a supergraph G_1 of G extended by vertex v and edges between v and V of G. Suppose $G_1 \approx G_2$. Then G_2 is a supergraph of G extended by vertex v and edges between v and V of G.

(49) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, and objects v_1, e, v_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and $v_1 \neq v$ and $v_2 \neq v$ and e joins v_1 and v_2 in G_1. Then e joins v_1 and v_2 in G_2.

(50) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then v is a vertex of G_1.

(51) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, a set E, and objects v_1, e, v_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup\, E$ and E misses the edges of G_2 and e joins v_1 and v_2 in G_1 and $e \notin$ the edges of G_2. Then

(i) $e \in E$, and

(ii) $v_1 = v$ and $v_2 \in V$ or $v_2 = v$ and $v_1 \in V$.

(52) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, and a set E. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup E$ and E misses the edges of G_2. Then there exist functions f, g from E into $V \cup \{v\}$ such that

(i) the source of $G_1 =$ (the source of G_2)$+\cdot f$, and

(ii) the target of $G_1 =$ (the target of G_2)$+\cdot g$, and

(iii) for every object e such that $e \in E$ holds e joins $f(e)$ to $g(e)$ in G_1 and ($f(e) = v$ iff $g(e) \neq v$).

Proof: Consider E_1 being a set such that $\overline{\overline{V}} = \overline{\overline{E_1}}$ and E_1 misses the edges of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup E_1$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E_1$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an object v_2 such that $\$_1$ joins $\$_2$ to v_2 in G_1. For every object e such that $e \in E$ there exists an object v_1 such that $v_1 \in V \cup \{v\}$ and $\mathcal{P}[e, v_1]$.

Consider f being a function from E into $V \cup \{v\}$ such that for every object e such that $e \in E$ holds $\mathcal{P}[e, f(e)]$. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv \$_1$ joins $f(\$_1)$ to $\$_2$ in G_1. For every object e such that $e \in E$ there exists an object v_2 such that $v_2 \in V \cup \{v\}$ and $\mathcal{Q}[e, v_2]$.

Consider g being a function from E into $V \cup \{v\}$ such that for every object e such that $e \in E$ holds $\mathcal{Q}[e, g(e)]$. For every object e such that $e \in \text{dom}$(the source of G_1) holds (the source of G_1)$(e) =$ ((the source of G_2)$+\cdot f$)(e). For every object e such that $e \in \text{dom}$(the target of G_1) holds (the target of G_1)$(e) =$ ((the target of G_2)$+\cdot g$)(e). □

(53) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then the edges of $G_2 = G_1$.edgesBetween(the vertices of G_2).
Proof: Set $B = G_1$.edgesBetween(the vertices of G_2). For every object e, $e \in$ the edges of G_2 iff $e \in B$. □

(54) Let us consider a graph G_2, sets v, V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_2 is a subgraph of G_1 with vertex v removed. The theorem is a consequence of (53).

(55) Every supergraph of G_2 extended by vertex v and edges between v and $\emptyset$ of G_2 is a supergraph of G_2 extended by v. The theorem is a consequence of (46).

(56) Let us consider an object v_1, and a supergraph G_1 of G_2 extended by vertex v and edges between v and $\{v_1\}$ of G_2. Suppose $v_1 \in$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then there exists an object e such that

(i) $e \notin$ the edges of G_2, and

(ii) G_1 is supergraph of G_2 extended by vertices v, v_1 and e between them or supergraph of G_2 extended by vertices v_1, v and e between them.

The theorem is a consequence of (52).

(57) Let us consider a subset W of V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then there exists a function f from W into G_1.edgesBetween$(W, \{v\})$ such that

(i) f is one-to-one and onto, and

(ii) for every object w such that $w \in W$ holds $f(w)$ joins w and v in G_1.

Proof: Consider E being a set such that $\overline{\overline{V}} = \overline{\overline{E}}$ and E misses the edges of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup\, E$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv \$_2$ joins $\$_1$ and v in G_1. For every object w such that $w \in W$ there exists an object e such that $e \in G_1$.edgesBetween$(W, \{v\})$ and $\mathcal{P}[w, e]$.

Consider f being a function from W into G_1.edgesBetween$(W, \{v\})$ such that for every object w such that $w \in W$ holds $\mathcal{P}[w, f(w)]$. For every objects w_1, w_2 such that $w_1, w_2 \in W$ and $f(w_1) = f(w_2)$ holds $w_1 = w_2$. For every object e such that $e \in G_1$.edgesBetween$(W, \{v\})$ holds $e \in \operatorname{rng} f$. □

(58) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and E misses the edges of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup\, E$. Then $E = G_1$.edgesBetween$(V, \{v\})$.

Proof: Consider E_1 being a set such that $\overline{\overline{V}} = \overline{\overline{E_1}}$ and E_1 misses the edges of G_2 and the edges of $G_1 =$ (the edges of G_2)$\cup E_1$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E_1$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. For every object e, $e \in E$ iff $e \in G_1$.edgesBetween$(V, \{v\})$. □

(59) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices

of G_2. Then

(i) G_1.edgesBetween$(V, \{v\})$ misses the edges of G_2, and

(ii) the edges of $G_1 =$ (the edges of G_2) $\cup$ G_1.edgesBetween$(V, \{v\})$.

PROOF: G_1.edgesBetween$(V, \{v\}) \cap$ (the edges of G_2) $= \emptyset$. For every object e such that $e \in$ the edges of G_1 holds $e \in$ (the edges of G_2) $\cup$ G_1.edgesBetween$(V, \{v\})$. □

(60) Let us consider a graph G_3, an object v, sets V_1, V_2, a supergraph G_1 of G_3 extended by vertex v and edges between v and $V_1 \cup V_2$ of G_3, and a subgraph G_2 of G_1 with edges G_1.edgesBetween$(V_2, \{v\})$ removed. Suppose $V_1 \cup V_2 \subseteq$ the vertices of G_3 and $v \notin$ the vertices of G_3 and V_1 misses V_2. Then G_2 is a supergraph of G_3 extended by vertex v and edges between v and V_1 of G_3.

PROOF: Consider E being a set such that $\overline{\overline{V_1 \cup V_2}} = \overline{\overline{E}}$ and E misses the edges of G_3 and the edges of $G_1 =$ (the edges of G_3) $\cup$ E and for every object v_1 such that $v_1 \in V_1 \cup V_2$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. $E = G_1$.edgesBetween$(V_1 \cup V_2, \{v\})$. For every object e such that $e \in$ the edges of G_3 holds $e \in$ (the edges of G_3) $\setminus$ G_1.edgesBetween$(V_2, \{v\})$. G_2 is a supergraph of G_3. □

(61) Let us consider a graph G_3, an object v, a set V, a vertex v_1 of G_3, and a supergraph G_1 of G_3 extended by vertex v and edges between v and $V \cup \{v_1\}$ of G_3. Suppose $V \subseteq$ the vertices of G_3 and $v \notin$ the vertices of G_3 and $v_1 \notin V$.

Then there exists a supergraph G_2 of G_3 extended by vertex v and edges between v and V of G_3 and there exists an object e such that $e \notin$ the edges of G_3 and G_1 is supergraph of G_2 extended by e between vertices v and v_1 or supergraph of G_2 extended by e between vertices v_1 and v.

PROOF: Reconsider $W = \{v_1\}$ as a subset of $V \cup \{v_1\}$. Consider f being a function from W into G_1.edgesBetween$(W, \{v\})$ such that f is one-to-one and onto and for every object w such that $w \in W$ holds $f(w)$ joins w and v in G_1. $f(v_1) \notin$ the edges of G_3. v is a vertex of G_1. □

(62) Let us consider a graph G_3, an object v, a set V, a vertex v_1 of G_3, an object e, and a supergraph G_2 of G_3 extended by vertex v and edges between v and V of G_3. Suppose $V \subseteq$ the vertices of G_3 and $v \notin$ the vertices of G_3 and $v_1 \notin V$ and $e \notin$ the edges of G_2.

Let us consider a graph G_1. Suppose G_1 is supergraph of G_2 extended by e between vertices v_1 and v or supergraph of G_2 extended by e between vertices v and v_1. Then G_1 is a supergraph of G_3 extended by vertex v and edges between v and $V \cup \{v_1\}$ of G_3.

Proof: Consider E being a set such that $\overline{\overline{V}} = \overline{\overline{E}}$ and E misses the edges of G_3 and the edges of $G_2 =$ (the edges of $G_3) \cup E$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in G_2 and for every object e_2 such that e_2 joins v_1 and v in G_2 holds $e_1 = e_2$. Consider f being a function such that f is one-to-one and $\mathrm{dom}\, f = E$ and $\mathrm{rng}\, f = V$. Set $f_1 = f {+\cdot} (e \overset{.}{\longmapsto} v_1)$. $\mathrm{rng}\, f \cap \mathrm{rng}(e \overset{.}{\longmapsto} v_1) = \emptyset$. For every object w such that $w \in \mathrm{rng}\, f \cup \mathrm{rng}(e \overset{.}{\longmapsto} v_1)$ holds $w \in \mathrm{rng}\, f_1$. v is a vertex of G_2 and v_1 is a vertex of G_3. □

Let us consider G_2, v, V, a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, and a walk W of G_1. Now we state the propositions:

(63) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then

(i) if W.edges() $\subseteq$ the edges of G_2 and W is not trivial, then $v \notin W$.vertices(), and

(ii) if $v \notin W$.vertices(), then W.edges() $\subseteq$ the edges of G_2.

Proof: Consider E being a set such that $\overline{\overline{V}} = \overline{\overline{E}}$ and E misses the edges of G_2 and the edges of $G_1 =$ (the edges of $G_2) \cup E$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. For every object e such that $e \in W$.edges() holds $e \in$ the edges of G_2. □

(64) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and (W.edges() $\subseteq$ the edges of G_2 and W is not trivial or $v \notin W$.vertices()). Then W is a walk of G_2. The theorem is a consequence of (63).

(65) If W.vertices() $\subseteq$ the vertices of G_2, then W.edges() $\subseteq$ the edges of G_2. The theorem is a consequence of (63).

(66) Let us consider supergraphs G_1, G_2 of G extended by vertex v and edges between v and V of G. Then

(i) the vertices of $G_1 =$ the vertices of G_2, and

(ii) every vertex of G_1 is a vertex of G_2.

Proof: The vertices of $G_1 =$ the vertices of G_2. □

(67) Let us consider supergraphs G_1, G_2 of G extended by vertex v and edges between v and V of G, and objects v_1, e_1, v_2. Suppose e_1 joins v_1 and v_2 in G_1. Then there exists an object e_2 such that e_2 joins v_1 and v_2 in G_2.

(68) Let us consider supergraphs G_1, G_2 of G extended by vertex v and edges between v and V of G. Then there exists a function f from the edges of G_1 into the edges of G_2 such that

(i) $f \restriction$(the edges of G) $= \mathrm{id}_\alpha$, and

(ii) f is one-to-one and onto, and

(iii) for every objects v_1, e, v_2 such that e joins v_1 and v_2 in G_1 holds $f(e)$ joins v_1 and v_2 in G_2,

where α is the edges of G. The theorem is a consequence of (67), (47), and (51).

Let G be a loopless graph. Let us consider v and V. Observe that every supergraph of G extended by vertex v and edges between v and V of G is loopless.

Let G be a non-directed-multi graph. Let us note that every supergraph of G extended by vertex v and edges between v and V of G is non-directed-multi.

Let G be a non-multi graph. Note that every supergraph of G extended by vertex v and edges between v and V of G is non-multi.

Let G be a directed-simple graph. One can verify that every supergraph of G extended by vertex v and edges between v and V of G is directed-simple.

Let G be a simple graph. Let us observe that every supergraph of G extended by vertex v and edges between v and V of G is simple.

Now we state the proposition:

(69) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2, a walk W of G_1, and vertices v_1, v_2 of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and W.first() $= v_1$ and W.last() $= v_2$ and $v_2 \notin G_2$.reachableFrom(v_1). Then $v \in W$.vertices(). The theorem is a consequence of (64).

Let us consider G_2, v, V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Now we state the propositions:

(70) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and G_2 is acyclic and for every component G_3 of G_2 and for every vertices w_1, w_2 of G_3 such that $w_1, w_2 \in V$ holds $w_1 = w_2$. Then G_1 is acyclic.

Proof: Consider E being a set such that $\overline{\overline{V}} = \overline{\overline{E}}$ and E misses the edges of G_2 and the edges of $G_1 =$ (the edges of G_2) $\cup E$ and for every object v_1 such that $v_1 \in V$ there exists an object e_1 such that $e_1 \in E$ and e_1 joins v_1 and v in G_1 and for every object e_2 such that e_2 joins v_1 and v in G_1 holds $e_1 = e_2$. There exists no walk W of G_1 such that W is cycle-like. □

(71) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and (G_2 is not acyclic or there exists a component G_3 of G_2 and there exist vertices w_1, w_2 of G_3 such that $w_1, w_2 \in V$ and $w_1 \neq w_2$). Then G_1 is not acyclic.

(72) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and for every component G_3 of G_2, there exists a vertex w of G_3 such that $w \in V$. Then G_1 is connected.

Proof: For every vertex u of G_1 such that $u \neq v$ there exists a walk W_1 of G_1 such that W_1 is walk from u to v. For every vertices u, w of G_1, there exists a walk W_1 of G_1 such that W_1 is walk from u to w. □

Let G be a connected graph, v be an object, and V be a non empty set. Note that every supergraph of G extended by vertex v and edges between v and V of G is connected.

Let us consider G_2, v, V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Now we state the propositions:

(73) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and there exists a component G_3 of G_2 such that for every vertex w of G_3, $w \notin V$. Then G_1 is not connected.

Proof: Consider G_3 being a component of G_2 such that for every vertex w of G_3, $w \notin V$. Set $v_1 =$ the vertex of G_3. There exists no walk W of G_1 such that W is walk from v_1 to v. □

(74) Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2 and there exists a component G_3 of G_2 such that the vertices of G_3 misses V. Then G_1 is not connected. The theorem is a consequence of (73).

Let G be a non connected graph and v be an object. One can check that every supergraph of G extended by vertex v and edges between v and $\emptyset$ of G is non connected.

(75) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_1 is complete if and only if G_2 is complete and $V =$ the vertices of G_2.

Proof: For every vertices u, v of G_1 such that $u \neq v$ holds u and v are adjacent. □

Let G be a complete graph. Observe that every supergraph of G extended by vertex the vertices of G and edges between the vertices of G and the vertices of G is complete.

Now we state the propositions:

(76) Let us consider a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then

(i) G_1.order() $= G_2$.order() $+ 1$, and

(ii) G_1.size() $= G_2$.size() $+ \overline{\overline{V}}$.

(77) Let us consider a finite graph G_2, an object v, a set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_1.order() $=$ G_2.order() $+ 1$.

(78) Let us consider a finite graph G_2, an object v, a finite set V, and a supergraph G_1 of G_2 extended by vertex v and edges between v and V of G_2. Suppose $V \subseteq$ the vertices of G_2 and $v \notin$ the vertices of G_2. Then G_1.size() $=$ G_2.size() $+ \overline{\overline{V}}$.

Let G be a finite graph, v be an object, and V be a set. One can verify that every supergraph of G extended by vertex v and edges between v and V of G is finite.

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Lowell W. Beineke and Robin J. Wilson, editors. *Selected Topics in Graph Theory.* Academic Press, London, 1978. ISBN 0-12-086250-6.

[4] John Adrian Bondy and U. S. R. Murty. *Graph Theory.* Graduate Texts in Mathematics, 244. Springer, New York, 2008. ISBN 978-1-84628-969-9.

[5] Sebastian Koch. About supergraphs. Part I. *Formalized Mathematics*, 26(**2**):101–124, 2018. doi:10.2478/forma-2018-0009.

[6] Gilbert Lee. Walks in graphs. *Formalized Mathematics*, 13(**2**):253–269, 2005.

[7] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[8] Klaus Wagner. *Graphentheorie.* B.I-Hochschultaschenbücher; 248. Bibliograph. Inst., Mannheim, 1970. ISBN 3-411-00248-4.

[9] Robin James Wilson. *Introduction to Graph Theory.* Oliver & Boyd, Edinburgh, 1972. ISBN 0-05-002534-1.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 141–147, 2018
DOI: 10.2478/forma-2018-0011

sciendo
https://www.sciendo.com/

On Algebras of Algorithms and Specifications over Uninterpreted Data

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. This paper continues formalization in Mizar [2, 1] of basic notions of the composition-nominative approach to program semantics [13] which was started in [8, 11].

The composition-nominative approach studies mathematical models of computer programs and data on various levels of abstraction and generality and provides tools for reasoning about their properties. Besides formalization of semantics of programs, certain elements of the composition-nominative approach were applied to abstract systems in a mathematical systems theory [4, 6, 7, 5, 3].

In the paper we introduce a definition of the notion of a binominative function over a set D understood as a partial function which maps elements of D to D. The sets of binominative functions and nominative predicates [11] over given sets form the carrier of the generalized Glushkov algorithmic algebra [14]. This algebra can be used to formalize algorithms which operate on various data structures (such as multidimensional arrays, lists, etc.) and reason about their properties.

We formalize the operations of this algebra (also called compositions) which are valid over uninterpretated data and which include among others the sequential composition, the prediction composition, the branching composition, the monotone Floyd-Hoare composition, and the cycle composition. The details on formalization of nominative data and the operations of the algorithmic algebra over them are described in [10, 12, 9].

MSC: 68Q60 68T37 03B70 03B35

Keywords: Glushkov algorithmic algebra; uninterpreted data

MML identifier: PARTPR_2, version: 8.1.08 5.53.1335

1. Preliminaries

From now on x denotes an object and n denotes a natural number.

Let X, Y be sets. Observe that every element of $X \dot{\rightarrow} Y$ is X-defined and every element of $X \dot{\rightarrow} Y$ is Y-valued.

Now we state the proposition:

(1) Let us consider sets X, Y, Z, T, objects x, y, z, and a function f from $X \times Y \times Z$ into T. Suppose $x \in X$ and $y \in Y$ and $z \in Z$ and $T \neq \emptyset$. Then $f(x, y, z) \in T$.

One can verify that there exists a set which is non empty and has not non empty elements.

Let A, B, C be sets. The functor $\cdot(A, B, C)$ yielding a function from $(A \dot{\rightarrow} B) \times (B \dot{\rightarrow} C)$ into $A \dot{\rightarrow} C$ is defined by

(Def. 1) for every partial function f from A to B and for every partial function g from B to C, $it(f, g) = g \cdot f$.

From now on D denotes a non empty set and p, q denote partial predicates of D.

Now we state the propositions:

(2) If q is total, then $\operatorname{dom} p \subseteq \operatorname{dom}(p \vee q)$.

(3) If q is total, then $\operatorname{dom} p \subseteq \operatorname{dom}(p \wedge q)$.

(4) If q is total, then $\operatorname{dom} p \subseteq \operatorname{dom}(p \Rightarrow q)$.

2. Operations in Algebras of Algorithms and Specifications over Uninterpreted Data

From now on D denotes a set.

Let us consider D. The functor $\mathrm{FPrg}(D)$ yielding a set is defined by the term

(Def. 2) $D \dot{\rightarrow} D$.

Observe that $\mathrm{FPrg}(D)$ is non empty and functional.

A binominative function of D is a partial function from D to D. Now we state the proposition:

(5) Let us consider a non empty set D, and a binominative function f of D. Then $\mathrm{id}_{\mathrm{field}\, f}$ is a binominative function of D.

In the sequel p, q denote partial predicates of D and f, g denote binominative functions of D.

Let us consider D and p. Let F be a function from $\Pr(D)$ into $\Pr(D)$. One can check that $F(p)$ is function-like and relation-like.

Let p be an element of $\mathrm{Pr}(D)$. One can check that $F(p)$ is function-like and relation-like.

Let us consider p and q. Let F be a function from $\mathrm{Pr}(D) \times \mathrm{Pr}(D)$ into $\mathrm{Pr}(D)$. Observe that $F(p, q)$ is function-like and relation-like.

Let p, q be elements of $\mathrm{Pr}(D)$. One can check that $F(p, q)$ is function-like and relation-like.

Let x be an element of $\mathrm{Pr}(D) \times \mathrm{Pr}(D)$. Observe that $F(x)$ is function-like and relation-like.

Let us consider f. Let F be a function from $\mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$. Let us observe that $F(f)$ is function-like and relation-like.

Let us consider p and g. Let F be a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D) \times \mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$. One can check that $F(p,\ f,\ g)$ is function-like and relation-like and $F(\langle p,\ f,\ g\rangle)$ is function-like and relation-like.

Let us consider q. Let F be a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D) \times \mathrm{Pr}(D)$ into $\mathrm{Pr}(D)$. One can check that $F(p,\ f,\ q)$ is function-like and relation-like and $F(\langle p,\ f,\ q\rangle)$ is function-like and relation-like.

Let D be a set. We introduce the notation $\mathrm{id}_{\mathrm{PP}}(D)$ as a synonym of id_D.

One can verify that the functor $\mathrm{id}_{\mathrm{PP}}(D)$ yields a binominative function of D. Let D be a non empty set and d be an element of D. The functor $\mathrm{id}_{\mathrm{PP}}(d)$ yielding an element of D is defined by the term

(Def. 3) $\mathrm{id}_{\mathrm{PP}}(D)(d)$.

Let us consider D. The functor $\bullet(D)$ yielding a function from $\mathrm{FPrg}(D) \times \mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$ is defined by the term

(Def. 4) $\cdot(D, D, D)$.

Let us consider D, f, and g. The functor $f \bullet g$ yielding a binominative function of D is defined by the term

(Def. 5) $\bullet(D)(f, g)$.

Let us consider D. The functor $\cdot(D)$ yielding a function from $\mathrm{FPrg}(D) \times \mathrm{Pr}(D)$ into $\mathrm{Pr}(D)$ is defined by the term

(Def. 6) $\cdot(D, D, \mathit{Boolean})$.

Let us consider D, f, and p. The functor $f \cdot p$ yielding a partial predicate of D is defined by the term

(Def. 7) $\cdot(D)(f, p)$.

Let F be a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D) \times \mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$, p be a partial predicate of D, and f, g be binominative functions of D. One can check that $F(p,\ f,\ g)$ is function-like and relation-like.

Now we state the proposition:

(6) If $x \in \operatorname{dom}(f \cdot p)$, then $x \in \operatorname{dom}(p \cdot f)$ and $((p \cdot f)(x) = \mathit{true}$ or $(p \cdot f)(x) = \mathit{false})$.

The scheme *PredToNomPredEx* deals with a set $\mathcal{D}$ and a set D_1 and a unary predicate $\mathcal{P}$ and states that

(Sch. 1) There exists a partial predicate p of $\mathcal{D}$ such that $\operatorname{dom} p = D_1$ and for every object d such that $d \in \operatorname{dom} p$ holds if $\mathcal{P}[d]$, then $p(d) = \mathit{true}$ and if not $\mathcal{P}[d]$, then $p(d) = \mathit{false}$

provided

- $D_1 \subseteq \mathcal{D}$.

The scheme *PredToNomPredUnique* deals with a set $\mathcal{D}$ and a set D_1 and a unary predicate $\mathcal{P}$ and states that

(Sch. 2) For every partial predicates p, q of $\mathcal{D}$ such that $\operatorname{dom} p = D_1$ and for every object d such that $d \in \operatorname{dom} p$ holds if $\mathcal{P}[d]$, then $p(d) = \mathit{true}$ and if not $\mathcal{P}[d]$, then $p(d) = \mathit{false}$ and $\operatorname{dom} q = D_1$ and for every object d such that $d \in \operatorname{dom} q$ holds if $\mathcal{P}[d]$, then $q(d) = \mathit{true}$ and if not $\mathcal{P}[d]$, then $q(d) = \mathit{false}$ holds $p = q$.

Let us consider D. The functor isEmpty(D) yielding a partial predicate of D is defined by

(Def. 8) $\operatorname{dom} \mathit{it} = D$ and for every object d such that $d \in \operatorname{dom} \mathit{it}$ holds if $d = \emptyset$, then $\mathit{it}(d) = \mathit{true}$ and if $d \neq \emptyset$, then $\mathit{it}(d) = \mathit{false}$.

Let D be a set with non non empty elements. The functor Empty_D yielding a binominative function of D is defined by the term

(Def. 9) $D \longmapsto \emptyset$.

Let us consider D. The functor $\perp_D$ yielding a binominative function of D is defined by the term

(Def. 10) $\emptyset$.

In the sequel D denotes a non empty set, p, q denote partial predicates of D, and f, g, h denote binominative functions of D.

Let us consider D. The functor $\mathrm{IF}(D)$ yielding a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D) \times \mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$ is defined by

(Def. 11) for every partial predicate p of D and for every binominative functions f, g of D, $\operatorname{dom} \mathit{it}(p, f, g) = \{d$, where d is an element of $D : d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ or $d \in \operatorname{dom} p$ and $p(d) = \mathit{false}$ and $d \in \operatorname{dom} g\}$ and for every object d, if $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$, then $\mathit{it}(p, f, g)(d) = f(d)$ and if $d \in \operatorname{dom} p$ and $p(d) = \mathit{false}$ and $d \in \operatorname{dom} g$, then $\mathit{it}(p, f, g)(d) = g(d)$.

Let us consider D, p, f, and g. The functor $\mathrm{IF}(p, f, g)$ yielding a binominative function of D is defined by the term

(Def. 12) $\mathrm{IF}(D)(p,\ f,\ g)$.

Now we state the proposition:

(7) Suppose $x \in \mathrm{dom}(\mathrm{IF}(p, f, g))$. Then

(i) $x \in \mathrm{dom}\, p$ and $p(x) = \mathit{true}$ and $x \in \mathrm{dom}\, f$, or

(ii) $x \in \mathrm{dom}\, p$ and $p(x) = \mathit{false}$ and $x \in \mathrm{dom}\, g$.

Let us consider D. The functor $\mathrm{FH}(D)$ yielding a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D) \times \mathrm{Pr}(D)$ into $\mathrm{Pr}(D)$ is defined by

(Def. 13) for every partial predicates p, q of D and for every binominative function f of D, $\mathrm{dom}\, \mathit{it}(p,\ f,\ q) = \{d$, where d is an element of $D : d \in \mathrm{dom}\, p$ and $p(d) = \mathit{false}$ or $d \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(d) = \mathit{true}$ or $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(d) = \mathit{false}\}$ and for every object d, if $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{false}$ or $d \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(d) = \mathit{true}$, then $\mathit{it}(p,\ f,\ q)(d) = \mathit{true}$ and if $d \in \mathrm{dom}\, p$ and $p(d) = \mathit{true}$ and $d \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(d) = \mathit{false}$, then $\mathit{it}(p,\ f,\ q)(d) = \mathit{false}$.

Let us consider D, p, q, and f. The functor $\mathrm{FH}(p, f, q)$ yielding a partial predicate of D is defined by the term

(Def. 14) $\mathrm{FH}(D)(p,\ f,\ q)$.

Now we state the proposition:

(8) Suppose $x \in \mathrm{dom}(\mathrm{FH}(p, f, q))$. Then

(i) $x \in \mathrm{dom}\, p$ and $p(x) = \mathit{false}$, or

(ii) $x \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(x) = \mathit{true}$, or

(iii) $x \in \mathrm{dom}\, p$ and $p(x) = \mathit{true}$ and $x \in \mathrm{dom}(q \cdot f)$ and $(q \cdot f)(x) = \mathit{false}$.

Let us consider D. The functor $\mathrm{WH}(D)$ yielding a function from $\mathrm{Pr}(D) \times \mathrm{FPrg}(D)$ into $\mathrm{FPrg}(D)$ is defined by

(Def. 15) for every partial predicate p of D and for every binominative function f of D, $\mathrm{dom}\, \mathit{it}(p, f) = \{d$, where d is an element of D : there exists a natural number n such that for every natural number i such that $i \leqslant n-1$ holds $d \in \mathrm{dom}(p \cdot (f^i))$ and $(p \cdot (f^i))(d) = \mathit{true}$ and $d \in \mathrm{dom}(p \cdot (f^n))$ and $(p \cdot (f^n))(d) = \mathit{false}\}$ and for every object d such that $d \in \mathrm{dom}\, \mathit{it}(p, f)$ there exists a natural number n such that for every natural number i such that $i \leqslant n - 1$ holds $d \in \mathrm{dom}(p \cdot (f^i))$ and $(p \cdot (f^i))(d) = \mathit{true}$ and $d \in \mathrm{dom}(p \cdot (f^n))$ and $(p \cdot (f^n))(d) = \mathit{false}$ and $\mathit{it}(p, f)(d) = (f^n)(d)$.

Let us consider D, p, and f. The functor $\mathrm{WH}(p, f)$ yielding a binominative function of D is defined by the term

(Def. 16) $\mathrm{WH}(D)(p, f)$.

The functor $\sim D$ yielding a function from $\mathrm{Pr}(D)$ into $\mathrm{Pr}(D)$ is defined by

(Def. 17) for every partial predicate p of D, $\mathrm{dom}(\mathit{it}(p)) = \{d$, where d is an element of $D : d \notin \mathrm{dom}\, p\}$ and for every element d of D such that $d \notin \mathrm{dom}\, p$ holds $\mathit{it}(p)(d) = \mathit{true}$.

Let D be a non empty set and p be a partial predicate of D. The functor $\sim p$ yielding a partial predicate of D is defined by the term

(Def. 18) $(\sim D)(p)$.

Now we state the propositions:

(9) Let us consider an element d of D. Then $d \in \mathrm{dom}\, p$ if and only if $d \notin \mathrm{dom}(\sim p)$.

(10) If p is total, then $\mathrm{dom}(\sim p) = \emptyset$.

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Ievgen Ivanov. On the underapproximation of reach sets of abstract continuous-time systems. In Erika Ábrahám and Sergiy Bogomolov, editors, *Proceedings 3rd International Workshop on Symbolic and Numerical Methods for Reachability Analysis, SNR@ETAPS 2017, Uppsala, Sweden, 22nd April 2017*, volume 247 of *EPTCS*, pages 46–51, 2017. doi:10.4204/EPTCS.247.4.

[4] Ievgen Ivanov. On representations of abstract systems with partial inputs and outputs. In T. V. Gopal, Manindra Agrawal, Angsheng Li, and S. Barry Cooper, editors, *Theory and Applications of Models of Computation – 11th Annual Conference, TAMC 2014, Chennai, India, April 11–13, 2014. Proceedings*, volume 8402 of *Lecture Notes in Computer Science*, pages 104–123. Springer, 2014. ISBN 978-3-319-06088-0. doi:10.1007/978-3-319-06089-7_8.

[5] Ievgen Ivanov. On local characterization of global timed bisimulation for abstract continuous-time systems. In Ichiro Hasuo, editor, *Coalgebraic Methods in Computer Science – 13th IFIP WG 1.3 International Workshop, CMCS 2016, Colocated with ETAPS 2016, Eindhoven, The Netherlands, April 2–3, 2016, Revised Selected Papers*, volume 9608 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2016. ISBN 978-3-319-40369-4. doi:10.1007/978-3-319-40370-0_13.

[6] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. On a decidable formal theory for abstract continuous-time dynamical systems. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, pages 78–99. Springer International Publishing, 2014. ISBN 978-3-319-13206-8. doi:10.1007/978-3-319-13206-8_4.

[7] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. Event-based proof of the mutual exclusion property of Peterson's algorithm. *Formalized Mathematics*, 23(4):325–331, 2015. doi:10.1515/forma-2015-0026.

[8] 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.

[9] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the

composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[10] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[11] 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.

[12] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Jerzy Świątek, Leszek Borzemski, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017: Part II*, pages 176–186. Springer International Publishing, 2018. ISBN 978-3-319-67229-8. doi:10.1007/978-3-319-67229-8_16.

[13] Nikolaj S. Nikitchenko. A composition nominative approach to program semantics. Technical Report IT-TR 1998-020, Department of Information Technology, Technical University of Denmark, 1998.

[14] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 149–158, 2018
DOI: 10.2478/forma-2018-0012

sciendo
https://www.sciendo.com/

On an Algorithmic Algebra over Simple-Named Complex-Valued Nominative Data

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. This paper continues formalization in the Mizar system [2, 1] of basic notions of the composition-nominative approach to program semantics [14] which was started in [8, 12, 10].

The composition-nominative approach studies mathematical models of computer programs and data on various levels of abstraction and generality and provides tools for reasoning about their properties. In particular, data in computer systems are modeled as nominative data [15]. Besides formalization of semantics of programs, certain elements of the composition-nominative approach were applied to abstract systems in a mathematical systems theory [4, 6, 7, 5, 3].

In the paper we give a formal definition of the notions of a binominative function over given sets of names and values (i.e. a partial function which maps simple-named complex-valued nominative data to such data) and a nominative predicate (a partial predicate on simple-named complex-valued nominative data). The sets of such binominative functions and nominative predicates form the carrier of the generalized Glushkov algorithmic algebra for simple-named complex-valued nominative data [15]. This algebra can be used to formalize algorithms which operate on various data structures (such as multidimensional arrays, lists, etc.) and reason about their properties.

In particular, we formalize the operations of this algebra which require a specification of a data domain and which include the existential quantifier, the assignment composition, the composition of superposition into a predicate, the composition of superposition into a binominative function, the name checking

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

predicate. The details on formalization of nominative data and the operations of the algorithmic algebra over them are described in [11, 13, 9].

MSC: 68Q60 68T37 03B70 03B35

Keywords: Glushkov algorithmic algebra; nominative data

MML identifier: `NOMIN_2`, version: `8.1.08 5.52.1328`

1. Preliminaries

From now on a, b, c, v, v_1, x, y denote objects, V, A denote sets, and d denotes a nominative data with simple names from V and complex values from A.

Now we state the proposition:

(1) $\{a, b, c\} \subseteq A$ if and only if a, b, $c \in A$.

Let a, b, c, d, e, f be objects. One can verify that $\{\langle a, b\rangle, \langle c, d\rangle, \langle e, f\rangle\}$ is relation-like.

Let us consider objects a, b, c, d, e, f. Now we state the propositions:

(2) $\mathrm{dom}\{\langle a, b\rangle, \langle c, d\rangle, \langle e, f\rangle\} = \{a, c, e\}$.

(3) $\mathrm{rng}\{\langle a, b\rangle, \langle c, d\rangle, \langle e, f\rangle\} = \{b, d, f\}$.

Let us consider V. Note that there exists a finite sequence which is one-to-one and V-valued.

(4) $\mathrm{dom}\langle a, b, c\rangle = \{1, 2, 3\}$.

Let us consider V and A. Let us note that $\mathrm{ND}_{\mathrm{SS}}(V, A)$ is non empty and has not non empty elements and $\mathrm{ND}_{\mathrm{SC}}(V, A)$ is non empty and has not non empty elements.

Now we state the propositions:

(5) If $v \in V$, then $\{\langle v, d\rangle\}$ is a non-atomic nominative data of V and A.

(6) Let us consider a finite function D. Suppose $\mathrm{dom}\, D \subseteq V$ and $\mathrm{rng}\, D \subseteq \mathrm{ND}_{\mathrm{SC}}(V, A)$. Then D is a non-atomic nominative data of V and A.
Proof: Define $\mathcal{P}[\text{set}] \equiv \$_1$ is a non-atomic nominative data of V and A. For every sets x, B such that $x \in D$ and $B \subseteq D$ and $\mathcal{P}[B]$ holds $\mathcal{P}[B \cup \{x\}]$. $\mathcal{P}[D]$. □

(7) Let us consider nominative data d_1, d_2 with simple names from V and complex values from A. Then $d_2 \subseteq d_1 \nabla_a d_2$.

(8) Every non-atomic nominative data of V and A is a nominative data with simple names from V and complex values from A.

(9) Let us consider non-atomic nominative data d_1, d_2 of V and A. Then $d_1 \nabla_a d_2$ is a non-atomic nominative data of V and A. The theorem is a consequence of (8).

Let us consider V and A. Let d_1, d_2 be non-atomic nominative data of V and A. Let us observe that $d_1 \nabla_a d_2$ is function-like and relation-like.

Let us consider v. One can verify that $d_1 \nabla_a^v d_2$ is function-like and relation-like.

Let d_1 be a non-atomic nominative data of V and A and d_2 be a nominative data with simple names from V and complex values from A. Let us observe that $d_1 \nabla_a^v d_2$ is function-like and relation-like.

Now we state the propositions:

(10) Suppose $v \in V$. Let us consider nominative data d_1, d_2 with simple names from V and complex values from A, and a function L. If $L = d_1 \nabla_a^v d_2$, then $L(v) = d_2$. The theorem is a consequence of (8).

(11) Suppose $v \in V$ and $v \neq v_1$. Let us consider a non-atomic nominative data d_1 of V and A, a nominative data d_2 with simple names from V and complex values from A, and a function L. Suppose $L = d_1 \nabla_a^v d_2$ and $v_1 \in \operatorname{dom} d_1$ and $d_1 \notin A$ and $\Rightarrow v(d_2) \notin A$. Then $L(v_1) = d_1(v_1)$. The theorem is a consequence of (8).

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. Now we state the propositions:

(12) Suppose $v \in V$ and $v \notin \operatorname{dom} d_1$ and $d_1 \notin A$ and $\Rightarrow v(d_2) \notin A$. Then $\operatorname{dom}(d_1 \nabla_a^v d_2) = \{v\} \cup \operatorname{dom} d_1$.

(13) If $v \in V$ and $v \in \operatorname{dom} d_1$ and $d_1 \notin A$ and $\Rightarrow v(d_2) \notin A$, then $\operatorname{dom}(d_1 \nabla_a^v d_2) = \operatorname{dom} d_1$.

(14) If $v \in V$ and $d_1 \notin A$ and $\Rightarrow v(d_2) \notin A$, then $\operatorname{dom}(d_1 \nabla_a^v d_2) = \{v\} \cup \operatorname{dom} d_1$. The theorem is a consequence of (13) and (12).

Let us consider V and A.

A partial predicate over simple-named complex-valued nominative data of V and A is a partial predicate of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. In the sequel p, q, r denote partial predicates over simple-named complex-valued nominative date of V and A.

Now we state the propositions:

(15) $\operatorname{dom}(p \vee q) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ or $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$ or $d \in \operatorname{dom} p$ and $p(d) = \mathit{false}$ and $d \in \operatorname{dom} q$ and $q(d) = \mathit{false}\}$.

(16) $\operatorname{dom}(p \wedge q) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom} p$ and $p(d) = \mathit{false}$ or $d \in$

$\operatorname{dom} q$ and $q(d) = \mathit{false}$ or $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}\}$.

(17) $\operatorname{dom}(p \Rightarrow q) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d \in \operatorname{dom} p$ and $p(d) = \mathit{false}$ or $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$ or $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} q$ and $q(d) = \mathit{false}\}$.

Let us consider V, A, and v. The functor $\exists_v^{V,A}$ yielding a function from $\Pr(\mathrm{ND}_{\mathrm{SC}}(V, A))$ into $\Pr(\mathrm{ND}_{\mathrm{SC}}(V, A))$ is defined by

(Def. 1) for every partial predicate over simple-named complex-valued nominative data p of V and A, $\operatorname{dom}(\mathit{it}(p)) = \{d$, where d is a nominative data with simple names from V and complex values from A : there exists a nominative data d_1 with simple names from V and complex values from A such that $d \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(d \nabla_a^v d_1) = \mathit{true}$ or for every nominative data d_1 with simple names from V and complex values from $A, d \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(d \nabla_a^v d_1) = \mathit{false}\}$ and for every nominative data d with simple names from V and complex values from A, if there exists a nominative data d_1 with simple names from V and complex values from A such that $d \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(d \nabla_a^v d_1) = \mathit{true}$, then $\mathit{it}(p)(d) = \mathit{true}$ and if for every nominative data d_1 with simple names from V and complex values from A, $d \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(d \nabla_a^v d_1) = \mathit{false}$, then $\mathit{it}(p)(d) = \mathit{false}$.

Let us consider p. The functor $\exists_v p$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 2) $(\exists_v^{V,A})(p)$.

Now we state the propositions:

(18) Suppose $x \in \operatorname{dom}(\exists_v p)$. Then

(i) there exists a nominative data d_1 with simple names from V and complex values from A such that $x \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(x \nabla_a^v d_1) = \mathit{true}$, or

(ii) for every nominative data d_1 with simple names from V and complex values from A, $x \nabla_a^v d_1 \in \operatorname{dom} p$ and $p(x \nabla_a^v d_1) = \mathit{false}$.

(19) $\exists_v \bot_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)) = \bot_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A))$. The theorem is a consequence of (18).

(20) Distributivity law:
$\exists_v(p \vee q) = \exists_v p \vee \exists_v q$.

2. On an Algorithmic algebra over Simple-Named Complex-Valued Nominative Data

From now on n denotes a natural number and X denotes a function.

Let F be a function yielding function and d be an object. We say that d is in doms F if and only if

(Def. 3) for every object x such that $x \in \operatorname{dom} F$ holds $d \in \operatorname{dom}(F(x))$.

Let g be a function yielding function and X be a function. The functor NDdataSeq(g, X, d) yielding a function is defined by

(Def. 4) $\operatorname{dom} \mathit{it} = \operatorname{dom} X$ and for every x such that $x \in \operatorname{dom} X$ holds $\mathit{it}(x) = \langle X(x), g(x)(d) \rangle$.

Let X be a finite function. Let us note that NDdataSeq(g, X, d) is finite.

Let X be a finite sequence. One can check that NDdataSeq(g, X, d) is finite sequence-like.

Let X be a function. The functor NDentry(g, X, d) yielding a set is defined by the term

(Def. 5) rng NDdataSeq(g, X, d).

Now we state the propositions:

(21) Let us consider a function f, and objects a, d. Then NDentry$(\langle f \rangle, \langle a \rangle, d) = \{\langle a, f(d) \rangle\}$.

(22) Let us consider functions f, g, and objects a, b, d. Then NDentry$(\langle f, g \rangle, \langle a, b \rangle, d) = \{\langle a, f(d) \rangle, \langle b, g(d) \rangle\}$.

(23) Let us consider functions f, g, h, and objects a, b, c, d. Then NDentry$(\langle f, g, h \rangle, \langle a, b, c \rangle, d) = \{\langle a, f(d) \rangle, \langle b, g(d) \rangle, \langle c, h(d) \rangle\}$. The theorem is a consequence of (4).

Let g be a function yielding function, X be a function, and d be an object. Let us note that NDentry(g, X, d) is relation-like.

Let X be a one-to-one function. One can verify that NDentry(g, X, d) is function-like.

Let X be a finite function. Observe that NDentry(g, X, d) is finite.

Now we state the proposition:

(24) Let us consider a function yielding function g, a function X, and an object d. Then $\operatorname{dom}(\text{NDentry}(g, X, d)) = \operatorname{rng} X$.

Let us consider V and A.

A binominative function over simple-named complex-valued nominative data of V and A is a partial function from $\mathrm{ND}_{\mathrm{SC}}(V, A)$ to $\mathrm{ND}_{\mathrm{SC}}(V, A)$. From now on f, g, h denote binominative functions over simple-named complex-valued nominative date of V and A.

Now we state the propositions:

(25) $\operatorname{rng} \mathrm{NDdataSeq}(\langle f\rangle, \langle v\rangle, d) = v \overset{\cdot}{\longmapsto} f(d)$.

(26) If $a \in V$ and $d \in \operatorname{dom} f$, then $\mathrm{NDentry}(\langle f\rangle, \langle a\rangle, d) = \Rightarrow a(f(d))$. The theorem is a consequence of (25).

(27) If $a \in V$ and $d \in \operatorname{dom} f$, then $\mathrm{NDentry}(\langle f\rangle, \langle a\rangle, d)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (26).

(28) Suppose $\{a, b\} \subseteq V$ and $a \neq b$ and $d \in \operatorname{dom} f$ and $d \in \operatorname{dom} g$. Then $\mathrm{NDentry}(\langle f, g\rangle, \langle a, b\rangle, d)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (22) and (6).

(29) Suppose $\{a, b, c\} \subseteq V$ and a, b, c are mutually different and $d \in \operatorname{dom} f$ and $d \in \operatorname{dom} g$ and $d \in \operatorname{dom} h$. Then $\mathrm{NDentry}(\langle f, g, h\rangle, \langle a, b, c\rangle, d)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (23), (2), (3), (1), and (6).

Let us consider V and A. Let f be a finite sequence. We say that f is (V,A)-FPrg-yielding if and only if

(Def. 6) for every n such that $1 \leqslant n \leqslant \operatorname{len} f$ holds $f(n)$ is a binominative function over simple-named complex-valued nominative data of V and A.

Let us consider f. Let us note that $\langle f\rangle$ is (V,A)-FPrg-yielding.

Let us consider g. Note that $\langle f, g\rangle$ is (V,A)-FPrg-yielding.

Let us consider h. Let us observe that $\langle f, g, h\rangle$ is (V,A)-FPrg-yielding.

Let us consider n. One can verify that there exists a finite sequence which is (V,A)-FPrg-yielding and n-element.

Let us consider x. Let g be a (V,A)-FPrg-yielding finite sequence. One can verify that $g(x)$ is function-like and relation-like and every finite sequence which is (V,A)-FPrg-yielding is also function yielding.

Now we state the propositions:

(30) Let us consider a (V,A)-FPrg-yielding finite sequence g, and a one-to-one finite sequence X. Suppose $\operatorname{dom} g = \operatorname{dom} X$ and d is in doms g. Then $\operatorname{rng} \mathrm{NDentry}(g, X, d) \subseteq \mathrm{ND}_{\mathrm{SC}}(V, A)$.

(31) Let us consider a (V,A)-FPrg-yielding finite sequence g, and a one-to-one, V-valued finite sequence X. Suppose $\operatorname{dom} g = \operatorname{dom} X$ and d is in doms g. Then $\mathrm{NDentry}(g, X, d)$ is a non-atomic nominative data of V and A. The theorem is a consequence of (24), (30), and (6).

Let us consider V, A, and v. The functor $\mathrm{Asg}^{V,A,v}$ yielding a function from $\mathrm{FPrg}(\mathrm{ND}_{\mathrm{SC}}(V, A))$ into $\mathrm{FPrg}(\mathrm{ND}_{\mathrm{SC}}(V, A))$ is defined by

(Def. 7) for every binominative function over simple-named complex-valued nominative data f of V and A, $\operatorname{dom}(it(f)) = \operatorname{dom} f$ and for every nominative data d with simple names from V and complex values from A such that $d \in \mathrm{dom}(\mathit{it}(f))$ holds $\mathit{it}(f)(d) = d\nabla_a^v f(d)$.

Let us consider V, A, v, and f. The functor $\mathrm{Asg}^v(f)$ yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 8) $\mathrm{Asg}^{V,A,v}(f)$.

Let d be a non-atomic nominative data of V and A. One can check that $\mathrm{Asg}^v(f)(d)$ is function-like and relation-like.

Now we state the proposition:

(32) Let us consider a non-atomic nominative data d of V and A. Suppose $v \in V$ and $d \notin A$ and $\Rightarrow v(f(d)) \notin A$ and $d \in \mathrm{dom}\, f$. Then $\mathrm{dom}((\mathrm{Asg}^v(f))(d)) = \mathrm{dom}\, d \cup \{v\}$. The theorem is a consequence of (14).

Let us consider V and A. Let g be a (V,A)-FPrg-yielding finite sequence. Assume $\prod g \neq \emptyset$. Let X be a function. The functor $\mathrm{S_P}(g, X)$ yielding a function from $\mathrm{Pr}(\mathrm{ND_{SC}}(V, A)) \times \prod g$ into $\mathrm{Pr}(\mathrm{ND_{SC}}(V, A))$ is defined by

(Def. 9) for every partial predicate over simple-named complex-valued nominative data p of V and A and for every element x of $\prod g$, $\mathrm{dom}\, \mathit{it}(p, x) = \{d$, where d is a nominative data with simple names from V and complex values from A : $d\nabla_a(\mathrm{NDentry}(g, X, d)) \in \mathrm{dom}\, p$ and d is in doms $g\}$ and for every nominative data d with simple names from V and complex values from A such that d is in doms g holds $\mathit{it}(p, x)(d) \cong p(d\nabla_a(\mathrm{NDentry}(g, X, d)))$.

Let us consider V, A, and p. Let g be a (V,A)-FPrg-yielding finite sequence. Assume $\prod g \neq \emptyset$. Let X be a function and x be an element of $\prod g$. The functor $\mathrm{S_P}(p, x, X)$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 10) $\mathrm{S_P}(g, X)(p, x)$.

Now we state the proposition:

(33) Let us consider a (V,A)-FPrg-yielding finite sequence g. Suppose $\prod g \neq \emptyset$. Let us consider an element x of $\prod g$. Suppose $d \in \mathrm{dom}(\mathrm{S_P}(p, x, X))$. Then

(i) d is in doms g, and

(ii) $\mathrm{S_P}(p, x, X)(d) = p(d\nabla_a(\mathrm{NDentry}(g, X, d)))$.

Let us consider V, A, and v. The functor $\mathrm{S_P^{V,A,v}}$ yielding a function from $\mathrm{Pr}(\mathrm{ND_{SC}}(V, A)) \times \mathrm{FPrg}(\mathrm{ND_{SC}}(V, A))$ into $\mathrm{Pr}(\mathrm{ND_{SC}}(V, A))$ is defined by

(Def. 11) for every partial predicate over simple-named complex-valued nominative data p of V and A and for every binominative function over simple-named complex-valued nominative data f of V and A, $\mathrm{dom}\, \mathit{it}(p, f) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d\nabla_a^v f(d) \in \operatorname{dom} p$ and $d \in \operatorname{dom} f\}$ and for every nominative data d with simple names from V and complex values from A such that $d \in \operatorname{dom} f$ holds $it(p, f)(d) \cong p(d\nabla_a^v f(d))$.

Let us consider V, A, v, p, and f. The functor $\mathrm{S_P}(p, f, v)$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 12) $(\mathrm{S_P}^{V,A,v})(p, f)$.

Now we state the propositions:

(34) If $d \in \operatorname{dom}(\mathrm{S_P}(p, f, v))$, then $\mathrm{S_P}(p, f, v)(d) = p(d\nabla_a^v f(d))$ and $d \in \operatorname{dom} f$.

(35) Let us consider an element x of $\prod\langle f\rangle$. Suppose $v \in V$ and $\prod\langle f\rangle \neq \emptyset$. Then $\mathrm{S_P}(p, f, v) = \mathrm{S_P}(p, x, \langle v\rangle)$. The theorem is a consequence of (26), (33), and (34).

Let us consider V and A. Let g be a (V,A)-FPrg-yielding finite sequence. Assume $\prod g \neq \emptyset$. Let X be a function. The functor $\mathrm{S_F}(g, X)$ yielding a function from $\mathrm{FPrg}(\mathrm{ND_{SC}}(V, A)) \times \prod g$ into $\mathrm{FPrg}(\mathrm{ND_{SC}}(V, A))$ is defined by

(Def. 13) for every binominative function over simple-named complex-valued nominative data f of V and A and for every element x of $\prod g$, $\operatorname{dom} it(f, x) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d\nabla_a(\mathrm{NDentry}(g, X, d)) \in \operatorname{dom} f$ and d is in doms $g\}$ and for every nominative data d with simple names from V and complex values from A such that d is in doms g holds $it(f, x)(d) \cong f(d\nabla_a(\mathrm{NDentry}(g, X, d)))$.

Let us consider V, A, and f. Let g be a (V,A)-FPrg-yielding finite sequence. Assume $\prod g \neq \emptyset$. Let X be a function and x be an element of $\prod g$. The functor $\mathrm{S_F}(f, x, X)$ yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 14) $\mathrm{S_F}(g, X)(f, x)$.

Now we state the proposition:

(36) Let us consider a (V,A)-FPrg-yielding finite sequence g. Suppose $\prod g \neq \emptyset$. Let us consider an element x of $\prod g$. Suppose $d \in \operatorname{dom}(\mathrm{S_F}(f, x, X))$. Then

(i) d is in doms g, and

(ii) $\mathrm{S_F}(f, x, X)(d) = f(d\nabla_a(\mathrm{NDentry}(g, X, d)))$.

Let us consider V, A, and v. The functor $\mathrm{S_F}^{V,A,v}$ yielding a function from $\mathrm{FPrg}(\mathrm{ND_{SC}}(V, A)) \times \mathrm{FPrg}(\mathrm{ND_{SC}}(V, A))$ into $\mathrm{FPrg}(\mathrm{ND_{SC}}(V, A))$ is defined by

(Def. 15) for every binominative functions over simple-named complex-valued nominative date f, g of V and A, $\operatorname{dom} it(f, g) = \{d$, where d is a nominative data with simple names from V and complex values from $A : d\nabla_a^v g(d) \in$

$\operatorname{dom} f$ and $d \in \operatorname{dom} g\}$ and for every nominative data d with simple names from V and complex values from A such that $d \in \operatorname{dom} g$ holds $it(f, g)(d) \cong f(d \nabla_a^v g(d))$.

Let us consider V, A, v, f, and g. The functor $\mathrm{S_F}(f, g, v)$ yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 16) $(\mathrm{S_F}^{V,A,v})(f, g)$.

Now we state the propositions:

(37) If $d \in \operatorname{dom}(\mathrm{S_F}(f, g, v))$, then $\mathrm{S_F}(f, g, v)(d) = f(d \nabla_a^v g(d))$ and $d \in \operatorname{dom} g$.

(38) Let us consider an element x of $\prod\langle g\rangle$. Suppose $v \in V$ and $\prod\langle g\rangle \neq \emptyset$. Then $\mathrm{S_F}(f, g, v) = \mathrm{S_F}(f, x, \langle v\rangle)$. The theorem is a consequence of (26), (36), and (37).

Let us consider V, A, and v. The functor $v!^{V,A}$ yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 17) $\operatorname{dom} it = \mathrm{ND_{SC}}(V, A) \setminus A$ and for every non-atomic nominative data d of V and A such that $d \in \operatorname{dom} it$ holds if $v \Rightarrow_a d \in \operatorname{dom} it$, then $it(d) = \mathit{true}$ and if $v \Rightarrow_a d \notin \operatorname{dom} it$, then $it(d) = \mathit{false}$.

REFERENCES

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Ievgen Ivanov. On the underapproximation of reach sets of abstract continuous-time systems. In Erika Ábrahám and Sergiy Bogomolov, editors, *Proceedings 3rd International Workshop on Symbolic and Numerical Methods for Reachability Analysis, SNR@ETAPS 2017, Uppsala, Sweden, 22nd April 2017*, volume 247 of *EPTCS*, pages 46–51, 2017. doi:10.4204/EPTCS.247.4.

[4] Ievgen Ivanov. On representations of abstract systems with partial inputs and outputs. In T. V. Gopal, Manindra Agrawal, Angsheng Li, and S. Barry Cooper, editors, *Theory and Applications of Models of Computation – 11th Annual Conference, TAMC 2014, Chennai, India, April 11–13, 2014. Proceedings*, volume 8402 of *Lecture Notes in Computer Science*, pages 104–123. Springer, 2014. ISBN 978-3-319-06088-0. doi:10.1007/978-3-319-06089-7_8.

[5] Ievgen Ivanov. On local characterization of global timed bisimulation for abstract continuous-time systems. In Ichiro Hasuo, editor, *Coalgebraic Methods in Computer Science – 13th IFIP WG 1.3 International Workshop, CMCS 2016, Colocated with ETAPS 2016, Eindhoven, The Netherlands, April 2–3, 2016, Revised Selected Papers*, volume 9608 of *Lecture Notes in Computer Science*, pages 216–234. Springer, 2016. ISBN 978-3-319-40369-4. doi:10.1007/978-3-319-40370-0_13.

[6] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. On a decidable formal theory for abstract continuous-time dynamical systems. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014,*

Revised Selected Papers, pages 78–99. Springer International Publishing, 2014. ISBN 978-3-319-13206-8. doi:10.1007/978-3-319-13206-8_4.

[7] Ievgen Ivanov, Mykola Nikitchenko, and Uri Abraham. Event-based proof of the mutual exclusion property of Peterson's algorithm. *Formalized Mathematics*, 23(4):325–331, 2015. doi:10.1515/forma-2015-0026.

[8] 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.

[9] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[10] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On algebras of algorithms and specifications over uninterpreted data. *Formalized Mathematics*, 26(**2**):141–147, 2018. doi:10.2478/forma-2018-0011.

[11] Artur Kornilowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the algebra of nominative data in Mizar. In Maria Ganzha, Leszek A. Maciaszek, and Marcin Paprzycki, editors, *Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, Prague, Czech Republic, September 3–6, 2017.*, pages 237–244, 2017. ISBN 978-83-946253-7-5. doi:10.15439/2017F301.

[12] 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.

[13] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. Formalization of the nominative algorithmic algebra in Mizar. In Jerzy Świątek, Leszek Borzemski, and Zofia Wilimowska, editors, *Information Systems Architecture and Technology: Proceedings of 38th International Conference on Information Systems Architecture and Technology – ISAT 2017: Part II*, pages 176–186. Springer International Publishing, 2018. ISBN 978-3-319-67229-8. doi:10.1007/978-3-319-67229-8_16.

[14] Nikolaj S. Nikitchenko. A composition nominative approach to program semantics. Technical Report IT-TR 1998-020, Department of Information Technology, Technical University of Denmark, 1998.

[15] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 159–164, 2018
DOI: 10.2478/forma-2018-0013

sciendo
https://www.sciendo.com/

An Inference System of an Extension of Floyd-Hoare Logic for Partial Predicates

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. In the paper we give a formalization in the Mizar system [2, 1] of the rules of an inference system for an extended Floyd-Hoare logic with partial pre- and post-conditions which was proposed in [7, 9]. The rules are formalized on the semantic level. The details of the approach used to implement this formalization are described in [5].

We formalize the notion of a semantic Floyd-Hoare triple (for an extended Floyd-Hoare logic with partial pre- and post-conditions) [5] which is a triple of a pre-condition represented by a partial predicate, a program, represented by a partial function which maps data to data, and a post-condition, represented by a partial predicate, which informally means that if the pre-condition on a program's input data is defined and true, and the program's output after a run on this data is defined (a program terminates successfully), and the post-condition is defined on the program's output, then the post-condition is true.

We formalize and prove the soundness of the rules of the inference system [9, 7] for such semantic Floyd-Hoare triples. For reasoning about sequential composition of programs and while loops we use the rules proposed in [3].

The formalized rules can be used for reasoning about sequential programs, and in particular, for sequential programs on nominative data [4]. Application of these rules often requires reasoning about partial predicates representing pre- and post-conditions which can be done using the formalized results on the Kleene algebra of partial predicates given in [8].

MSC: 68Q60 68T37 03B70 03B35

Keywords: Floyd-Hoare logic; Floyd-Hoare triple; inference rule; program verification

MML identifier: `NOMIN_3`, version: `8.1.08 5.53.1335`

From now on v, x denote objects, D, V, A denote sets, n denotes a natural number, p, q denote partial predicates of D, and f, g denote binominative functions of D.

Let us consider D, f, and p. We say that f coincides with p if and only if

(Def. 1) for every element d of D such that $d \in \operatorname{dom} p$ holds $f(d) \in \operatorname{dom} p$.

Let us consider g and q. We say that f and g coincide with p and q if and only if

(Def. 2) for every element d of D such that $d \in \operatorname{rng} f$ and $g(d) \in \operatorname{dom} q$ holds $d \in \operatorname{dom} p$.

Now we state the propositions:

(1) f coincides with $\bot_{\mathrm{PP}}(D)$.

(2) $\mathrm{id}_{\mathrm{PP}}(D)$ coincides with p.

Let us consider D, p, and q. We say that $p \models q$ if and only if

(Def. 3) for every element d of D such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ holds $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$.

Observe that the predicate is reflexive.

In the sequel D denotes a non empty set, d denotes an element of D, f, g denote binominative functions of D, and p, q, r, s denote partial predicates of D.

Now we state the propositions:

(3) If $p \models r$, then $p \wedge q \models r$.

(4) $p \wedge q \models p$.

(5) If $p \models q$ and $r \models s$, then $p \wedge r \models q \wedge s$.

(6) If $p \vee q \models r$, then $p \models r$.

(7) Suppose $p \models q \vee r$. If $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$, then $d \in \operatorname{dom} q$ and $q(d) = \mathit{true}$ or $d \in \operatorname{dom} r$ and $r(d) = \mathit{true}$.

(8) $p \vee p \models p$.

(9) If $p \models q$ and $r \models s$, then $p \vee r \models q \vee s$.

(10) If $p \vee q \models r$, then $p \wedge q \models r$.

Let us consider D. The functor SemanticFloydHoareTriples(D) yielding a set is defined by the term

(Def. 4) $\{\langle p, f, q\rangle$, where p, q are partial predicates of D, f is a binominative function of D : for every element d of D such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}\}$.

We introduce the notation SFHTs(D) as a synonym of SemanticFloydHoareTriples(D).

Now we state the propositions:

(11) Suppose $\langle p, f, q\rangle \in$ SFHTs(D). If $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$, then $q(f(d)) = \mathit{true}$.

(12) $\langle \emptyset, f, p\rangle \in$ SFHTs(D).

Let us consider D. Observe that SFHTs(D) is non empty.

A semantic Floyd-Hoare triple of D is an element of SemanticFloydHoareTriples(D).

An SFHT of D is an element of SFHTs(D). Now we state the propositions:

(13) $\langle p, \mathrm{id}_{\operatorname{dom} p}, p\rangle$ is an SFHT of D.

(14) $\langle p, \mathrm{id}_{\mathrm{field}\, f}, p\rangle$ is an SFHT of D.

(15) CONS$_1$ RULE:
If $\langle p, f, q\rangle$ is an SFHT of D and $r \models p$, then $\langle r, f, q\rangle$ is an SFHT of D. The theorem is a consequence of (11).

(16) CONS$_2$ RULE:
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $q \models r$ and $\operatorname{dom} r \subseteq \operatorname{dom} q$. Then $\langle p, f, r\rangle$ is an SFHT of D. The theorem is a consequence of (11).

(17) SKIP RULE:
$\langle p, \mathrm{id}_{\mathrm{PP}}(D), p\rangle$ is an SFHT of D.

(18) $\langle \mathrm{false}_{\mathrm{PP}}(D), f, p\rangle$ is an SFHT of D.

(19) INVERSION RULE:
If p is total, then $\langle \sim p, f, q\rangle$ is an SFHT of D. The theorem is a consequence of (18) and (15).

(20) COMPOSITION RULE:
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $\langle q, g, r\rangle$ is an SFHT of D and f and g coincide with q and r. Then $\langle p, f \bullet g, r\rangle$ is an SFHT of D.
PROOF: Set $F = f \bullet g$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} r$ holds $r(F(d)) = \mathit{true}$. □

(21) IF RULE:
Suppose $\langle r \wedge p, f, q\rangle$ is an SFHT of D and $\langle \neg r \wedge p, g, q\rangle$ is an SFHT of D. Then $\langle p, \mathrm{IF}(r, f, g), q\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{IF}(r, f, g)$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. □

(22) If f coincides with p and $\langle p, f, p\rangle$ is an SFHT of D, then $\langle p, f^n, p\rangle$ is an SFHT of D.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \langle p, f^{\$_1}, p\rangle$ is an SFHT of D. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. For every natural

number k, $\mathcal{P}[k]$. □

(23) WHILE RULE:
Suppose f coincides with p and $\operatorname{dom} p \subseteq \operatorname{dom} f$ and $\langle r \wedge p, f, p\rangle$ is an SFHT of D. Then $\langle p, \mathrm{WH}(r, f), \neg r \wedge p\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{WH}(r, f)$. Set $q = \neg r \wedge p$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. □

(24) UNCONDITIONAL COMPOSITION RULE (USEQ):
Suppose $\langle p, f, q\rangle$ is an SFHT of D and $\langle q, g, r\rangle$ is an SFHT of D and $\langle \sim q, g, s\rangle$ is an SFHT of D. Then $\langle p, f \bullet g, r \vee s\rangle$ is an SFHT of D.
PROOF: Set $F = f \bullet g$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom}(r \vee s)$ holds $(r \vee s)(F(d)) = \mathit{true}$. □

(25) UNCONDITIONAL WHILE RULE (UWH):
Suppose $\langle r \wedge p, f, p\rangle$ is an SFHT of D and $\langle r \wedge \sim p, f, p\rangle$ is an SFHT of D. Then $\langle p, \mathrm{WH}(r, f), \neg r \wedge p\rangle$ is an SFHT of D.
PROOF: Set $F = \mathrm{WH}(r, f)$. Set $q = \neg r \wedge p$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. □

(26) DP RULE:
Suppose $\langle p, f, r\rangle$ is an SFHT of D and $\langle q, f, r\rangle$ is an SFHT of D. Then $\langle p \vee q, f, r\rangle$ is an SFHT of D.
PROOF: Set $P = p \vee q$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} r$ holds $r(f(d)) = \mathit{true}$. □

In the sequel p, q denote partial predicates over simple-named complex-valued nominative date of V and A, f, g denote binominative functions over simple-named complex-valued nominative date of V and A, E denotes a (V,A)-FPrg-yielding finite sequence, e denotes an element of $\prod E$, and d denotes a nominative data with simple names from V and complex values from A.

Now we state the proposition:

(27) Suppose for every nominative data d with simple names from V and complex values from A such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}$. Then $\langle p, f, q\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: For every element d of $\mathrm{ND}_{\mathrm{SC}}(V, A)$ such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} f$ and $f(d) \in \operatorname{dom} q$ holds $q(f(d)) = \mathit{true}$. □

(28) ASSIGNMENT RULE:
$\langle \mathrm{S}_{\mathrm{P}}(p, f, v), \mathrm{Asg}^{v}(f), p\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.
PROOF: Set $P = \mathrm{S}_{\mathrm{P}}(p, f, v)$. Set $F = \mathrm{Asg}^{v}(f)$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} p$ holds

$p(F(d)) = \mathit{true}$ by [6, 34]. □

(29) SFID$_1$ rule:
$\langle \mathrm{S_P}(p,f,v), \mathrm{S_F}(\mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A)),f,v),p\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$.
Proof: Set $I = \mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A))$. Set $P = \mathrm{S_P}(p,f,v)$. Set $F = \mathrm{S_F}(I,f,v)$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} p$ holds $p(F(d)) = \mathit{true}$. □

(30) SFID rule:
Suppose $\prod E \neq \emptyset$. Then $\langle \mathrm{S_P}(p,e,E), \mathrm{S_F}(\mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A)),e,E),p\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$.
Proof: Set $I = \mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A))$. Set $P = \mathrm{S_P}(p,e,E)$. Set $F = \mathrm{S_F}(I,e,E)$. For every d such that $d \in \operatorname{dom} P$ and $P(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} p$ holds $p(F(d)) = \mathit{true}$. □

(31) SF$_1$ rule:
Suppose $\langle p, \mathrm{S_F}(\mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A)),g,v) \bullet f,q\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$. Then $\langle p, \mathrm{S_F}(f,g,v),q\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$.
Proof: Set $I = \mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A))$. Set $F = \mathrm{S_F}(f,g,v)$. Set $G = \mathrm{S_F}(I,g,v)$. Set $C = G \bullet f$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} C$ and $C(d) \in \operatorname{dom} q$ holds $q(C(d)) = \mathit{true}$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. □

(32) SF rule:
Suppose $\prod E \neq \emptyset$ and $\langle p, \mathrm{S_F}(\mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A)),e,E) \bullet f,q\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$. Then $\langle p, \mathrm{S_F}(f,e,E),q\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V,A)$.
Proof: Set $I = \mathrm{id_{PP}}(\mathrm{ND_{SC}}(V,A))$. Set $F = \mathrm{S_F}(f,e,E)$. Set $G = \mathrm{S_F}(I,e,E)$. Set $C = G \bullet f$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} C$ and $C(d) \in \operatorname{dom} q$ holds $q(C(d)) = \mathit{true}$. For every d such that $d \in \operatorname{dom} p$ and $p(d) = \mathit{true}$ and $d \in \operatorname{dom} F$ and $F(d) \in \operatorname{dom} q$ holds $q(F(d)) = \mathit{true}$. □

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Ievgen Ivanov and Mykola Nikitchenko. On the sequence rule for the Floyd-Hoare logic with partial pre- and post-conditions. In *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kyiv, Ukraine, May 14–17, 2018*, volume 2104 of *CEUR Workshop Proceedings*, pages 716–724, 2018.

[4] 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.

[5] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[6] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On an algorithmic algebra over simple-named complex-valued nominative data. *Formalized Mathematics*, 26(2):149–158, 2018. doi:10.2478/forma-2018-0012.

[7] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchenko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[8] 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.

[9] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. Extending Floyd-Hoare logic for partial pre- and postconditions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 9th International Conference, ICTERI 2013, Kherson, Ukraine, June 19–22, 2013, Revised Selected Papers*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 165–173, 2018
DOI: 10.2478/forma-2018-0014

sciendo
https://www.sciendo.com/

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. In this paper we present a formalization in the Mizar system [2, 1] of the correctness of the subtraction-based version of Euclid's algorithm computing the greatest common divisor of natural numbers. The algorithm is written in terms of simple-named complex-valued nominative data [11, 4].

The validity of the algorithm is presented in terms of semantic Floyd-Hoare triples over such data [7]. Proofs of the correctness are based on an inference system for an extended Floyd-Hoare logic with partial pre- and post-conditions [8, 10, 5, 3].

MSC: 68Q60 68T37 03B70 03B35

Keywords: greatest common divisor; nominative data; program verification

MML identifier: NOMIN_4, version: 8.1.08 5.53.1335

From now on v denotes an object, V, A denote sets, and f denotes a binominative function over simple-named complex-valued nominative data of V and A.

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

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

One can verify 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 not $\mathcal{P}[x, y]$, 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 not $\mathcal{P}[x, y]$, then $f(x, y) = \mathit{false}$ and for every objects x, y such that x, $y \in \mathcal{Y}$ holds if $\mathcal{P}[x, y]$, then $g(x, y) = \mathit{true}$ and if not $\mathcal{P}[x, y]$, 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 $d \in$ nonatomicsND(V, A). Then d is a non-atomic nominative data of V and A.

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

Let us consider V and A. One can verify that nonatomicsND(V, A) is non empty and functional.

We say that V is without nonatomic nominative data w.r.t. A if and only if

(Def. 3) A misses nonatomicsND(V, A).

Now we state the propositions:

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

(4) Suppose V is without nonatomic nominative data w.r.t. A 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 V is without nonatomic nominative data w.r.t. A. Let us consider a non-atomic nominative data d of V and A. Suppose $v \in V$ and $d \in \mathrm{dom}\, f$. Then $\mathrm{dom}((\mathrm{Asg}^v(f))(d)) = \mathrm{dom}\, d \cup \{v\}$. 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.

(6) Let us consider a non-atomic nominative data d_1 of V and A. Suppose $v \in V$ and V is without nonatomic nominative data w.r.t. A. 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 partial predicates over simple-named complex-valued nominative date of V and A.

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

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

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

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

We say that d is a value on a 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, d is a complex on a, then for every d, d is a value on a.

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

(9) If for every d, d is a value on a and for every d, d is a value on b, then $\mathrm{rng}\langle a \Rightarrow_a, b \Rightarrow_a \rangle \subseteq A \times A$. 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 partial predicate over simple-named complex-valued nominative data of V and 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 binominative function over simple-named complex-valued nominative data of V and 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 $it(a, b) = true$ and if $a \neq b$, then $it(a, b) = false$.

Let us consider V. Let x, y be elements of V. The functor Equality(A, x, y) yielding a partial predicate over simple-named complex-valued nominative data of V and A is defined by the term

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

Let x, y be objects. We say that x is less than 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. If x is not less than y, then y is less than x or $x = y$.

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 is less than y, then $it(x, y) = true$ and if x is not less than 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 partial predicate over simple-named complex-valued nominative data of V and 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, d is a value on a and for every d, d is a value on b. Then $\mathrm{dom}(\mathrm{Equality}(A, a, b)) = \mathrm{dom}(a \Rightarrow_a) \cap \mathrm{dom}(b \Rightarrow_a)$. The theorem is a consequence of (9).

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

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

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

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

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

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 subtraction A 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 subtraction(A, x, y) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 16) lift-binary-op(subtraction $A, x, y)$.

Let us consider a and b. The functor gcd-conditional-step(V, A, a, b) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 17) $\mathrm{IF}(\mathrm{less}(A, b, a), \mathrm{Asg}^{a}(\mathrm{subtraction}(A, a, b)), \mathrm{id}_{\mathrm{PP}}(\mathrm{ND}_{\mathrm{SC}}(V, A)))$.

The functor gcd-loop-body(V, A, a, b) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 18) gcd-conditional-step$(V, A, a, b) \bullet$ gcd-conditional-step(V, A, b, a).

The functor gcd-main-loop(V, A, a, b) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

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

Let us consider x and y. The functor gcd-var-init(V, A, a, b, x, y) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 20) $\mathrm{Asg}^{a}(x \Rightarrow_{a}) \bullet \mathrm{Asg}^{b}(y \Rightarrow_{a})$.

The functor gcd-main-part(V, A, a, b, x, y) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 21) gcd-var-init$(V, A, a, b, x, y) \bullet$ gcd-main-loop(V, A, a, b).

Let us consider z. The functor gcd-program(V, A, a, b, x, y, z) yielding a binominative function over simple-named complex-valued nominative data of V and A is defined by the term

(Def. 22) gcd-main-part$(V, A, a, b, x, y) \bullet \mathrm{Asg}^{z}(a \Rightarrow_{a})$.

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 x_0, y_0 and d constitute a valid input for the gcd w.r.t. V, A, x and y 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, $y \in \operatorname{dom} d_1$ 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 partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 24) dom *it* = $\mathrm{ND_{SC}}(V, A)$ and for every object d such that $d \in \mathrm{dom}\, it$ holds if x_0, y_0 and d constitute a valid input for the gcd w.r.t. V, A, x and y, then $it(d) =$ *true* and if x_0, y_0 and d do not constitute a valid input for the gcd w.r.t. V, A, x and y, then $it(d) =$ *false*.

One can check 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 x_0, y_0 and d constitute a valid output for the gcd w.r.t. V, A and z 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 partial predicate over simple-named complex-valued nominative data of V and A is defined by

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

Let us consider a and b. Let d be an object. We say that x_0, y_0 and d constitute a valid invariant for the gcd w.r.t. V, A, a and b 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, $b \in \mathrm{dom}\, d_1$ 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 partial predicate over simple-named complex-valued nominative data of V and A is defined by

(Def. 28) dom *it* = $\mathrm{ND_{SC}}(V, A)$ and for every object d such that $d \in \mathrm{dom}\, it$ holds if x_0, y_0 and d constitute a valid invariant for the gcd w.r.t. V, A, a and b, then $it(d) =$ *true* and if x_0, y_0 and d do not constitute a valid invariant for the gcd w.r.t. V, A, a and b, then $it(d) =$ *false*.

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

Now we state the propositions:

(15) $\langle \sim \mathrm{S_P}(p, x \Rightarrow_a, a), \mathrm{Asg}^a(x \Rightarrow_a), p\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$.

(16) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A 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 an SFHT of $\mathrm{ND_{SC}}(V, A)$.
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 $Q = \mathrm{S_P}(p, D_4, b)$. Set $P = \mathrm{S_P}(Q, D_3, a)$. Set $G = \mathrm{Asg}^b(D_4)$. Set $I =$ valid-gcd-input(V, A, x, y, x_0, y_0). $\langle \sim Q, G, p\rangle$ is an SFHT of $\mathrm{ND_{SC}}(V, A)$. $I \models P$. □

(17) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b.
Then $\langle \text{less}(A, b, a) \wedge \text{gcd-inv}(V, A, a, b, x_0, y_0), \text{Asg}^a(\text{subtraction}(A, a, b)), \text{gcd-inv}(V, A, a, b, x_0, y_0)\rangle$ is an SFHT of $\text{ND}_{\text{SC}}(V, A)$.
Proof: Set $i = \text{gcd-inv}(V, A, a, b, x_0, y_0)$. Set $l = \text{less}(A, b, a)$. Set $D = \text{subtraction}(A, a, b)$. Set $f = \text{Asg}^a(D)$. 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 $i(f(d)) = \mathit{true}$. □

(18) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b.
Then $\langle \text{less}(A, a, b) \wedge \text{gcd-inv}(V, A, a, b, x_0, y_0), \text{Asg}^b(\text{subtraction}(A, b, a)), \text{gcd-inv}(V, A, a, b, x_0, y_0)\rangle$ is an 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 $D = \text{subtraction}(A, b, a)$. Set $f = \text{Asg}^b(D)$. 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 [6, (23)], [9, (9),(10)]. □

(19) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b.
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 an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (17).

(20) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b.
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 an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (18).

(21) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b. 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 an SFHT of $\text{ND}_{\text{SC}}(V, A)$. The theorem is a consequence of (19) and (20).

(22) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b.
Then $\langle \sim \text{gcd-inv}(V, A, a, b, x_0, y_0), \text{gcd-loop-body}(V, A, a, b), \text{gcd-inv}$

$(V, A, a, b, x_0, y_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (20).

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

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

(25) Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and for every d, d is a value on a and for every d, d is a value on b. Then $\langle$Equality$(A, a, b) \wedge$ gcd-inv(V, A, a, b, x_0, y_0), $\mathrm{Asg}^z(a \Rightarrow_a)$, valid-gcd-output$(V, A, z, x_0, y_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$.

PROOF: Set $D_1 = a \Rightarrow_a$. Set $q =$ Equality$(A, a, b) \wedge$gcd-inv(V, A, a, b, x_0, y_0). Set $r =$ valid-gcd-output(V, A, z, x_0, y_0). Set $s_3 = \mathrm{S}_{\mathrm{P}}(r, D_1, z)$. $q \models s_3$. □

(26) PARTIAL CORRECTNESS OF GCD ALGORITHM:
Suppose V is not empty and V is without nonatomic nominative data w.r.t. A and $a \neq b$ and $a \neq y$ and A is complex containing and for every d, d is a complex on a and for every d, d is a complex on b. Then $\langle$valid-gcd-input(V, A, x, y, x_0, y_0), gcd-program(V, A, a, b, x, y, z), valid-gcd-output$(V, A, z, x_0, y_0)\rangle$ is an SFHT of $\mathrm{ND}_{\mathrm{SC}}(V, A)$. The theorem is a consequence of (7), (24), (25), and (11).

REFERENCES

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[3] Ievgen Ivanov and Mykola Nikitchenko. On the sequence rule for the Floyd-Hoare logic with partial pre- and post-conditions. In *Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume II: Workshops, Kyiv, Ukraine, May 14–17, 2018*, volume 2104 of *CEUR Workshop Proceedings*, pages 716–724, 2018.

[4] 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.

[5] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. Implementation of the

composition-nominative approach to program formalization in Mizar. *The Computer Science Journal of Moldova*, 26(1):59–76, 2018.

[6] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. On an algorithmic algebra over simple-named complex-valued nominative data. *Formalized Mathematics*, 26(2):149–158, 2018. doi:10.2478/forma-2018-0012.

[7] Ievgen Ivanov, Artur Korniłowicz, and Mykola Nikitchenko. An inference system of an extension of Floyd-Hoare logic for partial predicates. *Formalized Mathematics*, 26(**2**): 159–164, 2018. doi:10.2478/forma-2018-0013.

[8] Artur Korniłowicz, Andrii Kryvolap, Mykola Nikitchenko, and Ievgen Ivanov. An approach to formalization of an extension of Floyd-Hoare logic. In Vadim Ermolayev, Nick Bassiliades, Hans-Georg Fill, Vitaliy Yakovyna, Heinrich C. Mayr, Vyacheslav Kharchenko, Vladimir Peschanenko, Mariya Shyshkina, Mykola Nikitchenko, and Aleksander Spivakovsky, editors, *Proceedings of the 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15–18, 2017*, volume 1844 of *CEUR Workshop Proceedings*, pages 504–523. CEUR-WS.org, 2017.

[9] 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.

[10] Andrii Kryvolap, Mykola Nikitchenko, and Wolfgang Schreiner. Extending Floyd-Hoare logic for partial pre- and postconditions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications: 9th International Conference, ICTERI 2013, Kherson, Ukraine, June 19–22, 2013, Revised Selected Papers*, pages 355–378. Springer International Publishing, 2013. ISBN 978-3-319-03998-5. doi:10.1007/978-3-319-03998-5_18.

[11] Volodymyr G. Skobelev, Mykola Nikitchenko, and Ievgen Ivanov. On algebraic properties of nominative data and functions. In Vadim Ermolayev, Heinrich C. Mayr, Mykola Nikitchenko, Aleksander Spivakovsky, and Grygoriy Zholtkevych, editors, *Information and Communication Technologies in Education, Research, and Industrial Applications – 10th International Conference, ICTERI 2014, Kherson, Ukraine, June 9–12, 2014, Revised Selected Papers*, volume 469 of *Communications in Computer and Information Science*, pages 117–138. Springer, 2014. ISBN 978-3-319-13205-1. doi:10.1007/978-3-319-13206-8_6.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 175–181, 2018
DOI: 10.2478/forma-2018-0015

sciendo
https://www.sciendo.com/

Basic Diophantine Relations[1]

Marcin Acewicz
Institute of Informatics
University of Białystok
Poland

Karol Pąk
Institute of Informatics
University of Białystok
Poland

Summary. The main purpose of formalization is to prove that two equations $\mathtt{y}_a(z) = y$, $y = x^z$ are Diophantine. These equations are explored in the proof of Matiyasevich's negative solution of Hilbert's tenth problem.

In our previous work [6], we showed that from the diophantine standpoint these equations can be obtained from lists of several basic Diophantine relations as linear equations, finite products, congruences and inequalities. In this formalization, we express these relations in terms of Diophantine set introduced in [7]. We prove that these relations are Diophantine and then we prove several second-order theorems that provide the ability to combine Diophantine relation using conjunctions and alternatives as well as to substitute the right-hand side of a given Diophantine equality as an argument in a given Diophantine relation. Finally, we investigate the possibilities of our approach to prove that the two equations, being the main purpose of this formalization, are Diophantine.

The formalization by means of Mizar system [3], [2] follows Z. Adamowicz, P. Zbierski [1] as well as M. Davis [4].

MSC: 11D45 03B35 68T99

Keywords: Hilbert's 10th problem; Diophantine relations

MML identifier: `HILB10_3`, version: `8.1.08 5.52.1328`

1. Preliminaries

From now on n, m, k denote natural numbers, p, q denote n-element finite 0-sequences of $\mathbb{N}$, i_1, i_2, i_3, i_4, i_5, i_6 denote elements of n, and a, b, c, d, e denote integers.

[1] This work has been financed by the resources of the Polish National Science Centre granted by decision no. DEC-2015/19/D/ST6/01473.

Let X be a set, p be a $\mathbb{Z}$-valued series of X, $\mathbb{R}_{\rm F}$, and a be an integer element of $\mathbb{R}_{\rm F}$. Observe that $a \cdot p$ is $\mathbb{Z}$-valued.

Now we state the propositions:

(1) Let us consider a non empty ordinal number O, an element i of O, an add-associative, right zeroed, right complementable, well unital, distributive, non trivial double loop structure L, and a function x from O into L. Then $\mathrm{eval}(1\_1(i, L), x) = x(i)$.

(2) i_1 is an element of $n + k$.

(3) If $k < m$, then $n + k \in n + m$.

(4) Let us consider an $(n + k)$-element finite 0-sequence p. If $n \neq 0$ and $k \neq 0$, then $(p{\restriction}n)(i_1) = p(i_1)$.

2. Basic Diophantine Relations

Now we state the propositions:

(5) Let us consider a diophantine subset A of the n-xtuples of $\mathbb{N}$, and k. Suppose $k \leqslant n$. Then $\{p{\restriction}k : p \in A\}$ is a diophantine subset of the k-xtuples of $\mathbb{N}$.

Proof: Consider k_1 being a natural number, Q being a $\mathbb{Z}$-valued polynomial of $n + k_1$,$\mathbb{R}_{\rm F}$ such that for every object s, $s \in A$ iff there exists an n-element finite 0-sequence x of $\mathbb{N}$ and there exists a k_1-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\mathrm{eval}(Q, {}^{@}(x \frown y)) = 0$.

Set $D = \{p{\restriction}k$, where p is an n-element finite 0-sequence of $\mathbb{N} : p \in A\}$. $D \subseteq$ the k-xtuples of $\mathbb{N}$. Reconsider $k_2 = n - k$ as a natural number. Reconsider $P = Q$ as a $\mathbb{Z}$-valued polynomial of $k + (k_2 + k_1)$,$\mathbb{R}_{\rm F}$. For every object s, $s \in D$ iff there exists a k-element finite 0-sequence x of $\mathbb{N}$ and there exists a $(k_2 + k_1)$-element finite 0-sequence y of $\mathbb{N}$ such that $s = x$ and $\mathrm{eval}(P, {}^{@}(x \frown y)) = 0$ by [5, (13)], [8, (54),(17),(27)]. □

(6) Let us consider integers a, b, c, i_1, and i_2. Then $\{p : a \cdot p(i_1) = b \cdot p(i_2) + c\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (1).

(7) $\{p : a \cdot p(i_1) > b \cdot p(i_2) + c\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (2) and (1).

The scheme *UnionDiophantine* deals with a natural number n and a unary predicate $\mathcal{P}$, $\mathcal{Q}$ and states that

(Sch. 1) $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N}$: $\mathcal{P}[p]$ or $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$

provided

- $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$ and

- $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

The scheme *Eq* deals with a natural number n and a unary predicate $\mathcal{P}$, $\mathcal{Q}$ and states that

(Sch. 2) $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]\} = \{q$, where q is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{Q}[q]\}$

provided

- for every n-element finite 0-sequence p of $\mathbb{N}$, $\mathcal{P}[p]$ iff $\mathcal{Q}[p]$.

Now we state the propositions:

(8) $\{p : a \cdot p(i_1) \geqslant b \cdot p(i_2) + c\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
Proof: Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) + c$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) = b \cdot \$_1(i_2) + c$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}[\$_1]$ or $\mathcal{Q}[\$_1]$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) \geqslant b \cdot \$_1(i_2) + c$. $\{p : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{P}[p]$ or $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{R}[p]\} = \{q : \mathcal{S}[q]\}$. □

(9) $\{p : a \cdot p(i_1) = b \cdot p(i_2) \cdot p(i_3)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (1).

(10) $\{p :$ there exists a natural number z such that $a \cdot p(i_1) = b \cdot p(i_2) + z \cdot c \cdot p(i_3)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (2) and (1).

The scheme *IntersectionDiophantine* deals with a natural number n and a unary predicate $\mathcal{P}$, $\mathcal{Q}$ and states that

(Sch. 3) $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]$ and $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$

provided

- $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$ and

- $\{p$, where p is an n-element finite 0-sequence of $\mathbb{N} : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

The scheme *Substitution* deals with a 6-ary predicate $\mathcal{P}$ and a ternary functor $\mathcal{F}$ yielding a natural object and states that

(Sch. 4) For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5)), p(i_3), p(i_4), p(i_5)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$

provided

- for every i_1, i_2, i_3, i_4, i_5, and i_6, $\{p : \mathcal{P}[p(i_1), p(i_2), p(i_3), p(i_4), p(i_5), p(i_6)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$ and
- for every i_1, i_2, i_3, and i_4, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = p(i_4)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

The scheme *SubstitutionInt* deals with a ternary predicate $\mathcal{P}$ and a ternary functor $\mathcal{F}$ yielding an integer and states that

(Sch. 5) For every i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$

provided

- for every i_1, i_2, i_3, and a, $\{p : \mathcal{P}[p(i_1), p(i_2), a \cdot p(i_3)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$ and
- for every i_1, i_2, i_3, i_4, and a, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = a \cdot p(i_4)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

Now we state the propositions:

(11) $\{p : a \cdot p(i_1) = b \cdot p(i_2) + c \cdot p(i_3) + d\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (1).

(12) $\{p : p(i_1) = a \cdot p(i_2)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (6).

(13) $\{p : a \cdot p(i_1) = b\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Set $i_2 =$ the element of n. Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $a \cdot \$_1(i_1) = b$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) = 0 \cdot \$_1(i_2) + b$. $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$. □

(14) $\{p : p(i_1) = a\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Set $i_2 =$ the element of n. Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $\$_1(i_1) = a$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i_1) = 0 \cdot \$_1(i_2) + a$. $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$. □

(15) $\{p : p(i_1) = a \cdot p(i_2) + b\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv \$_1(i_1) = a \cdot \$_1(i_2) + b$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv 1 \cdot \$_1(i_1) = a \cdot \$_1(i_2) + b$. $\{p : \mathcal{P}[p]\} = \{q : \mathcal{Q}[q]\}$. □

(16) $\{p : a \cdot p(i_1) \neq b \cdot p(i_2) + c\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) + c$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) + -c < b \cdot \$_1(i_2)$. Define $\mathcal{R}$[finite

0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}[\$_1]$ or $\mathcal{Q}[\$_1]$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ $a \cdot \$_1(i_1) \neq b \cdot \$_1(i_2) + c$. $\{p : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{P}[p]$ or $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\mathcal{R}[p]$ iff $\mathcal{S}[p]$. $\{p : \mathcal{R}[p]\} = \{q : \mathcal{S}[q]\}$. □

(17) $\{p : a \cdot p(i_1) > b \cdot p(i_2) \cdot p(i_3)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Define $\mathcal{P}$[natural number, natural number, integer] $\equiv a \cdot \$_1 > \$_3 + 0$. Define $\mathcal{F}$(natural number, natural number, natural number) $= b \cdot \$_2 \cdot \$_3$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) \cdot \$_1(i_3) + 0$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) > b \cdot \$_1(i_2) \cdot \$_1(i_3)$.

For every n, i_1, i_2, i_3, and c, $\{p : \mathcal{P}[p(i_1), p(i_2), c \cdot p(i_3)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, i_2, i_3, i_4, and c, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = c \cdot p(i_4)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$. □

Let us consider a, b, c, i_1, i_2, and i_3. Now we state the propositions:

(18) $\{p : a \cdot p(i_1) < b \cdot p(i_2) + c \cdot p(i_3)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Define $\mathcal{P}$[natural number, natural number, integer] $\equiv a \cdot \$_1 + 0 < \$_3$. Define $\mathcal{F}$(natural number, natural number, natural number) $= b \cdot \$_2 + c \cdot \$_3 + 0$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) + 0 < b \cdot \$_1(i_2) + c \cdot \$_1(i_3) + 0$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) < b \cdot \$_1(i_2) + c \cdot \$_1(i_3)$. For every n, i_1, i_2, i_3, and d, $\{p : \mathcal{P}[p(i_1), p(i_2), d \cdot p(i_3)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

For every n, i_1, i_2, i_3, i_4, and d, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = d \cdot p(i_4)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\} = \{q : \mathcal{R}[q]\}$. □

(19) $\{p : a \cdot p(i_1) = b \cdot p(i_2) -' c \cdot p(i_3)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

Proof: Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) = b \cdot \$_1(i_2) + (-c) \cdot \$_1(i_3) + 0$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv b \cdot \$_1(i_2) \geqslant c \cdot \$_1(i_3) + 0$. Define $\mathcal{R}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) = 0 \cdot \$_1(i_2) \cdot \$_1(i_3)$. Define $\mathcal{S}$[finite 0-sequence of $\mathbb{N}$] $\equiv b \cdot \$_1(i_2) + 0 < c \cdot \$_1(i_3)$. Define $\mathcal{U}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{P}[\$_1]$ and $\mathcal{Q}[\$_1]$. $\{p : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{P}[p]$ and $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.

Define $\mathcal{W}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{R}[\$_1]$ and $\mathcal{S}[\$_1]$. $\{p : \mathcal{R}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{S}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{R}[p]$ and $\mathcal{S}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{V}$[finite 0-sequence of $\mathbb{N}$] $\equiv \mathcal{U}[\$_1]$ or $\mathcal{W}[\$_1]$. Define $\mathcal{T}$[finite 0-sequence of $\mathbb{N}$] $\equiv a \cdot \$_1(i_1) = b \cdot \$_1(i_2) -' c \cdot \$_1(i_3)$. $\{p : \mathcal{U}[p]$ or $\mathcal{W}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\mathcal{V}[p]$ iff $\mathcal{T}[p]$. $\{p : \mathcal{V}[p]\} = \{q : \mathcal{T}[q]\}$. □

(20) $\{p : a \cdot p(i_1) = b \cdot p(i_2) -' c\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Define $\mathcal{P}$[natural number, natural number, integer] $\equiv a \cdot \$_1 = b \cdot \$_2 -' \$_3$. For every n, i_1, i_2, i_3, and d, $\{p : \mathcal{P}[p(i_1), p(i_2), d \cdot p(i_3)]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. Define $\mathcal{F}$(natural number, natural number, natural number) $= c$. For every n, i_1, i_2, i_3, i_4, and d, $\{p : \mathcal{F}(p(i_1), p(i_2), p(i_3)) = d \cdot p(i_4)\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. For every n, i_1, i_2, i_3, i_4, and i_5, $\{p : \mathcal{P}[p(i_1), p(i_2), \mathcal{F}(p(i_3), p(i_4), p(i_5))]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. □

(21) $\{p : a \cdot p(i_1) \equiv b \cdot p(i_2) \pmod{c \cdot p(i_3)}\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$.
PROOF: Define $\mathcal{P}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ there exists a natural number z such that $a \cdot \$_1(i_1) = b \cdot \$_1(i_2) + z \cdot c \cdot \$_1(i_3)$. Define $\mathcal{Q}$[finite 0-sequence of $\mathbb{N}$] $\equiv$ there exists a natural number z such that $b \cdot \$_1(i_2) = a \cdot \$_1(i_1) + z \cdot c \cdot \$_1(i_3)$. $\{p : \mathcal{P}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. $\{p : \mathcal{P}[p]$ or $\mathcal{Q}[p]\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. Set $P = \{p : a \cdot p(i_1) \equiv b \cdot p(i_2) \pmod{c \cdot p(i_3)}\}$. $P \subseteq \{p : \mathcal{P}[p]$ or $\mathcal{Q}[p]\}$. $\{p : \mathcal{P}[p]$ or $\mathcal{Q}[p]\} \subseteq P$. □

(22) $\{p : \langle a \cdot p(i_1), b \cdot p(i_2) \rangle$ is Pell's solution of $(c \cdot p(i_3))^{\mathbf{2}} -' 1\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (2), (3), (9), (20), (6), (5), and (4).

3. Main Lemmas

Let us consider i_1, i_2, and i_3. Now we state the propositions:

(23) $\{p : p(i_1) = \mathrm{y}_{p(i_2)}(p(i_3))$ and $p(i_2) > 1\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (2), (3), (7), (22), (8), (21), (14), (12), (9), (5), and (4).

(24) $\{p : p(i_2) = p(i_1)^{p(i_3)}\}$ is a diophantine subset of the n-xtuples of $\mathbb{N}$. The theorem is a consequence of (2), (3), (14), (7), (6), (9), (23), (17), (8), (18), (5), and (4).

References

[1] Zofia Adamowicz and Paweł Zbierski. *Logic of Mathematics: A Modern Course of Classical Logic*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley-Interscience, 1997.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[4] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly, Mathematical Association of America*, 80(3):233–269, 1973. doi:10.2307/2318447.

[5] Yatsuka Nakamura and Hisashi Ito. Basic properties and concept of selected subsequence of zero based finite sequences. *Formalized Mathematics*, 16(**3**):283–288, 2008. doi:10.2478/v10037-008-0034-y.

[6] Karol Pąk. The Matiyasevich theorem. Preliminaries. *Formalized Mathematics*, 25(**4**): 315–322, 2017. doi:10.1515/forma-2017-0029.

[7] Karol Pąk. Diophantine sets. Preliminaries. *Formalized Mathematics*, 26(**1**):81–90, 2018. doi:10.2478/forma-2018-0007.

[8] Tetsuya Tsunetou, Grzegorz Bancerek, and Yatsuka Nakamura. Zero-based finite sequences. *Formalized Mathematics*, 9(**4**):825–829, 2001.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. **26**, No. **2**, Pages 183–191, **2018**
DOI: 10.2478/forma-2018-0016

https://www.sciendo.com/

Formalizing Two Generalized Approximation Operators

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Michał Sielwiesiuk
Institute of Informatics
University of Białystok
Poland

Summary. Rough sets, developed by Pawlak [15], are important tool to describe situation of incomplete or partially unknown information. In this article we give the formal characterization of two closely related rough approximations, along the lines proposed in a paper by Gomolińska [2]. We continue the formalization of rough sets in Mizar [1] started in [6].

MSC: 03E99 03B35 68T99

Keywords: rough approximation; rough set; generalized approximation operator

MML identifier: ROUGHS_5, version: 8.1.08 5.53.1335

0. Introduction

In the paper [9] published in 2010 we discussed some pros and cons of various approaches to rough operators dealing with some of the issues raised by Anna Gomolińska [2]. Even if our chosen formal framework [6] faithfully reflected Pawlak's ideas [15], also possibility of other views for the same topic was quite tempting. Our question was if the Mizar Mathematical Library is ready to do some formal reasoning without much additional work needed to bridge the gap between informal knowledge and its formal countepart present in the repository of automatically verified mathematical knowledge. This expectation is not really that trivial as we noted after an unsatisfactory – at least from our point of view – attempt to formalize Rough Concept Analysis in Mizar [12]. On the other hand, reuse of lattice theory to develop a rough framework [4] according to Järvinen

[13] or bulding a theory of approximations based on pure set theory in style of [16], [17] showed the usefulness of automated theorem proving methods [3] in order to obtain new results, with possibility of theory merging, taking care of possible duplications [11].

Our main aim was to use the existing implementation of rough sets in Mizar to provide the formal proof of the following theorem (original notation of [2]):

> **Theorem 4.1** For any sets $x, y \subseteq U$, objects $u, w \in U$, and $i = 0, 1$, it holds that:
>
> 1. $f_0^d \leqslant id \leqslant f_0$.
> 2. $f_1^d \leqslant id \leqslant f_1$.
> 3. $f_0(x)$ is definable.
> 4. $\forall_u \in f_1(x).\kappa(I(u), x) > 0$.
> 5. $\forall_u \in f_1^d(x).\kappa(I(u), x) = 1$.
> 6. If $\tau(u) = \tau(w)$, then $u \in f_0(x)$ iff $w \in f_0(x)$; and similarly for f_0^d.
> 7. If $I(u) = I(w)$, then $u \in f_1(x)$ iff $w \in f_1(x)$; and similarly for f_1^d.
> 8. $f_i(\emptyset) = \emptyset$ and $f_i(U) = U$; and similarly for f_i^d.
> 9. f_i and f_i^d are monotone.
> 10. $f_i(x \cup y) = f_i(x) \cup f_i(y)$.
> 11. $f_i^d(x \cup y) \supseteq f_i^d(x) \cup f_i^d(y)$.
> 12. $f_i(x \cap y) \subseteq f_i(x) \cap f_i(y)$.
> 13. $f_i^d(x \cap y) = f_i^d(x) \cap f_i^d(y)$.

With the exception of two subitems (4. and 5.) dealing with κ as rough inclusion operator, we succeeded.

It should be mentioned, that most of the reasoning on the properties of the generalized approximation operator was done under the assumption

$$\forall_{u \in U}\ u \in I(u),$$

which we called `map-reflexive` of the uncertainty mapping I. Another, more general relational aproach was adopted in [8] which is a Mizar counterpart of [17]. There the reflexivity of binary indiscernibility relation was assumed where needed.

Automated math-asistants can offer a new – semiautomated – insight [10] also for quite elementary notions: in Section 4, we introduced more general Mizar functor dealing with arbitrary maps from the universe into its powerset, so that we could obtain most of properties of mappings f_0 and f_1 as straightforward consequences. We kept them both however, to assure full compatibility with [2].

1. Preliminaries: Map-Reflexivity

Let R be a non empty set and I be a function from R into 2^R. We say that I is map-reflexive if and only if

(Def. 1) for every element u of R, $u \in I(u)$.

The functor $\mathrm{singleton}_R$ yielding a function from R into 2^R is defined by

(Def. 2) for every element x of R, $it(x) = \{x\}$.

Let us observe that $\mathrm{singleton}_R$ is map-reflexive.

Now we state the proposition:

(1) Let us consider a non empty relational structure R, and a function I from the carrier of R into 2^α. Suppose I is map-reflexive. Then the carrier of $R = \bigcup(I^\circ(\Omega_R))$, where α is the carrier of R.

From now on f, g denote functions and R denotes a non empty, reflexive relational structure.

Now we state the propositions:

(2) $\mathrm{LAp}(R) \mathrel{\dot\subseteq} \mathrm{id}_{2^\alpha}$, where α is the carrier of R.

Proof: Set $f = \mathrm{LAp}(R)$. Set $g = \mathrm{id}_{2^{(\text{the carrier of } R)}}$. For every set i such that $i \in \mathrm{dom}\, f$ holds $f(i) \subseteq g(i)$ by [7, (35)]. □

(3) $\mathrm{id}_{2^\alpha} \mathrel{\dot\subseteq} \mathrm{UAp}(R)$, where α is the carrier of R.

Proof: Set $f = \mathrm{id}_{2^{(\text{the carrier of } R)}}$. Set $g = \mathrm{UAp}(R)$. For every set i such that $i \in \mathrm{dom}\, f$ holds $f(i) \subseteq g(i)$. □

2. Properties of Flipping Operator f^d

From now on R denotes a non empty relational structure.

Now we state the propositions:

(4) Let us consider a map f of R, and subsets x, y of R. Then $\mathrm{Flip}\,\mathrm{Flip}\, f = f$.

(5) Let us consider maps f, g of R. Then $\mathrm{Flip}\, f \cdot g = (\mathrm{Flip}\, f) \cdot (\mathrm{Flip}\, g)$.

Proof: Set $f_2 = \mathrm{Flip}\, f \cdot g$. Set $f_1 = \mathrm{Flip}\, f$. Set $g_1 = \mathrm{Flip}\, g$. For every subset x of R, $f_2(x) = (f_1 \cdot g_1)(x)$. □

(6) Let us consider a map f of R. Then $f(\emptyset) = \emptyset$ if and only if $(\mathrm{Flip}\, f)(\text{the carrier of } R) = \text{the carrier of } R$.

3. Uncertainty Mappings I and τ

Let R be a non empty relational structure. The functor I_R yielding a function from the carrier of R into $2^{(\text{the carrier of } R)}$ is defined by

(Def. 3) for every element x of R, $it(x) = \mathrm{Coim}((\text{the internal relation of } R), x)$.

Now we state the proposition:

(7) Let us consider elements w, u of R. Then $\langle w, u\rangle \in$ the internal relation of R if and only if $w \in (I_R)(u)$.

Let R be a non empty relational structure. The functor τ_R yielding a function from the carrier of R into $2^{(\text{the carrier of } R)}$ is defined by

(Def. 4) for every element u of R, $it(u) = (\text{the internal relation of } R)^{\circ}u$.

Now we state the propositions:

(8) Let us consider elements u, w of R. Then $u \in (\text{the internal relation of } R)^{\circ}w$ if and only if $w \in \mathrm{Coim}((\text{the internal relation of } R), u)$.
Proof: If $u \in (\text{the internal relation of } R)^{\circ}w$, then $w \in \mathrm{Coim}((\text{the internal relation of } R), u)$. Consider t being an object such that $\langle w, t\rangle \in$ the internal relation of R and $t \in \{u\}$. □

(9) Let us consider elements w, u of R. Then $\langle w, u\rangle \in$ the internal relation of R if and only if $u \in (\tau_R)(w)$.
Proof: If $\langle w, u\rangle \in$ the internal relation of R, then $u \in (\tau_R)(w)$. $w \in \mathrm{Coim}((\text{the internal relation of } R), u)$. Consider x being an object such that $\langle w, x\rangle \in$ the internal relation of R and $x \in \{u\}$. □

4. Generalized Approximation Mappings

Let R be a non empty relational structure and f be a function from the carrier of R into $2^{(\text{the carrier of } R)}$. The functor UAp_f yielding a map of R is defined by

(Def. 5) for every subset x of R, $it(x) = \{u$, where u is an element of $R : f(u)$ meets $x\}$.

The functors: $f_0(R)$ and $f_1(R)$ yielding maps of R are defined by terms

(Def. 6) UAp_{τ_R},

(Def. 7) UAp_{I_R},

respectively. Now we state the propositions:

(10) If the internal relation of R is symmetric, then $I_R = \tau_R$.
Proof: Set $f = I_R$. Set $g = \tau_R$. For every element x of R, $f(x) = g(x)$ by [14, (20)]. □

(11) If the internal relation of R is symmetric, then $f_0(R) = f_1(R)$. The theorem is a consequence of (10).

(12) the internal relation of R is symmetric if and only if for every elements u, v of R such that $u \in (\tau_R)(v)$ holds $v \in (\tau_R)(u)$. The theorem is a consequence of (10), (7), and (9).

(13) $f_0(R) = \mathrm{UAp}(R)$.

(14) Flip $f_0(R) = \mathrm{LAp}(R)$. The theorem is a consequence of (13).

(15) Let us consider an approximation space R, and a subset x of R. Then $(f_0(R))(x)$ is exact. The theorem is a consequence of (13).

5. The Ordering of Approximation Mappings

Now we state the propositions:

(16) If the internal relation of R is total and reflexive, then $\mathrm{id}_{2^\alpha} \mathrel{\dot\subseteq} f_0(R)$, where α is the carrier of R.

Proof: Set $f = \mathrm{id}_{2^{(\text{the carrier of } R)}}$. Set $g = f_0(R)$. For every set i such that $i \in \mathrm{dom}\, f$ holds $f(i) \subseteq g(i)$ by [5, (1)], (9). □

(17) If R is reflexive, then Flip $f_0(R) \mathrel{\dot\subseteq} \mathrm{id}_{2^\alpha}$, where α is the carrier of R. The theorem is a consequence of (14) and (2).

(18) If the internal relation of R is total and reflexive, then $\mathrm{id}_{2^\alpha} \mathrel{\dot\subseteq} f_1(R)$, where α is the carrier of R.

Proof: Set $f = \mathrm{id}_{2^{(\text{the carrier of } R)}}$. Set $g = f_1(R)$. For every set i such that $i \in \mathrm{dom}\, f$ holds $f(i) \subseteq g(i)$. □

6. Acting on the Empty Set and the Universe

In the sequel f denotes a function from the carrier of R into $2^{(\text{the carrier of } R)}$.

Now we state the proposition:

(19) $(\mathrm{UAp}_f)(\emptyset) = \emptyset$.

Let us consider R and f. One can check that UAp_f preserves empty set.

(20) $(f_0(R))(\emptyset) = \emptyset$.

(21) $(f_1(R))(\emptyset) = \emptyset$.

Let R be a non empty, reflexive relational structure. Let us observe that the internal relation of R is total and reflexive.

(22) If f is map-reflexive, then $(\mathrm{UAp}_f)(\text{the carrier of } R) = \text{the carrier of } R$.

(23) Suppose the internal relation of R is reflexive and total.
Then $(f_0(R))$(the carrier of R) $=$ the carrier of R.
PROOF: The carrier of $R \subseteq \{u$, where u is an element of R : $(\tau_R)(u)$ meets $\Omega_R\}$. □

(24) Suppose the internal relation of R is reflexive and total.
Then $(f_1(R))$(the carrier of R) $=$ the carrier of R.
PROOF: The carrier of $R \subseteq \{u$, where u is an element of R : $(I_R)(u)$ meets $\Omega_R\}$. □

7. Standard Properties of Approximations

Let us consider elements u, w of R and a subset x of R. Now we state the propositions:

(25) If $f(u) = f(w)$, then $u \in (\mathrm{UAp}_f)(x)$ iff $w \in (\mathrm{UAp}_f)(x)$.

(26) If $(I_R)(u) = (I_R)(w)$, then $u \in (f_1(R))(x)$ iff $w \in (f_1(R))(x)$.

(27) If $(\tau_R)(u) = (\tau_R)(w)$, then $u \in (f_0(R))(x)$ iff $w \in (f_0(R))(x)$.

(28) Let us consider a function f from the carrier of R into 2^α, and a subset x of R. Then $(\mathrm{Flip}(\mathrm{UAp}_f))(x) = \{w$, where w is an element of $R : f(w) \subseteq x\}$, where α is the carrier of R.
PROOF: $(\mathrm{Flip}(\mathrm{UAp}_f))(x) \subseteq \{w$, where w is an element of $R : f(w) \subseteq x\}$. Consider w being an element of R such that $y = w$ and $f(w) \subseteq x$. Reconsider $y_1 = y$ as an element of R. $y_1 \notin (\mathrm{UAp}_f)(x^{\mathrm{c}})$. □

Let us consider a subset x of R. Now we state the propositions:

(29) $(\mathrm{Flip}\, f_0(R))(x) = \{w$, where w is an element of $R : (\tau_R)(w) \subseteq x\}$.
PROOF: $(\mathrm{Flip}\, f_0(R))(x) \subseteq \{w$, where w is an element of $R : (\tau_R)(w) \subseteq x\}$. Consider w being an element of R such that $y = w$ and $(\tau_R)(w) \subseteq x$. Reconsider $y_1 = y$ as an element of R. $y_1 \notin (f_0(R))(x^{\mathrm{c}})$. □

(30) $(\mathrm{Flip}\, f_1(R))(x) = \{w$, where w is an element of $R : (I_R)(w) \subseteq x\}$.
PROOF: $(\mathrm{Flip}\, f_1(R))(x) \subseteq \{w$, where w is an element of $R : (I_R)(w) \subseteq x\}$. Consider w being an element of R such that $y = w$ and $(I_R)(w) \subseteq x$. Reconsider $y_1 = y$ as an element of R. $y_1 \notin (f_1(R))(x^{\mathrm{c}})$. □

Let us consider elements u, w of R and a subset x of R. Now we state the propositions:

(31) If $f(u) = f(w)$, then $u \in (\mathrm{Flip}(\mathrm{UAp}_f))(x)$ iff $w \in (\mathrm{Flip}(\mathrm{UAp}_f))(x)$. The theorem is a consequence of (28).

(32) If $(\tau_R)(u) = (\tau_R)(w)$, then $u \in (\mathrm{Flip}\, f_0(R))(x)$ iff $w \in (\mathrm{Flip}\, f_0(R))(x)$. The theorem is a consequence of (29).

(33) If $(I_R)(u) = (I_R)(w)$, then $u \in (\mathrm{Flip}\, f_1(R))(x)$ iff $w \in (\mathrm{Flip}\, f_1(R))(x)$. The theorem is a consequence of (30).

Let us consider an element w of R. Now we state the propositions:

(34) If R is reflexive, then $w \in (I_R)(w)$. The theorem is a consequence of (7).

(35) If R is reflexive, then $w \in (\tau_R)(w)$. The theorem is a consequence of (9).

Let R be a reflexive, non empty relational structure. One can verify that I_R is map-reflexive and τ_R is map-reflexive.

Now we state the propositions:

(36) If R is reflexive, then $\mathrm{Flip}\, f_1(R) \mathrel{\dot{\subseteq}} \mathrm{id}_{2^\alpha}$, where α is the carrier of R. The theorem is a consequence of (34) and (30).

(37) $(f_0(R)) \cdot (f_0(R)) = f_0(R)$ if and only if $(\mathrm{Flip}\, f_0(R)) \cdot (\mathrm{Flip}\, f_0(R)) = \mathrm{Flip}\, f_0(R)$. The theorem is a consequence of (5).

(38) If R is reflexive, then $\bigcup((I_R)^\circ(\Omega_R)) =$ the carrier of R. The theorem is a consequence of (34).

8. Monotonicity of Approximations

Let R be a non empty relational structure. One can verify that $f_0(R)$ is $\subseteq$-monotone and $f_1(R)$ is $\subseteq$-monotone.

Now we state the propositions:

(39) Let us consider a map f of R. Suppose f is $\subseteq$-monotone. Then $\mathrm{Flip}\, f$ is $\subseteq$-monotone.

Proof: Set $g = \mathrm{Flip}\, f$. For every subsets A, B of R such that $A \subseteq B$ holds $g(A) \subseteq g(B)$. □

(40) $\mathrm{Flip}\, f_0(R)$ is $\subseteq$-monotone.

(41) $\mathrm{Flip}\, f_1(R)$ is $\subseteq$-monotone.

9. Distributivity wrt. Set-Theoretic Operations

Now we state the proposition:

(42) Let us consider a function f from the carrier of R into 2^α, and subsets x, y of R. Then $(\mathrm{UAp}_f)(x \cup y) = (\mathrm{UAp}_f)(x) \cup (\mathrm{UAp}_f)(y)$, where α is the carrier of R.

Let us consider subsets x, y of R. Now we state the propositions:

(43) $(f_0(R))(x \cup y) = (f_0(R))(x) \cup (f_0(R))(y)$. The theorem is a consequence of (42).

(44) $(f_1(R))(x \cup y) = (f_1(R))(x) \cup (f_1(R))(y)$. The theorem is a consequence of (42).

(45) Let us consider a function f from the carrier of R into 2^α, and subsets x, y of R. Then $(\mathrm{Flip}(\mathrm{UAp}_f))(x) \cup (\mathrm{Flip}(\mathrm{UAp}_f))(y) \subseteq (\mathrm{Flip}(\mathrm{UAp}_f))(x \cup y)$, where α is the carrier of R. The theorem is a consequence of (28).

Let us consider subsets x, y of R. Now we state the propositions:

(46) $(\mathrm{Flip}\, f_0(R))(x) \cup (\mathrm{Flip}\, f_0(R))(y) \subseteq (\mathrm{Flip}\, f_0(R))(x \cup y)$. The theorem is a consequence of (45).

(47) $(\mathrm{Flip}\, f_1(R))(x) \cup (\mathrm{Flip}\, f_1(R))(y) \subseteq (\mathrm{Flip}\, f_1(R))(x \cup y)$. The theorem is a consequence of (45).

(48) Let us consider a function f from the carrier of R into 2^α, and subsets x, y of R. Then $(\mathrm{UAp}_f)(x \cap y) \subseteq (\mathrm{UAp}_f)(x) \cap (\mathrm{UAp}_f)(y)$, where α is the carrier of R.

Let us consider subsets x, y of R. Now we state the propositions:

(49) $(f_0(R))(x \cap y) \subseteq (f_0(R))(x) \cap (f_0(R))(y)$. The theorem is a consequence of (48).

(50) $(f_1(R))(x \cap y) \subseteq (f_1(R))(x) \cap (f_1(R))(y)$. The theorem is a consequence of (48).

(51) Let us consider a function f from the carrier of R into 2^α, and subsets x, y of R. Then $(\mathrm{Flip}(\mathrm{UAp}_f))(x) \cap (\mathrm{Flip}(\mathrm{UAp}_f))(y) = (\mathrm{Flip}(\mathrm{UAp}_f))(x \cap y)$, where α is the carrier of R.

Let us consider subsets x, y of R. Now we state the propositions:

(52) $(\mathrm{Flip}\, f_0(R))(x) \cap (\mathrm{Flip}\, f_0(R))(y) = (\mathrm{Flip}\, f_0(R))(x \cap y)$. The theorem is a consequence of (51).

(53) $(\mathrm{Flip}\, f_1(R))(x) \cap (\mathrm{Flip}\, f_1(R))(y) = (\mathrm{Flip}\, f_1(R))(x \cap y)$. The theorem is a consequence of (51).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Anna Gomolińska. A comparative study of some generalized rough approximations. *Fundamenta Informaticae*, 51:103–119, 2002.

[3] Adam Grabowski. Automated discovery of properties of rough sets. *Fundamenta Informaticae*, 128:65–79, 2013. doi:10.3233/FI-2013-933.

[4] Adam Grabowski. Lattice theory for rough sets – a case study with Mizar. *Fundamenta Informaticae*, 147(2–3):223–240, 2016. doi:10.3233/FI-2016-1406.

[5] Adam Grabowski. Formalization of generalized almost distributive lattices. *Formalized Mathematics*, 22(**3**):257–267, 2014. doi:10.2478/forma-2014-0026.

[6] Adam Grabowski. Basic properties of rough sets and rough membership function. *Formalized Mathematics*, 12(**1**):21–28, 2004.

[7] Adam Grabowski. Relational formal characterization of rough sets. *Formalized Mathematics*, 21(**1**):55–64, 2013. doi:10.2478/forma-2013-0006.

[8] Adam Grabowski. Binary relations-based rough sets – an automated approach. *Formalized Mathematics*, 24(**2**):143–155, 2016. doi:10.1515/forma-2016-0011.

[9] Adam Grabowski and Magdalena Jastrzębska. A note on a formal approach to rough operators. In Marcin S. Szczuka and Marzena Kryszkiewicz et al., editors, *Rough Sets and Current Trends in Computing – 7th International Conference, RSCTC 2010, Warsaw, Poland, June 28-30, 2010. Proceedings*, volume 6086 of *Lecture Notes in Computer Science*, pages 307–316. Springer, 2010. doi:10.1007/978-3-642-13529-3_33.

[10] Adam Grabowski and Magdalena Jastrzębska. Rough set theory from a math-assistant perspective. In *Rough Sets and Intelligent Systems Paradigms, International Conference, RSEISP 2007, Warsaw, Poland, June 28–30, 2007, Proceedings*, pages 152–161, 2007. doi:10.1007/978-3-540-73451-2_17.

[11] Adam Grabowski and Christoph Schwarzweller. On duplication in mathematical repositories. In Serge Autexier, Jacques Calmet, David Delahaye, Patrick D. F. Ion, Laurence Rideau, Renaud Rioboo, and Alan P. Sexton, editors, *Intelligent Computer Mathematics, 10th International Conference, AISC 2010, 17th Symposium, Calculemus 2010, and 9th International Conference, MKM 2010, Paris, France, July 5–10, 2010. Proceedings*, volume 6167 of *Lecture Notes in Computer Science*, pages 300–314. Springer, 2010. doi:10.1007/978-3-642-14128-7_26.

[12] Adam Grabowski and Christoph Schwarzweller. Rough Concept Analysis - theory development in the Mizar system. In Asperti, Andrea and Bancerek, Grzegorz and Trybulec, Andrzej, editor, *Mathematical Knowledge Management, Third International Conference, MKM 2004, Bialowieza, Poland, September 19–21, 2004, Proceedings*, volume 3119 of *Lecture Notes in Computer Science*, pages 130–144, 2004. doi:10.1007/978-3-540-27818-4_10. 3rd International Conference on Mathematical Knowledge Management, Bialowieza, Poland, Sep. 19-21, 2004.

[13] Jouni Järvinen. Lattice theory for rough sets. *Transactions of Rough Sets, VI, Lecture Notes in Computer Science*, 4374:400–498, 2007.

[14] Eliza Niewiadomska and Adam Grabowski. Introduction to formal preference spaces. *Formalized Mathematics*, 21(**3**):223–233, 2013. doi:10.2478/forma-2013-0024.

[15] Zdzisław Pawlak. Rough sets. *International Journal of Parallel Programming*, 11:341–356, 1982. doi:10.1007/BF01001956.

[16] Y.Y. Yao. Two views of the theory of rough sets in finite universes. *International Journal of Approximate Reasoning*, 15(4):291–317, 1996. doi:10.1016/S0888-613X(96)00071-0.

[17] William Zhu. Generalized rough sets based on relations. *Information Sciences*, 177: 4997–5011, 2007.

Accepted June 29, 2018

FORMALIZED MATHEMATICS
Vol. 26, No. 2, Pages 193–198, 2018
DOI: 10.2478/forma-2018-0017

https://www.sciendo.com/

On Two Alternative Axiomatizations of Lattices by McKenzie and Sholander

Adam Grabowski
Institute of Informatics
University of Białystok
Poland

Damian Sawicki
Institute of Informatics
University of Białystok
Poland

Summary. The main result of the article is to prove formally that two sets of axioms, proposed by McKenzie and Sholander, axiomatize lattices and distributive lattices, respectively. In our Mizar article we used proof objects generated by Prover9. We continue the work started in [7], [21], and [13] of developing lattice theory as initialized in [22] as a formal counterpart of [11]. Complete formal proofs can be found in the Mizar source code of this article available in the Mizar Mathematical Library (MML).

MSC: 03B35 68T99 06B05 06D05

Keywords: lattice; distributive lattice; lattice axioms

MML identifier: ROBBINS5, version: 8.1.08 5.52.1328

0. Introduction

For years, automated theorem provers have proven to be useful tool to solve quite complex problems dealing with axiomatizations of various systems appearing in mathematics. Let us recall here the Robbins problem about the alternative axiomatization of Boolean algebras: this was probably the first time lots of mathematicians have heard of EQP/Otter [15]. The Mizar system, via interface ott2miz [19] allows for the automated translation of Otter (or Prover9) proof objects to allows such proofs to be included into the Mizar repository. Among the examples of such areas of mathematics within the Mizar Mathematical Library (MML) [1] explored by means of Prover9 we can give

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

either the aforementioned solution of the Robbins problem [7] according to [3], various short systems for ortholattices [21] inspired by [14], or axiom systems for Boolean algebras in terms of the Sheffer stroke [13]. An overview of the mechanization of lattice theory in MML can be found in [5]. The initial idea of this development was to provide a formal counterpart of [11] (or, more recently, [12]) or [2] and this Mizar challenge is alive for over thirty years now [9]. This is also quite feasible taking into account automatic treatment of the equality predicate in Mizar [10], and the equational axiomatics for lattices is strongly preferred in the MML over that based on the ordering relation [4], although we created a common – fully formal – Mizar framework where both can be used in parallel [8].

In 1951, in his paper [20] Marlow Sholander showed that the necessary and sufficient condition for an algebra $\langle L, \sqcup, \sqcap \rangle$ to be a distributive lattice is to satisfy one of the following sets of axioms:

$$a = a \sqcup (a \sqcap b),$$

$$a \sqcup (b \sqcap c) = (c \sqcup a) \sqcap (b \sqcup a);$$

or, dually

$$a = a \sqcap (a \sqcup b),$$

$$a \sqcap (b \sqcup c) = (c \sqcap a) \sqcup (b \sqcap a)$$

for arbitrary elements a, b, c of L.

We call the latter formula the Sholander axiom, and show in the first section, that together with the other one, which corresponds with the Mizar adjective `join-absorbing`, it implies all remaining standard axioms for distributive lattices as defined in [22]. The theorem stating full equivalence of both axiom sets is under number (11) in the present article.

Ralph McKenzie's [17] axiomatization of lattices consists of four formulas:

$$x \sqcup (y \sqcap (x \sqcap z)) = x$$

$$x \sqcap (y \sqcup (x \sqcup z)) = x$$

$$((y \sqcap x) \sqcup (x \sqcap z)) \sqcup x = x$$

$$((y \sqcup x) \sqcap (x \sqcup z)) \sqcap x = x$$

where x, y, z are arbitrary elements of the carrier of $\langle L, \sqcup, \sqcap \rangle$. These formulas were introduced in Section 2 in definitions (Def. 2) – (Def. 5), respectively, and the full equivalence of these four axioms with the classical axiomatics from [22] is proven as theorem (15) providing also appropriate registration of clusters allowing for automated reuse of both sets. Such approach is useful especially in the areas which use lattice theory as a kind of metalanguage, e.g., rough sets [6].

Our work can be seen as a step towards a Mizar support for [16] or [18], where original proof objects by Otter/Prover9 were used.

1. Sholander Axiom for Distributive Lattices

From now on L denotes a non empty lattice structure and v_4, v_5, v_6, v_7, w_3, v, w_2, w_1, w_0, z, y, x denote elements of L.

Let us consider L. We say that L satisfies Sholander axiom if and only if

(Def. 1) for every x, y, and z, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$.

Let us consider x. Now we state the propositions:

(1) If L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$, then $x \sqcap x = x$.

(2) If L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$, then $x \sqcup x = x$. The theorem is a consequence of (1).

Let us consider x and y. Now we state the propositions:

(3) If L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$, then $x \sqcap y = y \sqcap x$. The theorem is a consequence of (2).

(4) If L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$, then $x \sqcup y = y \sqcup x$. The theorem is a consequence of (1).

(5) Suppose L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$. $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$. The theorem is a consequence of (1), (2), (4), and (3).

(6) If for every y and x, $x \sqcap (x \sqcup y) = x$, then for every x and y, $x \sqcap (x \sqcup y) = x$.

(7) Suppose L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$. $x \sqcup (x \sqcap y) = x$. The theorem is a consequence of (1), (3), and (4).

Let us consider x, y, and z. Now we state the propositions:

(8) Suppose L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$. Then $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$. The theorem is a consequence of (1), (3), (7), (2), (5), and (4).

(9) Suppose L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$. Then $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$. The theorem is a consequence of (4) and (3).

(10) Suppose L is join-absorbing and for every x, z, and y, $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$. Then $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$. The theorem is a consequence of (5), (1), (4), (8), (2), and (3).

From now on L denotes a distributive, join-commutative, meet-commutative, non empty lattice structure and x, y, z denote elements of L.

Now we state the propositions:

(11) $x \sqcap (y \sqcup z) = (z \sqcap x) \sqcup (y \sqcap x)$.

(12) Let us consider a non empty lattice structure L. Then L is a distributive lattice if and only if L is join-absorbing and satisfies Sholander axiom. The theorem is a consequence of (11), (9), (3), (4), (5), (8), and (7).

Let us observe that every non empty lattice structure which is join-absorbing and satisfies Sholander axiom is also distributive and lattice-like and every non empty lattice structure which is distributive, join-commutative, and meet-commutative satisfies also Sholander axiom.

2. Four Axioms for Lattices Proposed by McKenzie

From now on L denotes a non empty lattice structure and w_3, v, w_2, w_1, w_0, z, y, x denote elements of L.

Let us consider L. We say that L satisfies first McKenzie axiom if and only if

(Def. 2) for every y, z, and x, $x \sqcup (y \sqcap (x \sqcap z)) = x$.

We say that L satisfies second McKenzie axiom if and only if

(Def. 3) for every y, z, and x, $x \sqcap (y \sqcup (x \sqcup z)) = x$.

We say that L satisfies third McKenzie axiom if and only if

(Def. 4) for every z, y, and x, $((x \sqcap y) \sqcup (y \sqcap z)) \sqcup y = y$.

We say that L satisfies fourth McKenzie axiom if and only if

(Def. 5) for every z, y, and x, $((x \sqcup y) \sqcap (y \sqcup z)) \sqcap y = y$.

Now we state the propositions:

(13) Suppose L satisfies first McKenzie axiom and second McKenzie axiom and for every z, y, and x, $((x \sqcap y) \sqcup (y \sqcap z)) \sqcup y = y$ and for every z, y, and x, $((x \sqcup y) \sqcap (y \sqcup z)) \sqcap y = y$. Then

(i) for every y and x, $x \sqcap (x \sqcup y) = x$, and

(ii) for every y and x, $x \sqcup (x \sqcap y) = x$, and

(iii) L is join-commutative, meet-commutative, meet-associative, and join-associative.

(14) Suppose L is join-commutative, join-associative, meet-commutative, and meet-associative and for every y and x, $x \sqcap (x \sqcup y) = x$ and for every y and x, $x \sqcup (x \sqcap y) = x$. Then

(i) for every y, z, and x, $x \sqcup (y \sqcap (x \sqcap z)) = x$, and

(ii) for every y, z, and x, $x \sqcap (y \sqcup (x \sqcup z)) = x$, and

(iii) for every z, y, and x, $((x \sqcap y) \sqcup (y \sqcap z)) \sqcup y = y$, and

(iv) for every z, y, and x, $((x \sqcup y) \sqcap (y \sqcup z)) \sqcap y = y$.

Let L be a non empty lattice structure. We say that L satisfies four McKenzie axioms if and only if

(Def. 6) L satisfies first McKenzie axiom, second McKenzie axiom, third McKenzie axiom, and fourth McKenzie axiom.

One can verify that every non empty lattice structure which satisfies four McKenzie axioms satisfies also first McKenzie axiom, second McKenzie axiom, third McKenzie axiom, and fourth McKenzie axiom and every non empty lattice structure which satisfies first McKenzie axiom, second McKenzie axiom, third McKenzie axiom, and fourth McKenzie axiom satisfies also four McKenzie axioms.

From now on L denotes a non empty lattice structure.

Now we state the proposition:

(15) L is a lattice if and only if L satisfies four McKenzie axioms. The theorem is a consequence of (14) and (13).

Let us observe that every non empty lattice structure which is lattice-like satisfies also four McKenzie axioms and every non empty lattice structure which satisfies four McKenzie axioms is also lattice-like.

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[2] Garrett Birkhoff. *Lattice Theory.* Providence, Rhode Island, New York, 1967.

[3] B. I. Dahn. Robbins algebras are Boolean: A revision of McCune's computer-generated solution of Robbins problem. *Journal of Algebra*, 208:526–532, 1998.

[4] B.A. Davey and H.A. Priestley. *Introduction to Lattices and Order.* Cambridge University Press, 2002.

[5] Adam Grabowski. Mechanizing complemented lattices within Mizar system. *Journal of Automated Reasoning*, 55:211–221, 2015. doi:10.1007/s10817-015-9333-5.

[6] Adam Grabowski. Lattice theory for rough sets – a case study with Mizar. *Fundamenta Informaticae*, 147(2–3):223–240, 2016. doi:10.3233/FI-2016-1406.

[7] Adam Grabowski. Robbins algebras vs. Boolean algebras. *Formalized Mathematics*, 9(**4**): 681–690, 2001.

[8] Adam Grabowski and Markus Moschner. Managing heterogeneous theories within a mathematical knowledge repository. In Andrea Asperti, Grzegorz Bancerek, and Andrzej Trybulec, editors, *Mathematical Knowledge Management Proceedings*, volume 3119 of *Lecture Notes in Computer Science*, pages 116–129. Springer, 2004. doi:10.1007/978-3-540-27818-4_9. 3rd International Conference on Mathematical Knowledge Management, Bialowieza, Poland, Sep. 19–21, 2004.

[9] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[10] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. Equality in computer proof-assistants. In Ganzha, Maria and Maciaszek, Leszek and Paprzycki, Marcin, editor, *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*, volume 5 of *ACSIS-Annals of Computer Science and Information Systems*, pages 45–54. IEEE, 2015. doi:10.15439/2015F229.

[11] George Grätzer. *General Lattice Theory.* Academic Press, New York, 1978.

[12] George Grätzer. *Lattice Theory: Foundation.* Birkhäuser, 2011.

[13] Violetta Kozarkiewicz and Adam Grabowski. Axiomatization of Boolean algebras based on Sheffer stroke. *Formalized Mathematics*, 12(**3**):355–361, 2004.

[14] W. McCune, R. Padmanabhan, M. A. Rose, and R. Veroff. Automated discovery of single axioms for ortholattices. *Algebra Universalis*, 52(4):541–549, 2005.

[15] William McCune. Prover9 and Mace4. 2005–2010.

[16] William McCune and Ranganathan Padmanabhan. *Automated Deduction in Equational Logic and Cubic Curves.* Springer-Verlag, Berlin, 1996.

[17] Ralph McKenzie. Equational bases for lattice theories. *Mathematica Scandinavica*, 27: 24–38, 1970. doi:10.7146/math.scand.a-10984.

[18] Ranganathan Padmanabhan and Sergiu Rudeanu. *Axioms for Lattices and Boolean Algebras.* World Scientific Publishers, 2008.

[19] Piotr Rudnicki and Josef Urban. Escape to ATP for Mizar. In *First International Workshop on Proof eXchange for Theorem Proving-PxTP 2011*, 2011.

[20] Marlow Sholander. Postulates for distributive lattices. *Canadian Journal of Mathematics*, 3:28–30, 1951. doi:10.4153/CJM-1951-003-5.

[21] Wioletta Truszkowska and Adam Grabowski. On the two short axiomatizations of ortholattices. *Formalized Mathematics*, 11(**3**):335–340, 2003.

[22] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Accepted June 29, 2018

Contents

Formaliz. Math. 26 (**2**)

Parity as a Property of Integers
By Rafał Ziobro **91**

About Supergraphs. Part I
By Sebastian Koch **101**

About Supergraphs. Part II
By Sebastian Koch **125**

On Algebras of Algorithms and Specifications over Uninterpreted Data
By Ievgen Ivanov *et al.* **141**

On an Algorithmic Algebra over Simple-Named Complex-Valued Nominative Data
By Ievgen Ivanov *et al.* **149**

An Inference System of an Extension of Floyd-Hoare Logic for Partial Predicates
By Ievgen Ivanov *et al.* **159**

Partial Correctness of GCD Algorithm
By Ievgen Ivanov *et al.* **165**

Basic Diophantine Relations
By Marcin Acewicz and Karol Pąk **175**

Formalizing Two Generalized Approximation Operators
By Adam Grabowski and Michał Sielwiesiuk **183**

On Two Alternative Axiomatizations of Lattices by McKenzie and Sholander

Continued on inside back cover

By Adam Grabowski and Damian Sawicki **193**