FORMALIZED MATHEMATICS
Volume 11, Number 3, 2003
University of Białystok

Construction of Gröbner bases. S-Polynomials and Standard Representations

Christoph Schwarzweller
University of Tübingen

Summary. We continue the Mizar formalization of Gröbner bases following [6]. In this article we introduce S-polynomials and standard representations and show how these notions can be used to characterize Gröbner bases.

MML Identifier: `GROEB_2`.

The notation and terminology used here are introduced in the following papers: [24], [31], [32], [34], [33], [8], [3], [15], [30], [29], [9], [7], [5], [14], [12], [19], [18], [25], [28], [17], [1], [4], [13], [22], [21], [27], [26], [16], [10], [23], [2], [20], [11], and [35].

1. Preliminaries

One can prove the following propositions:

(1) For every set X and for every finite sequence p of elements of X such that $p \neq \emptyset$ holds $p \restriction 1 = \langle p_1 \rangle$.

(2) Let L be a non empty loop structure, p be a finite sequence of elements of L, and n, m be natural numbers. If $m \leqslant n$, then $p \restriction n \restriction m = p \restriction m$.

(3) Let L be an add-associative right zeroed right complementable non empty loop structure, p be a finite sequence of elements of L, and n be a natural number. Suppose that for every natural number k such that $k \in \operatorname{dom} p$ and $k > n$ holds $p(k) = 0_L$. Then $\sum p = \sum (p \restriction n)$.

(4) Let L be an add-associative right zeroed Abelian non empty loop structure, f be a finite sequence of elements of L, and i, j be natural numbers. Then $\sum \operatorname{Swap}(f, i, j) = \sum f$.

ISSN 1426–2630

(5) Let n be an ordinal number, T be a term order of n, and b_1, b_2, b_3 be bags of n. If $b_1 \leqslant_T b_3$ and $b_2 \leqslant_T b_3$, then $\max_T(b_1, b_2) \leqslant_T b_3$.

(6) Let n be an ordinal number, T be a term order of n, and b_1, b_2, b_3 be bags of n. If $b_3 \leqslant_T b_1$ and $b_3 \leqslant_T b_2$, then $b_3 \leqslant_T \min_T(b_1, b_2)$.

Let X be a set and let b_1, b_2 be bags of X. Let us assume that $b_2 \mid b_1$. The functor $\frac{b_1}{b_2}$ yields a bag of X and is defined by:

(Def. 1) $b_2 + \frac{b_1}{b_2} = b_1$.

Let X be a set and let b_1, b_2 be bags of X. The functor $\mathrm{lcm}(b_1, b_2)$ yields a bag of X and is defined as follows:

(Def. 2) For every set k holds $\mathrm{lcm}(b_1, b_2)(k) = \max(b_1(k), b_2(k))$.

Let us observe that the functor $\mathrm{lcm}(b_1, b_2)$ is commutative and idempotent. We introduce $\mathrm{lcm}(b_1, b_2)$ as a synonym of $\mathrm{lcm}(b_1, b_2)$.

Let X be a set and let b_1, b_2 be bags of X. We say that b_1, b_2 are disjoint if and only if:

(Def. 3) For every set i holds $b_1(i) = 0$ or $b_2(i) = 0$.

We introduce b_1, b_2 are non disjoint as an antonym of b_1, b_2 are disjoint.

We now state several propositions:

(7) For every set X and for all bags b_1, b_2 of X holds $b_1 \mid \mathrm{lcm}(b_1, b_2)$ and $b_2 \mid \mathrm{lcm}(b_1, b_2)$.

(8) For every set X and for all bags b_1, b_2, b_3 of X such that $b_1 \mid b_3$ and $b_2 \mid b_3$ holds $\mathrm{lcm}(b_1, b_2) \mid b_3$.

(9) Let X be a set, T be a term order of X, and b_1, b_2 be bags of X. Then b_1, b_2 are disjoint if and only if $\mathrm{lcm}(b_1, b_2) = b_1 + b_2$.

(10) For every set X and for every bag b of X holds $\frac{b}{b} = \mathrm{EmptyBag}\, X$.

(11) For every set X and for all bags b_1, b_2 of X holds $b_2 \mid b_1$ iff $\mathrm{lcm}(b_1, b_2) = b_1$.

(12) For every set X and for all bags b_1, b_2, b_3 of X such that $b_1 \mid \mathrm{lcm}(b_2, b_3)$ holds $\mathrm{lcm}(b_2, b_1) \mid \mathrm{lcm}(b_2, b_3)$.

(13) For every set X and for all bags b_1, b_2, b_3 of X such that $\mathrm{lcm}(b_2, b_1) \mid \mathrm{lcm}(b_2, b_3)$ holds $\mathrm{lcm}(b_1, b_3) \mid \mathrm{lcm}(b_2, b_3)$.

(14) For every set n and for all bags b_1, b_2, b_3 of n such that $\mathrm{lcm}(b_1, b_3) \mid \mathrm{lcm}(b_2, b_3)$ holds $b_1 \mid \mathrm{lcm}(b_2, b_3)$.

(15) Let n be a natural number, T be a connected admissible term order of n, and P be a non empty subset of $\mathrm{Bags}\, n$. Then there exists a bag b of n such that $b \in P$ and for every bag b' of n such that $b' \in P$ holds $b \leqslant_T b'$.

Let L be an add-associative right zeroed right complementable non trivial loop structure and let a be a non-zero element of L. Note that $-a$ is non-zero.

Let X be a set, let L be a left zeroed right zeroed add-cancelable distributive non empty double loop structure, let m be a monomial of X, L, and let a be an element of L. One can verify that $a \cdot m$ is monomial-like.

Let n be an ordinal number, let L be a left zeroed right zeroed add-cancelable distributive integral domain-like non trivial double loop structure, let p be a non-zero polynomial of n, L, and let a be a non-zero element of L. One can verify that $a \cdot p$ is non-zero.

Next we state several propositions:

(16) Let n be an ordinal number, T be a term order of n, L be a right zeroed right distributive non empty double loop structure, p, q be series of n, L, and b be a bag of n. Then $b * (p + q) = b * p + b * q$.

(17) Let n be an ordinal number, T be a term order of n, L be an add-associative right zeroed right complementable non empty loop structure, p be a series of n, L, and b be a bag of n. Then $b * -p = -b * p$.

(18) Let n be an ordinal number, T be a term order of n, L be a left zeroed add-right-cancelable right distributive non empty double loop structure, p be a series of n, L, b be a bag of n, and a be an element of L. Then $b * (a \cdot p) = a \cdot (b * p)$.

(19) Let n be an ordinal number, T be a term order of n, L be a right distributive non empty double loop structure, p, q be series of n, L, and a be an element of L. Then $a \cdot (p + q) = a \cdot p + a \cdot q$.

(20) Let X be a set, L be an add-associative right zeroed right complementable non empty double loop structure, and a be an element of L. Then $-(a\,\_(X, L)) = -a\,\_(X, L)$.

2. S-Polynomials

The following proposition is true

(21) Let n be a natural number, T be a connected admissible term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and P be a subset of Polynom-Ring(n, L). Suppose $0_n L \notin P$. Suppose that for all polynomials p_1, p_2 of n, L such that $p_1 \neq p_2$ and $p_1 \in P$ and $p_2 \in P$ and for all monomials m_1, m_2 of n, L such that $\mathrm{HM}(m_1 * p_1, T) = \mathrm{HM}(m_2 * p_2, T)$ holds PolyRedRel(P, T) reduces $m_1 * p_1 - m_2 * p_2$ to $0_n L$. Then P is a Groebner basis wrt T.

Let n be an ordinal number, let T be a connected term order of n, let L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and let p_1, p_2 be polynomials of n, L. The functor S-Poly(p_1, p_2, T) yielding a polynomial of n, L is defined by:

(Def. 4) $\text{S-Poly}(p_1, p_2, T) = \text{HC}(p_2, T) \cdot (\frac{\text{lcm}(\text{HT}(p_1,T),\text{HT}(p_2,T))}{\text{HT}(p_1,T)} * p_1) - \text{HC}(p_1, T) \cdot (\frac{\text{lcm}(\text{HT}(p_1,T),\text{HT}(p_2,T))}{\text{HT}(p_2,T)} * p_2)$.

One can prove the following propositions:

(22) Let n be an ordinal number, T be a connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like Abelian non trivial double loop structure, P be a subset of $\text{Polynom-Ring}(n, L)$, and p_1, p_2 be polynomials of n, L. If $p_1 \in P$ and $p_2 \in P$, then $\text{S-Poly}(p_1, p_2, T) \in P$–ideal.

(23) Let n be an ordinal number, T be a connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and p_1, p_2 be polynomials of n, L. If $p_1 = p_2$, then $\text{S-Poly}(p_1, p_2, T) = 0_n L$.

(24) Let n be an ordinal number, T be a connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and m_1, m_2 be monomials of n, L. Then $\text{S-Poly}(m_1, m_2, T) = 0_n L$.

(25) Let n be an ordinal number, T be a connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and p be a polynomial of n, L. Then $\text{S-Poly}(p, 0_n L, T) = 0_n L$ and $\text{S-Poly}(0_n L, p, T) = 0_n L$.

(26) Let n be an ordinal number, T be an admissible connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and p_1, p_2 be polynomials of n, L. Then $\text{S-Poly}(p_1, p_2, T) = 0_n L$ or $\text{HT}(\text{S-Poly}(p_1, p_2, T), T) <_T \text{lcm}(\text{HT}(p_1, T), \text{HT}(p_2, T))$.

(27) Let n be an ordinal number, T be a connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and p_1, p_2 be non-zero polynomials of n, L. If $\text{HT}(p_2, T) \mid \text{HT}(p_1, T)$, then $\text{HC}(p_2, T) \cdot p_1$ top reduces to $\text{S-Poly}(p_1, p_2, T)$, p_2, T.

(28) Let n be a natural number, T be a connected admissible term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and G be a subset of $\text{Polynom-Ring}(n, L)$. Suppose G is a Groebner basis wrt T. Let g_1, g_2, h be polynomials of n, L. If $g_1 \in G$ and $g_2 \in G$ and h is a normal form of $\text{S-Poly}(g_1, g_2, T)$ w.r.t. $\text{PolyRedRel}(G, T)$, then $h = 0_n L$.

(29) Let n be a natural number, T be a connected admissible term order of n, L be an Abelian add-associative right complementable right zeroed com-

mutative associative well unital distributive field-like non degenerated non empty double loop structure, and G be a subset of Polynom-Ring(n, L). Suppose that for all polynomials g_1, g_2, h of n, L such that $g_1 \in G$ and $g_2 \in G$ and h is a normal form of S-Poly(g_1, g_2, T) w.r.t. PolyRedRel(G, T) holds $h = 0_n L$. Let g_1, g_2 be polynomials of n, L. If $g_1 \in G$ and $g_2 \in G$, then PolyRedRel(G, T) reduces S-Poly(g_1, g_2, T) to $0_n L$.

(30) Let n be a natural number, T be an admissible connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and G be a subset of Polynom-Ring(n, L). Suppose $0_n L \notin G$. Suppose that for all polynomials g_1, g_2 of n, L such that $g_1 \in G$ and $g_2 \in G$ holds PolyRedRel(G, T) reduces S-Poly(g_1, g_2, T) to $0_n L$. Then G is a Groebner basis wrt T.

Let n be an ordinal number, let T be a connected term order of n, let L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and let P be a subset of Polynom-Ring(n, L). The functor S-Poly(P, T) yielding a subset of Polynom-Ring(n, L) is defined by:

(Def. 5) S-Poly$(P, T) = \{$S-Poly$(p_1, p_2, T); p_1$ ranges over polynomials of n, L, p_2 ranges over polynomials of n, L: $p_1 \in P \ \wedge \ p_2 \in P\}$.

Let n be an ordinal number, let T be a connected term order of n, let L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, and let P be a finite subset of Polynom-Ring(n, L). One can check that S-Poly(P, T) is finite.

One can prove the following proposition

(31) Let n be a natural number, T be an admissible connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and G be a subset of Polynom-Ring(n, L). Suppose $0_n L \notin G$ and for every polynomial g of n, L such that $g \in G$ holds g is a monomial of n, L. Then G is a Groebner basis wrt T.

3. Standard Representations

The following three propositions are true:

(32) Let L be a non empty multiplicative loop structure, P be a non empty subset of L, A be a left linear combination of P, and i be a natural number. Then $A \restriction i$ is a left linear combination of P.

(33) Let L be a non empty multiplicative loop structure, P be a non empty subset of L, A be a left linear combination of P, and i be a natural number. Then $A_{\mid i}$ is a left linear combination of P.

(34) Let L be a non empty multiplicative loop structure, P, Q be non empty subsets of the carrier of L, and A be a left linear combination of P. If $P \subseteq Q$, then A is a left linear combination of Q.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let P be a non empty subset of Polynom-Ring(n, L), and let A, B be left linear combinations of P. Then $A \frown B$ is a left linear combination of P.

Let n be an ordinal number, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let f be a polynomial of n, L, let P be a non empty subset of Polynom-Ring(n, L), and let A be a left linear combination of P. We say that A is a monomial representation of f if and only if the conditions (Def. 6) are satisfied.

(Def. 6)(i) $\sum A = f$, and

(ii) for every natural number i such that $i \in \operatorname{dom} A$ there exists a monomial m of n, L and there exists a polynomial p of n, L such that $p \in P$ and $A_i = m * p$.

Next we state two propositions:

(35) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f be a polynomial of n, L, P be a non empty subset of Polynom-Ring(n, L), and A be a left linear combination of P. Suppose A is a monomial representation of f. Then Support $f \subseteq \bigcup\{\mathrm{Support}(m * p); m$ ranges over monomials of n, L, p ranges over polynomials of n, L: $\bigvee_{i\,:\,\text{natural number}} (i \in \operatorname{dom} A \ \wedge \ A_i = m * p)\}$.

(36) Let n be an ordinal number, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f, g be polynomials of n, L, P be a non empty subset of Polynom-Ring(n, L), and A, B be left linear combinations of P. Suppose A is a monomial representation of f and B is a monomial representation of g. Then $A \frown B$ is a monomial representation of $f + g$.

Let n be an ordinal number, let T be a connected term order of n, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let f be a polynomial of n, L, let P be a non empty subset of Polynom-Ring(n, L), let A be a left linear combination of P, and let b be a bag of n. We say that A is a standard representation of f, P, b, T if and only if the conditions (Def. 7) are satisfied.

(Def. 7)(i) $\sum A = f$, and

(ii) for every natural number i such that $i \in \operatorname{dom} A$ there exists a non-zero monomial m of n, L and there exists a non-zero polynomial p of n, L such that $p \in P$ and $A_i = m * p$ and $\mathrm{HT}(m * p, T) \leqslant_T b$.

Let n be an ordinal number, let T be a connected term order of n, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let f be a polynomial of n, L, let P be a non empty subset of Polynom-Ring(n, L), and let A be a left linear combination of P. We say that A is a standard representation of f, P, T if and only if:

(Def. 8) A is a standard representation of f, P, $\mathrm{HT}(f, T)$, T.

Let n be an ordinal number, let T be a connected term order of n, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let f be a polynomial of n, L, let P be a non empty subset of Polynom-Ring(n, L), and let b be a bag of n. We say that f has a standard representation of P, b, T if and only if:

(Def. 9) There exists a left linear combination of P which is a standard representation of f, P, b, T.

Let n be an ordinal number, let T be a connected term order of n, let L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, let f be a polynomial of n, L, and let P be a non empty subset of Polynom-Ring(n, L). We say that f has a standard representation of P, T if and only if:

(Def. 10) There exists a left linear combination of P which is a standard representation of f, P, T.

One can prove the following propositions:

(37) Let n be an ordinal number, T be a connected term order of n, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f be a polynomial of n, L, P be a non empty subset of Polynom-Ring(n, L), A be a left linear combination of P, and b be a bag of n. Suppose A is a standard representation of f, P, b, T. Then A is a monomial representation of f.

(38) Let n be an ordinal number, T be a connected term order of n, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f, g be polynomials of n, L, P be a non empty subset of Polynom-Ring(n, L), A, B be left linear combinations of P, and b be a bag of n. Suppose A is a standard representation of f, P, b, T and B is a standard representation of g, P, b, T. Then $A \frown B$ is a standard representation of $f + g$, P, b, T.

(39) Let n be an ordinal number, T be a connected term order of n, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f, g be polynomials of n, L, P be a non empty subset of Polynom-Ring(n, L), A, B be left linear combinations of P, b be a bag of n, and i be a natural number. Suppose A is a standard representation of f, P, b, T and $B = A \restriction i$ and $g = \sum(A_{\downharpoonright i})$.

Then B is a standard representation of $f-g$, P, b, T.

(40) Let n be an ordinal number, T be a connected term order of n, L be an Abelian right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f, g be polynomials of n, L, P be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$, A, B be left linear combinations of P, b be a bag of n, and i be a natural number. Suppose A is a standard representation of f, P, b, T and $B = A_{\restriction i}$ and $g = \sum(A \restriction i)$ and $i \leqslant \operatorname{len} A$. Then B is a standard representation of $f-g$, P, b, T.

(41) Let n be an ordinal number, T be a connected term order of n, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f be a non-zero polynomial of n, L, P be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$, and A be a left linear combination of P. Suppose A is a monomial representation of f. Then there exists a natural number i and there exists a non-zero monomial m of n, L and there exists a non-zero polynomial p of n, L such that $i \in \operatorname{dom} A$ and $p \in P$ and $A(i) = m * p$ and $\mathrm{HT}(f, T) \leqslant_T \mathrm{HT}(m * p, T)$.

(42) Let n be an ordinal number, T be a connected term order of n, L be a right zeroed add-associative right complementable unital distributive non trivial non empty double loop structure, f be a non-zero polynomial of n, L, P be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$, and A be a left linear combination of P. Suppose A is a standard representation of f, P, T. Then there exists a natural number i and there exists a non-zero monomial m of n, L and there exists a non-zero polynomial p of n, L such that $p \in P$ and $i \in \operatorname{dom} A$ and $A_i = m * p$ and $\mathrm{HT}(f, T) = \mathrm{HT}(m * p, T)$.

(43) Let n be an ordinal number, T be an admissible connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, f be a polynomial of n, L, and P be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$ such that $\mathrm{PolyRedRel}(P, T)$ reduces f to $0_n L$. Then f has a standard representation of P, T.

(44) Let n be an ordinal number, T be an admissible connected term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive field-like non trivial double loop structure, f be a non-zero polynomial of n, L, and P be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$. If f has a standard representation of P, T, then f is top reducible wrt P, T.

(45) Let n be a natural number, T be a connected admissible term order of n, L be an add-associative right complementable right zeroed commutative associative well unital distributive Abelian field-like non degenerated non empty double loop structure, and G be a non empty subset of $\mathrm{Polynom\text{-}Ring}(n, L)$. Then G is a Groebner basis wrt T if and only if for

every non-zero polynomial f of n, L such that $f \in G$–ideal holds f has a standard representation of G, T.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Reduction relations. *Formalized Mathematics*, 5(**4**):469–478, 1996.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Thomas Becker and Volker Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, Berlin, 1993.
[7] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_{\mathrm{T}}$. Arcs, line segments and special polygonal arcs. *Formalized Mathematics*, 2(**5**):617–621, 1991.
[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.
[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[13] Gilbert Lee and Piotr Rudnicki. On ordering of bags. *Formalized Mathematics*, 10(**1**):39–46, 2002.
[14] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.
[15] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.
[16] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[17] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[18] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.
[19] Christoph Schwarzweller. More on multivariate polynomials: Monomials and constant polynomials. *Formalized Mathematics*, 9(**4**):849–855, 2001.
[20] Christoph Schwarzweller. Characterization and existence of Gröbner bases. *Formalized Mathematics*, 11(**3**):293–301, 2003.
[21] Christoph Schwarzweller. Polynomial reduction. *Formalized Mathematics*, 11(**1**):113–123, 2003.
[22] Christoph Schwarzweller. Term orders. *Formalized Mathematics*, 11(**1**):105–111, 2003.
[23] Andrzej Trybulec. Introduction to arithmetics. *To appear in Formalized Mathematics*.
[24] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[25] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[26] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[27] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[28] Wojciech A. Trybulec. Partially ordered sets. *Formalized Mathematics*, 1(**2**):313–319, 1990.
[29] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[30] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[34] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(**1**):85–89, 1990.
[35] Hiroshi Yamazaki, Yoshinori Fujisawa, and Yatsuka Nakamura. On replace function and swap function for finite sequences. *Formalized Mathematics*, 9(**3**):471–474, 2001.

Received June 11, 2003