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

WWW: http://mizar.org/JFM/Vol15/groeb_2.html

The articles [23], [31], [32], [34], [33], [8], [3], [15], [28], [30], [9], [7], [5], [14], [12], [19], [18], [24], [27], [17], [1], [4], [13], [21], [20], [29], [26], [16], [10], [25], [2], [22], [11], and [35] provide the notation and terminology for this paper.

1. Preliminaries

The following propositions are true:

(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 $m \leq n$, 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 $k \in \mathrm{dom}\, p$ 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 $\sum \mathrm{Swap}(f, i, j) = \sum f$.

(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 $b_1 \leq_T b_3$ and $b_2 \leq_T b_3$, then $\max_T(b_1, b_2) \leq_T b_3$.

(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 $b_3 \leq_T b_1$ and $b_3 \leq_T b_2$, then $b_3 \leq_T \min_T(b_1, b_2)$.

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 as follows:

(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 by:

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

Let us note 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 $b \leq_T b'$.

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

One can prove the following 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

Next we state the proposition

(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 $0_nL \notin P$. 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_nL. 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 as follows:

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

The following propositions are true:

(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 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 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 S-Poly$(p_1,p_2,T) = 0_nL$.

(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 S-Poly$(m_1,m_2,T) = 0_nL$.

(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 S-Poly$(p,0_nL,T) = 0_nL$ and S-Poly$(0_nL,p,T) = 0_nL$.

(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 S-Poly$(p_1,p_2,T) = 0_nL$ or $\mathrm{HT}(\text{S-Poly}(p_1,p_2,T),T) <_T \mathrm{lcm}(\mathrm{HT}(p_1,T),\mathrm{HT}(p_2,T))$.

(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 $\mathrm{HT}(p_2,T) \mid \mathrm{HT}(p_1,T)$, then $\mathrm{HC}(p_2,T) \cdot p_1$ top reduces to 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 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 S-Poly(g_1,g_2,T) w.r.t. PolyRedRel(G,T), then $h = 0_nL$.

(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 commutative 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 $h = 0_nL$. 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_nL.

(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 $0_nL \notin G$. 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_nL. 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 verify that S-Poly(P,T) is finite.

The following proposition is true

(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 $0_nL \notin G$ 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 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 $A_{\downharpoonright i}$ is a left linear combination of P.

(34) Let L be a non empty multiplicative loop structure, P, Q be non empty subsets of 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 $i \in \mathrm{dom} A$ there exists a monomial m of n, L and there exists a polynomial p of n, L such that $p \in P$ and $A_i = m * p$.

We now 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 $\mathrm{Support} f \subseteq \bigcup\{\mathrm{Support}(m * p); m$ ranges over monomials of n, L, p ranges over polynomials of n, L: $\bigvee_{i:\text{natural number}} (i \in \mathrm{dom} A \ \wedge\ A_i = m * p)\}$.

(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 $i \in \mathrm{dom} A$ 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 $\mathrm{HT}(m * p, T) \leq_T b$.

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 $g = \sum(A_{\lfloor i})$. 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 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 $B = A_{\lfloor i}$ and $g = \sum(A \restriction i)$ and $i \leq \mathrm{len} A$. 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 Polynom-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 $i \in \mathrm{dom} A$ and $p \in P$ and $A(i) = m * p$ and $\mathrm{HT}(f,T) \leq_T \mathrm{HT}(m*p,T)$.

(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 Polynom-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 $i \in \mathrm{dom} A$ 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 Polynom-Ring(n,L) such that 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 Polynom-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 Polynom-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. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/ideal_1.html.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[3] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[4] Grzegorz Bancerek. Reduction relations. *Journal of Formalized Mathematics*, 7, 1995. http://mizar.org/JFM/Vol7/rewrite1.html.

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

[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. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/realset1.html.

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

[9] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finset_1.html.

[10] Agata Darmochwał and Yatsuka Nakamura. The topological space $\mathcal{E}^2_\mathrm{T}$. Arcs, line segments and special polygonal arcs. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/topreal1.html.

[11] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/rfinseq.html.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[13] Gilbert Lee and Piotr Rudnicki. On ordering of bags. *Journal of Formalized Mathematics*, 14, 2002. http://mizar.org/JFM/Vol14/bagorder.html.

[14] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/vectsp_2.html.

[15] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/algstr_1.html.

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

[17] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Journal of Formalized Mathematics*, 11, 1999. http://mizar.org/JFM/Vol11/polynom1.html.

[18] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Journal of Formalized Mathematics*, 12, 2000. http://mizar.org/JFM/Vol12/binom.html.

[19] Christoph Schwarzweller. More on multivariate polynomials: Monomials and constant polynomials. *Journal of Formalized Mathematics*, 13, 2001. http://mizar.org/JFM/Vol13/polynom7.html.

[20] Christoph Schwarzweller. Polynomial reduction. *Journal of Formalized Mathematics*, 14, 2002. http://mizar.org/JFM/Vol14/polyred.html.

[21] Christoph Schwarzweller. Term orders. *Journal of Formalized Mathematics*, 14, 2002. http://mizar.org/JFM/Vol14/termord.html.

[22] Christoph Schwarzweller. Characterization and existence of Gröbner bases. *Journal of Formalized Mathematics*, 15, 2003. http://mizar.org/JFM/Vol15/groeb_1.html.

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

[24] Andrzej Trybulec. Many-sorted sets. *Journal of Formalized Mathematics*, 5, 1993. http://mizar.org/JFM/Vol5/pboole.html.

[25] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. http://mizar.org/JFM/Addenda/numbers.html.

[26] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers operations: min, max, square, and square root. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/square_1.html.

[27] Wojciech A. Trybulec. Partially ordered sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/orders_1.html.

[28] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/rlvect_1.html.

[29] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[30] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseq_4.html`.

[31] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

[32] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

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

[34] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_2.html`.

[35] Hiroshi Yamazaki, Yoshinori Fujisawa, and Yatsuka Nakamura. On replace function and swap function for finite sequences. *Journal of Formalized Mathematics*, 12, 2000. `http://mizar.org/JFM/Vol12/finseq_7.html`.

Received June 11, 2003

Published January 2, 2004