FORMALIZED MATHEMATICS
Volume **31**, **2023**, Pages 1–8
DOI: 10.2478/forma-2023-0001
e-ISSN: 1898–9934

sciendo.com/journal/forma

On Bag of 1. Part I

Yasushige Watase
Suginami-ku Matsunoki 6, 3-21 Tokyo
Japan

Summary. The article concerns about formalizing multivariable formal power series and polynomials [3] in one variable in terms of “bag” (as described in detail in [9]), the same notion as multiset over a finite set, in the Mizar system [1], [2]. Polynomial rings and ring of formal power series, both in one variable, have been formalized in [6], [5] respectively, and elements of these rings are represented by infinite sequences of scalars. On the other hand, formalization of a multivariate polynomial requires extra techniques of using “bag” to represent monomials of variables, and polynomials are formalized as a function from bags of variables to the scalar ring. This means the way of construction of the rings are different between single variable and multi variables case (which implies some tedious constructions, e.g. in the case of ten variables in [8], or generally in the problem of prime representing polynomial [7]). Introducing bag-based construction to one variable polynomial ring provides straight way to apply mathematical induction to polynomial rings with respect to the number of variables. Another consequence from the article, a polynomial ring is a subring of an algebra [4] over the same scalar ring, namely a corresponding formal power series. A sketch of actual formalization of the article is consists of the following four steps:

1. translation between **Bags 1** (the set of all bags of a singleton) and $\mathbb{N}$;
2. formalization of a bag-based formal power series in multivariable case over a commutative ring denoted by **Formal-Series**(n, R);
3. formalization of a polynomial ring in one variable by restricting one variable case denoted by **Polynom-Ring**$(1, R)$. A formal proof of the fact that polynomial rings are a subring of **Formal-Series**(n, R), that is R-Algebra, is included as well;
4. formalization of a ring isomorphism to the existing polynomial ring in one variable given by sequence: **Polynom-Ring**$(1, R) \stackrel{\sim}{\longrightarrow}$ **Polynom-Ring** R.

MSC: 13F25 13B25 68V20

Keywords: bag; formal power series; polynomial ring

MML identifier: `POLYALGX`, version: `8.1.12 5.74.1441`

1. Preliminaries

From now on o, o_1, o_2 denote objects, n denotes an ordinal number, R, L denote non degenerated commutative rings, and b denotes a bag of 1.

Let us consider a sequence f of R. Now we state the propositions:

(1) Support $f = \emptyset$ if and only if $f = \mathbf{0}.R$.

(2) If Support f is finite, then f is a finite-Support sequence of R. The theorem is a consequence of (1).

(3) If f is a finite-Support sequence of R, then Support f is finite.

Let us consider a bag b of 1. Now we state the propositions:

(4) Translation Bags 1 notation to NAT:

(i) $\operatorname{dom} b = \{0\}$, and

(ii) $\operatorname{rng} b = \{b(0)\}$.

(5) $b = 1 \longmapsto b(0)$.

Proof: For every o such that $o \in \operatorname{dom} b$ holds $b(o) = (1 \longmapsto b(0))(o)$. $\square$

Let us consider bags b_1, b_2 of 1. Now we state the propositions:

(6) $b_1 + b_2 = 1 \longmapsto b_1(0) + b_2(0)$.

Proof: $\operatorname{dom}(b_1 + b_2) = \{0\}$. For every object x such that $x \in \operatorname{dom}(b_1 + b_2)$ holds $(b_1 + b_2)(x) = (1 \longmapsto b_1(0) + b_2(0))(x)$. $\square$

(7) $b_1 -' b_2 = 1 \longmapsto b_1(0) -' b_2(0)$.

Proof: $\operatorname{dom}(b_1 -' b_2) = \{0\}$. For every object x such that $x \in \operatorname{dom}(b_1 -' b_2)$ holds $(b_1 -' b_2)(x) = (1 \longmapsto b_1(0) -' b_2(0))(x)$. $\square$

(8) $b_1(0) \leqslant b_2(0)$ if and only if $b_1 \mid b_2$.

Proof: If $b_1(0) \leqslant b_2(0)$, then $b_1 \mid b_2$. $\square$

(9) Let us consider an ordinal number n. Then BagOrder n linearly orders Bags n.

The functor NBag1 yielding a function from $\mathbb{N}$ into Bags 1 is defined by

(Def. 1) for every element m of $\mathbb{N}$, $it(m) = 1 \longmapsto m$.

The functor BagN1 yielding a function from Bags 1 into $\mathbb{N}$ is defined by

(Def. 2) for every element b of Bags 1, $it(b) = b(0)$.

Now we state the propositions:

(10) $(\mathrm{BagN1}) \cdot (\mathrm{NBag1}) = \mathrm{id}_{\mathbb{N}}$.

Proof: For every o such that $o \in \operatorname{dom}((\mathrm{BagN1}) \cdot (\mathrm{NBag1}))$ holds $((\mathrm{BagN1}) \cdot (\mathrm{NBag1}))(o) = (\mathrm{id}_{\mathbb{N}})(o)$. $\square$

(11) $(\mathrm{NBag1}) \cdot (\mathrm{BagN1}) = \mathrm{id}_{\mathrm{Bags}\,1}$.

Proof: For every o such that $o \in \operatorname{dom}((\mathrm{NBag1}) \cdot (\mathrm{BagN1}))$ holds $((\mathrm{NBag1}) \cdot (\mathrm{BagN1}))(o) = (\mathrm{id}_{\mathrm{Bags}\,1})(o)$. $\square$

One can check that NBag1 is one-to-one and onto and BagN1 is one-to-one and onto. Now we state the proposition:

(12) Let us consider bags b_1, b_2 of 1. Then

(i) $b_2 \in \operatorname{rng} \operatorname{divisors} b_1$ iff $b_2(0) \leqslant b_1(0)$, and

(ii) $b_2 \in \operatorname{rng} \operatorname{divisors} b_1$ iff $b_2 \mid b_1$.

The theorem is a consequence of (9) and (8).

Let us consider a bag b of 1. Now we state the propositions:

(13) $\operatorname{rng} \operatorname{divisors} b = \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$. The theorem is a consequence of (12).

(14) $\operatorname{rng}(\mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1}) = \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$.
PROOF: For every o such that $o \in \operatorname{rng}(\mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1})$ holds $o \in \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$. For every o such that $o \in \{x$, where x is a bag of $1 : x(0) \leqslant b(0)\}$ holds $o \in \operatorname{rng}(\mathrm{NBag1} \restriction \mathbb{Z}_{b(0)+1})$. $\square$

(15) $\operatorname{len} \operatorname{divisors} b = b(0) + 1$. The theorem is a consequence of (14) and (13).

2. Natural Number vs. Bag of Singleton

Let n be an ordinal number. Let us consider L. The functor Formal-Series(n, L) yielding a strict, non empty algebra structure over L is defined by

(Def. 3) for every set x, $x \in$ the carrier of *it* iff x is a series of n, L and for every elements x, y of *it* and for every series p, q of n, L such that $x = p$ and $y = q$ holds $x + y = p + q$ and for every elements x, y of *it* and for every series p, q of n, L such that $x = p$ and $y = q$ holds $x \cdot y = p * q$ and for every element a of L and for every element x of *it* and for every series p of n, L such that $x = p$ holds $a \cdot x = a \cdot p$ and $0_{it} = 0_n L$ and $1_{it} = 1\_(n, L)$.

Let us observe that Formal-Series(n, L) is Abelian, add-associative, right zeroed, right complementable, commutative, and associative and Formal-Series(n, L) is well unital and right distributive.

Now we state the proposition:

(16) Let us consider an ordinal number n, L, an element a of L, and series p, q of n, L. Then $a \cdot (p + q) = a \cdot p + a \cdot q$.
PROOF: For every element i of $\operatorname{Bags} n$, $(a \cdot (p + q))(i) = (a \cdot p + a \cdot q)(i)$. $\square$

Let us consider an ordinal number n, L, elements a, b of L, and a series p of n, L. Now we state the propositions:

(17) $(a + b) \cdot p = a \cdot p + b \cdot p$.
PROOF: For every element i of $\operatorname{Bags} n$, $((a + b) \cdot p)(i) = (a \cdot p + b \cdot p)(i)$. $\square$

(18) $(a \cdot b) \cdot p = a \cdot (b \cdot p)$.

(19) Let us consider an ordinal number n, L, and a series p of n, L. Then $1_L \cdot p = p$.

Let n be an ordinal number. Let us consider L. One can verify that Formal-Series(n, L) is vector distributive, scalar distributive, scalar associative, and scalar unital. Now we state the proposition:

(20) Let us consider an ordinal number n, and L. Then Formal-Series(n, L) is mix-associative.

PROOF: For every element a of L and for every elements x, y of Formal-Series(n, L), $a \cdot (x \cdot y) = (a \cdot x) \cdot y$. $\square$

Let n be an ordinal number. Let us consider L. Let us observe that Formal-Series(n, L) is mix-associative.

3. Constructing R-Algebra of Multivariate Formal Power Series

Now we state the proposition:

(21) Polynom-Ring(n, R) is a subring of Formal-Series(n, R).

PROOF: Set P_2 = Polynom-Ring(n, R). Set F_2 = Formal-Series(n, R). If $o \in$ the carrier of P_2, then $o \in$ the carrier of F_2. The addition of P_2 = (the addition of F_2) $\restriction$ (the carrier of P_2). The multiplication of P_2 = (the multiplication of F_2) $\restriction$ (the carrier of P_2). $\square$

Let us consider R. Now we state the propositions:

(22) $(0_1 R) \cdot (\text{NBag}1) = \mathbf{0}.R$.

PROOF: For every o such that $o \in \text{dom}((0_1 R) \cdot (\text{NBag}1))$ holds $((0_1 R) \cdot (\text{NBag}1))(o) = (\mathbf{0}.R)(o)$. $\square$

(23) $(0_1 R +\cdot (\text{EmptyBag}\,1, 1_R)) \cdot (\text{NBag}1) = \mathbf{0}.R +\cdot (0, 1_R)$.

PROOF: For every o such that $o \in \text{dom}(\mathbf{0}.R +\cdot (0, 1_R))$ holds $((0_1 R +\cdot (\text{EmptyBag}\,1, 1_R)) \cdot (\text{NBag}1))(o) = (\mathbf{0}.R +\cdot (0, 1_R))(o)$. $\square$

(24) $(0_1 R +\cdot (1 \longmapsto 1, 1_R)) \cdot (\text{NBag}1) = \mathbf{0}.R +\cdot (1, 1_R)$.

PROOF: For every o such that $o \in \text{dom}(\mathbf{0}.R +\cdot (1, 1_R))$ holds $((0_1 R +\cdot (1 \longmapsto 1, 1_R)) \cdot (\text{NBag}1))(o) = (\mathbf{0}.R +\cdot (1, 1_R))(o)$. $\square$

(25) Let us consider a bag b of 1. Then

(i) SgmX(BagOrder 1, rng divisors b) = XFS2FS(NBag1 $\restriction \mathbb{Z}_{b(0)+1}$), and

(ii) divisors b = XFS2FS(NBag1 $\restriction \mathbb{Z}_{b(0)+1}$).

PROOF: Set F = NBag1 $\restriction \mathbb{Z}_{b(0)+1}$. For every natural numbers n, m such that $n, m \in \text{dom}(\text{XFS2FS}(F))$ and $n < m$ holds $(\text{XFS2FS}(F))_{/n} \neq (\text{XFS2FS}(F))_{/m}$ and $\langle (\text{XFS2FS}(F))_{/n}, (\text{XFS2FS}(F))_{/m} \rangle \in$ BagOrder 1. Reconsider S = rng divisors b as a non empty, finite subset of Bags 1. For every bag p of 1, $p \in S$ iff $p \mid b$. $\square$

4. Constructing Isomorphism from Formal-Series$(1, R)$ to Formal-Series R

Let us consider R. The functor BSFSeries(R) yielding a function from Formal-Series$(1, R)$ into Formal-Series R is defined by

(Def. 4) for every object x such that $x \in$ the carrier of Formal-Series$(1, R)$ there exists a series x_1 of 1, R such that $x_1 = x$ and $it(x) = x_1 \cdot$ (NBag1).

Let us observe that BSFSeries(R) is one-to-one and onto. Now we state the propositions:

(26) Let us consider a ring R, and series f, g of 1, R. Then $(f+g) \cdot (\text{NBag1}) = f \cdot (\text{NBag1}) + g \cdot (\text{NBag1})$.
Proof: For every o such that $o \in \mathbb{N}$ holds $((f + g) \cdot (\text{NBag1}))(o) = (f \cdot (\text{NBag1}) + g \cdot (\text{NBag1}))(o)$. $\square$

(27) Let us consider elements f, g of Formal-Series$(1, R)$. Then $(\text{BSFSeries}(R))(f + g) = (\text{BSFSeries}(R))(f) + (\text{BSFSeries}(R))(g)$. The theorem is a consequence of (26).

(28) Let us consider series f, g of 1, R. Then $(f * g) \cdot (\text{NBag1}) = f \cdot (\text{NBag1}) * g \cdot (\text{NBag1})$.
Proof: For every o such that $o \in \mathbb{N}$ holds $((f * g) \cdot (\text{NBag1}))(o) = (f \cdot (\text{NBag1}) * g \cdot (\text{NBag1}))(o)$. $\square$

(29) Let us consider elements f, g of Formal-Series$(1, R)$. Then $(\text{BSFSeries}(R))(f \cdot g) = (\text{BSFSeries}(R))(f) \cdot (\text{BSFSeries}(R))(g)$. The theorem is a consequence of (28).

(30) $(\text{BSFSeries}(R))(1_{\text{Formal-Series}(1,R)}) = 1_{\text{Formal-Series}\,R}$. The theorem is a consequence of (23).

Let us consider R. Let us note that BSFSeries(R) is additive, multiplicative, and unity-preserving. Now we state the proposition:

(31) (i) BSFSeries(R) inherits ring isomorphism, and

(ii) Formal-Series R is (Formal-Series$(1, R)$)-isomorphic.

Let us consider R. One can verify that Formal-Series R is (Formal-Series$(1, R)$)-homomorphic, (Formal-Series$(1, R)$)-monomorphic, and (Formal-Series$(1, R)$)-isomorphic.

The functor SBFSeries(R) yielding a function from Formal-Series R into Formal-Series$(1, R)$ is defined by

(Def. 5) for every object x such that $x \in$ the carrier of Formal-Series R there exists a sequence x_1 of R such that $x_1 = x$ and $it(x) = x_1 \cdot$ (BagN1).

Now we state the proposition:

(32) $(\mathrm{BSFSeries}(R))^{-1} = \mathrm{SBFSeries}(R)$.

PROOF: For every o such that $o \in \mathrm{dom}((\mathrm{SBFSeries}(R)) \cdot (\mathrm{BSFSeries}(R)))$ holds $((\mathrm{SBFSeries}(R)) \cdot (\mathrm{BSFSeries}(R)))(o) = (\mathrm{id}_{\mathrm{dom}(\mathrm{BSFSeries}(R))})(o)$. $\square$

Let us consider R. One can check that $\mathrm{SBFSeries}(R)$ is one-to-one and onto. Now we state the proposition:

(33) $\mathrm{SBFSeries}(R)$ inherits ring homomorphism.

PROOF: Set $P = \mathrm{BSFSeries}(R)$. Set $F_1 = \text{Formal-Series}(1, R)$. Set $F_2 = \text{Formal-Series}\, R$. For every elements x, y of F_2, $(P^{-1})(x+y) = (P^{-1})(x) + (P^{-1})(y)$ and $(P^{-1})(x \cdot y) = (P^{-1})(x) \cdot (P^{-1})(y)$ and $(P^{-1})(\mathbf{1}_{F_2}) = \mathbf{1}_{F_1}$. $\square$

Let us consider R. One can check that $\mathrm{SBFSeries}(R)$ is additive, multiplicative, and unity-preserving. Now we state the proposition:

(34) (i) $\mathrm{SBFSeries}(R)$ inherits ring isomorphism, and

(ii) $\text{Formal-Series}(1, R)$ is $(\text{Formal-Series}\, R)$-isomorphic.

Let us consider R. Let us observe that $\text{Formal-Series}(1, R)$ is $(\text{Formal-Series}\, R)$-homomorphic, $(\text{Formal-Series}\, R)$-monomorphic, and $(\text{Formal-Series}\, R)$-isomorphic.

5. Constructing Isomorphism from Polynom-Ring$(1, R)$ to Polynom-Ring R

Now we state the propositions:

(35) Polynom-Ring R is a subring of Formal-Series R.

(36) Let us consider sequences f_1, g_1 of R. Then $(f_1 + g_1) \cdot (\mathrm{BagN1}) = f_1 \cdot (\mathrm{BagN1}) + g_1 \cdot (\mathrm{BagN1})$.

PROOF: For every o such that $o \in \mathrm{dom}((f_1 + g_1) \cdot (\mathrm{BagN1}))$ holds $((f_1 + g_1) \cdot (\mathrm{BagN1}))(o) = (f_1 \cdot (\mathrm{BagN1}) + g_1 \cdot (\mathrm{BagN1}))(o)$. $\square$

(37) Let us consider a sequence f of the carrier of R. Then $f = f \cdot (\mathrm{BagN1}) \cdot (\mathrm{NBag1})$. The theorem is a consequence of (10).

(38) Let us consider a series f of 1, R. Then $f = f \cdot (\mathrm{NBag1}) \cdot (\mathrm{BagN1})$. The theorem is a consequence of (11).

(39) Let us consider a sequence f of R.
Then $(\mathrm{NBag1})^{\circ}(\mathrm{Support}\, f) = \mathrm{Support}\, f \cdot (\mathrm{BagN1})$.

PROOF: For every o, $o \in (\mathrm{NBag1})^{\circ}(\mathrm{Support}\, f)$ iff $o \in \mathrm{Support}\, f \cdot (\mathrm{BagN1})$. $\square$

(40) Let us consider a subset B of $\mathbb{N}$. Then $\overline{\overline{B}} = \overline{\overline{(\mathrm{NBag1})^{\circ} B}}$.

(41) Let us consider a sequence f of R. Then $\overline{\overline{\mathrm{Support}\, f}} = \overline{\overline{\mathrm{Support}\, f \cdot (\mathrm{BagN1})}}$. The theorem is a consequence of (40) and (39).

(42) Let us consider a series f of $1, R$. Then $(\mathrm{BagN1})^\circ(\mathrm{Support}\, f) = \mathrm{Support}\, f \cdot (\mathrm{NBag1})$.

PROOF: For every o, $o \in (\mathrm{BagN1})^\circ(\mathrm{Support}\, f)$ iff $o \in \mathrm{Support}\, f \cdot (\mathrm{NBag1})$. $\square$

(43) Let us consider a subset B of Bags 1. Then $\overline{\overline{B}} = \overline{\overline{(\mathrm{BagN1})^\circ B}}$.

(44) Let us consider a series f of $1, R$. Then $\overline{\overline{\mathrm{Support}\, f}} = \overline{\overline{\mathrm{Support}\, f \cdot (\mathrm{NBag1})}}$. The theorem is a consequence of (43) and (42).

Let us consider R. The functor $\mathrm{BSPoly}(R)$ yielding a function from Polynom-Ring$(1, R)$ into Polynom-Ring R is defined by the term

(Def. 6) $\mathrm{BSFSeries}(R) \restriction \Omega_{\text{Polynom-Ring}(1,R)}$.

Now we state the proposition:

(45) $\mathrm{BSPoly}(R)$ is one-to-one and onto.

PROOF: $\mathrm{BSPoly}(R)$ is onto. $\square$

Let us consider R. Let us observe that $\mathrm{BSPoly}(R)$ is one-to-one and onto.

Let us consider elements p, q of Polynom-Ring$(1, R)$ and elements f, g of Formal-Series$(1, R)$. Now we state the propositions:

(46) If $p = f$ and $q = g$, then $p + q = f + g$.

(47) If $p = f$ and $q = g$, then $p \cdot q = f \cdot g$.

Let us consider elements f, g of Polynom-Ring$(1, R)$. Now we state the propositions:

(48) $(\mathrm{BSPoly}(R))(f + g) = (\mathrm{BSPoly}(R))(f) + (\mathrm{BSPoly}(R))(g)$. The theorem is a consequence of (35), (27), and (46).

(49) $(\mathrm{BSPoly}(R))(f \cdot g) = (\mathrm{BSPoly}(R))(f) \cdot (\mathrm{BSPoly}(R))(g)$. The theorem is a consequence of (35), (29), and (47).

(50) $(\mathrm{BSPoly}(R))(1_{\text{Polynom-Ring}(1,R)}) = 1_{\text{Polynom-Ring}\, R}$. The theorem is a consequence of (35) and (30).

Let us consider R. Note that $\mathrm{BSPoly}(R)$ is additive, multiplicative, and unity-preserving. Now we state the proposition:

(51) (i) $\mathrm{BSPoly}(R)$ inherits ring isomorphism, and

(ii) Polynom-Ring R is (Polynom-Ring$(1, R)$)-isomorphic.

Let us consider R. Let us observe that Polynom-Ring R is (Polynom-Ring$(1, R)$)-homomorphic, (Polynom-Ring$(1, R)$)-monomorphic, and (Polynom-Ring$(1, R)$)-isomorphic.

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] Edward J. Barbeau. *Polynomials*. Springer, 2003.

[4] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[5] Ewa Grądzka. The algebra of polynomials. *Formalized Mathematics*, 9(**3**):637–643, 2001.

[6] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.

[7] Karol Pąk. Prime representing polynomial. *Formalized Mathematics*, 29(**4**):221–228, 2021. doi:10.2478/forma-2021-0020.

[8] Karol Pąk. Prime representing polynomial with 10 unknowns. *Formalized Mathematics*, 30(**4**):255–279, 2022. doi:10.2478/forma-2022-0021.

[9] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

Accepted March 31, 2023