Graded shuffle algebras over fields of prime characteristic

Gérard Duchamp and Alexander A. Mikhalev

Abstract. We describe the structure of the free associative algebra over a field of prime characteristic with the new multiplication given by the super shuffle product.

Résumé. Nous décrivons la structure de l'algèbre libre sur un corps de caractéristique première quand elle est munie de la nouvelle multiplication donnée par le super produit de shuffle.

Let G be an abelian monoid, K a commutative associative ring with identity element, $char K \neq 2$, $U(K)$ the group of invertible elements of K, $\varepsilon : G \times G \to U(K)$ a skew symmetric bilinear form (a bicharacter), that is

$$\varepsilon(g_1 + g_2, h) = \varepsilon(g_1, h)\varepsilon(g_2, h), \;\; \varepsilon(g, h_1 + h_2) = \varepsilon(g, h_1)\varepsilon(g, h_2),$$

$$\varepsilon(g, h)\varepsilon(h, g) = 1, \;\; \varepsilon(g, g) = \pm 1$$

for all $g, g_1, g_2, h, h_1, h_2 \in G$,

$$G_- = \{g \in G \mid \varepsilon(g, g) = -1\}, \;\; G_+ = \{g \in G \mid \varepsilon(g, g) = +1\}.$$

Let $X = \cup_{g \in G} X_g$ be a G-graded set, i.e. $X_g \cap X_f = \emptyset$ for $g \neq f$, $d(x) = g$ for $x \in X_g$; let also $S(X)$ be the free monoid of associative words on X. For

$u = x_1 \dots x_n \in S(X)$, $x_i \in X$, we consider the word length $l(u) = n$, and set $d(u) = \sum_{i=1}^{n} d(x_i) \in G$, $S(X)_g = \{u \in S(X) \mid d(u) = g\}$. Let $A(X)_g$ $(g \in G)$ be the K-linear spans of the subsets $S(X)_g$ in the free associative algebra $A(X)$. Then $A(X) = \oplus_{g \in G} A(X)_g$ is the free G-graded associative K-algebra on X.

Suppose that the set $X = \cup_{g \in G} X_g$ is totally ordered and the set $S(X)$ is ordered lexicographically, i.e. for $u = x_1 \dots x_r$ and $v = y_1 \dots y_m$ where $x_i, y_j \in X$ we have $u < v$ if either $x_i = y_i$ for $i = 0, 1, \dots, t-1$ and $x_t < y_t$ or $x_i = y_i$ for $i = 1, 2, \dots, m$ and $r > m$.

A word $u \in S(X)$ is said to be *regular* if $u \neq 1$ and it follows from $u = ab, a, b \in S(X), a, b \neq 1$, that $u = ab > ba$ (this condition is equivalent to the condition $u = ab > b$). A word $w \in S(X)$ is said to be *s-regular* if either w is a regular word, or $w = uu$ with u a regular word, $d(u) \in G_-$. Let p be a prime number not equal to 2. A word $w \in S(X)$ is said to be *ps*-regular if it is either an s-regular word, or $w = u^{p^t}$ with $t \in \mathbf{N}$, u an s-regular word, $d(u) \in G_+$.

Shuffle algebras were introduced by R. Ree in [Ree1, Ree2]. Details of applications of shuffle algebras to free Lie algebras may be found in [Reu].

Let V abd Z be G-graded sets, $V \cap Z = \emptyset$, $v_1, \dots, v_k$ pairwise distinct elements of V, $z_1 \dots, z_l$ pairwise distinct elements of Z. We say that a word $w \in S(V \cup Z) \backslash 1$ is a shuffle word of the words $v_1 \cdots v_k$ and $z_1 \cdots z_l$ if w has the multidegree

$$m(w) = v_1 + \dots + v_k + z_1 \cdots z_l$$

and

$$w|_{z_1=1,\dots,z_l=1} = v_1 \cdots v_k; \quad w|_{v_1=1,\dots,v_k=1} = z_1 \cdots z_l.$$

The parity $\sigma(w)$ of a shuffle word w of the words $v_1 \cdots v_k$ and $z_1 \cdots z_l$ is the sum of all $\varepsilon(z_i, v_j)$ such that z_i is situated before v_j in w.

Let X be a G-graded set. For $x_{i_1}, \dots x_{i_k}, x_{j_1}, \dots, x_{j_l} \in X$ we define the shuffle product $(x_{i_1} \cdots x_{i_k}) * (x_{j_1} \cdots x_{j_l})$ as the following linear combination of words of multidegree $x_{i_1} + \dots + x_{i_k} + x_{j_1} \dots + x_{j_l}$:

$$(x_{i_1} \cdots x_{i_k}) * (x_{j_1} \cdots x_{j_l}) = \textstyle\sum_w \sigma(w) w\big|_{v_s = x_{i_s}, s=1,\dots,k; z_t = x_{j_t}, t=1,\dots,l}$$

where w is running through all shuffle words of the words $v_1 \cdots v_k$ and $z_1 \cdots z_l$ with $d(v_s) = d(x_{i_s}), d(z_t) = d(x_{j_t})$. Taking $1 * u = u * 1 = u$ for all $u \in S(X) \setminus 1$ and extending $*$ on the free G-graded associative algebra $A(X)$ on X over a commutative associative ring K with the identity element by linearity, we define the shuffle product $*$ on $A(X)$. Then $A(X)$ with this product is an ε-commutative and associative algebra (see [Ree2]).

One can define the shuffle product $*$ on $A(X)$ in the following way:

$$1 * u = u * 1 = u; \quad (xu) * (yv) = x(u * (yv)) + \varepsilon(y, x)\varepsilon(y, u) y((xu) * v)$$

for all $x, y \in X$, $u, v \in S(X) \setminus 1$ (with the extension $*$ on $A(X)$ by linearity).

If we consider $A(X)$ as the universal enveloping algebra of the free color Lie superalgebra $L(X)$, then $*$ is the adjoint of coproduct δ of $A(X)$.

In fact, for this definition (and associativity of this law), ε need only be bilinear and (see [DKKT]) is the unique law for which 1 is neutral and the operators $(x^{-1})_{x\in X}$ (i.e. the adjoints of the multiplication by letters) are superderivations.

Let Y be a G-graded set, and let J be the two-sided ideal of the free G-graded associative algebra $A(Y)$ generated by the G–homogeneous elements

$$ab - \varepsilon(d(a), d(b))ba,$$

where a, b are elements of $S(Y)$, and $K_\varepsilon[Y] = A(Y)/J$. Then the algebra $K_\varepsilon[Y]$ is the free ε-commutative associative K-algebra with the set Y of free generators. If $G_- = \emptyset$, then $K_\varepsilon[Y]$ is the algebra of quantum polynomials. If $\varepsilon \equiv 1$, then $K_\varepsilon[Y]$ is the usual polynomial algebra. In general case the algebra $K_\varepsilon[Y]$ is the universal enveloping algebra of a Abelian color Lie superalgebra (see [BMPZ], [MZ3]).

D. Radford in [Rad] proved that in the case of trivial grading group the free associative algebra as a shuffle algebra is the free commutative associative algebra with a set of free generators consisting of Lyndon words (see also [Reu]). A. A. Mikhalev and A. A. Zolotykh showed in [MZ1, MZ2] that if K is a $\mathbf{Q}$-algebra, then $A(X)$ with the shuffle product $*$ is the free ε-commutative algebra with a set of free generators consisting of s-regular words.

We consider the case where K is a field, $char K = p > 2$. Let $R(X)$ be the set of ps-regular words of $S(X)$, $R(X) = R_+ \cup R_-$, where

$$R_+ = \{r \in R(X) \mid d(r) \in G_+\}, \quad R_- = \{r \in R(X) \mid d(r) \in G_-\}.$$

By $K_\varepsilon[R(X)]$ we denote the free ε-commutative K-algebra generated by the set $R(X)$.

Theorem *Let K be a field, $char K = p > 2$. Then the free G-graded associative algebra $A(X)$ with the new multiplication given by the shuffle product $*$ is isomorphic to the factor algebra $K_\varepsilon[R(X)]/I$, where I is the ideal of $K_\varepsilon[R(X)]$ generated by the set $\{u^p \mid u \in R_+\}$. In particular, if $G = \{e\}$, then the algebra $A(X)$ with the shuffle multiplication is isomorphic to the algebra of p-reduced polynomials on regular (or on Lyndon) words.*

[BMPZ] Yu. A. Bahturin, A. A. Mikhalev, V. M. Petrogradsky, and M. V. Zaicev, *Infinite Dimensional Lie Superalgebras*. Walter de Gruyter Publ., Berlin–New York, 1992.

[DKKT] G. Duchamp, A. Klyachko, D. Krob, and J.-Y. Thibon, *Noncommutative symmetric functions III: Deformation of Cauchy and convolution algebras*. Disc. Math. and Th. Comp. Sci. **1** (1997), 159–216.

[MZ1] A. A. Mikhalev and A. A. Zolotykh, *Natural basis for ε-shuffle algebras*. 7th Conf. *Formal Power Series and Algebraic Combinatorics*, Univ. Marne-la-Vallée, 1995, 423–426.

[MZ2] A. A. Mikhalev and A. A. Zolotykh, *Bases of free super shuffle algebras*. Uspekhi Matem. Nauk **50** (1995), no. 1, 199–200. English translation: Russian Math. Surveys **50** (1995), no. 1, 225–226.

[MZ3] A. A. Mikhalev and A. A. Zolotykh, *Combinatorial Aspects of Lie Superalgebras*. CRC Press, Boca Raton, New York, 1995.

[Rad] D. E. Radford, *A natural ring basis for the shuffle algebra and an application to group schemes*. J. Algebra **58** (1979), 432–454.

[Ree1] R. Ree, *Lie elements and an algebra associated with shuffles*. Annals of Math. **68** (1958), 210–220.

[Ree2] R. Ree, *Generalized Lie elements*. Canadian J. Math. **12** (1960), 493–502.

[Reu] Ch. Reutenauer, *Free Lie Algebras*. Clarendon Press, Oxford, 1993.