УДК 512.54 DOI 10.17223/20710410/56/3

SUPERPOSITIONS OF FREE FOX DERIVATIONS[1]

V. Roman'kov

Dostoevsky Omsk State University, Omsk, Russia
Siberian Federal University, Krasnoyarsk, Russia

E-mail: romankov48@mail.ru

Fox derivations are an effective tool for studying free groups and their group rings. Let F_r be a free group of finite rank r with basis $\{f_1, \ldots, f_r\}$. For every i, the partial Fox derivations $\partial/\partial f_i$ and $\partial/\partial f_i^{-1}$ are defined on the group ring $\mathbb{Z}[F_r]$. For $k \geqslant 2$, their superpositions $D_{f_i^\epsilon} = \partial/\partial f_i^{\epsilon_k} \circ \ldots \circ \partial/\partial f_i^{\epsilon_1}, \epsilon = (\epsilon_1, \ldots, \epsilon_k) \in \{\pm 1\}^k$, are not Fox derivations. In this paper, we study the properties of superpositions $D_{f_i^\epsilon}$. It is shown that the restrictions of such superpositions to the commutant F_r' are Fox derivations. As an application of the obtained results, it is established that for any rational subset R of F_r' and any i there are parameters k and ϵ such that R is annihilated by $D_{f_i^\epsilon}$.

Keywords: *free group, group ring, Fox derivations, annihilators, rational subsets.*

СУПЕРПОЗИЦИИ СВОБОДНЫХ ПРОИЗВОДНЫХ ФОКСА

В. А. Романьков

Омский государственный университет им. Ф. М. Достоевского, г. Омск, Россия
Сибирский федеральный университет, г. Красноярск, Россия

Дифференцирования Фокса являются эффективным инструментом исследования свободных групп и их групповых колец. Пусть F_r — свободная группа конечного ранга r с базисом $\{f_1, \ldots, f_r\}$. Для любого i частные дифференцирования Фокса $\partial/\partial f_i$ и $\partial/\partial f_i^{-1}$ определены на групповом кольце $\mathbb{Z}[F_r]$. Для $k \geqslant 2$ их суперпозиции $D_{f_i^\epsilon} = \partial/\partial f_i^{\epsilon_k} \circ \ldots \circ \partial/\partial f_i^{\epsilon_1}, \epsilon = (\epsilon_1, \ldots, \epsilon_k) \in \{\pm 1\}^k$ не являются дифференцированиями Фокса. В работе изучаются свойства суперпозиций $D_{f_i^\epsilon}$. Показано, что ограничения таких суперпозиций на коммутант F_r' являются дифференцированиями Фокса. В качестве приложения полученных результатов установлено, что для любого рационального подмножества R коммутанта F_r' и любого i существуют параметры k и ϵ, такие, что R аннулируется суперпозицией $D_{f_i^\epsilon}$.

Ключевые слова: *свободная группа, групповое кольцо, дифференцирования Фокса, аннуляторы, рациональные подмножества.*

1. Introduction

Let F_r be a free group of finite rank r with basis $\{f_1, \ldots, f_r\}$ and let $\mathbb{Z}[F_r]$ be the integral group ring. In the paper, we consider the partial free derivations introduced by Fox [1]. In our notation, these are defined as follows.

[1]The research was supported by the grant from the Russian Science Foundation (project no. 19-71-10017).

For $j = 1, \ldots, r$, the (left) Fox derivation associated with f_j is the linear map $D_j : \mathbb{Z}[F_r] \to \mathbb{Z}[F_r]$ satisfying the conditions

$$D_j(f_j) = 1,\ D_j(f_i) = 0 \ \text{ for } \ i \neq j,$$
$$D_j(uv) = D_j(u) + uD_j(v) \ \text{ for all } \ u, v \in F_r.$$

Obviously, an element $u \in F_r$ is trivial if and only if $D_i(u) = 0$ for all $i = 1, \ldots, r$. Also, note that for an arbitrary element g from F_r and for each $j = 1, \ldots, n$ we have $D_j(g^{-1}) = = -g^{-1}D_j(g)$. An excellent introduction to Fox's theory of derivations and their possible uses can be found in [2], see also [3, 4]. Free derivations of group rings were introduced by R. Fox for their use in knot theory. Later, the tools of free derivations began to be widely used in algebra. See, for example, the paper [5], where free derivations are applied to solve algorithmic problems in solvable groups. Nowadays, there are applications of Fox derivations to cryptography; namely, to generation of pseudorandom sequences over solvable groups. See, e.g., [6, Part II], where the ergodic theory for polynomials over solvable groups with operators is developed, or [7], where main results of the theory are announced (or an earlier expository paper [8]). The techniques used in these works also utilizes Fox derivations.

Also, for each $i = 1, \ldots, r$ there is a unique derivation D_j^- with respect to the inverse f_i^{-1} for which $D_j^-(f_j^{-1}) = 1$ and $D_j^-(f_i) = 0$ for any $i \neq j$. Then $D_j^-(f_j) = -f_j$. The *trivialization* homomorphism $\tau : \mathbb{Z}[F_r] \to \mathbb{Z}$ is defined on the generators of F_r by $\tau(f_i) = 1$ for all $i = 1, \ldots, r$ and extended linearly to the group ring $\mathbb{Z}[F_r]$.

The Fox derivations appear in another setting as well. Let ΔF_r denote the fundamental ideal of the group ring $\mathbb{Z}[F_r]$. It is a free left $\mathbb{Z}[F_r]$-module with a free basis consisting of $\{f_1 - 1, \ldots, f_r - 1\}$. This leads us to the following formula, which is called the *main identity* for the Fox derivations:

$$\sum_{i=1}^{r} D_i(\alpha)(f_i - 1) = \alpha - \tau(\alpha), \tag{1}$$

where $\alpha \in \mathbb{Z}[F_r]$. Conversely, if for any element $f \in F_r$ and $\alpha_i \in \mathbb{Z}[F_r]$ we have equality

$$\sum_{i=1}^{r} \alpha_i(f_i - 1) = f - 1,$$

then $D_i(f) = \alpha_i$ for $i = 1, \ldots, r$.

Frequently, the free derivations D_j are denoted by $\partial/\partial f_j$ for $j = 1, \ldots, r$. If $w = = w(v_1, \ldots, v_m)$ is a group word in variables $v_1, \ldots, v_m$, we consider the values of the formal derivations $\partial w/\partial v_i$, for $i = 1, \ldots, m$.

Proposition 1 (chain rule). If w and $v_1, \ldots, v_m$ are words in F_r, with $w = w(v_1, \ldots, v_m)$ and $v_i = v_i(f_1, \ldots, f_r)$ for $i = 1, \ldots, m$, then

$$\frac{\partial}{\partial f_i}(w(v_1, \ldots, v_m)) = \sum_{k=1}^{m} \partial w/\partial v_k \cdot \partial v_k/\partial f_i \text{ for any } i = 1, \ldots, r.$$

More generally, we call a linear map $D : \mathbb{Z}F_r \to \mathbb{Z}F_r$ the *Fox derivation* if D satisfies the property

$$D(uv) = D(u) + uD(v)$$

for all $u, v \in F_r$. Every such derivation has the form

$$D = \alpha_1 D_1 + \ldots + \alpha_n D_r,$$

where $\alpha_i = D(f_i)$ for $i = 1, \dots, r$. By definition, $(\alpha D)(u) = D(u)\alpha$ for any $\alpha \in \mathbb{Z}[F_r]$, $u \in F_r$. Conversely, we can define a derivation $D = \sum_{i=1}^{r} \alpha_i D_i$ for arbitrary tuple of elements $\alpha_i \in \mathbb{Z}[F_r]$.

In the paper, we consider superpositions of partial derivations with respect to some variable f_i and its inverse f_i^{-1}. Let $k \in \mathbb{N}$. For any i and $\epsilon = (\epsilon_1, \dots, \epsilon_k) \in \{\pm 1\}^k$ the corresponding superposition is

$$D_{f_i^\epsilon} = \partial/\partial f_i^{\epsilon_k} \circ \dots \circ \partial/\partial f_i^{\epsilon_1}.$$

Recall that for $g \in F_r$ we have $D_{f_i^\epsilon}(g) = \partial/\partial f_i^{\epsilon_k}(\partial/\partial f_i^{\epsilon_{k-1}}(\dots(\partial/\partial f_i^{\epsilon_1}(g))))$.

We use the following notation: $\sigma_i(v)$ — the sum of all exponents in which the variable x_i occurs in the word v, F_r' — the derived subgroup (commutant) of the group F_r, $F_r'(i) \leqslant F_r$ — the subgroup of all words v for which $\sigma_i(v) = 0$ $(i = 1 \dots, r)$ (i-commutant). Hence, $F_r' = \bigcap_{i=1}^{r} F_r'(i)$.

2. Basic results

Let $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, be superposition of derivations on F_r. By definition, $\mathrm{Ann}(D)$ is the set of all elements $g \in F_r$ such that $D(g) = 0$ (annihilator of D on F_r).

Lemma 1. For any $i = 1, \dots, r$ and any finite set V of elements of F_r, there exists a number $k \in \mathbb{N}$ and a superposition of derivations $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, such that $V \subseteq \mathrm{Ann}(D)$.

Proof. We use induction on the maximum number $m_i(V)$ of occurrences of $f_i^{\pm 1}$ in elements from V. If $m_i(V) = 0$, then we take $D = D_i$. Let us apply to each of the words $v \in V$ the superposition of derivations $D_{f_i^\epsilon}$ for $\epsilon = (1, -1)$. It is obvious that the value of m_i for the set of all resulting elements V' of F_r will become strictly smaller. By the inductive hypothesis, there exists a superposition of derivations $D' = D_{f_i^\varepsilon}$, $\varepsilon \in \{\pm 1\}^l$, for which all these elements belong to $\mathrm{Ann}(V')$. Therefore, we can take $\epsilon = (1, -1, \varepsilon) \in \{\pm 1\}^{l+2}$ and get $V \subseteq \mathrm{Ann}(D(V))$. ■

Proposition 2. Let $v \in F_r$, $\sigma_i(v) = 0$. Then for any superposition of derivations $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, $k \in \mathbb{N}$, we have $\tau(D(v)) = 0$, i.e., the trivialization of $D(v)$ is zero.

Proof. We use induction on the (even) number $m_i(v)$ of occurrences of $f_i^{\pm 1}$ in v. If $m_i(v) = 0$, the statement is obvious. Let's represent v in the (reduced) form $v = u f_i^\nu z f_i^{-\nu} w$, $\nu \in \{\pm 1\}$, where z does not depend on $f_i^{\pm 1}$. Then we consider the corresponding reduced word $v' = u f_t w$, where $f_t \neq f_i$. By the induction hypothesis, the assertion of the proposition holds for v'.

Without changing the generality of reasoning, we assume that $\nu = 1$. We will sequentially perform derivations from the superposition D, starting from the element v. Consider the terms corresponding to the elements f_i and f_i^{-1} from the selected block $x = f_i z f_i^{-1}$. We have $u(1 - f_i z f_i^{-1})$ or $u(-f_i + f_i z)$. Further derivations do not change the factor u, results of derivations of the expression in brackets always has zero trivialization. Therefore, when calculating the trivialization, we can ignore the terms corresponding to the variables of the selected block.

There is a one-to one correspondence between the values of derivations corresponding to the occurences of $f_i^{\pm 1}$ for u and w in v and the corresponding occurences in v'. By the induction hypothesis, they all have zero trivialization. ■

Corollary 1. Any superposition of derivations of the form $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, $k \in \mathbb{N}$, is derivation on $F_r'(i)$. Therefore, it is derivation on F_r'.

Proof. We use induction on k. For $k = 1$ the statement is true. Let it be true for superposition $D' = D_{f_i^{\epsilon'}}$, $\epsilon' \in \{\pm 1\}^{k-1}$. By induction we have

$$D'(uw) = D'(u) + uD'(w).$$

By Proposition 2, $\tau(D'(w)) = 0$. Therefore,

$$D(uv) = \partial/\partial f_i^{\epsilon_k}(D'(u)) + \partial/\partial f_i^{\epsilon_k}(u)(\tau(D'(u)) + u\partial/\partial f_i^{\epsilon_k}(D'(w)) = D(u) + uD(w).$$

Corollary 1 is proved. ■

Lemma 2. Let $v \in F_r$ and let $v = uw$ be the reduced presentation. For any superposition D of the form $D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, such that $D(v) = 0$ we have $D(w) = 0$, and if $\sigma_i(w) = 0$, then $D(u) = 0$.

Proof. The equality $D(w) = 0$ is obvious, since the results of computing D with respect to occurrences of elements $f_i^{\pm 1}$ in w can cancel only among themselves. The second assertion follows from Proposition 2. ■

3. Applications. Rational sets

Following R. H. Gilman [9], we define for a given group G the set $Rat(G)$ of all *rational subsets* of G as the closure of the set of all finite subsets of G under the rational operations: union, product, and generation of a submonoid (Kleene's star operation). It is known [9] that a subset R of a group G is rational in G if and only if R is accepted by a finite automaton over G. For basic information about rational sets in groups see [9, 10]. Special aspects of the theory are contained in [11 – 13].

Theorem 1. Let F_r be a free group and let R be a rational subset of F_r'. Then for any $i = 1, \ldots, r$ there is a superposition $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, $k \in \mathbb{N}$, such that R belongs to $\mathrm{Ann}(D)$.

Proof. It is well known [9, 10] that any rational subset of an arbitrary group lies in a finitely generated submonoid. Let R lies in submonoid M generated by finite set $V \subseteq F_r'$. Let $V = \{v_1, \ldots, v_s\}$. By Lemma 1, there exists a superposition of derivations of the form $D = D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, such that $V \subseteq \mathrm{Ann}(D)$.

Let α be any element of M (in particular, $\alpha \in R$). We write α as the word $\alpha(v_1, \ldots, v_s)$. Let D_{v_i} be formal partial derivation. Then by (1) we have

$$\sum_{i=1}^{r} D_{v_i}(\alpha)(v_i - 1) = \alpha - \tau(\alpha).$$

Then by Proposition 2 we have

$$D\left(\sum_{i=1}^{r} D_{v_i}(\alpha)(v_i - 1)\right) = \sum_{i=1}^{r} D_{v_i}(\alpha)D(v_i) = 0.$$

Therefore, $D(\alpha - \tau(\alpha)) = D(\alpha) = 0$. ■

4. Conclusion

We have proved some results about superpositions of Fox partial derivations. In particular, we have established that the F_r'-restrictions of superpositions of the form $D_{f_i^\epsilon}$, $\epsilon \in \{\pm 1\}^k$, are Fox derivations. This allows us to use such superpositions to study the structure of subsets of the commutant F_r'. As an application, we have shown that any rational subset R of F_r' lies in an annihilator $\mathrm{Ann}(D_{f_i^\epsilon})$ for some $k \in \mathbb{N}$ and $\epsilon \in \{\pm 1\}^k$.

REFERENCES

1. *Fox R. H.* Free differential calculus I — Derivation in the free group ring. Ann. Math., 1953, vol. 57, pp. 547–560.
2. *Crowell R. H. and Fox R. H.* Introduction to Knot Theory. N.Y., Springer Verlag, 1963, X + 182 p.
3. *Timoshenko E. I.* Endomorfizmy i universal'nye teorii razreshimykh grupp [Endomorphisms and Universal Theories of Solvable Groups]. Novosibirsk, Novosibirsk State Technical University, 2011. 327 p. (in Russian)
4. *Roman'kov V. A.* Essays in Algebra and Cryptology. Solvable Groups. Omsk, Dostoevsky Omsk State University, 2017. 267 p.
5. *Myasnikov A., Roman'kov V., Ushakov A., and Vershik A.* The word and geodesic problems for free solvable groups. Trans. Amer. Math. Soc., 2010, vol. 362, no. 9, pp. 4655–4682.
6. *Anashin V. and Khrennikov A.* Applied Algebraic Dynamics (de Gruyter Expositions in Math., vol. 49). Berlin, N.Y., Walter de Gruyter GmbH & Co., 2009. 557 p.
7. *Anashin V.* Noncommutative algebraic dynamics: Ergodic theory for profinite groups. Proc. Steklov Institute of Mathematics, 2009, vol. 265, pp. 30–58.
8. *Anashin V. S.* Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers. J. Math. Sci., 1998, vol. 89, no. 4, pp. 1355–1390.
9. *Gilman R. H.* Formal languages and infinite groups. Geometric and Computational Perspectives of Infinite Groups, Minneapolis, MN, and New Brunswick, NJ, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 1994, vol. 25, pp. 27–51.
10. *Roman'kov V. A.* Ratsional'nye podmnozhestva v gruppakh [Rational subsets in groups]. Omsk, Dostoevsky Omsk State University, 2014. 176 p. (in Russian)
11. *Roman'kov V. A.* Polycyclic, metabelian or soluble of type $(FP)_\infty$ groups with Boolean algebra of rational sets and biautomatic soluble groups are virtually abelian. Glasgow Math. J., 2018, vol. 60, no. 1, pp. 209–218.
12. *Roman'kov V. A.* Rationality of verbal subsets in solvable groups. Algebra and Logic, 2018. vol. 57, no. 1, pp. 39–48.
13. *Roman'kov V. and Myasnikov A.* On rationality of verbal subsets in a group. Theory of Computing Systems, 2013, vol. 52, no. 4, pp. 587–598.