ISSN 2075-9827 **e-ISSN 2313-0210**
Carpathian Math. Publ. 2026, **18** (1), 211–221
doi:10.15330/cmp.18.1.211-221

https://journals.pnu.edu.ua/index.php/cmp
Карпатські матем. публ. 2026, Т.18, №1, С.211–221

Liftability and contracting property of multi-EGS groups

Malik A.A.[1], Savchuk D.[2]

We provide sufficient conditions for the multi-EGS groups to be liftable and thus produce new examples of groups acting transitively on regular trees of finite degree stabilizing one of the ends, whose closures are scale groups as defined by G.A. Willis. Additionally, we explicitly compute the contracting nuclei of the groups in this class. We also specialize our results to the classes of multi-edge spinal groups and EGS-groups.

Key words and phrases: liftable group, multi-EGS group, contracting group, group acting on trees.

[1] Indiana University South Bend, 1700 Mishawaka Ave., IN 46615, South Bend, USA
[2] University of South Florida, 4202 E Fowler Ave., FL 33620-5700, Tampa, USA
E-mail: malikaa@iu.edu (Malik A.A.), savchuk@usf.edu (Savchuk D.)

1 Introduction

The classes of groups studied in this paper have their origins in the pioneering works of R.I. Grigorchuk [10] and N. Gupta, S. Sidki [12]. The *GGS-groups* were introduced and studied from the early 1990s with the term initially introduced by G. Baumslag in [5]. These groups often share common unusual properties with the second Grigorchuk group acting on a 4-ary regular rooted tree, and Gupta-Sidki p-groups, such as being infinite finitely generated periodic, just infinite, or branch [4, 28]. Several further extensions of the class of GGS-groups was introduced afterwards. First, the construction was extended by E. Pervova [24] in 2007, who coined the term *extended Gupta-Sidki groups* (*EGS-groups*) and constructed the first examples of groups acting on rooted trees, whose closures in the corresponding tree automorphism groups do not coincide with their profinite completions. Each EGS-group contains a GGS-group as a subgroup and can be uniquely identified by it. Another generalization of GGS-groups, the class of *multi-edge spinal groups*, was proposed by T. Alexoudas, B. Klopsch and A. Thillaisundaram in 2016 [1]. This class is also called *multi-GGS groups* by A. Garrido and J. Uria-Albizuri in [9]. Finally, the latter groups were generalized by B. Klopsch and A. Thillaisundaram [16] to *generalized multi-edge spinal groups*, which were renamed to shorter *multi-EGS groups* in [27]. It was shown in [16] that under certain common conditions these groups are regular branch, just-infinite, and do not have a congruence subgroup property, in particular extending the result from [9] on multi-GGS groups. Some recent papers have studied the sizes of congruence quotients in GGS-groups [8] and the exponents of these quo-

УДК 512.54
2020 *Mathematics Subject Classification:* 20E08, 22D05.

The authors greatly acknowledge the support of American Institute of Mathematics (AIM). Part of this work was done in June 2024 during the workshop “Groups of dynamical origin” funded by AIM. The authors express sincere gratitude to anonymous referees whose comments and suggestions helped to improve the paper.

tients in multi-EGS groups [17]. We review the explicit connection between all these classes of groups in Section 3.

The class of *liftable self-similar groups* was introduced by R.I. Grigorchuk and the second author in [11] in connection with groups of isometries of local fields. The groups in this class admit natural ascending HNN extensions with respect to their *lifting endomorphisms* that act transitively on $(d+1)$-regular (unrooted) trees $\widetilde{T}_{d+1}$ (obtained as the union of a countable family of rooted d-ary trees T_d) preserving one of the ends and embed into the groups of isometries of local fields. Moreover, under mild conditions, their closures in the automorphism groups of $\widetilde{T}_{d+1}$ preserving a fixed end are scale groups as defined by G.A. Willis in [29]. The class of scale groups plays an important role in the theory of totally disconnected locally compact (TDLC) groups. It is shown in [11] that many well-known self-similar groups are liftable, including the first Grigorchuk group, the Basilica group, and the lamplighter group. It was also shown that not invertible symmetric GGS-groups [7] (in which the defining vector is nonsymmetric in the sense that it has a zero component, such that the symmetric component is non-zero) are also liftable.

The main purpose of this paper is to provide sufficient conditions for the multi-EGS groups to be liftable, thus providing new examples of liftable groups and at the same time suggesting new applications of multi-EGS groups. Each multi-EGS group acting on a p-ary rooted tree (for an odd prime p) is defined by a collection of p subspaces (not all empty) of the vector space $(\mathbb{Z}/p\mathbb{Z})^{p-1}$ that are defined by their bases $\mathbf{E}^{(l)} = \left\{\mathbf{e}_i^{(l)} = (e_{i,1}^{(l)}, \dots, e_{i,p-1}^{(l)}), 1 \le i \le r_l\right\}$ for each $1 \le l \le p$, where for each $1 \le l \le p$ the number $r_l \ge 0$ represents the dimension of the lth subspace $\mathbf{E}^{(l)}$. The collection

$$\mathbf{E} = \left(\mathbf{E}^{(1)}, \dots, \mathbf{E}^{(p)}\right) \tag{1}$$

is called the *datum* that defines a multi-EGS group $G_{\mathbf{E}}$. The explicit definition is given in Subsection 3.1. The core of this paper is the following theorem.

Theorem 1. *For an odd prime p, let $G_{\mathbf{E}}$ be a multi-EGS group defined by datum $\mathbf{E}$ given by* (1) *such that for some $m \in \{1, \dots, p\}$, there exist $k \in \{1, \dots, r_m\}$ and $j \in \{1, \dots, p-1\}$ that satisfy:*

(i) $e_{k,j}^{(m)} \neq 0$,

(ii) $e_{i,p-j}^{(l)} = 0$ *for all* $i \in \{1, \dots, r_l\}$ *and* $l \in \{1, \dots, p\}$.

Then $G_{\mathbf{E}}$ is liftable with a lifting $\sigma\colon G \to \mathrm{St}_{G_{\mathbf{E}}}(0)$ given by

$$\sigma\colon \begin{cases} a & \mapsto \left(\left(b_k^{(m)}\right)^{a^{m+j-1}}\right)^f, \quad \text{where } f = \left(e_{k,j}^{(m)}\right)^{-1} \in \mathbb{Z}/p\mathbb{Z}, \\ b_i^{(l)} & \mapsto \left(b_i^{(l)}\right)^{a^{l-1}}, \qquad i \in \{1, \dots, r_l\},\ l \in \{1, \dots, p\}. \end{cases} \tag{2}$$

To better visualize the conditions of the above theorem, we can represent the collections $\mathbf{E}^{(l)}$ by $r_l \times (p-1)$ matrices $M^{(l)}$ whose rows are elements of $\mathbf{E}^{(l)}$. Then the conditions of Theorem 1 can be restated as follows: there is a column index j such that the jth column in each $M^{(l)}$ is zero, and there is at least one nonzero entry in the column $(p-j)$ in at least one of $M^{(l)}$.

As an immediate corollary of [11, Theorem A and Theorem B] we obtain embedding results for ascending HNN extensions of multi-EGS groups.

Corollary A. *Let $G_{\mathbf{E}}$ be a multi-EGS group acting on a p-ary rooted tree T_p and defined by the datum* **E** *given by* (1) *that satisfies conditions of Theorem 1, with the lifting σ given by* (2)*. Then*

(i) there is an embedding θ of the ascending HNN extension $\widetilde{G}_{\mathbf{E}}$ of $G_{\mathbf{E}}$ by σ

$$\widetilde{G}_{\mathbf{E}} = G_{\mathbf{E}}{*_\sigma} = \langle G_{\mathbf{E}}, t \mid \text{relations in } G_{\mathbf{E}}, tgt^{-1} = \sigma(g) \text{ for all } g \in G_{\mathbf{E}} \rangle$$

into the group of automorphisms of $\widetilde{T}_{p+1}$ preserving one of its ends ω;

(ii) $G_{\mathbf{E}}$ is self-replicating, $\theta(\widetilde{G}_{\mathbf{E}})$ acts transitively on the set of vertices of $\widetilde{T}_{p+1}$, and the closure of $\theta(\widetilde{G}_{\mathbf{E}})$ in the group of automorphisms of $\widetilde{T}_{p+1}$ that preserve ω is a scale group.

In Section 3 we also state Corollaries 1 and 2 in which, for the sake of notation simplicity, we specialize a more general Theorem 1 to the classes of EGS-groups and multi-edge spinal groups.

We finish the paper by showing that the multi-EGS groups are contracting in Section 4 and explicitly computing their contracting nuclei. This property was first introduced by V. Nekrashevych (see, for example, [22]) in connection with the holomorphic dynamics via the theory of iterated monodromy groups, but its origins trace back to the original construction of the Grigorchuk group [10]. The class of contracting groups has also nice algebraic and algorithmic properties, and includes interesting examples of groups acting on rooted trees, such as Grigorchuk group, Gupta-Sidki p-groups, Basilica group and other iterated monodromy groups, and many others. All groups in this class admit a polynomial-time algorithm solving the word problem with the polynomial degree depending on the size of the nucleus [25]. This algorithm, along with many computational routines for both contracting and self-similar groups, are implemented in two GAP packages [3, 19].

Furthermore, contracting groups can be used as a platform for group-based post-quantum cryptography protocols [14, 20] (such as the Anshel-Anshel-Goldfeld protocol [2]) while using *nucleus portraits* to represent their elements uniquely and efficiently. The detailed description of this approach is laid out in [15]. A.G. Myasnikov and A. Ushakov have suggested in [21] that a well-known class of heuristic attacks on group-based cryptosystems, which are broadly referred to as length-based attacks [13], generically works well against groups that have many free subgroups. By a result of V. Nekrashevych [23] contracting groups have no free nonabelian subgroups, so they constitute a natural class where such attacks may not be effective. In [15], D. Kahrobaei et al. investigated the effectiveness of the length-based attack variants against the simultaneous conjugacy search problem in contracting groups and discovered that the efficiency of the attack generally decreases as the group nucleus size increases. In Section 4, we prove the following proposition.

Theorem 2. *For an odd prime p, the multi-EGS group $G_{\mathbf{E}}$ defined by the numerical datum* **E** *given by* (1) *is a contracting group with nucleus*

$$\mathcal{N}_{\mathbf{E}} = \langle a \rangle \cup \bigcup_{l=1}^{p} \langle b_i^{(l)} : 1 \le i \le r_l \rangle \quad \text{and} \quad |\mathcal{N}_{\mathbf{E}}| = p^{r_1} + \cdots + p^{r_p}.$$

This result shows that it is easy to construct multi-EGS groups with large nuclei, and thus suggests that multi-EGS groups, used as platforms in cryptographic protocols, have potential

to withstand against length-based-type attacks. The contracting property of the multi-EGS groups also follows from the fact that they are generated by bounded automata in the sense of S. Sidki [26], which are proved to be contracting by E. Bondarenko and V. Nekrashevych in [6]. But for some applications as shown above nucleus size plays an important role.

2 Preliminaries and notation

We recall some definitions and establish notation that will be used in rest of this paper.

We use X^* to denote the free monoid on the set $X = \{0, 1, \dots, d-1\}$ and recall that X^* can be endowed with the structure of a rooted d-ary tree $T(X) \cong T_d$ by defining v to be adjacent to vx for every $v \in X^*$ and $x \in X$. Finite words over X naturally label vertices of $T(X)$. Given $n \in \mathbb{N}$, the set X^n of words of length n over X corresponds to the nth level of $T(X)$. Each element of the group $\mathrm{Aut}(T(X))$ of automorphisms of the tree preserves its root and adjacency of vertices. Below, we will use X^* to denote the set of all finite words over X, and $T(X)$ to denote the corresponding rooted tree with the set of vertices identified with X^*.

Given $g \in \mathrm{Aut}(T(X))$ and $x \in X$, for each $v \in X^*$ there is a unique $v' \in X^*$ such that $g(xv) = g(x)v'$.

Definition 1. *The map $g|_x \colon X^* \to X^*$ given by $g|_x(v) = v'$ defines an automorphism of $T(X)$ called the* section *of g at x. For a word $v = x_1 x_2 \dots x_n \in X^*$ we define the section $g|_v$ of g at v as $g|_v = g_{x_1}|_{x_2}| \dots |_{x_n}$.*

Definition 2. *A subgroup of $\mathrm{Aut}(T(X))$ is called* self-similar *if it is closed under taking sections at the vertices of $T(X)$.*

The aforementioned definitions allow us to use the language of wreath recursions as for each self-similar group G there is a natural embedding $G \hookrightarrow G \wr \mathrm{Sym}(X)$, where $\wr$ denotes the permutational wreath product, and $\mathrm{Sym}(X)$ denotes the symmetric group on X. This embedding is given by

$$G \ni g \mapsto (g|_0, g|_1, \dots, g|_{d-1})\sigma_g \in G \wr \mathrm{Sym}(X), \tag{3}$$

where σ_g is the permutation of X induced by the action of g on the first level of the tree. The decomposition at the first level of all generators red a self-similar subgroup G of $\mathrm{Aut}(T(X))$ under the embedding (3) is called the *wreath recursion defining the group*. With a slight abuse of notation it is standard to identify an element of G with its image in $G \wr \mathrm{Sym}(X)$ and write $g = (g|_0, g|_1, \dots, g|_{d-1})\sigma_g$.

Wreath recursion is particularly convenient for computing the sections of group elements. Indeed, the products and inverses of automorphisms can be found as follows. In this paper we will consider only right actions. In particular, for $g, h \in \mathrm{Aut}(T(X))$ and a vertex v of $T(X)$ we have $gh(v) = h(g(v))$. With this convention, if $g = (g_0, g_1, \dots, g_{d-1})\sigma_g$ and $h = (h_0, h_1, \dots, h_{d-1})\sigma_h$ are two elements of $\mathrm{Aut}(T(X))$, then

$$gh = \big(g_0 h_{\sigma_g(0)}, g_1 h_{\sigma_g(1)}, \dots, g_{d-1} h_{\sigma_g(d-1)}\big)\sigma_g\sigma_h \tag{4}$$

and the wreath recursion of g^{-1} is

$$g^{-1} = \Big(g^{-1}_{\sigma_g^{-1}(0)}, g^{-1}_{\sigma_g^{-1}(1)}, \dots, g^{-1}_{\sigma_g^{-1}(d-1)}\Big)\sigma_g^{-1}. \tag{5}$$

2.1 Liftable groups

We recall that for a group G acting on $T(X)$ and $v \in X^*$ the stabilizer $\mathrm{St}_G(v)$ of vertex v is the subgroup of G consisting of all elements that fix v. For each $n \geq 1$ the (pointwise) stabilizer $\mathrm{St}_G(X^n)$ of level n in G is the subgroup of G consisting of all elements that fix all vertices of level n. Stabilizers of levels are normal finite index subgroups of G such that

$$\bigcap_{n\geq 1} \mathrm{St}_G(X^n) = \{1\}.$$

For each $v \in X^*$ the map

$$\begin{array}{rccc} \pi_v\colon & \mathrm{St}_{\mathrm{Aut}(T(X))}(v) & \to & \mathrm{Aut}(T(X)) \\ & g & \mapsto & g|_v \end{array} \tag{6}$$

defines a homomorphism that we will call *projection*. For each subgroup G of $\mathrm{Aut}(T(X))$ the homomorphism π_v restricts to a homomorphism $\mathrm{St}_G(v) \to \mathrm{Aut}(T(X))$. Moreover, if G is a self-similar group, then, since G is closed under taking the sections, π_v is a homomorphism from $\mathrm{St}_G(v)$ to G. In the case $X = \{0, 1, \ldots, d-1\}$ the corresponding projections are denoted by π_i, $i = 0, 1, \ldots, d-1$.

Definition 3. *A self-similar group G acting on a tree $T_d = T(X)$ is called* liftable *if there exist some $i \in X$ and a homomorphism $\sigma\colon G \to \mathrm{St}_G(i)$, called the* lifting*, that is the right inverse of the projection map π_i defined in equation* (6)*, that is, such that $\pi_i \circ \sigma$ is the identity on G.*

The idea of the lifting is related to the construction of finitely L-presented groups acting on rooted trees (e.g., the first Grigorchuk group), where the lifting endomorphism corresponds to the substitution used in the L-presentation of the group [11].

Recall that a self-similar group G acting on $T(X)$ by automorphisms is called *self-replicating* if for every vertex v of $T(X)$, the restriction of the projection π_v to $\mathrm{St}_G(v)$ has G as the image. From the definition of a liftable group it follows that the projection map $\pi_i\colon \mathrm{St}_G(i) \to G$ must be surjective, i.e. liftable groups are self-replicating as long as they act transitively on X.

3 Liftable extensions of Multi-EGS groups

3.1 Multi-EGS groups

In the rest of the paper for an odd prime p we consider the alphabet $X = \{0, 1, \ldots, p-1\}$. The multi-EGS groups are defined as follows.

Definition 4. *For an odd prime p and $l \in \{1, \ldots, p\}$, let $\mathbf{E}^{(l)}$ denote a collection of $r_l \geq 0$ linearly independent vectors in $(\mathbb{Z}/p\mathbb{Z})^{(p-1)}$ with at least one $r_l > 0$. For $l \in \{1, \ldots, p\}$, we denote the vectors in this collection by $\mathbf{e}_i^{(l)} = (e_{i,1}^{(l)}, \ldots, e_{i,p-1}^{(l)})$ where $i \in \{1, \ldots, r_l\}$. Then a* multi-EGS group *given by the datum $\mathbf{E} = \left(\mathbf{E}^{(1)}, \ldots, \mathbf{E}^{(p)}\right)$ is defined to be the group $G_{\mathbf{E}}$ acting faithfully on $T(X)$ generated by the set $\{a\} \cup \{b_i^{(l)} \mid 1 \leq i \leq r_l, 1 \leq l \leq p\}$ with the following wreath recursions:*

$$\begin{aligned} a &= (1, 1, \ldots, 1, 1)\varepsilon, \\ b_i^{(l)} &= (a^{e_{i,p-l+1}^{(l)}}, \ldots, a^{e_{i,p-1}^{(l)}}, b_i^{(l)}, a^{e_{i,1}^{(l)}}, \ldots, a^{e_{i,p-l}^{(l)}}), \quad 1 \leq i \leq r_l,\ 1 \leq l \leq p, \end{aligned}$$

where $\varepsilon = (0, 1, \ldots, p-1) \in \mathrm{Sym}(X)$.

It follows immediately from the wreath recursions that all generators of $G_{\mathbf{E}}$ have order p. Also, linear independence of vectors in $\mathbf{E}^{(l)}$ implies that $B_l = \langle b_1^{(l)}, \dots, b_{r_l}^{(l)} \rangle \cong (\mathbb{Z}/p\mathbb{Z})^{r_l}$ is an elementary abelian p-group of order p^{r_l}. We will also use the convention that if $r_l = 0$ then $\mathbf{E}^{(l)}$ is empty and B_l is trivial.

We now prove Theorem 1 from the Introduction that we restate here for convenience.

Theorem 1. *For an odd prime p, let $G_{\mathbf{E}}$ be a multi-EGS group defined by datum $\mathbf{E}$ given by* (1) *such that for some $m \in \{1, \dots, p\}$, there exist $k \in \{1, \dots, r_m\}$ and $j \in \{1, \dots, p-1\}$ that satisfy:*

(i) $e_{k,j}^{(m)} \neq 0$,

(ii) $e_{i,p-j}^{(l)} = 0$ *for all* $i \in \{1, \dots, r_l\}$ *and* $l \in \{1, \dots, p\}$.

Then $G_{\mathbf{E}}$ is liftable with a lifting $\sigma\colon G \to \mathrm{St}_{G_{\mathbf{E}}}(0)$ given by:

$$\sigma\colon \begin{cases} a & \mapsto \left(\left(b_k^{(m)}\right)^{a^{m+j-1}} \right)^f, & \text{where } f = \left(e_{k,j}^{(m)}\right)^{-1} \in \mathbb{Z}/p\mathbb{Z}, \\ b_i^{(l)} & \mapsto \left(b_i^{(l)}\right)^{a^{l-1}}, & i \in \{1, \dots, r_l\}, l \in \{1, \dots, p\}. \end{cases}$$

Proof. In [16, Proposition 3.9], it is shown that for a multi-EGS group, the abelianization $G_{\mathbf{E}}/G_{\mathbf{E}}' \cong (\mathbb{Z}/p\mathbb{Z})^{1+r_1+\dots+r_p}$. First, we note that f is well defined by condition *(i)*. Since we have $\left(a^{e_{k,j}^{(m)}}\right)^f = a^{e_{k,j}^{(m)} f} = a$, using equalities (4) and (5) we compute the following wreath recursions for $l \in \{1, \dots, p\}$ and $i \in \{1, \dots, r_l\}$:

$$\begin{array}{rcccccccccc} \left(b_i^{(l)}\right)^{a^{l-1}} &=& (b_i^{(l)}, & a^{e_{i,1}^{(l)}}, & \dots, & a^{e_{i,p-j-1}^{(l)}}, & 1, & a^{e_{i,p-j+1}^{(l)}}, & \dots, & a^{e_{i,p-2}^{(l)}}, & a^{e_{i,p-1}^{(l)}}), \\ \left(\left(b_k^{(m)}\right)^{a^{m+j-1}}\right)^f &=& (a, & a^{e_{k,j+1}^{(m)} f}, & \dots, & a^{e_{k,p-1}^{(m)} f}, & (b_k^{(m)})^f, & a^{e_{k,1}^{(m)} f}, & \dots, & a^{e_{k,j-2}^{(m)} f}, & a^{e_{k,j-1}^{(m)} f}), \\ & & \text{positions} & 0 & 1 & \dots & p-j-1 & p-j & p-j+1 & \dots & p-2 & p-1 \end{array}$$

where the third row indicates positions of coordinates of the wreath recursions given in the first two rows. Note that $\pi_0 \circ \sigma(a) = a$ and $\pi_0 \circ \sigma\left(b_i^{(l)}\right) = b_i^{(l)}$ for $i \in \{1, \dots, r_l\}$ and $l \in \{1, \dots, p\}$, so we immediately get that $\pi_0 \circ \sigma =_{G_{\mathbf{E}}} 1$ by construction. It also follows from condition *(ii)* of the statement that the decomposition of $\left(b_i^{(l)}\right)^{a^{l-1}}$ has identity at the position $p-j$.

We show that the substitution σ defined by (2) extends to an injective endomorphism of $G_{\mathbf{E}}$. Suppose we have a relator in $G_{\mathbf{E}}$ represented by a word $w = w(a, b_i^{(l)} : 1 \le i \le r_l, 1 \le l \le p)$ in the free group $F(a, b_i^{(l)} : 1 \le i \le r_l, 1 \le l \le p)$. Then

$$\pi_n \circ \sigma(w) = \pi_n \left(w\left(\left(\left(b_k^{(m)}\right)^{a^{m+j-1}} \right)^f, \left(b_i^{(l)}\right)^{a^{l-1}} \right) \right) = \begin{cases} w\left(a, b_i^{(l)}\right) =_{G_{\mathbf{E}}} 1, & \text{if } n = 0, \\ w\left((b_k^{(m)})^f, 1\right), & \text{if } n = p-j, \\ w\left(a^{e_{j+n}^{(m)} f}, a^{e_{i,n}^{(l)}}\right), & \text{otherwise.} \end{cases}$$

Since $G_{\mathbf{E}}/G_{\mathbf{E}}' \cong (\mathbb{Z}/p\mathbb{Z})^{1+r_1+\dots+r_p}$ and $w =_{G_{\mathbf{E}}} 1$, w represents the trivial element in $G_{\mathbf{E}}/G_{\mathbf{E}}'$ as well. Thus, we must have that the total exponents of a and $b_i^{(l)}$'s in w are all equal to 0 modulo p. Note that it is important to know the structure of abelianization of $G_{\mathbf{E}}$ to make this deduction. It is not enough to only use that the generators a and $b_i^{(l)}$ have order p. This implies that $w((b_k^{(m)})^f, 1)$ and $w(a^{(e_{j+n}^{(m)})f}, a^{e_{i,n}^{(l)}})$ are trivial in $G_{\mathbf{E}}$ since a and all $b_i^{(l)}$ have order p. Thus, σ is a lifting of $G_{\mathbf{E}}$ and $G_{\mathbf{E}}$ is liftable. □

3.2 Multi-edge spinal groups

The class of multi-edge spinal groups defined in [1] is a subclass of the class of multi-EGS groups and is a generalization of the class of GGS-groups. In this section we specialize Theorem 1 to this class in order to obtain simpler description of liftability conditions and of the lifting itself.

Given an odd prime p, multi-edge spinal groups act on the regular p-ary rooted tree $T_p = T(X)$.

Definition 5. *For a fixed prime $p > 2$, $1 \le r < p$ and an r-tuple*

$$\mathbf{E}^{(p)} = \left(\mathbf{e}_i = (e_{i,1}, \dots, e_{i,p-1}) \in (\mathbb{Z}/p\mathbb{Z})^{p-1}\right)_{i=1,\dots,r} \tag{7}$$

of linearly independent vectors in $(\mathbb{Z}/p\mathbb{Z})^{p-1}$, a multi-edge spinal group $G_{\mathbf{E}^{(p)}} = \langle a, b_1, \dots, b_r \rangle$ *acts on a regular rooted tree $T_p = T(X)$ for $X = \mathbb{Z}/p\mathbb{Z}$, with the generators defined by the following wreath recursions:*

$$\begin{aligned} a &= (1, 1, \dots, 1, 1)\varepsilon, \\ b_i &= (a^{e_{i,1}}, a^{e_{i,2}}, \dots, a^{e_{i,p-1}}, b_i), \quad 1 \le i \le r, \end{aligned}$$

where $\varepsilon = (0, 1, \dots, p-1) \in \mathrm{Sym}(X)$.

The multi-edge spinal groups correspond to the multi-EGS groups defined by a datum $\mathbf{E} = \left(\mathbf{E}^{(1)}, \dots, \mathbf{E}^{(p)}\right)$ in which all collections $\mathbf{E}^{(i)}$ except the last one $\mathbf{E}^{(p)}$ are empty.

The following result follows from Theorem 1.

Corollary 1. *Let $p \ge 3$ be a prime, $1 \le r < p$, and $G_{\mathbf{E}^{(p)}}$ be a multi-edge spinal group defined by an r-tuple $\mathbf{E}^{(p)}$ of linearly independent vectors in $(\mathbb{Z}/p\mathbb{Z})^r$ as denoted in* (7)*, such that there exist $k \in \{1, \dots, r\}$ and $j \in \{1, \dots, p-1\}$ that satisfy:*

- $e_{k,j} \neq 0$,
- $e_{i,p-j} = 0$ *for all* $1 \le i \le r$.

Then $G_{\mathbf{E}}$ is liftable. A lifting is witnessed by the following σ:

$$\sigma\colon \begin{cases} a & \mapsto & (b_k^{a^{1j-1}})^{e_{k,j}^{-1}}, \\ b_i & \mapsto & a^{-1} b_i a\,, \qquad i \in \{1, \dots, r\}. \end{cases}$$

3.3 EGS-groups

The class of EGS-groups defined in [24] is another subclass of the class of multi-EGS groups. Here we also specialize Theorem 1 to this class for simplicity of notation. Given an odd prime p, EGS-groups act on a regular p-ary rooted tree $T_p = T(X)$. Each group in this class is defined by a non-zero vector in $(\mathbb{Z}/p\mathbb{Z})^{p-1}$ and contains the corresponding GGS-group defined by the same vector.

Definition 6. *For an odd prime p, an EGS-group G_{e} is defined by a non-zero vector $\mathrm{e} = (e_1, e_2, \dots, e_{p-1}) \in (\mathbb{Z}/p\mathbb{Z})^{p-1}$ as the group acting on the regular rooted tree $T_p = T(X)$ for $X = \mathbb{Z}/p\mathbb{Z}$ with the following wreath recursion:*

$$\begin{aligned} a &= (1, 1, \dots, 1, 1)\varepsilon, \\ b &= (a^{e_1}, a^{e_2}, \dots, a^{e_{p-1}}, b), \\ c &= (c, a^{e_1}, a^{e_2}, \dots, a^{e_{p-1}}), \end{aligned}$$

where $\varepsilon = (0, 1, \dots, p-1) \in \mathrm{Sym}(X)$. We will denote the corresponding group as $G_{\mathrm{e}} = \langle a, b, c\rangle$.

The EGS-groups correspond to multi-EGS groups defined by datum $\mathbf{E} = \left(\mathbf{E}^{(1)}, \dots, \mathbf{E}^{(p)}\right)$ in which all collections $\mathbf{E}^{(i)}$, $2 \le i \le p-1$ are empty and $\mathbf{E}^{(1)} = \mathbf{E}^{(p)}$ consists of only one vector e. The subgroup $\langle a, b\rangle$ of G_{e} is the GGS-group associate to G_{e}.

The following result follows from Theorem 1.

Corollary 2. *Let $p \ge 3$ be a prime and G_{e} be an EGS-group defined by a not invertible symmetric vector $\mathrm{e} = (e_1, e_2, \dots, e_{p-1}) \in (\mathbb{Z}/p\mathbb{Z})^{p-1}$ with the property that there is $j \in \{1, 2, \dots, p-1\}$ such that $e_j \ne 0$ and $e_{p-j} = 0$. Then G_{e} is a liftable group. A lifting is given by the following $\sigma\colon G_{\mathrm{e}} \to \mathrm{St}_{G_{\mathrm{e}}}(0)$:*

$$\sigma\colon \begin{cases} a \mapsto (b^{a^{j-1}})^{e_j^{-1}}, \\ b \mapsto a^{-1}ba, \\ c \mapsto c. \end{cases}$$

4 Contracting property and nucleus of multi-EGS groups

Contracting groups can be defined as self-similar groups in which the length of the sections of any word decreases to a constant length when going down the tree. We will use here the following result from [22, Lemma 12.1.2] that can also be used as a formal definition of contracting groups.

Lemma 1. *A self-similar group G with generating set S such that $S = S^{-1}$ and $1 \in S$ is contracting if and only if there exists a finite set $\mathcal{N} \subset G$ and $k \ge 1$ such that for all $n_1 n_2 \in (S \cup \mathcal{N})^2$ and $v \in X^k$: $(n_1 n_2)|_v \in \mathcal{N}$.*

Any set satisfying the conditions of Lemma 1 is called a *quasinucleus* of G and the minimal such set under inclusion is the *nucleus* of G. The nucleus of a contracting group can also be characterized as the self-similar closure of the union of all the cycles in the full automaton of the group. To find the nucleus of a group it is sufficient to find a quasinucleus satisfying conditions of Lemma 1 and then select elements from that set that are either sections of themselves or are sections of such elements.

We now prove Theorem 2 from the Introduction that we also restate here for convenience.

Theorem 2. *For an odd prime p, the multi-EGS group $G_{\mathbf{E}}$ defined by the numerical datum $\mathbf{E}$ given by* (1) *is a contracting group with nucleus*

$$\mathcal{N}_{\mathbf{E}} = \langle a\rangle \cup \bigcup_{l=1}^{p} \langle b_i^{(l)} \colon 1 \le i \le r_l\rangle \qquad \text{and} \qquad |\mathcal{N}_{\mathbf{E}}| = p^{r_1} + \dots + p^{r_p}.$$

Proof. We recall the wreath recursions for the generators of multi-EGS groups from Definition 4:

$$\begin{aligned} a &= (1,1,\dots,1,1)\varepsilon, \\ b_i^{(l)} &= (a^{e_{i,p-l+1}^{(l)}},\dots,a^{e_{i,p-1}^{(l)}}, b_i^{(l)}, a^{e_{i,1}^{(l)}},\dots,a^{e_{i,p-l}^{(l)}}),\ 1 \le i \le r_l,\ 1 \le l \le p. \end{aligned}$$

For each $1 \le l \le p$ such that $r_l > 0$, the group $B_l = \langle b_1^{(l)},\dots,b_{r_l}^{(l)}\rangle \subset \mathcal{N}_{\mathbf{E}}$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{r_l}$ and has order p^{r_l}. Every element of this group has itself as a section at a vertex of the first level, so must be in the nucleus. Additionally, since there is $1 \le l \le p$ such that $r_l > 0$, there must be at least one nonzero component of $\mathrm{e}_1^{(l)}$, which yields a nontrivial element of $\langle a\rangle$ as a section of $b_1^{(l)}$. Since $b_1^{(l)}$ stabilizes all vertices of the first level, all elements of $\langle a\rangle$ will occur as sections of elements $(b_1^{(l)})^k$ for $0 \le k < p$ because p is prime. Thus, all powers of a are sections of elements of the nucleus and hence must be in the nucleus themselves. We conclude that the set $\mathcal{N}_{\mathbf{E}}$ is contained in the nucleus of $G_{\mathbf{E}}$.

To prove the converse inclusion, we show using Lemma 1 that $\mathcal{N}_{\mathbf{E}}$ is a quasinucleus of $G_{\mathbf{E}}$. Since $\mathcal{N}_{\mathbf{E}}$ is a symmetric generating set for $G_{\mathbf{E}}$, we only need to prove that the product of any two elements $n_1, n_2 \in \mathcal{N}_{\mathbf{E}}$ is either in $\mathcal{N}_{\mathbf{E}}$ or contracts to $\mathcal{N}_{\mathbf{E}}$ at most at the second level of the tree (i.e., the sections of n_1n_2 at the vertices of the second level belong to $\mathcal{N}_{\mathbf{E}}$). There are four following possibilities.

Case I. If both n_1, n_2 are powers of a, then n_1n_2 is also a power of a and is in $\mathcal{N}_{\mathbf{E}}$.

Case II. If both n_1, n_2 are elements of B_l for some $1 \le l \le p$, then n_1n_2 is again in B_l, so is an element of $\mathcal{N}_{\mathbf{E}}$.

Case III. If one of n_1, n_2 is a power a and the other is in B_l for some $1 \le l \le p$, then the set of sections of n_1n_2 at the first level will coincide with the set of sections of n_i that is not a power of a. Therefore, all sections of n_1n_2 at the vertices of the first level are in $\mathcal{N}_{\mathbf{E}}$.

Case IV. If $n_1 \in B_l$ and $n_2 \in B_{l'}$ for some $l \ne l'$, then from the wreath recursions we see that each section of n_1n_2 will either be a power a, or an element of B_l or $B_{l'}$, or a product of a power of a and an element from either B_l or $B_{l'}$. In the former cases we immediately obtain an element of $\mathcal{N}_{\mathbf{E}}$, while in the latter case we get to Case III, which shows that the sections of n_1n_2 at the vertices of the second level are in $\mathcal{N}_{\mathbf{E}}$.

Thus, by Lemma 1 (with $k = 2$) the multi-EGS group $G_{\mathbf{E}}$ is contracting with the nucleus $\mathcal{N}_{\mathbf{E}}$. Since the groups $\langle a\rangle$ and $B_l, 1 \le l \le p$ pairwise intersect at the identity of $G_{\mathbf{E}}$, the size of $\mathcal{N}_{\mathbf{E}} = \langle a\rangle \cup \bigcup_{l=1}^{p} B_l$ is

$$|\mathcal{N}_{\mathbf{E}}| = 1 + (|\langle a\rangle| - 1) + \sum_{l=1}^{p}(|B_l| - 1) = 1 + (p-1) + \sum_{l=1}^{p}(p^{r_l} - 1) = \sum_{l=1}^{p} p^{r_l}.$$

We finally note that the above argument and formula are alse valid when some of the r_l's are 0 or, equivalently, when B_l's are trivial subgroups of $G_{\mathbf{E}}$. □

Theorem 2 specializes to the class of multi-edge spinal groups as follows. We use the notation from Definition 5.

Corollary 3. *For a prime $p \geq 3$ and $1 \leq r < p$, the multi-edge spinal group $G_{\mathbf{E}^{(p)}}$ defined by an r-tuple $\mathbf{E}^{(p)}$ of linearly independent vectors in $(\mathbb{Z}/p\mathbb{Z})^{p-1}$ is a contracting group with the nucleus $\mathcal{N}_{\mathbf{E}^{(p)}} = \langle a \rangle \cup \langle b_1, \ldots, b_r \rangle$ of size $p^r + p - 1$.*

In the case of EGS-groups Theorem 2 takes even simpler form.

Corollary 4. *For a prime $p > 2$, an EGS-group G_{e}, defined by a non-zero vector*

$$\mathrm{e} = (e_1, e_2, \ldots, e_{p-1}) \in (\mathbb{Z}/p\mathbb{Z})^{p-1}$$

is a contracting group with the nucleus

$$\mathcal{N}_{\mathbf{E}} = \{1, a^i, b^j, c^k \mid 1 \leq i, j, k \leq p-1\} \quad \text{of size} \quad 3p-2.$$

The GAP code to generate some classes of groups studied in the paper is provided in [18].

References

[1] Alexoudas T., Klopsch B., Thillaisundaram A. *Maximal subgroups of multi-edge spinal groups*. Groups Geom. Dyn. 2016, **10** (2), 619–648. doi:10.4171/GGD/359

[2] Anshel I., Anshel M., Goldfeld D. *Non-abelian key agreement protocols*. Discrete Appl. Math. 2003, **130** (1), 3–12. doi:10.1016/S0166-218X(02)00585-1

[3] Bartholdi L. *FR, computations with functionally recursive groups, Version 2.4.13*. GAP package 2024. `https://gap-packages.github.io/fr`

[4] Bartholdi L., Grigorchuk R.I., Šuniḱ Z. Branch groups. In: Handbook of algebra, Vol. 3. North-Holland, Amsterdam, 2003, 989–1112. doi:10.1016/S1570-7954(03)80078-5

[5] Baumslag G. Topics in combinatorial group theory. Lectures in Mathematics ETH Zürich. Birkhäuser Verlag, Basel, 1993.

[6] Bondarenko E., Nekrashevych V. *Post-critically finite self-similar groups*. Algebra Discrete Math. 2003, **4**, 21–32.

[7] Di Domenico E., Fernández-Alcober G.A., Gavioli N. *GGS-groups over primary trees: branch structures*. Monatsh. Math. 2023, **200** (4), 781–797. doi:10.1007/s00605-022-01705-1

[8] Fernández-Alcober G.A., Zugadi-Reizabal A. *GGS-groups: order of congruence quotients and Hausdorff dimension*. Trans. Amer. Math. Soc. 2014, **366** (4), 1993–2017.

[9] Garrido A., Uria-Albizuri J. *Multi-GGS groups have the congruence subgroup property*. Proc. Edinb. Math. Soc. (2) 2019, **62** (3), 889–894.

[10] Grigorchuk R.I. *On Burnside's problem on periodic groups*. Funktsional. Anal. i Prilozhen. 1980, **14** (1), 53–54.

[11] Grigorchuk R., Savchuk D. *Liftable self-similar groups and scale groups*. Trans. Amer. Math. Soc. 2026, **379** (1), 341–385. doi:10.1090/tran/9563

[12] Gupta N., Sidki S. *On the Burnside problem for periodic groups*. Math. Z. 1983, **182** (3), 385–388.

[13] Hughes J., Tannenbaum A. *Length-based attacks for certain group based encryption rewriting systems*. Preprint arXiv:cs/0306032 [cs.CR]. doi:10.48550/arXiv.cs/0306032

[14] Kahrobaei D., Flores R., Noce M., Habeeb M.E., Battarbee C. Applications of Group Theory in Cryptography: Post-quantum Group-based Cryptography. In: Mathematical Surveys and Monographs, **278**. Amer. Math. Soc., Providence, RI, 2024.

[15] Kahrobaei D., Malik A.A., Savchuk D. *Contracting self-similar groups in group-based cryptography*. Preprint arXiv:2408.14355 [math.GR]. doi:10.48550/arXiv.2408.14355 (to appear in Experimental Mathematics)

[16] Klopsch B., Thillaisundaram A. *Maximal subgroups and irreducible representations of generalized multi-edge spinal groups*. Proc. Edinb. Math. Soc. (2) 2018, **61** (3), 673–703.

[17] Maini E. *Multi-EGS groups: exponent of congruence quotients*. Monatsh. Math. 2025, **207** (1), 95–106.

[18] Malik A., Savchuk D. *Implementation of multi-EGS groups in GAP*. 2024. https://github.com/Arsalan-A-M/Multi-EGS

[19] Muntyan Y., Savchuk D. AutomGrp – GAP package for computations in self-similar groups and semigroups, Version 1.3.3. Accepted GAP package, 2025. http://www.gap-system.org/Packages/automgrp.html

[20] Myasnikov A., Shpilrain V., Ushakov A. Non-commutative cryptography and complexity of group-theoretic problems. In: Mathematical Surveys and Monographs, **177**. Amer. Math. Soc., Providence, RI, 2011.

[21] Myasnikov A.G., Ushakov A. *Random subgroups and analysis of the length-based and quotient attacks*. J. Math. Cryptol. 2008, **2** (1), 29–61.

[22] Nekrashevych V. Self-similar groups. In: Mathematical Surveys and Monographs, **117**. Amer. Math. Soc., Providence, RI, 2005.

[23] Nekrashevych V. *Free subgroups in groups acting on rooted trees*. Groups Geom. Dyn. 2010, **4** (4), 847–862. doi:10.4171/GGD/110

[24] Pervova E. *Profinite completions of some groups acting on trees*. J. Algebra 2007, **310** (2), 858–879.

[25] Savchuk D.M. *On word problem in contracting automorphism groups of rooted trees*. Visn. Kyiv. Univ. Ser. Fiz.-Mat. Nauki 2003, **1**, 51–56.

[26] Sidki S. *Finite automata of polynomial growth do not generate a free group*. Geom. Dedicata 2004, **108**, 193–204.

[27] Thillaisundaram A., Uria-Albizuri J. *The profinite completion of multi-EGS groups*. J. Group Theory 2021, **24** (2), 321–357.

[28] Vovkivsky T. Infinite torsion groups arising as generalizations of the second Grigorchuk group. In: Proc. of the Intern. Conf. on the 90th birthday of A.G. Kurosh, Walter de Gruyter, Berlin, New York, 2000, 357–377.

[29] Willis G.A. *Scale groups*. Preprint arXiv:2008.05220 [math.GR]. doi:10.48550/arXiv.2008.05220

Received 29.08.2025
Revised 13.09.2025

Малік А.А., Савчук Д. *Властивість піднімості та стисливості мульти-EGS груп* // Карпатські матем. публ. — 2026. — Т.18, №1. — С. 211–221.

Ми наводимо достатні умови для того, щоб мульти-EGS групи були піднімними, і таким чином отримуємо нові приклади груп, які транзитивно діють на регулярних деревах скінченного степеня та стабілізують один із їхніх кінців, і замикання яких є масштабними групами у сенсі Г.А. Вілліса. Крім того, ми явно обчислюємо стискуючі ядра груп цього класу. Ми також конкретизуємо отримані результати для класів мульти-реберних спінальних груп та EGS-груп.

Ключові слова і фрази: піднімна група, мульти-EGS група, стискуюча група, група на деревах.