THE DERIVED SERIES OF GGS-GROUPS

JAN MORITZ PETSCHICK

ABSTRACT. Given a GGS-group $G$ with non-constant defining tuple over a prime-
regular rooted tree, we calculate the indices $|G : G^{(n)}|$ and describe the structure of
the higher derived subgroups $G^{(n)}$ for all $n \in \mathbb{N}$. We find that the values $|G : G^{(n)}|$ depend only mildly on the structure of the defining tuple.

1. Introduction

The class of groups of automorphisms of regular rooted trees provides many ex-
amples with interesting asymptotic and structural properties. One particularly well-
studied case is the family of Grigorchuk–Gupta–Sidki-groups (usually abbreviated
as ‘GGS-groups’). It contains at least one group of intermediate growth [5] and
many finitely generated infinite periodic groups, cf. [8]. GGS-groups are groups of
automorphisms of the $p$-regular rooted tree, for an odd prime $p$, and generalise the
Gupta–Sidki $p$-groups. They are easily defined by a non-zero element $e$ of $\mathbb{F}_p$ as
‘input data’, and many of their properties can be read off this element $e$: One can
determine whether the corresponding GGS-group is periodic or contains elements of
infinite order, if the group is just-infinite, cf. [15], whether it is a branch group, cf.
[6], or if it has the congruence subgroup property, cf. [7], one may compute its Haus-
dorff dimension, cf. [6], or decide if two GGS-groups are isomorphic, cf. [11], just by
considering the defining tuples. Most of these results require subtle insights into the
structure of a general GGS-group, and some involve heavy computation. Many of the
results extend to larger classes of groups, cf. for example [1, 2, 12], but have been
established first for GGS-groups, making the class of GGS-groups a fertile soil for
establishing new techniques.

However, other questions remain open. In contrast to features related to the action
on the tree, many purely algebraic properties of GGS-groups are not well-understood.
In this work, we describe the derived series $(G^{(n)})_{n \in \mathbb{N}}$ of all GGS-groups, excluding
those that arising from constant tuples, i.e. elements of the form $(\lambda, \lambda, \ldots, \lambda) \in \mathbb{F}_p$ for some $\lambda \in \mathbb{F}_p^\times$. A description of the derived series has previously been obtained
for the special case of the Gupta–Sidki 3-group $\tilde{\Gamma}$ by Vieira in [14], along with some
results concerning the lower central series of $\tilde{\Gamma}$. The proof, however, does not carry
over to general GGS-groups.

We now state our main result.

**Theorem 1.1.** Let $p$ be an odd prime and let $G$ be a GGS-group acting on a $p$-regular
tree with non-constant defining tuple $e \in \mathbb{F}_p$. Denote by $e'$ the tuple of differences

2010 Mathematics Subject Classification. Primary 20E08; Secondary 20F14, 20E15.

Key words and phrases. Derived series, GGS-groups, branch groups, self-similar groups, circulant
matrices, automorphism groups of regular rooted trees.

The research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foun-
dation) — 380258175.
between the entries of \( e \), and by \( e'' \) the tuple of differences of \( e' \). Then

\[
\log_p |G : G^{(n)}| = \begin{cases} 
\frac{p^{n-2}(p + \text{con}(e') + \text{sym}(e'')) - \frac{p^{n-1}}{p-1} \text{sym}(e)}{2} + 1 & \text{if } n \geq 2, \\
1 & \text{for } n = 1,
\end{cases}
\]

where

\[
\text{sym}(d) = \begin{cases} 
1 & \text{if } d \text{ is symmetric,} \\
0 & \text{otherwise,}
\end{cases} \quad \text{and} \quad \text{con}(d) = \begin{cases} 
1 & \text{if } d \text{ is constant,} \\
0 & \text{otherwise.}
\end{cases}
\]

A tuple is called symmetric if its \( i \)th entry is equal to its \( i \)th-to-last entry. It is no surprise that the vector \( e' \in \mathbb{F}_p^{p-2} \) of differences between neighbouring entries in \( e \) is associated to the determination of the structure of the derived subgroups, since it describes the sections of the commutator \([b, a]\) of the two generators of a GGS-group. Interestingly, the indices of the derived subgroups do not depend on the higher iterates of the differences.

It is worthwhile to compare our result with the main result of [6], where the indices of the congruence subgroups, i.e. the pointwise stabilisers \( \text{Stab}_G(n) \) of all elements of a given distance \( n \in \mathbb{N} \) from the root of the tree, are computed to be

\[
\log_p |G : \text{Stab}_G(n)| = \begin{cases} 
 tp^{n-2} + \frac{p^{n-2} - 1}{p-1} \text{sym}(e) + 1 & \text{if } n \geq 2, \\
1 & \text{for } n = 1,
\end{cases}
\]

where \( t \) is the rank of a certain matrix associated to \( e \), which takes values in \( \{2, \ldots, p\} \).

In particular, the number of configurations of the indices \( |G : \text{Stab}_G(n)| \) grows linearly with \( p \). In comparison, the indices of the derived series are more uniform and depend only on three (interconnected) binary invariants of \( e \); hence the indices of the derived subgroups of any GGS-groups (aside from the dependency on the prime \( p \) itself), fall in precisely four distinct classes.

From a group-theoretic standpoint, it is an inherently interesting problem to determine the derived series of a given intriguing group. This is especially true since GGS-groups are hypoabelian, i.e. the intersection of all members of the derived series is trivial; hence every element of \( G \) appears as a non-trivial element in some quotient \( G^{(n)}/G^{(n+1)} \). Furthermore, the derived series fulfils the analogue of the congruence subgroup property: all finite index subgroups contain some derived subgroup. This is an immediate consequence of the congruence subgroup property of GGS-groups, that was established in [7], and the fact that the \( n \)th derived subgroup \( G^{(n)} \) is contained in the \( n \)th level stabiliser \( \text{Stab}_G(n) \). The analogy to the congruence subgroups goes further. We prove the following theorem.

**Theorem 1.2.** Let \( G \) be a GGS-group with defining tuple \( e \) and let \( n \in \mathbb{N}_{\geq 3} \). Then

\[
\psi(G^{(n)}) = G^{(n-1)} \times \ldots \times G^{(n-1)}.
\]

If \( \text{con}(e') + \text{sym}(e'') - \text{sym}(e) = 0 \), the same holds for \( n = 2 \).

Note that the equivalent statement is true for the congruence subgroups of GGS-groups. To make the connexion between congruence and derived subgroups more transparent, we introduce the series of iterated local laws. It is a descending series \( (L_n(G))_{n \in \mathbb{N}} \) of normal subgroups of a group \( G \) acting on a rooted tree, such that \( L_n(G) \leq \text{Stab}_G(n) \) for all \( n \in \mathbb{N} \), and is formed by the elements that have to stabilise vertices of a certain distance by virtue of fulfilling certain algebraic equations in \( G \).
In this sense, it is the ‘algebraic analogue’ of the sequence of layer stabilisers. See Definition 2.2 for a precise definition.

As a corollary to Theorem 1.1, we prove that the series of iterated local laws and the derived series coincide for all GGS-groups defined by a non-constant vector $e$, thus explaining, at least heuristically, the similarities mentioned above; see Corollary 3.4.

The paper is organised in the following way. After establishing our notation, we prove some structural results on GGS-groups. Then we prove Proposition 3.1, in which we compute the index of the second derived subgroup in the full group. This is the main technical step. Afterwards, we proceed to derive our other results. Being aware of the multitude of subgroups appearing, we point the reader to Fig. 1, which depicts the relevant portion of the top of the subgroup lattice of a GGS-groups.

Acknowledgements. This is part of the author’s Ph.D. thesis, written under the supervision of Benjamin Klopsch at the Heinrich-Heine-Universität Düsseldorf. The author thanks Karthika Rajeev for helpful discussions and bringing his attention to the problem, and Gustavo Fernández-Alcober, Mikel Garciaarena Perez, Margherita Piccolo and Djurre Tijsma for their respective comments on preliminary versions of this paper.

2. On Grigorchuk–Gupta–Sidki-groups

We begin with some generalities. We fix an odd prime $p$. Given a group $G$ and two elements $g, h$, we use the following conventions for conjugation and the commutator 

$$g^h = h^{-1}gh \quad \text{and} \quad [g, h] = g^{-1}h^{-1}gh = (h^{-1})^g h.$$ 

2.1. Groups of automorphisms of regular rooted trees. Write $X$ for the set \( \{0, \ldots, p-1\} \). We will sometimes identify $X$ with the set underlying the field $\mathbb{F}_p$. We write $X^*$ for the Cayley graph of the free monoid on $X$, which is a rooted $p$-regular tree, i.e. a loop-free graph in which all but one vertex have valency $p + 1$, and the remaining vertex $\emptyset$, called the root of the tree, has valency $p$. The vertices of $X^*$ are the set of finite sequences in $X$. We write $X^n$ for the set of all vertices of a given length $n \in \mathbb{N}$, and call this set the $n^{th}$ level of $X^*$. The root $\emptyset$ has length 0.

Any (graph) automorphism $g \in \text{Aut}(X^*)$ necessarily fixes $\emptyset$, since it has fewer neighbours than every other vertex, and must consequently leave the levels $X^n$ invariant for all $n \in \mathbb{N}$. We write $\text{Stab}(n)$ for the stabiliser of $X^n$, and $\text{Stab}_G(n)$ for its intersection with some subgroup $G \leq \text{Aut}(X^*)$. Let $u$ and $v$ be vertices of $X^*$. We write $u^g$ for the image of $u$ under $g$. Since levels are invariant under $g$, the equation

$$(uv)^g = u^g v^g$$

uniquely defines a map $|_u : \text{Aut}(X^*) \to \text{Aut}(X^*)$, called the section map at $u$. The image is consequently called the section of $g$ at $u$. Using these images, any tree automorphism $g$ can be decomposed into the sections prescribing the action at the subtrees of the first level, and the action of $g$ at the root $g|_{\emptyset} \in \text{Sym}(X)$, which is defined as the action of $g$ on the first level $X = X^1$. In particular, the map

$$\psi : \text{Stab}(1) \to \text{Aut}(X^*) \times \ldots \times \text{Aut}(X^*)$$

$$g \mapsto \left( g|_{\emptyset} \right)$$

is a group isomorphism. Here we adopt the convention that the expression

$$(i_0 : a_0, \ldots, i_k : a_k, \emptyset : a_{\emptyset})$$
denotes the tuple indexed by \( X \), with the object \( a_0 \) at position \( i_0 \), the object \( a_1 \) at position \( i_1 \) and so forth, and the object \( a_\infty \) (maybe varying in \( \infty \)) at all other positions \( \infty \in X \setminus \{i_m \mid m = 0, \ldots, k\} \). The symbol \( \infty \) will be reserved for this use. An automorphism with at most one non-trivial section is called \textit{rooted}. Rooted automorphisms must necessarily permute the subtrees \( \{xX^* \mid x \in X\} \) of the first level and can be identified with permutations of \( X \).

We record some equations for sections. Let \( u \) and \( v \) be vertices of \( X^* \) and \( g \) and \( h \) be any automorphisms, then
\[
(g|_u)|_v = g|_{uv}, \quad (gh)|_u = g|_uh|_u, \quad g^{-1}|_u = (g|_{u^{-1}})^{-1}.
\]

A subgroup \( G \leq \text{Aut}(X^*) \) is called \textit{self-similar}, if for all vertices \( u \in X^* \), the image of the section map \( |_u : g \mapsto g|_u \) is contained in \( G \). A self-similar group \( G \) is called \textit{contracting}, if there exists a finite set \( N \subseteq G \), such that for all \( g \in G \) there exists some \( n \in \mathbb{N} \) such that for all \( m \geq n \) and all \( v \in X^m \) the section \( g|_v \) is an element of the finite set \( N \). For a contracting group, there is a unique minimal set \( N \) with this property, which is called the \textit{nucleus} of \( G \). A group \( G \leq \text{Aut}(X^*) \) is called \textit{fractal}, if for every \( g \in G \) and every \( x \in X \) there is an element \( \tilde{g} \) stabilising the vertex \( x \) such that \( \tilde{g}|_x = g \). A group \( G \leq \text{Aut}(X^*) \) is called \textit{spherically transitive} if it acts transitively on every level \( X^n \).

A self-similar group \( G \leq \text{Aut}(X^*) \) is called a \textit{regular branch group}, if it is spherically transitive, and if there is a finite index subgroup \( K \leq G \) such that
\[
K \times \cdots \times K \leq \psi(K).
\]

A standard technique for establishing that a group is regular branch is given by the following lemma, cf. \cite[Proposition 2.18]{6}.

\begin{proposition}
Let \( G \leq \text{Aut}(X^*) \) be a spherically transitive fractal group, \( H \leq G \) a subgroup and let \( S \subseteq G \) be a subset. If \( \{(0 : s, \infty : \text{id}) \mid s \in S\} \) is contained in \( \psi(H) \), then
\[
\langle S \rangle^G \times |X| \times \langle S \rangle^G \leq \psi(H^G).
\]
\end{proposition}

We now come to the definition of the series of iterated local laws for a spherically transitive group \( G \leq \text{Aut}(X^*) \). Consider the set \( \{(g|_u)|^\infty \mid g \in G, u \in X^*\} \subseteq \text{Sym}(X) \). In view of the equations for sections above, it is easily seen that this set forms a subgroup \( P(G) \leq \text{Sym}(X) \) of the symmetric group on \( X \). Given a subgroup \( H \leq \text{Sym}(X) \), we may define a corresponding subgroup of \( \text{Aut}(X^*) \) by
\[
\Lambda(H) = \{g \in \text{Aut}(X^*) \mid (g|_u)|^\infty \in H \text{ for all } u \in X^*\}.
\]
If \( H \) is a \( p \)-group, it is necessarily cyclic, and \( \Lambda(H) \) is a Sylow pro-\( p \)-subgroup of \( \text{Aut}(X^*) \).

Let \( R = R(H) \) be the collection of all group laws of \( H \), i.e. elements of the free group \( F_\infty \) on infinitely many generators that evaluate to the trivial element for all assignments of the generators to elements of \( H \). Given any group \( K \), we may consider the subgroup \( L_R(K) \) generated by all verbal subgroups of \( K \) corresponding to elements in \( R \), i.e. by all images of \( R \) under any assignment of the generators of \( F_\infty \) to elements of \( K \).

Returning to the subgroup \( P(G) \) defined by a group of tree automorphisms, we see that \( L_{R(P(G))}(G) \) is contained in the first level stabiliser, since \( L_{R(P(G))}(G|^\infty) \) is trivial by construction; note that the map \( |^\infty : G \to P(G) \leq \text{Sym}(X) \) is a (not necessarily
surjective) homomorphism. Consider the iterates \( R_n \) of \( R \), that are recursively defined by

\[
R_n = \left\{ s(r_1, \ldots, r_n) \mid s \in R_{n-1}, r_i \in R \text{ for } i \in \{1, \ldots, n\},
\begin{array}{l}
s \text{ an element involving } n \text{ generators, and } \vspace{2mm} \\
r_1, \ldots, r_n \text{ share no generator of } F_\infty
\end{array}
\right\},
\]

for \( n > 1 \) and \( R_1 = R \), where by the expression \( s(r_1, \ldots, r_n) \) we mean the element of \( F_\infty \) obtained by replacing the \( n \) generators occurring in \( s \) by the elements \( r_1 \) to \( r_n \), these are a generalised form of the \( S \)-type iterated identities defined in [4]. By the same argument as above,

\[
L_{R_n(P(G))}(G) \leq \text{Stab}_G(n).
\]

**Definition 2.2.** Given a spherically transitive group of \( G \leq \text{Aut}(X^*) \), we write \( L_n(G) \) for \( L_{R_n(P(G))}(G) \). We call \( (L_n(G))_{n \in \mathbb{N}} \) the *series of iterated local laws of G*.

We consider this series in the case of GGS-groups. It will be apparent from the definition that every GGS-group \( G \) acts locally by permutations from a cyclic group of order \( p \), i.e. it fulfils

\[
P(G) = \langle (01 \ldots p - 1) \rangle,
\]

The laws of such a group are generated by the commutators and \( p^{th} \) powers of generators in \( F_\infty \). Consequently, the group \( L_1(G) \) is the subgroup generated by \( G' \) and the \( p^{th} \) powers in \( G \). We shall prove that \( L_n(G) \) is in fact equal to \( G^{(n)} \).

2.2. **GGS-groups and their defining tuples.** Let \( \mathbf{e} = (e_1, \ldots, e_{p-1}) \in \mathbb{F}_p^{p-1} \) be a non-constant tuple, i.e. such that there are at least two different entries. We call the group \( G_\mathbf{e} \) generated by the rooted automorphism \( a = (01 \ldots p - 1) \) and the automorphism defined by

\[
b = \psi^{-1}(0 : b, \diamond : a^{e_0})
\]

the **GGS-group defined by** \( \mathbf{e} \), and we call \( \mathbf{e} \) the *defining tuple of* \( G_\mathbf{e} \).

Note that we exclude all constant tuples (in particular the zero tuple). The groups defined by constant non-zero tuples in the same fashion as above are usually also referred to as GGS-groups. Furthermore, groups defined by the same construction using elements of \( \mathbb{Z}/m \mathbb{Z} \) whose entries are set-wise coprime are sometimes also referred to as GGS-groups. In general, the structure of these groups is much less understood than in the case we consider here. Even for prime powers \( m = p^n \), the situation is much more involved, see for example [3], where the branching structures for these groups have been evaluated.

We consider the derived subgroups of a GGS-group \( G = G_\mathbf{e} \). Since \( G \) is two-generated, the first derived subgroup is normally generated by the commutator \( c = [b, a] \), whose action on the tree is given by

\[
\psi([b, a]) = \psi(b^{-1})\psi(b^{a})
\]

\[
= (0 : b^{-1}, \diamond : a^{-e_0})(1 : b, \diamond : a^{e_0 - 1})
\]

\[
= (0 : b^{-1}a^{e_0 - 1}, 1 : a^{-e_1}b, \diamond : a^{e_0 - 1 - e_0}).
\]

This signifies the importance of the first difference tuple of \( \mathbf{e} \), which we define as

\[
\mathbf{e}' = (e'_2, e'_3, \ldots, e'_{p-2}, e'_{p-1}) \in \mathbb{F}_p^{p-2},
\]
where \( e'_i = e_{i-1} - e_i \) for all \( i \in \{2, \ldots, p-1\} \). We shall see that the index of the second derived subgroup in \( G \) depends furthermore on the second difference tuple of \( e \), given by

\[
e'' = (e''_3, e''_4, \ldots, e''_{p-2}, e''_{p-1}) \in \mathbb{F}_p^{p-3},
\]

where \( e''_i = e_{i-2} - 2e_{i-1} + e_i = e'_{i-1} - e'_i \) for all \( i \in \{3, \ldots, p-1\} \). In case \( p = 3 \) the tuple \( e'' \) is the empty tuple. Clearly, we have described the beginning of an iterative procedure, but surprisingly, the indices of the higher derived subgroup do not depend on 'higher' difference tuples.

In the following, we consider the elements of the vector space \( \mathbb{F}_p^p \) and more generally of direct products of groups \( G \times \cdots \times G \) as indexed by the set \( X \). The choice of indexing for the defining tuple and its differences we have made above is for the following reason. Let \( \log_a : \langle a \rangle \to \mathbb{F}_p \) be the map assigning the power \( (i \mod p) \) to any \( a^i \), and \( \theta : G \to \mathbb{F}_p \) the map \( g \mapsto (\log_a(g0), \ldots, \log_a(g|p-1)^{\mathbb{Z}}) \) assigning to \( g \) its local actions under the first layer vertices. Then, by definition,

\[
\theta(b) = (0, e_1, \ldots, e_{p-1}).
\]

Thus we think of the defining tuple as an 'incomplete element' of \( \mathbb{F}_p^p \), and the element above as its full counterpart; similarly we think of \( e' \) and \( e'' \) as the 'tails' of regularly formed elements of

\[
\theta(c) = (e_{p-1}, -e_1, e'_2, e'_3, \ldots, e'_{p-1})
\]

and

\[
\theta([c, a]) = (e_{p-2} - 2e_{p-1}, e_1 + e_{p-1}, -2e_1 + e_2, e''_3, e''_4, \ldots, e''_{p-1})
\]

respectively.

We call \( e \), resp. \( e'' \), symmetric if and only if

\[
e_i = e_{p-i} \quad \text{for all } i \in \{1, \ldots, p-1\}, \text{ resp.}
\]

\[
e''_{i+1} = e''_{p+1-i} \quad \text{for all } i \in \{2, \ldots, p-2\}.
\]

These are clearly linear conditions. We define two linear subspaces \( S = \ker(M) \) and \( \tilde{S} = \ker(\tilde{M}) \) of \( \mathbb{F}_p^{p-1} \) as the kernels of the two linear maps given by the matrices

\[
M = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 & 0 & -1 \\
1 & 0 & \cdots & 0 & -1 & \cdots & \\
\vdots & & \ddots & & & & \\
1 & -1 & & & & & \\
\end{pmatrix}^t,
\]

in \( \text{Mat}(p-1,(p-1)/2;\mathbb{F}_p) \) and

\[
\tilde{M} = \begin{pmatrix}
1 & -2 & 1 & 0 & 0 & \cdots & \cdots & 0 & 0 & -1 & 2 & -1 \\
1 & -2 & 1 & 0 & \cdots & \cdots & 0 & -1 & 2 & -1 & & \\
\vdots & & \ddots & & & & & & & & & \\
1 & -2 & 1 & -1 & 2 & 1 & & & & & & \\
1 & -3 & 3 & -1 & & & & & & & & \\
\end{pmatrix}^t
\]

in \( \text{Mat}(p-1,(p-3)/2;\mathbb{F}_p) \). Clearly \( e \) is symmetric if and only if \( e \) is an element of \( S \), and we have \( e \in \tilde{S} \) if and only if \( e'' \) is symmetric. Using this description, the following lemma becomes apparent.

**Lemma 2.3.** Let \( e \) be symmetric. Then \( e'' \) is symmetric.
Proof. It can be easily seen that the subspace generated by the columns (displayed above as rows) of $\tilde{M}$ is contained in the subspace generated by the columns of $M$, i.e. that $S \subseteq \tilde{S}$. Thus all symmetric $e$ yield symmetric $e''$. □

Of course, if a vector is constant, all its difference tuples are trivial, hence in particular constant and symmetric.

We can also see that the containment of Lemma 2.3 is proper and that $\text{codim}_{\tilde{S}}S = 1$. For further computations, we simplify the basis given by the columns of $\tilde{M}$ using Gauß-Jordan elimination, and obtain

$$\tilde{N} = \begin{pmatrix}
1 & 0 & \ldots & 0 & 2 & -2 & 0 & \ldots & 0 & -1 \\
1 & \ldots & 0 & 4 & -4 & 0 & \ldots & 0 & -1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
1 & -3 & 3 & -1
\end{pmatrix}^t.$$

Lemma 2.4. Let $e \in \mathbb{F}_p^{p-1}$. If the second difference tuple $e''$ is symmetric, then

$$2(e_{p-1} - e_1) + (e_2 - e_{p-2}) = 0.$$

Proof. Since $e''$ is symmetric, the vector $e$ is contained in $\tilde{S}$. But the given linear equation is a linear combination of the first two columns of $\tilde{N}$, from whence the equality follows. □

For convenient use in formulas, we define the shorthand notation

$$\text{con}(d) = 1 \quad \text{if } d \text{ is constant, and } \text{sym}(d) = 1 \quad \text{if } d \text{ is symmetric,}$$

and otherwise.

Aside from the first and second difference tuples and the defining tuple itself, all cyclic shifts of $e$ (under the action of $a$) influence the structure of the GGS-group $G_e$. Fernández-Alcober and Zugadi-Reizabal [6] demonstrated that the index of the level stabilisers in a GGS-group depends only on whether the defining tuple is symmetric, and the rank of the circulant matrix $\text{Circ}(0 \ e) \in \text{Mat}(p, p; \mathbb{F}_p)$ associated to the ‘full version’ $\theta(b)$ of the defining tuple $(0 \ e)$, that is the matrix whose rows are the cyclic shifts of the vector $\theta(b)$.

For the computation of the indices of the level stabilisers and the derived subgroups, we use the König-Rados theorem, cf. e.g. [10, §134] or [9], which solves the problem of determining the rank of a circulant matrix over a prime field.

Theorem 2.5 (König-Rados). Let $p$ be a prime and $d \in \mathbb{F}_p^n$ a vector. Then

$$\text{rk} \text{Circ}(d) = n - m,$$

where $m$ is the multiplicity of 1 as a root of the polynomial $E_d = \sum_{i=0}^{n-1} d_i X^i$. In particular, $\text{rk} \text{Circ}(d) = n$ if and only if $\sum_{i=0}^{n-1} d_i \neq 0$.

For our purposes, we make a more general definition. Let $V$ be a finite-dimensional vector space over a finite field, let $B$ be an (ordered) basis for $V$, and let $C$ be the linear map that cyclically permutes the basis elements. Given a subset $M \subseteq V$, we denote by $\text{Circ}(M)$ the smallest $C$-invariant subspace containing $M$, the circulant space of $M$. The notational conflict with the definition of the circulant matrix given above is negligible; the circulant space is just the row space of the circulant matrix. We will often make no a distinction between the two.
There are not many $C$-invariant subspaces. This is no surprise, since $C$ defines the regular representation of a group of order $p$, which is the sum of $p$ one-dimensional irreducible sub-representations. In fact, there is a unique (full) flag of $C$-invariant subspaces in $V$, which we record in the following proposition.

**Proposition 2.6.** Let $V$ be an $\mathbb{F}_p$-vector space of dimension $n \in \mathbb{N}$, with basis $\mathcal{B} = \{b_0, \ldots, n-1\}$. Then the set of circulant spaces of $V$ has cardinality $n+1$ and forms a full flag of $V$. In particular, for any $M \subseteq V$,

$$\text{Circ}(M) = \bigcup_{m \in M} \text{Circ}(m).$$

Furthermore, the dimension of $\text{Circ}(m)$ for some $m = \sum_{i=0}^{n-1} m_i b_i = m \in V$ is $i$ if and only if $i$ is minimal such that

$$\sum_{j=n-i}^{n-1} \binom{j}{n-i} m_i = 0.$$  

**Proof.** We prove that, for every $i \in \{0, \ldots, n\}$, the set

$$\text{Circ}_i(V) = \{d \in V \mid \text{rk Circ}(d) \leq i\}$$

is an $i$-dimensional $C$-invariant subspace of $V$. If this is true, the circulant space associated to any $d \in \text{Circ}_i(V) \setminus \text{Circ}_{i-1}(V)$ is in fact equal to $\text{Circ}_i(V)$; since it is the minimal invariant subspace containing $d$, it is contained in $\text{Circ}_i(V)$, and by the choice of $d$ it has the same dimension as $\text{Circ}_i(V)$. Now for any subset $M \subseteq V$, the circulant space is equal to the smallest invariant subspace containing all $\text{Circ}(m)$ for $m \in M$. It is easy to see that these spaces are linearly ordered, hence $\text{Circ}(M)$ is equal to the maximal subspace of the form $\text{Circ}(m)$.

It remains to prove the claim. Fix $i \in \{0, \ldots, n\}$ and $d \in \text{Circ}_i(V)$. Clearly the image of $d$ under $C$ defines the same circulant space, hence $\text{Circ}_i(V)$ is invariant. It remains to prove that it is an $i$-dimensional subspace.

To achieve this, we review some combinatorics of polynomials. Let $Q = Q^{(n)} = \sum_{k=0}^{n-1} q_k X^k \in \mathbb{F}_p[X]$ be a polynomial of degree $n - 1$. In view of Theorem 2.5, we conduct Euclidean division by $(X - 1)$, and write $Q^{(n)} = (X - 1)Q^{(n-1)} + R_n(Q)$, for a polynomial $Q^{(n-1)}$ and a constant $R_n(Q) \in \mathbb{F}_p$. Iterating this, we write $Q^{(i)} = (X - 1)Q^{(i-1)} + R_i(Q)$ for $i \in \{0, \ldots, n-1\}$. Clearly $\deg Q^{(i)} = i - 1$. The coefficients of $Q^{(i)}$ and the value of $R_i(Q)$ can be calculated in terms of the starting polynomial $Q^{(n)}$. We shall now perform this calculation. (Alternatively, we could compute the coefficients of $Q^{(n)}$ as a polynomial in $(X - 1)$. Indeed, it is easy to check that

$$Q^{(n-1)} = \sum_{k=0}^{n-2} \sum_{\ell=k+1}^{n-1} q_{\ell} X^k \quad \text{and} \quad R_n(Q) = \sum_{k=0}^{n-1} q_k.$$  

Thus, both the coefficient of $X^k$ in $Q^{(i)}$ and the value $R_i(Q)$ are weighted sums (i.e. positive $\mathbb{F}_p$-linear combinations) of the coefficients of $Q$. Write $\kappa(i, j, k)$ for the multiplicity of $q_j$ in the coefficient of $X^k$ in $Q^{(i)}$. The equation above shows that

$$\kappa(i, j, k) = \sum_{\ell=k+1}^{n-1} \kappa(i + 1, j, \ell).$$

Consequently, for $i < n$, we find the familiar (at least when ignoring $j$) recursion formula
\[ \kappa(i, j, k) = \kappa(i, j, k + 1) + \kappa(i + 1, j, k + 1), \]
using that $\kappa(i, j, n) = 0$ for all $i, j \in \{0, \ldots, n\}$. Since $\kappa(n - 1, j, k)$ is 1 for $j > k$, and is equal to 0 otherwise, we find
\[ \kappa(i, j, j + i - n) = 1 \quad \text{and} \quad \kappa(i, j, k) = 0 \quad \text{for } k > j + i - n, \]
and obtain the equality
\[ \kappa(i, j, k) = \binom{j - k - 1}{n - i - 1}, \]
where we agree on $\binom{l}{r} = 0$ for $r < s$. The remainder $R_i(Q)$ is equal to the sum of all coefficients of $Q^{(i)}$. Since $\deg Q^{(i)} = i - 1$, we have to calculate the sum
\[ R_i(Q) = \sum_{k=0}^{i-1} \sum_{j=0}^{n-1} \kappa(i, j, k) q_j = \sum_{j=0}^{n-1} q_j \sum_{k=0}^{i-1} \binom{j - k - 1}{n - i - 1}. \]
We may ignore all summands with $j < n - i$, since then $j - k - 1 < n - i - 1$ for all $k \in \{0, \ldots, i - 1\}$, and the binomial coefficient is zero. Likewise we may ignore all cases where $k > j + i - n$. It remains to use ‘Stifel’s law’. We find
\[ R_i(Q) = \sum_{j=n-i}^{n-1} q_j \sum_{k=0}^{j-i} \binom{j - k - 1}{n - i - 1} = \sum_{j=n-i}^{n-1} q_j \sum_{k=n-i-1}^{j-1} \binom{k}{n - i - 1} = \sum_{j=n-i}^{n} q_j \binom{j}{n - i}. \]
Coming back to our circulant spaces, Theorem 2.5 tells us that the condition $d \in \text{Circ}_i(V)$, for any $i$, translates to $R_j(E_d) = 0$ for all $j \in \{i+1, \ldots, n\}$, and $R_i(E_d) \neq 0$. By our computations, the map $R_j : V \to \mathbb{F}_p$ (for any $j \in \{1, n\}$) assigning to an element $d = (d_0, \ldots, d_{n-1})$, represented in the basis $B$, the value of $R_j(E_d)$ as given above is $\mathbb{F}_p$-linear. Define $R : V \to \mathbb{F}_p^n$ by $dR = (dR_1, \ldots, dR_n)$. This map is, due to $B$ and the standard basis, represented by the matrix
\[
\begin{pmatrix}
\binom{n}{0} & \binom{n-2}{0} & \binom{n-1}{0} \\
\binom{1}{0} & \binom{n-2}{1} & \binom{n-1}{1} \\
\vdots & \vdots & \vdots \\
0 & \binom{n-2}{n-2} & \binom{n-1}{n-2} \\
& & \binom{n-1}{n-1}
\end{pmatrix},
\]
a right-justified Pascal triangle. The subspace $\text{Circ}_i(V)$ is the kernel of the composition $R \circ \pi_{\leq i}$, where $\pi_{\leq n-i}$ denotes the projection to the first $n - i$ coordinates. Since $R$ has full rank, the image under this map has dimension $n - i$, whence the kernel has dimension $i$. Thus $\dim \text{Circ}_i(V) = i$. \hfill \square

It is not true that every defining tuple gives rise to a unique GGS-group. In particular, multiples of a given $e$ define the same group (as a subgroup of $\text{Aut}(X^*)$). Furthermore, certain reorderings of the entries give isomorphic groups, which helps us to reduce the difficulty of our computations. We use the following characterisation.

**Theorem 2.7.** [11] Let $G$ and $H$ be two GGS-groups over the $p$-regular tree defined by $e$ and $d$, respectively. Then the following two statements are equivalent:

(i) $G \cong H$;
(ii) there exist \( \lambda, \mu \in \mathbb{F}_p^\times \) such that \( e_i = \mu \cdot d_{\lambda,i} \) for all \( i \in \{1, \ldots, p - 1\} \).

This allows us to choose defining tuples with desirable properties.

**Corollary 2.8.** Let \( G \) be a GGS-group. Then

(i) there is an GGS-group \( G_{\mathbf{e}} \) isomorphic to \( G \) such that \( e_1 = 1 \), and

(ii) there is an GGS-group \( G_{\mathbf{e}} \) isomorphic to \( G \) such that \( e'_i = 1 \) for some \( i \in \{1, \ldots, p - 1\} \).

### 2.3. Properties and structure of GGS-groups

We shall fix some further notation. Recall that, working with a given GGS-group \( G \), we shall denote the rooted generator \( a \), the directed generator \( b \), and we write \( c = [b, a] \). Furthermore we shall use the following shorthand notation for the conjugates of \( c \), \( c^i = c a^i = [b a^i, a] \).

In particular, \( c^0 = c \). We now describe the sections of the elements \( c^i \). We will use this computation often and without constant reference. The sections of \( c^i \) are the sections of \( c^0 \) cyclically shifted; in general, for any \( g \in \text{Aut}(X^*) \) and for any \( i \in \mathbb{Z} \), the first level sections of \( g^a^i \) are the sections of \( g \), permuted by the inverse \( a^{-i} \), since the sections of \( a \) are trivial and \( g^a^i |_j = a^{-i} |_j g |_{a^i} |_j = g |_{j-i} \), i.e. \( \psi(g^a^i) = \psi(g)^{a^{-i}} \), with \( a^{-i} \) acting as a permutation of the index set \( X \).

It is well-known that all GGS-groups posses strong ‘self-similarity’ properties, which is one reason making this class of groups an interesting object to study. We collect some statements into a lemma, for proofs see e.g. [11].

**Lemma 2.9** (Fractality properties of GGS-groups). Let \( G \) be a GGS-group. Then \( G \) is self-similar, fractal and contracting with nucleus \( \langle a \rangle \cup \langle b \rangle \).

Furthermore, due to Fernández-Alcober and Zugadi-Reizabal, every GGS-group is a regular branch group (see below). The same is not true for the analogues of GGS-groups defined by constant tuples, explaining their divergent behaviour.

**Theorem 2.10** (Branching properties of GGS-groups, cf. [6]). Let \( G \) be a GGS-group with defining tuple \( \mathbf{e} \). Then

(i) \( \psi(\gamma_3(\text{Stab}_G(1))) = \gamma_3(G) \times . \times \gamma_3(G) \), and

(ii) \( [G' \times . \times G' : \psi(\text{Stab}_G(1)')] = p^{\text{sym}(\mathbf{e})} \).

Also \( \text{Stab}_G(2) \leq \gamma_3(G) \). In particular, \( G \) is regular branch over \( \gamma_3(G) \), and it is regular branch over \( G' \) if \( \mathbf{e} \) is non-symmetric.

This allows the application of the following lemma of Šunič, which provides the analogue of Theorem 1.2 for level stabilisers.

**Lemma 2.11.** [13, Lemma 10] Let \( G \) be a regular branch group over \( K \leq G \), such that \( \text{Stab}_G(n) \leq K \) for some \( n \in \mathbb{N} \). Then for all \( m \geq n \)

\[ \psi(\text{Stab}_G(m + 1)) = \text{Stab}_G(m) \times . \times \text{Stab}_G(m). \]

For GGS-groups in particular, the value of \( n \) is 2.

We now begin with a study of certain small quotients of GGS-groups which will play a role in the determination of the derived series. Most of these results are known, but using the next lemma, we give new and short proofs that have the benefit of
being easily generalised to larger families of groups, as they (for the most part) do not involve $p$-group methods.

**Lemma 2.12** (Spine-counting lemma). Let $G$ be a GGS-group, let $g \in G$, and let $w(a, b)$ be a word in the letters $a$ and $b$ that evaluates to $g$ in $G$. Then clearly $w(1, b)$ evaluates to an element in $(b) \equiv \mathbb{F}_p$. The map

$$\varepsilon : G \to \mathbb{F}_p, \quad g \to w(1, b)$$

that assigns to $g$ its $b$-exponent sum is well-defined and a homomorphism. In other words, the quotient of $G$ by the normal closure of $(a)$ is a group of order $p$.

**Proof.** Rewrite $w(a, b)$ into a word of the form

$$b^{a^j} b^{a^j} b^{a^j} \ldots b^{a^n} a^{k_0} a^{k_1} \ldots a^{k_{n-1}}$$

with $k_i, k_i \in \mathbb{F}_p$ for $i \in \{0, \ldots, n\}$ and $k_i \neq k_{i+1}$ for $i \in \{0, \ldots, n-2\}$. We may also assume $n \geq 1$, since the statement is clearly true for $n = 0$. Let $x$ be any letter of $X$. Since all conjugates of $b$ fix $x$, a word representing $w(a, b)|_x$ is

$$b^{[\ell_0, \ell_1]} b^{[\ell_1, \ell_2]} \ldots b^{[\ell_{n-1}, \ell_n]}.$$

Look at a length-2 subword $b^{[\ell_j]} b^{[\ell_{j+1}]}$. Since $k_j \neq k_{j+1}$, at least one of the two sections is a power of $a$, since only one section of $b$ is not. We collect all resulting elements of $(a)$ and combine consecutive powers of $b$ (which does not change the $b$-exponent sum) and obtain a word $w_x(a, b)$ with fewer syllables representing $w(a, b)|_x$, such that $\sum_{x=0}^{n-1} w_x(1, b) = w(1, b)$. Since $G$ is contracting (which is a consequence of the same argument), for every $w(a, b)$ there is a level $X^n$ for $n \in \mathbb{N}$, such that all sections of $w(a, b)$ at vertices $v \in X^n$ are in the nucleus of $G$, hence powers of $a$ or $b$. Clearly, all sections are minimal words, and the sum of their $b$-exponent sums is the $b$-exponent sum of $w(a, b)$. Thus this value does not depend on the word representing a certain element. Consequently $\varepsilon$ is well-defined and a homomorphism. \hfill $\square$

Using this lemma, we are able to quickly recover some well-known facts about certain small quotients of GGS-groups.

**Lemma 2.13.** Let $G$ be a GGS-group. Then

(i) $G/G'$ is isomorphic to an elementary abelian $p$-group of rank 2,

(ii) $G/\gamma_3(G)$ is isomorphic to the Heisenberg group over $\mathbb{F}_p$,

(iii) $G/Stab(1)'$ has order $p^{p+1}$, and

(iv) the subgroup generated by the $p^k$ powers of $G$ is contained in $G'$.

**Proof.** (i): The quotient $G/G'$ is generated by the images of $a$ and $b$, hence a quotient of an elementary abelian $p$-group of rank 2. Clearly $b$ is not a power of $a$, and $a$ is not a stabiliser of the first level, hence not in the commutator subgroup. Since the $b$-exponent sum of any element in the commutator subgroup is $0$ mod $p$, by Lemma 2.12 the generator $b$ is not in $G'$ either.

(ii): The centre of $G/\gamma_3(G)$ is generated by $c = [b, a]$. Since $c^p \equiv \gamma_3(G) \equiv [b, a]^p = 1$, the group $G/\gamma_3(G)$ is isomorphic to the Heisenberg group over $\mathbb{F}_p$.

(iii): The first level stabiliser is generated by the conjugates of $b$ by powers of $a$. Since the position of the section equal to $b$ is different for every different power of $a$, it is generated by $p$ elements of order $p$, all of $b$-exponent sum $1$. Thus, as in (i), the quotient $Stab_{G}(1)/Stab_{G}(1)'$ is an elementary abelian $p$-group of rank $p$. Since $G/Stab_{G}(1)$ is cyclic of order $p$, the result follows.
(vi): Lastly, it is enough to prove that \( b \) is not a \( p \)th power. But the \( b \)-exponent sum of a \( p \)th power is 0 mod \( p \), hence \( b \) is not a \( p \)th power by Lemma 2.12. \( \square \)

**Proposition 2.14.** Let \( G \) be a GGS-group. Then

\[
[\text{Stab}_G(1)', G'] = \gamma_3(\text{Stab}_G(1)).
\]

In particular, \( \gamma_3(\text{Stab}_G(1)) \leq G'' \).

**Proof.** Recall from Theorem 2.10 that

\[
\psi(\gamma_3(\text{Stab}_G(1))) = \gamma_3(G) \times \ldots \times \gamma_3(G).
\]

The inclusion \( [\text{Stab}_G(1)', G'] \leq \gamma_3(\text{Stab}_G(1)) \) holds vacuously. We have to establish the other inclusion. Using Proposition 2.1, it is enough to prove that \( (0 : [c, b], \odot : \text{id}) \) and \( (0 : [c, a], \odot : \text{id}) \in \psi([\text{Stab}_G(1)', G']) \), since \( \gamma_3(G) \) is normally generated by \([c, b]\) and \([c, a]\). We distinguish two cases.

**Case 1:** The defining tuple is non-symmetric. Then by Theorem 2.10(ii)

\[
\psi(\text{Stab}_G(1)') = G' \times \ldots \times G',
\]

and \( (0 : c, \odot : \text{id}) \in \psi(\text{Stab}_G(1)') \). By Corollary 2.8(ii) we may assume \( e_i' = 1 \) for some \( i \in \{2, \ldots, p - 1\} \). Consequently \( c_i = a \), hence

\[
c_{p-i}|0 = c_i|0 = a,
\]

\[
(c_{p-i}^{e_{p-1}} - 1)|0 = a^{e_{p-1}a - e_{p-1}b} = b.
\]

Since \( c_{p-i} \) and \( c \) are elements of \( G' \), we obtain that

\[
[0 : c, \odot : \text{id}), \psi(c_{p-i}^{e_{p-1}} - 1)] = (0 : [c, a], \odot : \text{id}), \quad \text{and}
\]

\[
[0 : c, \odot : \text{id}, \psi(c_{p-i}^{e_{p-1}} - 1)] = (0 : [c, b], \odot : \text{id})
\]

are both elements of \( \psi([\text{Stab}_G(1)', G']) \).

**Case 2:** The defining tuple is symmetric. Since it is not constant, the prime \( p \) is necessarily greater than 3. By Corollary 2.8(i), we may assume \( e_1 = e_{p-1} = 1 \). Observe that

\[
\psi([b, b^a]) = [\psi(b), \psi(b^a)] = (0 : [b, a], 1 : [a, b], \odot : \text{id}) = (0 : c, 1 : c^{-1}, \odot : \text{id}).
\]

Now let \( j \in \mathbb{F}_p \setminus \{1, p - 1\} \), which exists since \( p > 3 \). Then

\[
\psi([a^{2j}, b^j]) = (0 : a^{-e_{p-2j}}b, 2j : b^{-1}a^{e_{2j}}} \odot : a^{e_{-e_2} - 2j}),
\]

in particular \([a^{2j}, b^j]) = e_{j-1} - e_{p-j-1} = \text{id}, \) since \( e \) is symmetric. Thus

\[
[a^{2j}, b^j]|_1 = 1, \quad \text{and}
\]

\[
[a^{2j}, b^j]|_0 = a^{e_{j-1} - e_{p-j-1}},
\]

since \( j \not\in \{1, p - 1\} \). If there is such a \( j \) with \( e_{j-1} \neq e_{p-j-1} \), let \( i \in \mathbb{Z} \) be such that \( i \equiv_p (e_{j-1} - e_{p-j-1})^{-1} \), and observe that

\[
\psi([b^a, b^j]) = [(0 : c, 1 : c^{-1}, \odot : \text{id}), (0 : a, 1 : \text{id}, \odot : [a^{2j}, b^j])|_0
\]

\[
= (0 : [c, a], \odot : \text{id}).
\]
But such an element $j$ must always exist. Assume otherwise, for contradiction. Then for any $j \notin \{1, p-1\}$

$$e_j = e_{(1+j)-1} = e_{p-(1+j)-1} = e_{j+2}. $$

But since every element of $F_p^*$ is a multiple of 2, this implies that $e$ is constant.

It remains to show $(0 : [c, b], \circ : \text{id}) \in \psi([\text{Stab}_G(1)'', G''])$. If $e_{p-2} \neq 0$, consider the element $g = [a^{2j}, b]^{i_{e_{p-2}}}[a^2, b]$, which fulfills

$$g|_0 = a^{e_{p-2}}a^{-e_{p-2}}b \quad \text{and} \quad g|_1 = a^{e_1-e_{p-1}} = \text{id},$$

using the fact that $e$ is assumed to be symmetric. If otherwise $e_{p-2} = 0$, set $g = [a^2, b]$, which has the sections

$$g|_0 = a^{-e_{p-2}}b = b, \quad \text{and} \quad g|_1 = a^{e_1-e_{p-1}} = \text{id}.$$  

In both cases

$$\psi([b^p, b], g)) = (0 : [c, b], \circ : \text{id}). \quad \square$$

Using Proposition 2.14, we may derive a nice corollary.

**Corollary 2.15.** Let $G$ be a GGS-group. Then $G$ is branch over $G''$, independent on the value of $\text{sym}(e)$.

**Proof.** Using Theorem 2.10(i) and Proposition 2.14 we find the inclusion

$$G'' \times \mathfrak{p} \times G'' \leq \gamma_3(G) \times \mathfrak{p} \times \gamma_3(G) = \psi(\gamma_3(\text{Stab}(1)))$$

$$= \psi([\text{Stab}(1)', G']) \leq \psi(G''). \quad \square$$

3. The derived series of GGS-groups

The main difficulty for the computation of the index $|G : G^{(n)}|$ for all $n > 1$ is the calculation of $|G : G''|$. We now begin with this case, applying the theory of circulant spaces sketched in Proposition 2.6. Recall that we can compute the circulant space generated by some vector $d \in F_p^n$ by counting the number of trailing zeros in the image of $d$ under the linear map $R$, and that the last three components may be computed as

$$dR_p = \sum_{i=0}^{p-1} d_i, \quad dR_{p-1} = \sum_{i=0}^{p-1} id_i, \quad \text{and} \quad dR_{p-2} = \sum_{i=0}^{p-1} \binom{i}{2} d_i.$$

**Proposition 3.1.** Let $G$ be a GGS-group with defining tuple $e$. Then

$$\log_p |G : G''| = p + 1 + \text{con}(e') + \text{sym}(e'') - \text{sym}(e).$$

**Proof.** Since $G' \leq \text{Stab}_G(1)$, the second derived subgroup $G''$ is contained in $\text{Stab}_G(1)'$, which is in turn contained in $G' \times \mathfrak{p} \times G'$ by Theorem 2.10. By Proposition 2.14 and Theorem 2.10 we find

$$\psi(G'') \geq \psi(\gamma_3(\text{Stab}(1))) = \gamma_3(G) \times \mathfrak{p} \times \gamma_3(G),$$

so that $G''$ is wedged in between the subgroups $\psi^{-1}(\gamma_3(G) \times \mathfrak{p} \times \gamma_3(G))$ and $\psi^{-1}(G' \times \mathfrak{p} \times G')$. Since the quotient $G'/\gamma_3(G)$ is cyclic of order $p$ by Lemma 2.13(i) and (ii), we may identify the quotient

$$(G' \times \mathfrak{p} \times G')/\gamma_3(G) \cong G'\gamma_3(G) \times \mathfrak{p} \times G'/\gamma_3(G)$$

with a $p$-dimensional $F_p$-vector space $V$, such that $G'' \cdot \gamma_3(G) \times \mathfrak{p} \times \gamma_3(G)$ represents a sub-vector space $W$ of $V$. We calculate the dimension of this subspace. Knowing it,
we can easily deduce the index of the second derived subgroup. Recall that \( \log_p [G' \times \mathcal{P} : \text{Stab}(1)''] = \text{sym}(e) \) by Theorem 2.10, and has that \( \text{Stab}(1)' \) has \( p \)-logarithmic index \( p + 1 \) in \( G \) by Lemma 2.13. Thus

\[
\log_p |G : G''| = \log_p |G : \text{Stab}(1)'| + \log_p [\text{Stab}(1)' : G''] = \log_p |G : \text{Stab}(1)'| + \log_p [G' \times \mathcal{P} : G''] - \log_p [G'' : \text{Stab}(1)'] = p + 1 + \text{dim}_V(W) - \text{sym}(e).
\]

Note that it is a consequence of [6, Lemma 3.5] (and indeed, of the calculation of \([b, b^0]\) at the beginning of ‘Case 2’ in the proof of Proposition 2.14) that the subspace \( U \) represented by \( \text{Stab}(1)' \) in \( V \) is equal to \( \text{Circ}_{p-1}(V) \) if \( e \) is symmetric. We will not use this fact here, but find it helpful to keep in mind.
To compute the dimension of $W$, we calculate the images of a set of generators of $W$ in $V$. Since $G'$ is generated by the elements \( \{ c^g \mid g \in G \} \), the second derived subgroup $G''$ is generated by elements of the form
\[
[c^{g_1}, c^{g_2}]^{g_3} = [c, c^{g_2}g_1^{-1}]g_3
\]
for some $g_1, g_2$ and $g_3 \in G$, i.e. a generating set is given by
\[
\{ [c, c^g]^h \mid g, h \in G \}.
\]
Since we calculate modulo $\gamma_3(G) \times \ldots \times \gamma_3(G)$, we may restrict the choices of $g$ and $h$ significantly. Indeed, writing $g = a^i s$ and $h = a^j t$ for some $i, j \in \mathbb{F}_p$ and $s, t \in \text{Stab}(1)$, we see that, for any $x \in X$ (and writing $y = x^{a^i}$ and $z = y^{a^j} = x^{a^{i+j}}$), and using the fact that the section map is a homomorphism on $\text{Stab}(1)$,
\[
[c, c^{a^i}]^{a^j t}|_x = [c, c^{a^i}]|_y = [c^{s_y}, c]^{s_z} = [c_x, c] = \gamma_3(G), \quad c|_y, c|_z.
\]
Thus $s$ and $t$ play no role modulo $\gamma_3(G) \times \ldots \times \gamma_3(G)$, and we may restrict to the generating set
\[
\{ [c, c^{a^{i+j}}]^{a^{-j}} | i, j \in \mathbb{F}_p \} = \{ \{ c_i, c_j \mid i, j \in \mathbb{F}_p \}.
\]
We do also know how $a$ acts (via the conjugation action on $\text{Stab}(1)'$) on the vector space $U$. To describe this action, we choose a basis; since $G'/\gamma_3(G)$ is generated by the image $\tau$ of $c$, we decide to consider this abelian quotient as a group written additively, i.e. $c^i\gamma_3(G) = i\tau$ for any $i \in \mathbb{F}_p$. Our basis is hence the standard basis with respect to $\tau$
\[
((\tau, 0, \ldots, 0), (0, \tau, 0, \ldots, 0), \ldots, (0, \ldots, 0, \tau))
\]
Now conjugation by $a$ (on any element $s$ of the stabiliser) cyclically permutes the entries of the tuple $\psi_1(s)$. This corresponds to the linear map cyclically permuting the basis elements, hence extends naturally to an action on the full space $V$. Since $W$ is the subspace representing $G''$, a normal subgroup, it is invariant under this action, i.e. it is a circulant space. Notice that $\{ c_i, c_j \} a^{-k} = [c_{i+k}, c_{j+k}]$. Furthermore
\[
[c, c_i]^{-1} = [c_i, c] = [c^{a^i}, c] = [c, c^{a^{-i}}],
\]
thus the set $\{ [c, c_i] \mid i \in \{1, \ldots, (p-1)/2\} \}$ normally generates $G''$. Equivalently, the images under $\theta$ (the map $\text{Stab}(1) \ni g \mapsto (\log_a(g_0), \ldots, \log_a(g_{p-1}))$ defined at the beginning of Section 2.2)
\[
\theta([c, c_i])
\]
generate $W$ as a cyclically invariant subspace, i.e.
\[
W = \text{Circ}(\{ d_i \mid i \in \{1, \ldots, (p-1)/2\} \})
\]
By Proposition 2.6, it is enough to compute the rank of $\text{Circ}(d_i)$ for every $i$. So let us compute the images of $[c, c_i]$ under $\theta$. We begin with the cases $i \in \{2, \ldots, (p-1)/2\}$, where we find
\[
\psi([c, c_i]) = \begin{pmatrix}
0 : \quad [b^{-1}a^{b^{-1}}, a^{b^{-1}}], & 1 : \quad [a^{-e_1}b, a^{e_1}b^{p-1}] \\
1 : \quad [a^{e_1}, b^{-1}a^{e_1}], & i + 1 : \quad [a^{e_1}b^{-1}, a^{-e_1}] \\
\end{pmatrix} \equiv \begin{pmatrix}
0 : \quad [b, a]^{-e_p}, & 1 : \quad [b, a]^{e_p}, \\
i : \quad [b, a]^{e_i}, & i + 1 : \quad [b, a]^{-e_i}, \\
\end{pmatrix} \pmod{\gamma_3(G) \times \ldots \times \gamma_3(G)}.
\]
By our choice of basis for $V$, we find
\[(*) \quad d_1 = \theta([c, c_i]) = (0 : -e'_{p-i}, 1 : e'_{p-i+1}, i : e'_i, i + 1 : -e'_{i+1}).\]
The last generator $[c, c_1]$ has a slightly different form,
\[
\psi([c, c_1]) = (0 : [b^{-1} a^{e_{p-1}} a^{e'_{p-1}}], 1 : [a^{-e_1} b, b^{-1} a^{e_{p-1}}], 2 : [a^{e_2}, a^{-e_1} b], \cdot : \text{id})
\equiv (0 : -e''_{p-1}, 1 : e''_{p-1} - e_1, 2 : c^{-e_2}, \cdot : \text{id}) \mod \gamma_3(G) \times \langle \hat{p} \rangle \times \gamma_3(G),
\]and gives rise to the vector
\[(*)_1 \quad d_1 = \theta([c, c_1]) = (0 : -e'_{p-1}, 1 : e_{p-1} - e_1, 2 : -e'_2, \cdot : 0).
\]Using these descriptions, we are able to compute some of the circulant spaces associated to $d_1$ by applying the maps $R_p, R_{p-1}$ and $R_{p-2}$ to $d_1$. To do so, we make a case distinction.

\textit{Case 1:} If the second differences vector $e''$ is not symmetric, there is some index $i \in \{3, \ldots, p-1\}$ such that $e''_{i+1} \neq e''_{p-i+1}$. In this case, the sum of the components of the corresponding vector $d_1$ is
\[d_1 R_p = (e'_{p-i} - e'_{p-i+1}) - (e'_i - e'_{i+1}) = e''_{p-i+1} - e''_{i+1} \neq 0,
\]and by Theorem 2.5 the rank of the circulant matrix $\text{Circ}(d_1) = p$, since the sum of the coefficients of $d_1$ is not 0. The subspace $W$ is equal to the full space $V$, and we find
\[\log_p|G : G''| = \log_p|G : G' \times \langle \hat{p} \rangle \times G'|.
\]Assume that the first differences vector $e'$ is constant. Then $e''$ is constant 0, hence symmetric, a contradiction. Also, by Lemma 2.3, the asymmetry of $e''$ forces $e$ to not be symmetric, hence $G' \times \langle \hat{p} \rangle \times G'$ is in fact equal to $\text{Stab}(1)'$ and a subgroup of $G$. We conclude that the index of the second derived subgroup fulfils
\[\log_p|G : G''| = p + 1 = p + 1 + \underbrace{\text{con}(e')}_{=0} + \underbrace{\text{sym}(e'')}_{=0} - \underbrace{\text{sym}(e)}_{=0}.
\]

\textit{Case 2:} Now assume that the defining tuple $e''$ is symmetric. Using the description of the generators given in the first case, we see that $\text{Circ}(\theta([c, c_i])) \subseteq \text{Circ}_{p-1}(V)$. We furthermore need to consider the generator $[c, c_1]$, that played no role in the previous case. Since
\[d_1 R_p = -e'_{p-1} + e_{p-1} - e_1 - e'_2 = 2(e_{p-1} - e_1) + (e_2 - e_{p-2}) = 0
\]by Lemma 2.4, the sum of the coefficients of $[c, c_1]$ vanishes, and $\text{Circ}([c, c_1])$ is contained in $\text{Circ}_{p-1}(V)$ as well. Consequently, $W$ is a subspace of $\text{Circ}_{p-1}(V)$. We can go on and reduce the possible size of $\text{Circ}([c, c_1])$ further. Consider the image of the cyclic shift $[c, c_1]a^{-1}$ under $\theta$,
\[\hat{d}_1 = \theta([c, c_1]a^{-1}) = (e_{p-1} - e_1, -e'_1, 0, \ldots, 0, -e'_{p-2}).
\]Of course, this vector generates the same circulant space. But clearly
\[\hat{d}_1 R_1 = 0 \cdot (e_{p-1} - e_1) - e'_1 - (p - 1)e'_{p-2} = -e'_1 + e'_{p-2} = 0,
\]since $e'$ is symmetric. Hence $\text{Circ}(d_1) \subseteq \text{Circ}_{p-2}(V)$.

Contrary to the situation in the previous case, the symmetry of $e''$ does not force $e$ or $e'$ to be symmetric (resp. constant). Therefore, we have to make another case
Subcase 2.1: Assume additionally that $e'$ is not constant, i.e. that $e''$ is not zero. We want to show that $\text{Circ}(d_1) = \text{Circ}_{p-2}(V)$ for some $i \in \{1, \ldots, (p-1)/2\}$. Notice that for all $i \in \{2, \ldots, p-1\}$ we find

$$e'_{i+1} - e'_{p-i+1} = e''_{i+1} + e'_{i+2} - e'_{p-i} - e''_{p-i+1} = e'_{i+2} - e'_{p-i},$$

since $e''$ is symmetric, and consequently

$$(1) \quad e'_{i+1} - e'_{p-i+1} = e'(p-1)/2 - e'(p+1)/2 = e'(p+1)/2.$$

Building on this calculation, we can compute

$$d_1 R_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot e'_{p-i} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} e'_{p-i+1} + \begin{pmatrix} i \\ 1 \end{pmatrix} e'_i - \begin{pmatrix} i + 1 \\ 1 \end{pmatrix} e'_{i+1} = e'_{p-i+1} - e'_{i+1} + i(e'_i - e'_{i+1}) = ie''_{i+1} - e''(p+1)/2.$$

This is not 0 if $e''(p+1)/2 = 0$, since there must exist some $i \in \{3, \ldots, (p-3)/2\}$ such that $e''_{i+1} \neq 0$, because $e''$ is by assumption symmetric and non-zero. If otherwise $e''(p+1)/2 \neq 0$, for $i = (p-1)/2$ the equation becomes

$$d_1 R_{p-1} = ie''_{i+1} - e''(p+1)/2 = (p-3)/2 \cdot e''(p+1)/2 \neq 0.$$

Thus $\text{Circ}_{p-1}(V) = \text{Circ}(d_1) \subseteq W \subseteq \text{Circ}_{p-1}$, and we can verify that

$$\log_p |G : G''| = p + 1 + \text{codim}_V(W) - \text{sym}(e)$$

$$= p + 2 - \text{sym}(e)$$

$$= p + 1 + \text{sym}(e') + \text{sym}(e'') - \text{sym}(e).$$

Subcase 2.2: Finally, assume, in addition to $e''$ being symmetric, that $e'$ is constant. Write $k \in \mathbb{F}_p^*$ for the constant value of $e'$. Note that $k \neq 0$, since otherwise $e'$ is zero and $e$ constant.

As we have argued above, $W$ is contained in $\text{Circ}_{p-1}(V)$. In view of the formula we want to establish, we aim to prove that $W = \text{Circ}_{p-2}(V)$. We first show that $\text{Circ}_{p-2}(V) \subseteq W$, by computing

$$d_1 R_{p-2} = -\begin{pmatrix} 0 \\ 2 \end{pmatrix} e'_{p-2} + \begin{pmatrix} 1 \\ 2 \end{pmatrix} (e_{p-1} - e_1) - \begin{pmatrix} 2 \\ 2 \end{pmatrix} e'_1 = -e'_1 = -k \neq 0,$$

hence $\text{Circ}_{p-2}(V) = \text{Circ}(y_1) \subseteq W$.

It remains to show that $\text{Circ}(d_1) \subseteq \text{Circ}_{p-2}(V)$ for all $i \in \{2, \ldots, \frac{p-1}{2}\}$, i.e. to show that $d_1 R_1 = 0$. We calculate

$$d_1 R_{p-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot e'_{p-i} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} e'_{p-i+1} + \begin{pmatrix} i \\ 1 \end{pmatrix} e'_{i+1} - \begin{pmatrix} i + 1 \\ 1 \end{pmatrix} e'_{i+1} = k + ik - (i+1)k = 0$$

Thus $W = \text{Circ}_{p-2}(V)$ and

$$\log_p |G : G''| = p + 3 - \text{sym}(e) = p + 1 + \text{con}(e') + \text{sym}(e'') - \text{sym}(e),$$

which concludes the proof. 

$\square$
In fact, our proof gives more than just the index, but allows for some structural description of $G''$. We record this in the following corollary.

**Corollary 3.2.** Let $G$ be a GGS-group. Write $V$ for the vector space $G'/\gamma_3(G) \times \mathcal{P} \times G'/\gamma_3(G)$. Write $\pi$ for the quotient map $G \to G/\gamma_3(\text{Stab}(1))$. Then

$$\psi(G'') = \{(g_1, \ldots, g_p) \in G' \times \mathcal{P} \times G' \mid (\pi(g_1), \ldots, \pi(g_p)) \in \text{Circ}_{p-i}(V)\},$$

where $i = \text{con}(\mathbf{e}) + \text{sym}(\mathbf{e}'') - \text{sym}(\mathbf{e})$.

To describe the series of iterated local laws, we record the following lemma.

**Lemma 3.3.** The group of $p$th powers of $G'$ is contained in $\gamma_3(\text{Stab}_G(1))$. In particular, it is contained in $G''$.

**Proof.** The group $G'$ is geometrically contained in the direct product $G \times \mathcal{P} \times G$. Now $G/\gamma_3(G)$ is isomorphic to the Heisenberg group over $\mathbb{F}_p$, hence of exponent $p$. Consequently $(G')^p \leq \psi^{-1}(\gamma_3(G) \times \mathcal{P} \times G(3)) = \gamma_3(\text{Stab}_G(1))$. □

Now that we have established the value of $|G : G''|$, it remains derive our main results.

**Proof of Theorem 1.2.** Assume that the given equation holds true for some $n \in \mathbb{N}$. Then we find

$$\psi(G^{(n+1)}) = \psi(G^{(n)})' = (G^{(n-1)} \times \mathcal{P} \times G^{(n-1)})' = G^{(n)} \times \mathcal{P} \times G^{(n)},$$

since $G^{(n)} \leq \text{Stab}_G(1)$. Thus by induction it is enough to consider the case $n = 3$, or the case $n = 2$, respectively.

First assume that $\text{con}(\mathbf{e}') + \text{sym}(\mathbf{e}'') - \text{sym}(\mathbf{e}) = 0$. By Theorem 2.10 we find $\psi(\text{Stab}_G(1)') = G' \times \mathcal{P} \times G'$, and by Proposition 3.1 $\log_p |G : G''| = p + 1$. By Lemma 2.13(iii), we also have $\log_p |G : \text{Stab}_G(1)'| = p + 1$, and since $G'' \leq \text{Stab}_G(1)'$, the subgroups $G''$ and $\text{Stab}(1)' = \psi^{-1}(G' \times \mathcal{P} \times G')$ coincide. Hence the equation holds for $n = 2$.

Now we drop the assumption on the defining tuple, and prove the desired equation for $n = 3$. Since $G''$ is normally generated by the elements $\{[c, \mathbf{e}^g] \mid g \in G\}$, we have to prove that $(0 : [c, \mathbf{e}^g], \circ : \text{id}) \in \psi(G^{(3)})$ for any $g \in G$, then an application of Proposition 2.1 concludes the proof.

Let $g \in G$ be arbitrary. Since $G$ is fractal, we may find $\widehat{g} \in \text{Stab}(1)$ such that $\widehat{g}|_0 = g$. Furthermore, we know by Corollary 3.2 that we find

$$h = (0 : c, 1 : c^{-2}, 2 : c, \circ : \text{id}) \in \psi(G'').$$

Thus

$$[h, h\widehat{g}^{p^{-2}}] = (\circ : [h|_o, h\widehat{g}|_o+2]) = (0 : [c, \mathbf{e}^g], \circ : \text{id}) \in \psi(G^{(3)}).$$

**Proof of Theorem 1.1.** Using Theorem 1.2, Proposition 3.1 and Theorem 2.10, we obtain

$$\log_p |G'' : G^{(3)}| = \log_p |G' \times \mathcal{P} \times G' : G''| - \log_p |G' \times \mathcal{P} \times G' : \psi(G'')| = \log_p (|G' : G''|) - \text{con}(\mathbf{e}') + \text{sym}(\mathbf{e}'') = (p - 1)(p + \text{con}(\mathbf{e}') + \text{sym}(\mathbf{e}'')) - p \text{sym}(\mathbf{e})$.}
Using Theorem 1.2 yet again, we find for $n > 2$
\[
\log_p |G^{(n-1)} : G^{(n)}| = \log_p |G^{(n-2)} \times P \times G^{(n-2)} : G^{(n-1)} \times P \times G^{(n-1)}| = p \log_p |G^{(n-2)} : G^{(n-1)}|,
\]
and consequently
\[
\log_p |G'' : G^{(n)}| = \sum_{i=2}^{n-1} \log_p |G^{(i)} : G^{(i+1)}| = \frac{(p^{n-2} - 1)}{(p-1)} \cdot \log_p |G'' : G^{(3)}| = \frac{(p^{n-2} - 1)}{(p-1)} (p + \text{con}(e') + \text{sym}(e'')) - (p^{n-1} - p)/(p-1) \cdot \text{sym}(e),
\]
hence by Proposition 3.1
\[
\log_p |G : G^{(n)}| = p^{n-2}(p + \text{con}(e') + \text{sym}(e'')) - (p^{n-1} - 1)/(p-1) \cdot \text{sym}(e) + 1. \quad \square
\]

**Corollary 3.4.** Let $G$ be a GGS-group defined by a non-constant vector. Then the series of iterated local laws $(L_n(G))_{n \in \mathbb{N}}$ coincides with the derived series $(G^{(n)})_{n \in \mathbb{N}}$.

**Proof.** Let $G$ be a GGS-group. We have to show $G^{(n)} = L_n(G)$ for all $n \in \mathbb{N}$. It is enough to show that all $p$th powers in $G^{(n)}$ are contained in $G^{(n+1)}$ for all $n \in \mathbb{N}$; for in this case all words involving a $p$th power give rise to verbal subgroups that are contained in the $(n+1)$st derived subgroup.

By Lemma 2.13(iv) and Lemma 3.3 this holds for $n \in \{1, 2\}$. Hence we assume that $n > 2$. Then, by Theorem 1.2, the group $\psi(G^{(n)})$ is contained in $G^{(n-1)} \times P \times G^{(n-1)}$.

Using induction, we see that
\[
\psi(G^{(n)})^p = (G^{(n-1)} \times P \times G^{(n-1)})^p \leq (G^{(n-1)})^p \times P \times (G^{(n-1)})^p \leq (G^{(n)}) \times P \times (G^{(n)}).
\]

**References**

[1] Theofanis Alexoudas, Benjamin Klopsch, and Anitha Thillaisundaram, *Maximal subgroups of multi-edge spinal groups*, Groups, Geometry, and Dynamics 10 (2016), no. 2, 619–648. Cited on p. 1

[2] Laurent Bartholdi and Zoran Šunič, *On the word and period growth of some groups of tree automorphisms*, Communications in Algebra 29 (2001), no. 11, 4923–4964. Cited on p. 1

[3] E. Di Domenico, G. A. Fernández-Alcober, and N. Gavioli, *GGS-groups over primary trees: Branch structures*, Monatshefte für Mathematik (2022). Cited on p. 5

[4] Anna Erschler, *Iterated identities and iterational depth of groups*, Journal of Modern Dynamics 9 (2015), no. 01, 257–284. Cited on p. 5

[5] Jacek Fabrykowski and Narain Gupta, *On groups with sub-exponential growth functions*, The Journal of the Indian Mathematical Society. New Series 49 (1985), no. 3-4, 249–256. Cited on p. 1

[6] Gustavo Fernández-Alcober and Amaia Zugadi-Reizabal, *GGS-groups: Order of congruence quotients and Hausdorff dimension*, Transactions of the American Mathematical Society 366 (2013), no. 4, 1993–2017. Cited on p. 1, 2, 4, 7, 10, 14

[7] Gustavo A. Fernández-Alcober, Alejandra Garrido, and Jone Uria-Albizuri, *On the congruence subgroup property for GGS-groups*, Proceedings of the American Mathematical Society 145 (2017), no. 8, 3311–3322. Cited on p. 1, 2

[8] Narain Gupta and Said Sidki, *On the Burnside problem for periodic groups*, Mathematische Zeitschrift 182 (1983), no. 3, 385–388. Cited on p. 1
[9] A. W. Ingleton, *The Rank of Circulant Matrices*, Journal of the London Mathematical Society 31 (1956), no. 4, 445–460. Cited on p. 7

[10] L. Kronecker, *Vorlesungen über Zahlentheorie*, Vorlesungen über allgemeine Arithmetik, vol. 1, B. G. Teubner, Leipzig, 1901. Cited on p. 7

[11] Jan Moritz Petschick, *On conjugacy of GGS-groups*, Journal of Group Theory 22 (2019), no. 3, 347–358. Cited on p. 1, 9, 10

[12] , *Two periodicity conditions for spinal groups*, December 2021. Cited on p. 1

[13] Zoran Šunić, *Hausdorff dimension in a family of self-similar groups*, Geometriae Dedicata 124 (2007), no. 1, 213–236. Cited on p. 10

[14] Ana Cristina Vieira, *On the lower central series and the derived series of the Gupta-Sidki 3-group*, Communications in Algebra 26 (1998), no. 4, 1319–1333. Cited on p. 1

[15] Taras Vovkivsky, *Infinite torsion groups arising as generalizations of the second Grigorchuk group*, Algebra (Moscow), de Gruyter, Berlin, 2000, pp. 357–377. Cited on p. 1

Jan Moritz Petschick: Mathematisches Institut, Heinrich-Heine-Universität, 40225 Düsseldorf, Germany

Email address: jan.petschick@hhu.de