International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 13 No. 3 (2024), pp. 307-318.

http://ijgt.ui.ac.ir

www.ui.ac.ir

ENUMERATING WORD MAPS IN FINITE GROUPS

BOGDAN S. CHLEBUS, WILLIAM COCKE* AND MENG-CHE "TURBO" HO

Abstract. We consider word maps over finite groups. An n-variable word w is an element of the free group on n-symbols. For any group G, a word w induces a map from $G^n \mapsto G$ where $(g_1, \ldots, g_n) \mapsto w(g_1, \ldots, g_n)$. We observe that many groups have word maps that decompose into components. Such a decomposition facilitates a recursive approach to studying word maps. Building on this observation, and combining it with relevant properties of the word maps, allows us to develop an algorithm to calculate representatives of all the word maps over a finite group. Given these representatives, we can calculate word maps with specific properties over a given group, or show that such maps do not exist. In particular, we have computed an explicit a word on A_5 such that only generating tuples are nontrivial in its image.

We also discuss how our algorithm could be used to computationally address many open questions about word maps. Promising directions of potential applications include Amit's conjecture, questions of chirality and rationality, and the search for multilinear maps over a group. We conclude with open questions regarding these problems.

1. Introduction

This paper discusses the challenge of enumerating the word maps of a finite group. Explicit enumerations can be used to computationally explore a variety of different questions about word maps over finite groups. We comment on many of these questions in Section 4.

Keywords: Word maps, Relatively free groups, Algorithms on groups, Amit–Ashurst conjecture.

MSC(2020): Primary: 20E10; Secondary: 20F10.

Communicated by Patrizia Longobardi.

Article Type: 2022 CCGTA IN SOUTH FLA.

*Corresponding author.

Received: 01 March 2023, Accepted: 18 November 2023.

Cite this article: B. S. Chlebus, W. Cocke and M.-C. "Turbo" Ho, Enumerating Word Maps in Finite Groups, Int. J. Group Theory, **13** no. 3 (2024) 307–318. http://dx.doi.org/10.22108/ijgt.2023.136972.1833 .

A *word* is an element of the free group $\mathbf{F}_n$ on n symbols. On a group G, the word $w \in \mathbf{F}_n$ induces a map $w : G^n \to G$ by $(g_1, \ldots, g_n) \mapsto w(g_1, \ldots, g_n)$. Such maps are called *word maps*. We write $w(G)$ for the image of the word map induced by w on the group G. For example, if G is the group S_3, i.e., the symmetric group on 3 symbols, and w is the word x^2, then $w(G)$ is the set of all squares in S_3, i.e, the identity and the two 3-cycles.

Many structural properties of a group G can be determined by the behavior of specific word maps over G. A word w is a *law* on G if for all $g_1, \ldots, g_n \in G$ we have $w(g_1, \ldots, g_n) = 1$, or equivalently $w(G) = \{1\}$. For example, the word $w = [x, y] = x^{-1}y^{-1}xy$ is a law on G if and only if the group G is abelian. For the same word $w = [x, y]$, the statement that $w(G) = G$ for each finite non-abelian simple group G is known as the Ore conjecture; it was recently proven [17]. Similarly, there is a word w such that a finite group G is solvable if and only if $w(G) = 1$ [25].

The set $K_n(G)$ of n-variable laws of a group G forms a characteristic subgroup of $\mathbf{F}_n$. Two words give the same map if they are in the same coset of $K_n(G)$. We write $\mathbf{F}_n(G)$ for the quotient $\mathbf{F}_n/K_n(G)$. The group $\mathbf{F}_n(G)$ is the relatively free group of rank n in the variety generated by G as defined by Neumann [20]. Elements of $\mathbf{F}_n(G)$ correspond to the word maps $w : G^n \to G$, in the sense that the group $\mathbf{F}_n(G)$ is isomorphic to the group of n-variable word maps over G. We present an algorithm to enumerate the cosets of $K_n(G)$ in $\mathbf{F}_n$.

Throughout the paper, we always implicitly fix a transversal of $K_n(G)$ in $\mathbf{F}_n$ that consists of words, and identify the word with the induced word map as well as the corresponding element of $\mathbf{F}_n(G)$. We will further assume the words corresponding to *commutator word maps*, i.e., elements of $\mathbf{F}_n(G)'$, are commutator words.

For a group G, the sequence

$$(|\mathbf{F}_1(G)|, |\mathbf{F}_2(G)|, |\mathbf{F}_3(G)|, \ldots, |\mathbf{F}_n(G)|, \ldots)$$

is called the *free spectrum of* G. Free spectra of groups has been the subject of studies by various authors [9, 22]. Nevertheless, there are few groups G for which the free spectrum of G is known. For example, Kovács [15] determined the free spectrum of all dihedral groups. Recently, Cocke and Skabelund [7] calculated the free spectrum of A_5.

This paper is organized as follows. Section 2 includes some preliminary results and observations. In Section 3, we give an algorithm to enumerate all of the n-variable word maps over a finite group. In particular, Section 3.1 includes an example describing how to enumerate all of the 2-variable word maps over S_3. Finally, in Section 4, we present a few open questions related to word maps as potential applications of our algorithm.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

2. Preliminaries

This section contains some observations about word maps that we will use in our algorithm in Section 3.

We will use a decomposition of words into powers and commutators. Specifically, by collecting powers [19], a word w in $\mathbf{F}_n$ can be written as $x_1^{i_1}, \ldots, x_n^{i_n} c$ for some $c \in \mathbf{F}'_n$. We will write $e(G)$ for the exponent of G.

Lemma 2.1. *The word $w = x_1^{i_1}, \ldots, x_n^{i_n} c$, where $c \in \boldsymbol{F}'_n$, is a law on a group G if and only if $e(G) \mid i_j$ for all j and c is a law on G.*

Proof. The "if" direction is clear. Suppose w is a law. Since $c(1, 1, \ldots, 1, x, 1, \ldots, 1) = 1$ for every x, we have that $w(1, 1, \ldots, 1, x, 1, \ldots, 1) = x^{i_{j_0}} = 1$ for every x as a map from $G^n \to G$. Hence we obtain that $e(G) \mid i_{j_0}$. This applies to every index $j = j_0$, so $x_1^{i_1}, \ldots, x_n^{i_n}$ takes on 1 for any assignment of values to the symbols $x_1, \ldots, x_n$, and c must be a law. □

By Lemma 2.1, the problem of enumerating laws on a finite group G is reduced to enumerating commutator word maps over G that are laws on G. Therefore the problem of enumerating the word maps over G can be reduced to enumerating the commutator word maps over G.

We can represent a function $f : G^n \to G$ as the set of tuples $\{(g_1, \ldots, g_n, f(g_1, \ldots, g_n)) : g_i \in G\}$.

Lemma 2.2. *If $\phi : \langle g_1, \ldots, g_n \rangle \to H$ is a homomorphism, then $\phi(w(g_1, \ldots, g_n)) = w(\phi(g_1), \ldots, \phi(g_n))$.*

For a word map w, we do not need all of the $|G|^n$ tuples to define w. Specifically, by Lemma 2.2, we can restrict our attention to orbit representatives of the diagonal action of $\mathbf{End}(G)$ on G^n. We can actually refine via a slightly stronger criterion, which is given next as Lemma 2.4.

Definition 2.3. *We will call a set X of elements of G^n a **noncommutative covering of** G^n if for every tuple $(g_1, \ldots, g_n)$ in G^n such that $\langle g_1, \ldots, g_n \rangle$ is nonabelian there are some homomorphism $\phi : G \to G$ and $(x_1, \ldots, x_n) \in X$ satisfying $(\phi(x_1), \ldots, \phi(x_n)) = (g_1, \ldots, g_n)$. If no proper subset of a noncommutative covering X is a noncommutative covering itself, then X is a **minimal noncommutative covering**.*

Lemma 2.4. *Let G be a finite group and let X be a noncommutative covering of G^n. For any word map w in $\boldsymbol{F}_n(G)'$, the word map w is uniquely determined by its values on X.*

Proof. For any $(g_1, \ldots, g_n) \in G^n$ such that $\langle g_1, \ldots, g_n \rangle$ is abelian, we have that $w(g_1, \ldots, g_n) = 1$. If $(g_1, \ldots, g_n) \in G^n$ and $\langle g_1, \ldots, g_n \rangle$ is not abelian, then there is some $(x_1, \ldots, x_n) \in X$ and a homomorphism $\phi : G \to G$ such that $(\phi(x_1), \ldots, \phi(x_n)) = (g_1, \ldots, g_n)$. Then $w(g_1, \ldots, g_n) = \phi(w(x_1, \ldots, x_n))$, by Lemma 2.2. □

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

Computing a covering of G^n is in general nontrivial.

Definition 2.5. *Let G be a group and let X be a noncommutative covering of G^n. A set $W \subseteq \boldsymbol{F}_n(G)'$ **isolates** an element $x = (g_1, \ldots, g_n) \in X$ if the following two criteria hold:*

(1) *For all $w \in W$ and $z \in X \setminus \{x\}$ we have that $w(z) = 1$.*
(2) *$\langle w(x) : w \in W\rangle = \langle g_1, \ldots, g_n\rangle'$.*

Isolation is a useful concept for computations involving relatively free groups. Lemma 2.7 shows explicitly how to use isolation. To state it, we define what we mean by associating commutator word maps with a set of n-tuples of G by restricting their domains.

Definition 2.6. *Given a set $X \subseteq G^n$, **the set of commutator word maps over** X is the set of all word maps $w \in \boldsymbol{F}_n(G)'$ with domains restricted to X. Note that this is a homomorphic image of $\boldsymbol{F}_n(G)'$.*

Lemma 2.7. *Let G be a group, X a noncommutative covering of G^n, and $x = (g_1, \ldots, g_n) \in X$. If there is a set $W \subseteq \boldsymbol{F}_n(G)'$ of commutator word maps that isolates x, then $\boldsymbol{F}_n(G)' \cong \langle g_1, \ldots, g_n\rangle' \times H$ where H is the set of commutator word maps over $X \setminus \{x\}$.*

Proof. Suppose that a set $W \subseteq \mathbf{F}_n(G)'$ of commutator word maps isolates $x \in X$. Consider a commutator word $c \in \mathbf{F}_n(G)'$. It follows that $c(x) \in \langle g_1, \ldots, g_n\rangle'$. There is some $w \in \langle W\rangle$ such that $w(x) = c(x)$. Such an element $w \in \langle W\rangle$ is unique since, as an element of $\mathbf{F}_n(G)'$, w is determined by its value on X by Lemma 2.4. We have $w(x) = c(x)$ and $w(x) = 1$ for every $z \in X \setminus \{x\}$. Writing $h = w^{-1}c$, we obtain $c = wh$. Observe that $h(x) = 1$ and $w(z) = 1$ for $z \in X \setminus \{x\}$, so w commutes with h. This process defines a map $c \mapsto (c(x), h \mid_{X\setminus\{x\}})$ from $\mathbf{F}_n(G)'$ to $\langle g_1, \ldots, g_n\rangle' \times H$.

The image determines the value of c on x and $X \setminus \{x\}$, so the map is injective. It is also surjective as every element of $\langle g_1, \ldots, g_n\rangle'$ is in the image by condition (2) of Definition 2.6 and every element of H is realized by some word map w which is mapped to $(w(x), w \mid_{X\setminus\{x\}})$. Finally, the map is a homomorphism, since if $c = wh$ and $c' = w'h'$, then we have $cc' = whw'h' = (ww')(hh')$ so cc' is mapped to $((cc')(x), (hh') \mid_{X\setminus\{x\}}) = ((c)(x), (h) \mid_{X\setminus\{x\}}) \cdot ((c')(x), (h') \mid_{X\setminus\{x\}})$. □

By (the proof) of a theorem by Lubotzky [18], in a finite simple group, any generating tuple in a noncommutative covering is isolated by some set of commutator word maps. It has been shown that for the holomorphs of groups of prime order, there are noncommutative covering sets of $\mathbf{F}_2(G)'$ where every element is isolated [5]. This means that $\mathbf{F}_2(G)'$ is a direct product of copies of C_{p-1}.

In many cases, we cannot isolate every element of a noncommutative covering set. It appears however that many noncommutative covering sets decompose nicely. We formalize this observation by generalizing the definition of isolation as follows.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

Definition 2.8. *Let G be a group and let X be a noncommutative covering of G^n. Given a subset Y of X, we say that a set of commutator word maps W **separates** Y in X if the following hold:*

(1) *For all $w \in W$ and $z \in X \setminus Y$ we have that $w(z) = 1$.*
(2) *$\langle W \rangle$ is the group of all commutator word maps over Y.*

Note that if $Y = \{y\}$, then W separating Y in X is equivalent to W isolating y in X. The argument of Lemma 2.7 also generalizes to the following fact:

Lemma 2.9. *Let G be a group and let X be a noncommutative covering of a group G^n. If there is a set $W \subseteq \boldsymbol{F}_n(G)'$ of commutator word maps that separates $Y \subseteq X$, then $\boldsymbol{F}_n(G)' \cong H_1 \times H_2$ where H_1 (respectively, H_2) is the set of commutator word maps over Y (respectively, $X \setminus Y$).*

After we split X into Y and $X \setminus Y$, we can further split Y and $X \setminus Y$ into smaller subsets if a proper subset is separated. This observation is the key idea behind Algorithm 1 in the next section. For this further splitting, we need the following generalization of Lemma 2.9, with a similar proof.

Lemma 2.10. *Let G be a group, $X \subseteq X' \subseteq G^n$ where X' is a noncommutative covering of G^n, and $C \subseteq \boldsymbol{F}_n(G)'$ is a subgroup that separates X in X'. If there are a set $W \subseteq C$ of commutator word maps and $Y \subseteq X$ such that W separates Y in X', then $C \cong H_1 \times H_2$ where H_1 is the set of commutator word maps over Y and H_2 is the set of commutator word maps over $X \setminus Y$.*

3. An algorithm to calculate the commutator word maps

We first present an example before stating the general algorithm.

3.1. **Example: counting 2-variable word maps over S_3.** As noted in Section 2, this is equivalent to enumerating all of the 2-variable commutator word maps over S_3. Since commutator maps are defined by their values on non-commuting tuples, we can restrict to non-commuting 2-tuples from S_3. A minimal noncommutative covering of $(S_3)^2$ is given by

$$X = \{((1,2,3),(1,2)),((1,2),(1,2,3)),((1,2),(2,3))\}.$$

Commutator words can only map $S_3 \times S_3 \to S_3' \cong C_3$. Since a word map is determined by its value on X and $|X| = |C_3| = 3$, there are at most $3^3 = 27$ commutator word maps on 2 variables over S_3. The word maps $[x^2, y]$, $[x, y^2]$, and $[x^3, y^3]$ each isolate a unique element of X. We see that any 2-variable word map on S_3 can be uniquely expressed in the form

$$x^i y^j [x, y^2]^a [x^2, y]^b [x^3, y^3]^c$$

where $i, j \in \{0, \ldots, 5\}$ and $a, b, c \in \{0, 1, 2\}$. Hence there are 27 word maps over X, and we conclude that $|\mathbf{F}_2'(S_3)| = 27$. Thus $|\mathbf{F}_2(S_3)| = 6^2 \cdot 27 = 972$.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

3.2. **The algorithm.** The motivation of our algorithm is to essentially walk the Cayley graph of commutator word maps $\mathbf{F}_n(G)'$ over G. These maps have images in G', and given a noncommutative covering X of G^n, can be thought of as maps from $X \to G'$. In practice, the graph can be quite large, making the naive approach of simply constructing all such maps infeasible due to time and computational resource limits. Nevertheless, it is often the case that the group of commutator word maps decomposes nicely into direct products of commutator word maps over smaller sets. Identifying the existence of word maps that separate subsets of the noncommutative covering of G^n reduces the size of the computation drastically.

Hence we need a function which checks whether or not a subset V of a set $W \subseteq \mathbf{F}_n(G)'$ of commutator word maps separates a subset Y of a noncommutative covering X of G. For the function `separates(X,Y,V,B)` to compute if a set of words V separates Y from X, we need to check that V vanishes on $X \setminus Y$ and that every commutator word map is replicated over Y. To do this, we consider the following generating set of $\mathbf{F}'_n$ and check that for every basis word b, there is a word in $\langle V \rangle$ that is equal to b on Y.

We describe how to calculate a free basis for $\mathbf{F}'_n$ and reduce to a generating set of $\mathbf{F}_n(G)'$ by examining when two maps are equal over X. We first reduce the powers modulo the exponent $e(G)$. We note that when $n = 2$ there is a well-known basis for $\mathbf{F}_2(G)'$: $\{[x^i, y^j] : i, j \leq e(G)\}$. In general, we can use the following basis, or a variation thereof:

$$\{x_1^{i_1} \cdots x_n^{i_n} x_j x_1^{-i_1} \cdots x_j^{-i_j-1} \cdots x_n^{-i_n} : i_k \leq e(G)\}.$$

We then detect and remove any repetition of these sets as word maps. Note that the resulting set B is a generating set of $\mathbf{F}_n(G)'$ which may not be free.

The function below is not meant to represent code in any language, but to be a convenient pseudocode.

Our main algorithm will consist of generating balls of the Cayley graph of $\mathbf{F}_n(G)'$ with respect to the generating set B. Here we use $W * B$ to denote the set of word maps in W that are concatenated with the elements of B. Note that both W and $W * B$ are stored as maps, i.e., maps from $G^n \to G$ are stored as $n + 1$ tuples with elemenets form G. Since there are only finitely many possibilities, eventually we will have $W = W * B$.

We will need the following function in our main algorithm.

Then our algorithm can be summarized as:

Algorithm 1. *To enumerate the word maps over a group G first calculate a noncommutative covering X for the set G^n and a generating set B for $\boldsymbol{F}_n(G)'$. Then*

This algorithm returns a list of direct summands of $\mathbf{F}_n(G)'$, where each element is given as a map from a subset Y of X to G'. One can then use these to reconstruct $\mathbf{F}_n(G)$ as described in Section 2.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

3.3. **Remarks on the Algorithm.** For some groups G, it may be feasible to execute Algorithm 1 by hand. To streamline computations, the choice of when to separate a set could be done using either theoretical bounds or other information about the group in question.

For example, over a finite simple group, the tuples in a noncommutative covering that generate the group naturally separate from the tuples in the noncommutative covering that do not. Using this fact, we were able to enumerate enough word maps over A_5 to compute the word

$$w(x,y) = [[x^2, y^2], [xy, yx]][[x, y], [xy^2, yx^2]].$$

Over A_5 we have that $w(a,b) \neq 1$ if and only if $\langle a, b\rangle = A_5$. Such words were shown to exist by Lubotzky [18], but no examples were known.

Next, we discuss the performance bounds. The algorithm traverses the Cayley graph of the commutators over the noncommutative covering. Assuming the functions of conducting group multiplications and comparing maps are constant, simply traversing the graph will take $O\left(|B| \cdot |\mathbf{F}_n(G)'|\right)$ time, where B is the generating set of $\mathbf{F}_n(G)'$, while the amount of space required is $O\left(|X| \cdot |\mathbf{F}_n(G)'|\right)$. However, the splitting of the noncommutative covering X significantly speeds up the algorithm and reduces storage requirements. Returning to the example of $\mathbf{F}_2(S_3)'$, using the noncommutative covering in Example 3.1, we only need to store $3 + 3 + 3$ word maps. Moreover, once subsets split in the noncommutative covering, we can distribute the computation further reducing requirements.

There is an interesting phenomenon here which we describe heuristically: if the noncommutative covering has a high degree of splitting, then $\mathbf{F}_n(G)'$ is a product among the independent components, making our algorithm computationally less expensive. An extreme family of examples in this case are the finite simple groups wherein every tuple, which generates the whole group, in a noncommutative covering is isolated in the covering. If the noncommutative covering does not split, then $\mathbf{F}_n(G)'$ is more complex since there are interdependencies among the elements of the noncommutative covering meaning our algorithm for enumerating $\mathbf{F}_n(G)'$ is computationally more expensive.

4. Applications and Connections to Other Topics

In this section, we give some problems for which our algorithm may be able to provide examples or counterexamples to help further investigations.

4.1. **Amit's Conjecture.** Sometime in the early 2000's, Alon Amit made a conjecture about how word maps behave on finite nilpotent groups. This conjecture was quoted in several places, Abert [1] in 2006, Nikolov and Segal [21] in 2007, and later by Ashurst [2] and Levy [16]. As of 2023, Amit's work containing the conjecture has not been published. The conjecture, known as Amit's Conjecture, is the following:

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

Question 4.1 (Amit's Conjecture)**.** *Given an n-variable word map w over a finite nilpotent group G, the number of n-tuples mapping to 1 is at least $|G|^{n-1}$.*

The Amit conjecture itself has been shown to hold for some families of different groups. For example, both Levy [16], and Iñiguez and Sangroniz [10] showed that the Amit conjecture holds for groups of nilpotency class two by using commutator calculus and character theory, respectively. There is also a solvable analog of Amit conjecture, which has been proven, that says a group is solvable if and only if there is some constant $c = c(G)$ such that for every natural number n and n-variable word map w, the number of n-tuples mapping to 1 by w is at least $c|G|^{n-1}$ [1, 21].

As part of the history of Amit's conjecture, we mention a generalization of Amit's Conjecture, which appeared in peer-review form as the "generalized Amit conjecture" in [4]. This generalization also appeared in Ashurst's thesis [2]. In her thesis, Ashurst showed that the Amit conjecture and the generalization hold for the nilpotent dihedral groups and nilpotent generalized quaternion groups. For this reason, Camina, Cocke, and Thillaisundaram [3] have chosen to call it the Amit–Ashurst Conjecture; extending Ashurst's work they showed that the Amit–Ashurst Conjecture holds for all p-groups with a cyclic maximal subgroup.

Question 4.2 (The Amit–Ashurst Conjecture)**.** *Given an n-variable word map w over a finite nilpotent group G and an element $g \in w(G)$, the number of n-tuples mapping to g is at least $|G|^{n-1}$.*

In [3, Theorem A], it is shown that the Amit–Ashurst Conjecture holds for p-groups with a cyclic maximal subgroup. Work by Kishnani and Kulshrestha [14] shows that in certain other classes, e.g., extra special groups, the Amit–Ashurst conjecture also holds.

One could use Algorithm 1 to enumerate word maps of a nilpotent group G and test the Amit or Amit–Ashurst conjectures for G. In fact, given the nilpotency class of G and the exponents of the factors in the lower central series of G, one may replace the free basis with a Mal'cev basis of the relatively free group of G. However, enumerating the n-variable word maps over a group G is not enough to prove that the Amit–Ashurst conjecture holds for the group G. This leads to the following question, which is also of some interest:

Question 4.3. *Is there a recursive function $f = f(G)$ such that the truth of the Amit–Ashurst conjecture for G depends only on knowing the truthfulness of the Amit–Ashurst conjecture for word maps on $f(G)$ variables?*

One could further ask if such a function exists which takes as input the nilpotency, number of generators, or other group theoretic invariants of G.

4.2. **Images of word maps, chirality, and rationality.** The question of chirality is motivated by the definition of symmetrized w-values in G where $G_w = \{w(g_1, \ldots, g_n)^{\pm 1} : g_1, \ldots, g_n \in G\}$ in Dan

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

Segal's *Words* [23]. The question of whether the ± 1 in the exponent is necessary led to the following definition of chirality [6].

Definition 4.4. *A pair consisting of a group G and a word w is called* ***chiral*** *if $w(G)$ is not closed under inverses. The group G is called chiral if it is chiral for some word w and* ***achiral*** *if it is not chiral.*

It is straightforward to see that abelian groups are achiral. In [6] families of chiral groups are given. In contrast, Singh and Reddy [24] show that many families of words are achiral.

Definition 4.5. *A pair consisting of a group G and a word w is called* ***rational*** *if the number of tuples evaluating to g and h are equal whenever $\langle g \rangle = \langle h \rangle$.*

Chirality is a generalization of ratonality, because if a pair is rational, then it is chiral. Many authors have investigated rational words in various settings, see for example [8]. In particular, Camina, Iniguez and Thillaisundaram [4] showed that every finite nilpotent group of class 2 is rational. Kaur, Kishnani, and Kulshrestha [13] also explore the images of word maps in finite nilpotent groups.

Many questions about word maps over a specific group can be answered using our algorithm. For example, as noted in [6], enumerating all word maps over two variables is sufficient to determine if a group is chiral. However, an algorithm to identify subsets of a group that occur as word maps would be very interesting. There are only a finite number of subsets of a finite group, and determining if a subset is the image of a word map is recursively enumerable; it is unclear if it is recursive. The below question has been informally discussed in many settings:

Question 4.6 (The Big Question)**.** *Is there a decision procedure that takes as input a finite group and a subset thereof and returns whether or not the subset occurs as the image of a word map?*

Question 4.6 could be restricted to relatively free groups:

Question 4.7. *Is there a decision procedure that takes as input a finite relatively free group and a subset thereof and returns whether or not the subset occurs as the image of a word map?*

Lemma 4.8. *The Question 4.7 is equivalent to Question 4.6.*

Proof. Given a finite group G that is n-generated, we can construct $\mathbf{F}_n(G)$. Every image of a word map in G is the quotient of an image of a word map in $\mathbf{F}_n(G)$ by one of the maps $\mathbf{F}_n(G) \to G$. If we can enumerate all such images in $\mathbf{F}_n(G)$, then we can enumerate all such images in G. □

The proof of Lemma 4.6 shows the stronger statement: If G is a quotient of H, then every image of a word map over G is the quotient of an image of a word map over H. Thus, the problem of enumerating images of word maps over G can be reduced to the problem of enumerating word maps over H.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

4.3. **Multilinear word maps.** Recent work by Kahrobaei, Tortora, and Tota [11, 12] investigate cryptographic protocols arising from multilinear maps over groups.

Definition 4.9. *A map f from $G^n \to G$ is **multilinear** if for all $a_1, \ldots, a_n \in \mathbb{Z}$ we have $f(g_1^{a_1}, \ldots, g_n^{a_n}) = f(g_1, \ldots, g_n)^{a_1,\ldots,a_n}$, i.e., the powers factor through the function.*

Kahrobaei, Tortora, and Tota note that the n-fold commutator word defined by the recursive rules $[x_1, x_2] = x_1^{-1}x_2^{-1}x_1x_2$ and $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$ is a multilinear word map on nilpotent groups of class n. This raises the question of what other word maps are multilinear.

Using our enumeration algorithm we rediscovered the following: the Burnside groups $B(3, n)$ (exponent 3 and n-generated) have the property that $[x, y]$ is multilinear as a two-variable map and $[x, y, z]$ is multilinear as a three-variable map. Our observation is actually equivalent to the fact that every two-generated subgroup of the Burnside group $B(3, n)$ has nilpotency class 2, while the group itself has nilpotency class 3. Groups with a family of multilinear maps could be used to establish protocols for multiple participants at once.

We have the following lemma about multilinear maps over G.

Lemma 4.10. *If G is a group and w is a multilinear map on G, then either w is a commutator map or w is a single variable map.*

Proof. Suppose that w is not a map on a single variable map. Write

$$w(x_1, \ldots, x_n) = x_1^{k_1} \cdots x_n^{k_2} c(x_1, \ldots, x_n).$$

Then we note that for any i,

$$x^{i \cdot k_1} = w(x, 1, \ldots, 1)^i = w(x, 1^i, \ldots, 1) = x^{k_1},$$

which implies $(i-1)(k_1) \equiv 0 \pmod{\mathbf{exp}(G)}$. Hence $k_1 \equiv 0 \pmod{\mathbf{exp}(G)}$. By symmetry $k_i \equiv 0 \pmod{\mathbf{exp}(G)}$ for all i and we conclude that w is a commutator map. □

Currently, the best-known examples of multilinear maps are $(n+1)$-fold commutators since the maps $[x_0, x_1, \ldots, x_n]$ are multilinear in nilpotent groups of step n.

Question 4.11. *What groups have multilinear word maps from G^k to G for $k \geq 2$ and what are these word maps?*

Acknowledgements

The third author acknowledges support from the National Science Foundation under Grant No. DMS-2054558.

The views expressed in this presentation are those of the authors and do not represent the views of the United States Government, the Department of Defense, or ARCYBER.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

References

[1] M. Abért, On the probability of satisfying a word in a group, *J. Group Theory*, **9** no. 5 (2006) 685–694.

[2] C. Ashurst, *Fibres of words in finite groups, a probabilistic approach*, University of Bath, 2012.

[3] R. D. Camina, W. L. Cocke and A. Thillaisundaram, The Amit-Ashurst conjecture for finite metacyclic p-groups, *Eur. J. Math.*, **9** no. 3 (2023) 13 pp.

[4] R. D. Camina, A. Iniguez and A. Thillaisundaram, Word problems for finite nilpotent groups, *Arch. Math. (Basel)*, **115** (2020) no. 6 599–609.

[5] W. Cocke, Size of free groups in varieties generated by fnite groups, *Internat. J. Algebra Comput.*, **29** (2019) no. 8 1419–1430.

[6] W. Cocke and M.-Ch. Ho, On the symmetry of images of word maps in groups, *Comm. Algebra*, **46** (2018) no. 2 756–763.

[7] W. Cocke and D. Skabelund, The free spectrum of A_5, *Internat. J. Algebra Comput.*, **30** (2020) no. 4 685–691.

[8] R. Guralnick and P. Shumyatsky, On rational and concise words, *J. Algebra*, **429** (2015) 213–217.

[9] G. Higman, *The orders of relatively free groups*, Proc. Internat. Conf. Theory of Groups (Canberra, 1965), Gordon and Breach, New York-London-Paris, 1967 153–165.

[10] A. Iñiguez and J. Sangroniz, Words and characters in finite p-groups, *J. Algebra*, **485** (2017) 230–246.

[11] D. Kahrobaei, A. Tortora and M. Tota, *Multilinear cryptography using nilpotent groups*, Elementary theory of groups and group rings, and related topics, De Gruyter Proc. Math., De Gruyter, Berlin, 2020 127–133.

[12] ———, A closer look at the multilinear cryptography using nilpotent groups, *Int. J. Comput. Math. Comput. Syst. Theory*, **7** (2022) no. 1 63–67.

[13] D. Kaur, H. Kishnani and A. Kulshrestha, Word images and their impostors in finite nilpotent groups, (2022) 14 pp. arXiv preprint arXiv:2205.15369.

[14] H. Kishnani and A. Kulshrestha, Automorphic word maps and amit–ashurst conjecture, (2023) 10 pp. arXiv preprint arXiv:2309.09010, 2023.

[15] L. G. Kovács, Free groups in a dihedral variety, *Proc. Roy. Irish Acad. Sect. A*, **89** (1989) no. 1 115–117.

[16] M. Levy, On the probability of satisfying a word in nilpotent groups of class 2, (2011). arXiv preprint arXiv:1101.4286.

[17] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, The Ore conjecture, *J. Eur. Math. Soc. (JEMS)*, **12** (2010) no. 4 939–1008.

[18] A. Lubotzky, Images of word maps in finite simple groups, *Glasg. Math. J.*, **56** (2014) no. 2 465–469.

[19] W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory*, Presentations of groups in terms of generators and relations, Second revised edition, Dover Publications, Inc., New York, 1976.

[20] H. Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967.

[21] N. Nikolov and D. Segal, A characterization of finite soluble groups, *Bull. Lond. Math. Soc.*, **39** (2007) no. 2 209–213.

[22] A. Ju. Olšanskiĭ, The orders of free groups of locally finite varieties, (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.*, **37** (1973) 89–94.

http://dx.doi.org/10.22108/ijgt.2023.136972.1833

[23] D. Segal, *Words: notes on verbal width in groups*, London Mathematical Society Lecture Note Series, **361**, Cambridge University Press, Cambridge, 2009.

[24] S. Singh and A. Satyanarayana Reddy, Achiral words, (2023). arXiv preprint arXiv:2302.02761.

[25] J. S. Wilson, Finite axiomatization of finite soluble groups, *J. London Math. Soc. (2)*, **74** (2006) no. 3 566–582.

Bogdan S. Chlebus

School of Computer and Cyber Sciences, Augusta University, Augusta, GA, USA

Email: bchlebus@augusta.edu

William Cocke

School of Computer and Cyber Sciences, Augusta University, Augusta, GA, USA

Email: wcocke@augusta.edu

Meng-Che "Turbo" Ho

Department of Mathematics, California State University, Northridge, Northridge, CA, USA

Email:mengche.ho@csun.edu

http://dx.doi.org/10.22108/ijgt.2023.136972.1833