THE PROBABILITY DISTRIBUTION OF WORD MAPS ON FINITE GROUPS

WILLIAM COCKE AND MENG-CHE "TURBO" HO

Abstract. Word maps provide a wealth of information about finite groups. We examine the connection between the probability distribution induced by a word map and the underlying structure of a finite group. We show that a finite group is nilpotent if and only if every surjective word map has fibers of uniform size. Moreover, we show that probability distributions themselves are sufficient to identify nilpotent groups, and these same distributions can be used to determine abelian groups up to isomorphism. In addition we answer a question of Amit and Vishne.

Keywords: Word maps; nilpotent groups

1. Introduction

A word \( w \) is an element of the free group \( \mathbb{F}_n = \mathbb{F}\langle x_1, \ldots, x_n \rangle \). The length of \( w \) is the number of variables and their inverses that appear in \( w \). For any group \( G \), the word \( w \) induces a map \( w : G^n \to G \). We write \( w \) for both the word \( w \) and the word map on \( G \), and write \( w(G) \) to mean the image \( w(G^n) \) of the word map. We will also write \( \mathbb{F} \) to mean the tuple \( (g_1, g_2, \ldots, g_n) \). If \( G \) is finite then the word map \( w \) induces a probability distribution on \( G \) where

\[
\mu_{G,w}(g) = \frac{|\{ \mathbb{F} \in G^n : w(\mathbb{F}) = g \}|}{|G|^n}.
\]

There has been some interest in examining the relationship between the probability distributions induced by word maps on \( G \) and the structure of the underlying finite group \( G \); for example, see Abért [Abe06]. Nikolov and Segal [NS07] show that a finite group is solvable if and only there is some \( \epsilon > 0 \) for which \( \mu_{G,w}(1) \geq \epsilon \) for all words \( w \). Since a finite group admits infinitely many word maps, results about all word maps are in general not computable. However, a finite group admits only finitely many word maps on a fixed number of variables, it is natural to ask what structural information about \( G \) can be observed from the collection of probability distributions induced by all \( n \)-variable word maps on \( G \).

We formalize the above approach as the following question:

**Question 1.** Fix \( n \in \mathbb{N} \), a finite group \( G \), and an enumeration of the elements of \( G \). Let \( g_i \) be the \( i \)-th element of \( G \). Consider the probability distribution of the word map \( w \) as a function \( f_w : |G| \to \mathbb{N} \) where \( f_w(i) = |w^{-1}(g_i)| \). Given the distributions of all \( n \)-variable word maps of \( G \) as a set, what information can be recovered about \( G \)?

In particular the actual distribution \( \mu_{G,w}(g) \) takes as input an element \( g \) of the group \( G \). The distribution \( f_w \) takes as input a natural number, which corresponds
to an unknown element \( g \) of an unknown group \( G \). To the reader uninterested in the semantics of our formalization, it suffices to say that we are interested in distributions that are disconnected from the underlying group. We then ask what information about the group remains.

In this article we show the following:

**Theorem A.** For all \( n \in \mathbb{N} \), we can identify when a finite group \( G \) is nilpotent from the set of distributions of all \( n \)-variable word maps on \( G \).

In particular, part of our proof of Theorem A relies on the following theorem, which is certainly of independent interest:

**Theorem B.** Let \( G \) be a finite group. Then \( G \) is nilpotent if and only if for every surjective word map \( w \), the distribution \( \mu_{G,w} \) is uniform.

The authors are not aware of any two finite groups that have the same set of probability distributions for all \( n \). In this direction we also show the following:

**Theorem C.** For \( n > 1 \), the set of distributions of all \( n \)-variable word maps on \( G \) can be used to identify whether \( G \) is abelian; moreover, if \( G \) is abelian, then the set of distributions identifies \( G \) up to isomorphism.

Before giving an outline of the paper, we give the example of all four probability distributions induced by two-variable word maps on the \( Q_8 \). Note that there are 32 two-variable word maps on \( Q_8 \), but they induce only 4 probability distributions. Moreover, out of the 32 two-variable word maps, there are only 5 automorphism classes of words on \( Q_8 \).

\[
\begin{align*}
(1, 1, 1, 1) \\
(1, 0, 0, 0, 0, 0, 0) \\
(\frac{5}{8}, \frac{3}{8}, 0, 0, 0, 0, 0) \\
(\frac{1}{8}, \frac{3}{8}, 0, 0, 0, 0, 0)
\end{align*}
\]

A theme of this paper is what type of information can be gained from the sequences of tuples. Note, we are not assuming that the individual elements in the ordering of \( G \) are known, nor that one can naturally associate a distribution to a word map, (or for that matter a word map to a word). We do require that the enumeration of \( G \) is consistent across the various probability distributions. Clearly the position of the identity element of \( G \) can be determined from the ordering.

There are many open questions regarding the connection between the probability distributions of word maps on a group \( G \) and the underlying group \( G \). In section 2 we give an answer to a question of Amit and Vishne [AV11].

In Section 3 we provide a proof of Theorem B and in Section 4 we prove Theorems A and C.

## 2. Probability distributions of word maps

We will denote the group of all word maps on \( d \)-variables over a group \( G \) as \( F_d(G) \). The multiplication is point-wise multiplication, or equivalently, the concatenation of the words inducing the word maps. The groups \( F_d(G) \) are very interesting and are examples of reduced free groups. If \( G \) is finite then \( F_d(G) \) is finite. We will write \( F_r \) for the free group of rank \( r \).

Amit and Vishne asked the following two questions [AV11]:
Question 2. Suppose $N_{w,G} = N_{w',G}$ for every finite group $G$. Does it follow that $w'$ is mapped to $w$ by some automorphism of $F_r$?

Question 3. Suppose $N_{w,G} = N_{w',G}$ for a fixed group $G$. Does it follow that $w'$ is mapped to $w$ by some automorphism of $F_r(G)$?

We will answer Question 3 in the negative below. Work by Puder and Parzanchevski has shown that in certain situations Question 2 is true: if $N_{w,G}$ and $N_{w',G}$ are uniform for all groups $G$, then there is some automorphism of $F_r$ taking $w'$ to $w$ [PPT13]. It is unknown whether Question 2 holds in general.

Recall that a word $w$ is called a law on $G$ if it induces the trivial map on $G$. We note the following observation:

**Lemma 4.** Let $G$ be a finite group. A word $w(x, y) = x^k c(x, y)$ where $k \in \mathbb{Z}$ and $c \in F'$, is a law if and only if $x^k$ is a law and $c(x, y)$ is a law.

**Proof.** Clearly the product of two laws of $G$ is a law of $G$. If $w(x, y)$ is a law of $G$, then $w(x, x)$ is a law of $G$. Hence $x^k$ and consequently $x^{-k}$ are laws of $G$. Therefore $x^{-k}w(x, y) = c(x, y)$ is a law of $G$. \hfill \Box

The below example is the answer in the negative to Question 3 of Amit and Vishne:

**Example 5.** There are word maps over $S(3)$ that induce the same probability distribution on $S(3)$ but are not automorphic. Consider the words $w = x^2$ and $v = [x, yx^2y^2]$. Over $S(3)$ the words $w$ and $v$ induce the same probability distribution. But, they are not automorphic since if $w$ were automorphic to $v$, then $x^2$ would be in the commutator subgroup. Hence over $S(3)$, $x^2c$ would be a law for some $c \in F'$. But, from the above lemma, this is impossible.

Even restricting to nilpotent groups, the authors have found that there are 5 automorphism classes of word maps over $Q_8$, but only 4 probability distributions over it.

### 3. Nilpotent Groups

The lemma below was noted by the first author in [Coc]. It establishes an interesting condition for a group to be nilpotent based solely on a property of the order function. We will use this condition in Theorem 13 to construct for a non-nilpotent group $G$ a surjective word $w$ such that $w$ does not induce the uniform distribution on $G$.

**Lemma 6.** [Coc] For a prime $p$, a finite group $G$ is not $p$-nilpotent if and only if there are $x, y \in G$, both of order $q^k$ for some prime $q \neq p$ such that the order of $xy$ is $p$ (or the order of $xy$ is either 2 or 4 when $p = 2$.)

**Lemma 7.** Let $N$ be a finite nilpotent group, and $w(x; \overline{f})$ be a word with parameters $\overline{f} \in N$. Then the following are equivalent:

1. $w(x; \overline{f})$ has uniform fiber size over $N$.
2. $w(x; \overline{f})$ is surjective.
3. The greatest common divisor of the exponents of variables in $x$ in $w(x; \overline{f})$ together with the exponent of $N$ is 1.
Proof: (1) $\rightarrow$ (2) is obvious.

(2) $\rightarrow$ (3): Suppose (2) holds, but the greatest common divisor of the exponents of variables in $\pi$ in $w(\pi, \overline{\pi})$ together with the exponent of $N$ is $d > 1$. Let $p$ be a prime divisor of $d$. Then $p$ divides the exponent of the abelianization $ab(N)$. In $ab(N)$, the image of $w(\pi, \overline{\pi})$ is a coset of $w(\pi, \overline{\pi})$. However, if $p$ divides the greatest common divisor of the exponents of $\pi$ in $w$, we have that $w(ab(N); \overline{\pi}) \subseteq (ab(N))^p$, which is strictly smaller than $ab(N)$ since $p$ divides the exponent of $ab(N)$.

(3) $\rightarrow$ (1): Suppose (3) holds, then without loss of generality, we may assume the word has the form $x_1hc$ where $h$ is a word in $\overline{\pi}$ and $c$ is a commutator word in the variables $\pi$ and parameters $\overline{\pi}$. It is clear that this has uniform fiber size over an abelian group.

We now induct on the nilpotency class of $N$. Let $Z(N)$ be the center of $Z$. By the induction hypothesis, $w(\pi, \overline{\pi})$ has uniform fiber size over $N/Z(N)$, after replacing the parameters by their canonical image. Thus, it suffices to show that for every $a, b \in N$ such that $a^{-1}b \in Z(N)$, $w$ has the same fiber size over $a$ and $b$. However, we have the bijection $(x_1, x_2, x_3, \cdots) \rightarrow (x_1a^{-1}b, x_2, x_3, \cdots)$ between the fibers of $a$ and $b$. Indeed, suppose that $w(x_1, x_2, \cdots) = a$. As $a^{-1}b$ is in the center and $c$ is a commutator word, we have $c(x_1a^{-1}b, x_2, \cdots) = c(x_1, x_2, \cdots)$, thus $w(x_1, x_2, \cdots) = x_1a^{-1}bhc(x_1a^{-1}b, x_2, \cdots) = (a^{-1}b)(x_1hc(x_1, x_2, \cdots)) = a^{-1}ba = b$. The other implication can be established similarly. So $w$ has uniform fiber size over $N$, completing the proof. \qed

We now prove a slightly stronger version of Theorem 8.

**Theorem 8.** Let $G$ be a finite group. Then the following are equivalent:

(1) $G$ is nilpotent.

(2) For every surjective word map $w$, the distribution $\mu_{G,w}$ is uniform.

(3) There is some $n > 1$ such that for every $n$-variable surjective word map $w$, the distribution $\mu_{G,w}$ is uniform.

**Proof:** (1) $\rightarrow$ (2) We first suppose that $G$ is nilpotent. Then by the previous lemma, if a word map is surjective, then is has uniform fiber size.

(2) $\rightarrow$ (3) is obvious.

(3) $\rightarrow$ (1) Now suppose that $n > 1$ and every $n$-variable surjective word map on $G$ induces the uniform distribution. We will show $G$ is $p$-nilpotent for every prime $p$. Suppose by way of contradiction that $G$ is not $p$-nilpotent for the prime $p$. Then by Lemma above, there are two elements $a, b$ of $G$, such that $o(a) = o(b) = q^k$ and

$$o(ab) \begin{cases} = p & \text{for } p \text{ an odd prime} \\ \in \{2, 4\} & \text{for } p = 2. \end{cases}$$

Since $p$ and $q$ are coprime there are $r, s \in \mathbb{Z}$ such that $rp + sq^k = 1$; (in the event $o(ab) = 4$ we will assume that $4r + sq^k = 1$). Consider the $n$-variable word

$$w(\pi) = x_1^{sq^k}x_2^{sq^k}(x_1x_2)^{rp},$$

(if necessary let $p = 4$). We have the following facts about $w$:

(a) For any $g \in G$, we have $w(\pi) = g$ if $x_1 = g$ and $x_2 = 1$.

(b) For any $g \in G$, we have $w(\pi) = 1$ if $x_1 = g$ and $x_2 = g^{-1}$.

(c) If $x_1 = a$ and $x_2 = b$, we have

$$w(a, b) = a^{sq^k}b^{sq^k}(ab)^{rp} = 1.$$
By (a), \( w \) is surjective. By (b) and (c), there are at least \((|G| + 1) \cdot |G|^{n-2}\) tuples in \( G^n \) that map to the identity. So \( w \) is a surjective word map on \( G \) that does not induce the uniform distribution. We conclude that if every \( n \)-variable surjective word map on \( G \) induces the uniform distribution, then \( G \) is \( p \)-nilpotent for every prime \( p \), and hence nilpotent. \( \square \)

**Corollary 9.** There are two word maps over a reduced free group that are homomorphic images of each other, but not related via an automorphism.

**Proof.** Consider a non-nilpotent reduced free group \( G \). By the previous theorem, there is a surjective word map \( w \) on \( G \) such that it does not induce the uniform distribution. However, as it is surjective, there is a homomorphism of \( G \) taking \( w \) to \( x \), and vice versa. Thus \( w \) and \( x \) are homomorphic images of each other, but not automorphic, since \( x \) induces the uniform distribution. \( \square \)

**Corollary 10.** In a finite nilpotent group \( G \), the equation \( x = c(x, y) \) where \( c \in F'[x, y] \) has exactly \( |G| \) solutions; moreover the solution set is exactly the two-tuples in the set \( \{(1, g) : g \in G\} \).

**Proof.** We note that a solution \((a, b)\) to \( x = c(x, y) \) is also a solution to \( w(x, y) = 1 \) where \( w = x^{-1}c(x, y) \). Since \( G \) is nilpotent and \( w \) is surjective, we see that there are exactly \( |G| \) such solutions. Clearly, \((1, g)\) is a solution for all \( g \in G \). \( \square \)

The above corollary can easily be generalized to the following:

**Corollary 11.** In a finite nilpotent group \( G \), the equation \( w(\overline{x}) = c(\overline{x}) \), where \( c \in F'(G)[\overline{x}] \) and \( w \) is a surjective word map on \( G \), has exactly \( |G|^{|\overline{x}|-1} \) solutions.

**Proof.** By Theorem 8 there is an automorphism \( \sigma \) of \( G \) that takes \( w \) to \( x_1 \). Then \( \sigma(w^{-1}c) = x_1^{-1}\sigma(c) \) and we conclude that \( x_1^{-1}\sigma(c) \) is a surjective word map on \( G \). Hence, there are exactly \( |G|^{|\overline{x}|-1} \) solutions to \( x_1^{-1}\sigma(c) \) and these are in bijection (via \( \sigma \)) with the solutions to \( w(\overline{x}) = c(\overline{x}) \). \( \square \)

It is natural to ask about the generalization of Corollary 11 to the equation \( w(\overline{x}) = v(\overline{x}) \), without any restriction on \( w \) or \( v \), which is equivalent to considering the equation \( w(\overline{x}) = 1 \). Amit conjectured the following in unpublished work [Ami] (see also [Nik11, Question 24]):

**Conjecture 12** (Amit). For every word map \( w(\overline{x}) \) on a finite nilpotent group \( G \),

\[
\mu_{G,w}(1) \geq \frac{1}{|G|},
\]

i.e., the number of solutions to \( w(\overline{x}) = 1 \) is greater than or equal to \( |G|^{|\overline{x}|-1} \).

There are only some partial results in this direction. Levy has shown that when \( G \) has nilpotent class 2, then for any word \( w \) we have \( \mu_{G,w}(1) \geq \frac{1}{|G|} \) [Lev11]; showing that Amit’s Conjecture holds for class 2 groups. Iniguez and Sangroniz have shown the stronger condition that for free \( p \)-groups of nilpotency class 2 and exponent 2, it is true that \( \mu_{G,w}(g) \geq \frac{1}{|G|} \) [InS17]. Klyachko and Mkrtchyan [KMi14] considered first-order formula in any finite group, which implies \( \mu_{G,w}(1) \geq \frac{1}{|G|} \) when \( w \) has only 2 variables.
4. Information Content of Distributions

In this section we are interested in understanding the information content of the distributions of word maps of a group. Recall that we are interested in the following question:

Question 13. Fix \( n \in \mathbb{N} \), a finite group \( G \), and an enumeration of the elements of \( G \). Let \( g_i \) be the \( i \)-th element of \( G \). Consider the probability distribution of the word map \( w \) as a function \( f_w : |G| \to \mathbb{N} \) where \( f_w(i) = |w^{-1}(g_i)| \). Given the distributions of all \( n \)-variable word maps of \( G \) as a set, what information can be recovered about \( G \)?

A priori, the answer of the question depends on \( n \). We ask:

Question 14. Do we get more information as \( n \) gets larger?

From the distributions of word maps we can easily read off the size of the group. Moreover, we can identify the identity element in \( G \) as it is the image of the only word map (the identity map) that has an image of size 1.

We mention the following example:

Example 15. \( D_8 \) and \( Q_8 \) have the same reduced free group on two variables, i.e.,

\[ F_2(D_8) = F_2(Q_8) = \text{SmallGroup}(32,2). \]

However using Magma \[\text{[BCP97]}\] we find that they have different sets of distributions of 2-variable word maps.

4.1. \( n = 1 \): words with a single variable. When \( n = 1 \), the images of the word maps are exactly the sets \( G^k = \{g^k \mid g \in G\} \).

Example 16. The distribution of 1-variable word maps does not determine even nilpotent groups up to isomorphism. Consider the extra-special groups of exponent \( p \). When looking at word maps on 1-variable, they are indistinguishable from the elementary abelian groups of the same order.

In order to prove Theorem A we will show that the distribution of 1-variable word maps on \( G \) determines whether or not \( G \) is nilpotent; to do this we need the following theorem originally conjectured by Frobenius and proven by Iliyori and Yamaki \[\text{[IY91]}\]:

Theorem 17 (Frobenius Solutions Theorem). Let \( G \) be a finite group and let \( d \) divide the exponent of \( G \). Let \( X(d) = \{x \in G : x^d = 1\} \). Then \( d \) divides \( |X(d)| \) and if \( |X(d)| = d \) then \( X(d) \) is a normal subgroup of \( G \).

Using the Frobenius Solutions Theorem we can now show:

Theorem 18. The distribution of 1-variable word maps on a finite group \( G \) determines whether or not \( G \) is nilpotent.

Proof. We first note, that the identity element is always determined by the set of distributions, i.e., the only element for which there is a distribution mapping entirely onto it. Moreover, we can always identify \( |G| \) from the set of distributions, namely by looking for a uniform distribution.

Let \( |G| = p^k m \) where \( \gcd(p, m) = 1 \) and \( k \geq 1 \). Then, if \( G \) is nilpotent, there are exactly \( p^k \) solutions to the equation \( xx^k = 1 \). Moreover, letting \( w = x^p^k \), we see that for every \( g \in w(G) \) there are exactly \( p^k \) preimages in \( G \) and \( |w(G)| = m \).
Now suppose $G$ is a group of order $p^k m$, where $(p, m) = 1$, and $w = x^d$ such that the following hold:

- For every $g \in w(G)$ there are exactly $p^k$ preimages in $G$.
- $|w(G)| = m$.

We claim $G$ must be nilpotent. We first note that by the Frobenius Solutions Theorem the number $d$ is a $p$-th power.

Let $X(m)$ be the solutions to the equation $x^m = 1$. Also by the Frobenius Solutions Theorem, $|X(m)| \geq m$. But every element of $X(m)$ is a solution to $x^m = 1$, hence they have order coprime to $p$. Since $w = x^{p^j}$ for some $j \geq 1$ and $\gcd(p^j, m) = 1$, the elements in $X(m)$ must also be in $w(G)$. But, $|w(G)| = m$ and we conclude that $w(G) = X(m)$ and contains no elements of order $p$. Hence every element whose order is a power of $p$ is a solution to $w$. Thus, $G$ is nilpotent if and only if there is such a $w$ for all $p$ dividing $|G|$.

4.2. $n > 1$: words with more than one variable. From Theorem B, we see that for $n > 1$, the set of all distributions of $n$-variable word maps on $G$ is enough to determine whether or not $G$ is nilpotent, i.e., a finite group $G$ is not nilpotent if and only if there is some $n$-variable surjective map that is not uniform. This, together with Theorem 18, proves Theorem A, which we restate here:

**Theorem 19.** For all $n \in \mathbb{N}$, we can identify when a finite group $G$ is nilpotent from the set of distributions of all $n$-variable word maps on $G$.

Interestingly enough the set of all distributions of $n$-variable word maps can also identify abelianness:

**Lemma 20.** For any $n > 1$, a finite group $G$ is abelian if and only if the distribution of every $n$-variable word map is uniform over its image.

**Proof.** If $G$ is abelian, then for every word map $w$, $w^{-1}(0)$ is a subgroup of $G^k$, and $w^{-1}(g)$ is either a coset of it or empty. Thus every word map is uniform over its image.

If $G$ is not abelian, then as shown by Ashurst, for $w = [x, y]$, we have that $\mu_G, w(1) > \mu_G, w(g)$ for all $g \in G$ [Ash12, Lemma 2.2.8]. Also, as $G$ is not abelian, $\mu_G, w(g)$ is not all zero for $g \neq 1$. If we regard $w$ as an $n$-variable word, then $\mu_G, w$ is not uniform over its image.

We will use the following Theorem from Cocke and Jensen [?]:

**Theorem 21.** Let $G$ and $H$ be finite abelian groups. Let $X$ be the set of natural numbers $r$ such that there exists a $k$ so that the word $w = x^k$ satisfies $|G| - |w(G)| = r$. Let $Y$ be the set of natural numbers $s$ such that there exists a $k$ so that the word $w = x^k$ satisfies $|H| - |w(H)| = s$. If $X = Y$, then $G \cong H$.

We now restate and prove Theorem C:

**Theorem 22.** For $n > 1$, the set of distributions of all $n$-variable word maps on $G$ can be used to identify whether $G$ is abelian; moreover, if $G$ is abelian, then the set of distributions identifies $G$ up to isomorphism.

**Proof.** In an abelian group, every word is automorphic to a power word, as can be seen by using a series of Nielson transformation to cancel out all but a single
variable. Since the number of not \( k \)-powers in \( G \) is determined by the word map \( x^k \), the set of distributions of word maps on \( G \) for any number of variables determines the set of natural numbers \( m \) such that there exists a \( k \) so that the word \( w = x^k \) satisfies \( |G| - |w(G)| = m \). If we are looking at all distributions induced by \( n \)-variable word maps where \( n > 1 \), then we can determine if \( G \) is abelian. If \( G \) is abelian, then by Theorem 21 above we have determined \( G \) up to isomorphism. \( \square \)

**Remark 23.** Note that as shown in Example 16 the distribution of 1-variable word maps is not enough to identify whether a group is abelian. However, if in addition to knowing that the distribution of 1-variable word maps, we also assume that \( G \) is abelian, then Theorem 21 applies and we can still identify \( G \) up to isomorphism.

The reduced free group of a nilpotent group is the direct product of the reduced free groups of its Sylow subgroups [Neu67, p. 41]. We show that without the group structure, the distributions of word maps of a nilpotent group determine the distributions of word maps of its Sylow subgroups, and similarly the distributions of word maps of all the Sylow subgroups determine the distributions of word maps of \( G \).

**Theorem 24.** The distributions of word maps of a nilpotent group uniquely determines the distributions of word maps of its Sylow \( p \)-subgroups for all \( p \), and vice versa.

**Proof.** Given the distributions of word maps of a finite group \( G \), we will show how to identify the sub-lists of the enumerated list \( G \) that correspond to the Sylow \( p \)-subgroups. First, we note that from the distributions of word maps of \( G \) we can determine the order of \( G \). Write \( |G| = p^n k \) such that \( p \mid k \). Then the word map \( x^k \) is uniformly distributed on its image, the Sylow \( p \)-subgroup. Since \( G \) is nilpotent, we have \( G = PK \) where \( |P| = p^n \) and \( |K| = k \). Then the following holds for every word map \( w \) and \( g \in P \), \( h \in K \):

\[
w_G^{-1}(gh) = w_P^{-1}(g)w_K^{-1}(h).
\]

Suppose \( w \) have image of size \( p^n \) and is uniform. Then it is uniform when projected to both \( P \) and \( K \). However, this means that the size of the image in \( K \) must divide \( |K|^2 = k^2 \). But \( k \) and \( p \) are co-prime, so the size of the image of \( w \) in \( K \) is 1. Thus, the image of \( w \) in \( G \) must be \( P \). This allows us to identify the Sylow \( p \)-subgroups. For every word map, we may find its distribution as a word map on \( P \) by looking at its distribution on \( P \) and scale accordingly.

For the backward direction, if we enumerate elements in \( G \) as the Cartesian product of the elements in the Sylow \( p \)-subgroups, then from the above discussion we have that any distribution on \( G \) is a product of distributions on the Sylow subgroups in the sense that

\[
w_G^{-1}(g_1 \cdots g_e) = w_P^{-1}(g_1) \cdots w_P^{-1}(g_e).
\]

Thus, we only need to show that the products of distributions on the Sylow subgroups are actually realized as the distribution of some word map on \( G \). Let \( P \) be a Sylow \( p \)-subgroup, and \( K \) be its complement. Suppose \( |P| = p^n \) and \( |K| = k \), and \( rp^n + sk = 1 \). Then for any word \( w \), define \( \tilde{w}_P(x_1, x_2, \cdots) = w(x_1^k, x_2^k, \cdots) \). Then \( w = \tilde{w}_P \) in \( P \), and \( \tilde{w}_P \) is a law on \( K \). Thus, the product of distributions on the Sylow subgroups are realized by the product of the \( \tilde{w}_P \) as a word map in \( G \). \( \square \)
5. ACKNOWLEDGMENTS

This material is based upon work done while the first author was supported by the National Science Foundation under Grant No. DMS-1502553. Some of the work was done while the first author was visiting the Army Cyber Institute. The views expressed are those of the author and do not reflect the official policy or position of the Army Cyber Institute, West Point, the Department of the Army, the Department of Defense, or the US Government.

REFERENCES

[Abe06] Miklós Abert, *On the probability of satisfying a word in a group*, J. Group Theory 9 (2006), no. 5, 685–694. MR 2253960

[Ami] A. Amit, *On equations in nilpotent groups*.

[Ash12] Carolyn Ashurst, *Fibres of words in finite groups, a probabilistic approach*, 2012, Thesis (Ph.D.)–University of Bath.

[AV11] Alon Amit and Uzi Vishne, *Characters and solutions to equations in finite groups*, J. Algebra Appl. 10 (2011), no. 4, 675–686. MR 2834108

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[Coc] William Cocke, *Two characterizations of finite nilpotent groups*, J. Group Theory to appear.

[InS17] Ainhoa Iñiguez and Josu Sangroniz, *Words and characters in finite p-groups*, J. Algebra 485 (2017), 230–246. MR 3659332

[IY91] Nobuo Iiyori and Hiroyoshi Yamaki, *On a conjecture of Frobenius*, Bull. Amer. Math. Soc. (N.S.) 25 (1991), no. 2, 413–416. MR 1102753

[KM14] Anton A. Klyachko and Anna A. Mkrtchyan, *How many tuples of group elements have a given property?*, Internat. J. Algebra Comput. 24 (2014), no. 4, 413–428, With an appendix by Dmitrii Y. Trushin. MR 3227820

[Lev11] Matthew Levy, *On the probability of satisfying a word in nilpotent groups of class 2*, arXiv preprint arXiv:1101.4286 (2011).

[Neu67] Hanna Neumann, *Varieties of groups*, Springer-Verlag New York, Inc., New York, 1967. MR 0215899

[Nik11] Nikolay Nikolov, *Algebraic properties of profinite groups*, arXiv preprint arXiv:1108.5130 (2011).

[NS07] Nikolay Nikolov and Dan Segal, *A characterization of finite soluble groups*, Bull. Lond. Math. Soc. 39 (2007), no. 2, 209–213. MR 2323450

[PP15] Doron Puder and Ori Parzanchevski, *Measure preserving words are primitive*, J. Amer. Math. Soc. 28 (2015), no. 1, 63–97. MR 3264763

William Cocke, Department of Mathematics, University of Wisconsin-Madison

E-mail address: cocke@math.wisc.edu

Meng-Che “Turbo” Ho, Department of Mathematics, Purdue University

E-mail address: ho140@purdue.edu