#A58 INTEGERS 19 (2019)

POWER MAPS IN FINITE GROUPS

Matt Larson
Department of Mathematics, Yale University, New Haven, Connecticut
matthew.larson@yale.edu

Received: 5/22/18, Revised: 3/21/19, Accepted: 10/6/19, Published: 11/4/19

Abstract

In recent work, Pomerance and Shparlinski have obtained results on the number of cycles in the functional graph of the map $x \mapsto x^a$ in $\mathbb{F}_p^*$. We prove similar results for other families of finite groups. In particular, we obtain estimates for the number of cycles for cyclic groups, symmetric groups, dihedral groups and $SL_2(\mathbb{F}_q)$. We also show that the cyclic group of order n minimizes the number of cycles among all nilpotent groups of order n for a fixed exponent a. Finally, we pose several problems.

1. Introduction

Let H be a finite group, and let $a \geq 2$ be an integer. The iterations of the map $x \mapsto x^a$ form a sort of dynamical system in a finite group. As such, it is natural to study the structure of the periodic points of this map. Define the undirected multigraph $G(a, H)$ with vertex set H and $x \sim y$ if $x^a = y$, with an additional edge if $y^a = x$. Note that $G(a, H)$ may have loops (for example at the identity) or cycles of length 2. The orbit structure of the map $x \mapsto x^a$ in G is encoded in $G(a, H)$. This graph has been extensively studied in the case of $H = (\mathbb{Z}/n\mathbb{Z})^*$ in connection with algorithmic number theory and cryptography (see, e.g., [6], [13] and [17]). In particular, the properties of the well-known Blum-Blum-Shub psuedorandom number generator [4] are determined by the properties of $G(2, (\mathbb{Z}/pq\mathbb{Z})^*)$.

Note that $G(a, H)$ is a refinement of the power graph of H (see [1] and references therein). In particular, the power graph of H is the graph with vertex set H and $x \sim y$ if $x \in \langle y \rangle$ or $y \in \langle x \rangle$. One can build the power graph of H out of $G(a, H)$ by taking the union of the edges of $G(a, H)$ for $1 \leq a \leq |H|$ and deleting any loops or multiple edges.

Let $N(a, H)$ denote the number of connected components in $G(a, H)$. Since each connected component contains a unique cycle, $N(a, H)$ is also the number of cycles in $G(a, H)$. In recent work, Pomerance and Shparlinski gave results on the average order, normal order, and extremal order of $N(a, \mathbb{F}_p^*)$ for p prime.

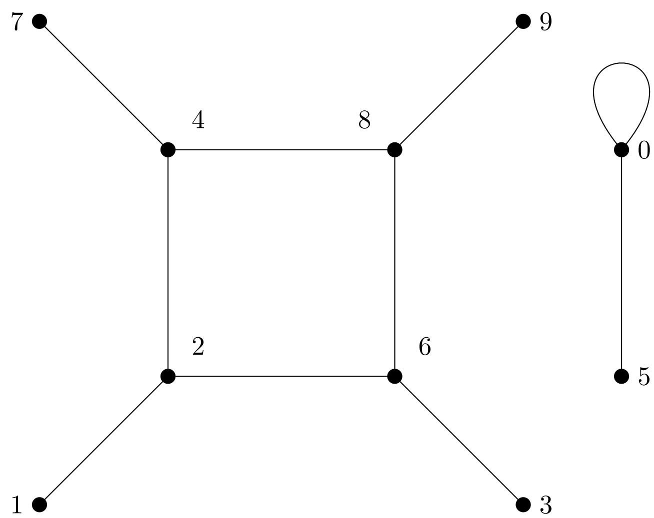

Figure 1: $G(2, \mathbb{Z}/10\mathbb{Z})$

Theorem 1 ([15, Theorems 1.1 and 1.2]). *For any $a \geq 2$:*

- *There exist infinitely many primes p such that $N(a, \mathbb{F}_p^*) > p^{5/12+o(1)}$.*
- *For almost all primes p, $N(a, \mathbb{F}_p^*) < p^{1/2+o(1)}$.*
- $\frac{1}{\pi(x)} \sum_{p \leq x} N(a, \mathbb{F}_p^*) \gg x^{0.293}$.

Under the assumption of the Elliot-Halberstam conjecture and a strong Linnik's constant, we can improve this to

$$\frac{1}{\pi(x)} \sum_{p \leq x} N(a, \mathbb{F}_p^*) \geq x^{1+o(1)}.$$

Pomerance and Shparlinski asked for an extension of these results to other groups. We consider the question of the size of $N(a, G)$ for various families of groups. Using results from number theory, group theory, and probability theory, we obtain results on the size of $N(a, G)$ for cyclic groups, dihedral groups, symmetric groups and the special linear group of degree 2 over a finite field.

Next, we conjecture that, for any a, the cyclic groups have the fewest connected components over any groups of a given order. More precisely, we have the following conjecture.

Conjecture 1. Let G be a group of order n. Then

$$N(a,G) \geq N(a,C_n).$$

We have verified this conjecture using Sage [16] for all groups of order at most 1000, except for groups of order 768, if $a \in \{2,3,\ldots,20\}$. We prove the following partial result.

Theorem 2. *Let G be a nilpotent group of order n. Then*

$$N(a,G) \geq N(a,C_n).$$

In Section 2, we introduce results used to estimate $N(a,G)$. In Section 3, we estimate the normal order, average order, and extremal order of $N(a,G)$ for several families of groups. In Section 4, we prove Theorem 2. In Section 5, we discuss further directions and ask several questions.

1.1. Notation

Throughout this paper, p denotes a prime number, q denotes a prime power, and a denotes a positive integer at least 2. All groups are finite, and group multiplication is always written multiplicatively.

For a set A, we denote the characteristic function of A by $1_A(x)$. For $g \in G$, a group, let $|g|$ denote the order of g. Let $\mathrm{ord}_n(a)$ denote the multiplicative order of a in $\mathbb{Z}/n\mathbb{Z}$. For a group G, let $w_G(d)$ denote the number of elements of order d. We will often write $w(d)$ for $w_G(d)$ if the group is obvious. Let C_n denote the cyclic group of order n, D_n denote the dihedral group of order $2n$, $SL_n(\mathbb{F}_q)$ denote the special linear group of degree n over the finite field of q elements and let S_n denote the symmetric group of order $n!$. Let λ denote the Carmichael lambda function, i.e., $\lambda(n)$ is the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$. Let φ denote the Euler φ-function.

We use standard Vinogradov notation and Landau notation. Recall that the statements $U = O(V)$, $U \ll V$ and $V \gg U$ all mean $|U| \leq cV$ for some $c > 0$. We also use the notation $o(1)$ to denote a quantity that tends to 0 as some parameter goes to infinity. The dependency of the constant on a parameter will be denoted as a subscript. We say almost all elements of a set $S \subseteq \mathbb{N}$ have a property P if the proportion of the elements of S that have P and are at most n is $1 + o(1)$.

2. General Tools

Our main tool for estimating $N(a,G)$ is the following lemma.

Lemma 1. *Let ρ denote the largest factor of $|G|$ relatively prime to a. Then*

$$N(a,G) = \sum_{d|\rho} \frac{w(d)}{\mathrm{ord}_d(a)}.$$

Proof. We generalize an argument of Chou and Shparlinski in [6]. Consider the map $x \mapsto x^a$. Let $t \geq 0, c > 0$ be minimal such that $x^{a^t} = x^{a^{t+c}}$ for all x, which exist since the map $x \mapsto x^a$ is preperiodic. Let d denote the order of x. Then $d | a^t(a^c - 1)$, so $t = 0$ if and only if $\gcd(a, d) = 1$. If $t = 0$, then x lies in a cycle of length $\mathrm{ord}_d(a)$, and there are $w(d)$ elements that lie in such cycles, showing the result. □

We will often use this result in the form

$$N(a, G) = \sum_{\substack{g \in G \\ \gcd(|g|, a) = 1}} \frac{1}{\mathrm{ord}_{|g|}(a)},$$

which follows from Lemma 1 by grouping terms by order. We observe that if a group G has many elements of large order, then $N(a, G)$ is likely to be small. This gives some justification to Conjecture 1. We will also make use of the following lemma.

Lemma 2. *Let $H_1, \ldots, H_n \leq G$, and suppose $H_i \cap H_j = \{e\}$ for $i \neq j$, where e is the identity of G. Then*

$$N(a, G) \geq \sum_{i=1}^{n} N(a, H_i) - n + 1.$$

Proof. Note that the subgraph in $G(a, G)$ induced by H_i is isomorphic to $G(a, H_i)$. These induced subgraphs overlap only at the identity, and, in these induced subgraphs, each connected component contains a unique cycle. In $G(a, G)$, these induced subgraphs cannot be connected to each other, except for the connected component containing the identity. □

Before proving the last general result, we state a lemma.

Lemma 3. *If $\frac{dd'}{\gcd(d,d')} = n$, then $\mathrm{ord}_d(a)\,\mathrm{ord}_{d'}(a) \geq \mathrm{ord}_n(a)$.*

Proof. As $d \mid a^{\mathrm{ord}_d(a)} - 1$ and $d' \mid a^{\mathrm{ord}_{d'}(a)} - 1$, $n \mid a^{\mathrm{ord}_d(a)\,\mathrm{ord}_{d'}(a)} - 1$. □

Theorem 3. *Let G, H be finite groups. Then*

$$N(a, G \times H) \geq N(a, G) N(a, H).$$

Proof. Let ρ_1 and ρ_2 be the largest divisors coprime to a of $|G|$ and $|H|$ respectively.

Then

$$\begin{aligned}
\left(\sum_{d\mid\rho_1}\frac{w_G(d)}{\mathrm{ord}_d(a)}\right)\left(\sum_{d'\mid\rho_2}\frac{w_H(d')}{\mathrm{ord}_{d'}(a)}\right) &= \sum_{d\mid\rho_1, d'\mid\rho_2}\frac{w_G(d)w_H(d')}{\mathrm{ord}_d(a)\,\mathrm{ord}_{d'}(a)}\\
&= \sum_{k\mid\rho_1\rho_2}\sum_{\substack{d\mid\rho_1, d'\mid\rho_2,\\ dd'/\gcd(d,d')=k}}\frac{w_G(d)w_H(d')}{\mathrm{ord}_d(a)\,\mathrm{ord}_{d'}(a)}\\
&\le \sum_{k\mid\rho_1\rho_2}\sum_{\substack{d\mid\rho_1, d'\mid\rho_2,\\ dd'/\gcd(d,d')=k}}\frac{w_G(d)w_H(d')}{\mathrm{ord}_k(a)}\\
&= \sum_{k\mid\rho_1\rho_2}\frac{w_{G\times H}(k)}{\mathrm{ord}_k(a)}\\
&= N(a, G\times H),
\end{aligned}$$

where in the inequality we use Lemma 3. □

3. Size of $N(a, G)$

3.1. Cyclic Groups

We show results on the average order, normal order, and extremal order of $N(a, C_n)$.

Theorem 4. *Let $\delta = 0.2961$. Then*

$$\frac{1}{x}\sum_{n\le x} N(a, C_n) \ge x^{1-\delta+o(1)}.$$

Theorem 5. *For any fixed a, there exist infinitely many n such that*

$$N(a, C_n) \ge n^{1+o(1)}.$$

Theorem 6. *For almost all n, we have that*

$$N(a, C_n) \le n^{1/2+o(1)}.$$

Remark 1. Under the Elliott-Halberstam conjecture, we can remove δ from Theorem 4, i.e., we can show that $\frac{1}{x}\sum_{n\le x} N(a, C_n) \ge x^{1+o(1)}$. Under the generalized Riemann hypothesis, we can remove the 1/2 from Theorem 6 and show that for almost all n, $N(a, C_n) \le n^{o(1)}$.

In conjunction with the following lemma, the above theorems immediately give results on dihedral groups.

Lemma 4. *If a is even, then $N(a, D_n) = N(a, C_n)$. If a is odd, then $N(a, D_n) = n + N(a, C_n)$.*

Proof. Recall that D_n consists of a cyclic subgroup of order n and n elements of order 2 lying outside this cyclic subgroup. If a is even, then each element of order 2 is connected to the component that contains the identity. If a is odd, then each element of order 2 lies in a component that consists of a single vertex with a loop. □

Proof of Theorem 4. We use the strategy of Pomerance and Shparlinski in [15]. First we recall a result of Baker and Harman.

Lemma 5 ([3], Theorem 1)**.** *There is an absolute constant κ with the following property: Let x sufficiently large, and let*

$$v = \frac{\log x}{\log \log x}, \quad w = v^{1/0.2961}.$$

Let

$$\mathcal{Q} = \{p \in \left[\frac{w}{(\log w)^\kappa}, w\right] \ : \ p - 1 \mid M_v\},$$

where M_v is the least common multiple of the integers in $[1, v]$. Then

$$|\mathcal{Q}| \geq \frac{w}{(\log w)^\kappa}.$$

Now we prove the result. Let $\mathcal{Q}$ be the set of primes given by Lemma 5. Let

$$k = \left\lfloor \frac{\log x}{\log w} \right\rfloor.$$

Let $\mathcal{S}$ denote the set of products of k distinct elements of $\mathcal{Q}$. We see that

$$|\mathcal{S}| = \binom{|\mathcal{Q}|}{k} = \left(\frac{w}{k}\right)^k x^{o(1)},$$

using that $(n/k)^k \leq \binom{n}{k} \leq (ne/k)^k$. We compute that $k^k = x^{0.2961+o(1)}$ and $w^k = x^{1+o(1)}$, so

$$|\mathcal{S}| = x^{1-0.2961+o(1)}.$$

We also note that, for any $m \in \mathcal{S}$,

$$x \geq w^k \geq m \geq (w/(\log w)^\kappa)^k = x^{1+o(1)}.$$

By Lemma 3, we have that for any $m \in \mathcal{S}$, $\mathrm{ord}_m(a) \mid M_v$. By the prime number theorem, this implies that

$$\mathrm{ord}_m(a) \leq M_v = \exp(v(1 + o(1))) = x^{o(1)}.$$

Therefore, for each $m \in \mathcal{S}$, we have

$$N(a, C_m) \geq \frac{\varphi(m)}{\mathrm{ord}_m(a)} = x^{1+o(1)},$$

since $\varphi(m) = m^{1+o(1)} = x^{1+o(1)}$ [11, Theorem 328]. Therefore we have found $x^{1-0.2961+o(1)}$ positive integers m less than or equal to x such that $N(a, C_m) = x^{1+o(1)}$, which implies the result. □

Remark 2. One can obtain the same result by using the work of Ambrose; it follows from the specialization to $\mathbb{Q}$ of [2, Theorem 1]. As we can remove δ from the result of Ambrose under the Elliott-Halberstam conjecture, we can show that the average value of $N(a, C_n)$ is $x^{1+o(1)}$ under the Elliott-Halberstam conjecture.

Proof of Theorem 5. Let k be a large integer, and set $n = a^k - 1$. Then, using [11, Theorem 328],

$$N(a, C_n) \geq \frac{\varphi(a^k - 1)}{k} \gg \frac{n}{\log n \log\log n}.$$

□

Before proving Theorem 6, we recall some properties of the Carmichael lambda function.

Lemma 6 ([9, Lemma 2])**.** *If $d|n$, then*

$$\varphi(d)/\lambda(d)|\varphi(n)/\lambda(n).$$

Theorem 7 ([8, Theorem 2])**.** *For almost all n,*

$$\lambda(n) = n^{1+o(1)}.$$

Lemma 7 ([13, Lemma 5])**.** *We have*

$$\mathrm{ord}_n(a) \geq \frac{\lambda(n)}{n} \prod_{p|n} \mathrm{ord}_p(a).$$

Let B denote the set of primes p such that $\mathrm{ord}_p(a) < \sqrt{p}/\log p$.

Lemma 8 ([7])**.** *With B defined as above,* $|B \cap \{1, \ldots, N\}| = O(N/(\log N)^3)$.

Remark 3. Using the results in [12], we can show that the set of primes p, with $p \leq n$ and $\mathrm{ord}_p(a) \leq p^{1+o(1)}$, has size $O(n/(\log n)^3)$ under the generalized Riemann hypothesis, which would lead to a corresponding improvement in Theorem 6 to $N(a, C_n) \leq n^{o(1)}$ for almost all n.

For an integer n, let n_B denote the largest divisor of n that is a product of primes from B.

Lemma 9. *For almost all $n \le N$, $n_B < \log n$.*

Proof. By the density estimate in Lemma 8, we see that

$$\sum_{n=n_B} \frac{1}{n} = \prod_{p \in B} \left(1 - \frac{1}{p}\right)^{-1} = O(1).$$

Therefore, for any $\varepsilon > 0$, there is $C = C(\varepsilon)$ such that

$$\sum_{\substack{n=n_B,\\ n>C}} \frac{1}{n} < \varepsilon.$$

Thus for all but εN integers $n \le N$, we have that $n_B < C$. As ε was arbitrary and eventually $\log n > C$, this proves the claim. □

Lemma 10 ([13, Lemma 7])**.** *Let A denote the set of positive integers n such that there is a positive integer s such that $s^2 \mid n$ and $s^2 \ge \log n$. Then $|A \cap \{1, \ldots, N\}| = O(N/\log N)$.*

Proof of Theorem 6. By Lemma 7, Lemma 9, and Lemma 10 there is a set S of density 1 such that $n_B < \log n$, $s^2 < \log n$ for every s such that s^2 divides n, and $\lambda(n) = n^{1+o(1)}$ for all $n \in S$. By Lemma 7, we have that

$$N(a, C_n) \le \sum_{d|n} \frac{d\varphi(d)}{\lambda(d) \prod_{p|d} \mathrm{ord}_p(a)}.$$

Using the bound that $\varphi(n) < n$ and Lemma 6, in form of $\varphi(d)/\lambda(d) \le \varphi(n)/\lambda(n)$ for $d|n$, we have that, for almost all n,

$$\begin{aligned} N(a, C_n) &\le \sum_{d|n} \frac{d\varphi(d)}{\lambda(d) \prod_{p|d} \mathrm{ord}_p(a)} \\ &\le \sum_{d|n} \frac{d\varphi(n)}{\lambda(n) \prod_{p|d} \mathrm{ord}_p(a)} \\ &= \sum_{d|n} \frac{dn^{o(1)}}{\prod_{p|d} \mathrm{ord}_p(a)} \\ &\le n^{1/2+o(1)}, \end{aligned}$$

where in the last inequality we are using that the square part of n is at most $\log n$ and the product of the primes in B dividing n is at most $\log n$. □

3.2. Symmetric Groups

As Lemma 2 implies that the sequence $\{N(a, S_n)\}_{n\in\mathbb{N}}$ is non-decreasing, since S_{n-1} embeds into S_n, it makes less sense to discuss the average order, normal order, and extremal order of $N(a, S_n)$. We instead prove bounds on the size of $N(a, S_n)$.

Theorem 8. *We have*

$$N(a, S_n) \geq \frac{n!}{\exp\left(\frac{\varphi(a)}{2a}\log^2 n(1+o(1))\right)}.$$

Let $T_n = T_n(a)$ denote the set of permutations in S_n with order coprime to a, and let $S(n)$ denote the set of positive integers coprime to a that are at most n. We will use concentration bounds to show that almost all elements of T_n have large order, and then we use the trivial bound that $\mathrm{ord}_d(a) \leq d$ to bound $N(a, S_n)$.

Theorem 9 ([14, Theorem 1])**.** *There exist constants $C = C(a)$ and $\delta = \delta(a)$ such that*

$$|T_n| = C(n-1)!n^{\varphi(a)/a} + O((n-1)!n^{\varphi(a)/a-\delta}).$$

Lemma 11 ([18, Theorem 1])**.** *For some permutation σ, let $M(\sigma)$ denote the order of the permutation. Choose a random permutation τ_n from T_n. Then*

$$P\left(\frac{\log M(\tau_n) - \sum_{i\in S(n)}(\log i)/i}{\sqrt{\sum_{i\in S(n)}(\log i)^2/i}} \leq x\right) \xrightarrow{d} \Phi(x),$$

where $\Phi(x)$ is the standard normal distribution and $\xrightarrow{d}$ denotes convergence in distribution.

We use Lemma 11 to bound the order of most elements of T_n and then use the trivial upper bound on $\mathrm{ord}_d(a)$. First we obtain an asymptotic for $\sum_{i\in S(n)}(\log i)^2/i$.

Lemma 12. *We have*

$$\sum_{i\in S(n)} \frac{\log i}{i} = \frac{\varphi(a)}{2a}\log^2 n + o(\log^2 n).$$

Proof. Observe that, using partial summation,

$$\sum_{i\in S(n)} \frac{\log i}{i} = \log n \sum_{i=1}^{n} \frac{1_{S(n)}(i)}{i} + \sum_{m=1}^{n-1}(\log m - \log(m+1)) \sum_{i=1}^{m} \frac{1_{S(n)}(i)}{i}$$

and

$$\sum_{i=1}^{n} \frac{1_{S(n)}(i)}{i} = \sum_{m=1}^{n-1}\left(\frac{1}{m} - \frac{1}{m+1}\right) m\frac{\varphi(a)}{a} + O(1)$$
$$= \frac{\varphi(a)}{a}\log n + O(1).$$

Using partial summation again, we have that

$$\sum_{i=1}^{n}\frac{\log i}{i}=\log^2 n+\sum_{m=1}^{n-1}(\log m-\log m+1)\log m+O(\log n).$$

On the other hand,

$$\sum_{i=1}^{n}\frac{\log i}{i}=\int_1^n\frac{\log x}{x}dx+o(\log n)=\frac{\log^2 n}{2}+o(\log n).$$

Hence

$$\sum_{m=1}^{n-1}(\log m-\log m+1)\log m=\frac{\log^2 n}{2}+o(\log n),$$

showing that

$$\sum_{i\in S(n)}\frac{\log i}{i}=\frac{\varphi(a)}{2a}\log^2 n+o(\log^2 n).$$

□

Proof of Theorem 8. We have the trivial bound

$$\sum_{i\in S(n)}\frac{(\log i)^2}{i}=O(\log^3 n).$$

For all but $o_a(|T_n|)$ permutations τ_n in T_n, we have that

$$\log M(\tau_n)\le\sum_{i\in S(n)}\frac{\log i}{i}+O(\log\log n(\log n)^{3/2}).$$

Hence, for almost all permutations in T_n, we have that

$$M(\tau_n)\le\exp\left(\frac{\varphi(a)}{2a}\log^2 n(1+o(1))\right).$$

In order to turn this into a lower bound for $N(a,S_n)$, we need an upper bound on $\mathrm{ord}_d(a)$ for d coprime to a. Using the trivial bound that $\mathrm{ord}_d(a)\le d\le\exp\left(\frac{\varphi(a)}{2a}\log^2 n(1+o(1))\right)$ for almost all permutations $\tau_n\in T_n$, we have that

$$N(a,S_n)\gg_a\frac{(n-1)!n^{\varphi(a)/a}}{\exp\left(\frac{\varphi(a)}{2a}\log^2 n(1+o(1))\right)}=\frac{n!}{\exp\left(\frac{\varphi(a)}{2a}\log^2 n(1+o(1))\right)}.$$

□

We conjecture that this lower bound is of the correct order, as the trivial bound $\mathrm{ord}_d(a) \leq d$ is usually fairly sharp for most d. Without finer control over the orders of permutations than is known, it seems difficult to prove a sharp upper bound. However, we can show that

$$N(a, S_n) = o_a((n-1)! n^{\varphi(a)/a}).$$

Indeed, by Lemma 11, we have that for all but $o_a(|T_n|)$ elements of T_n,

$$M(\tau_n) \geq \exp\left(\frac{\varphi(a)}{2a} \log^2 n(1 + o(1))\right).$$

Hence

$$N(a, S_n) \leq o_a(|T_n|) + \frac{(n-1)! n^{\varphi(a)/a}}{\exp\left(\frac{\varphi(a)}{2a} \log^2 n(1+o(1))\right)} = o_a((n-1)! n^{\varphi(a)/a}).$$

3.3. Special Linear Groups Over Finite Fields

Because of highly explicit knowledge of the conjugacy class structure of $SL_2(\mathbb{F}_q)$, we are able to compute $N(a, SL_2(\mathbb{F}_q))$.

Theorem 10. *Let $q = p^c$ be an odd prime power. If $\gcd(a, q) = 1$, then*

$$N(a, SL_2(\mathbb{F}_q)) = \frac{q^2 - q}{2} N(a, C_{q+1}) + \frac{q^2 + q}{2} N(a, C_{q-1}) + (q^2 - 1)(1 + 1_{2\nmid a})(\frac{1}{\mathrm{ord}_p(a)} - 1),$$

where $1_{2\nmid a}$ is 1 if a is odd and 0 otherwise. If $\gcd(a, q) > 1$, then the last term does not appear.

Before we begin the proof, we recall some facts about conjugacy classes in $SL_2(\mathbb{F}_q)$ for q odd. We break the conjugacy classes into 4 types (see, e.g., [10]).

- Type 1: The $(q-3)/2$ conjugacy classes of elements which are diagonalizable of $\mathbb{F}_q$; they are parametrized by matrices of the form $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ for $\alpha \in \mathbb{F}_q^* \setminus \{1, -1\}$. Each conjugacy class has $q(q+1)$ elements.
- Type 2: The $(q-1)/2$ conjugacy classes of elements which are diagonalizable of $\mathbb{F}_{q^2}$ but not $\mathbb{F}_q$; they are parametrized by matrices of the form $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$ for $\alpha \in \mathbb{F}_{q^2}^* \setminus \{1, -1\}$ and satisfying $\alpha \cdot Fr(\alpha) = \alpha^{q+1} = 1$, where Fr denotes the Frobenius endomorphism. Each conjugacy class has $q(q-1)$ elements.
- Type 3: The central conjugacy classes $\{I\}$ and $\{-I\}$.

- Type 4: The 4 conjugacy classes that are not semi-simple. These conjugacy classes are parametrized by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$, where b is a non-square in $\mathbb{F}_q$. There are $(q^2-1)/2$ elements in each conjugacy class.

Proof. Note that the order of an element in a type 1 conjugacy classes is just the order of the eigenvalue, and the eigenvalues lie in the cyclic group $\mathbb{F}_q^*$. Therefore, because each type 1 conjugacy class has eigenvalues α and α^{-1}, there are $\varphi(d)/2$ type 1 conjugacy classes of order d for each divisor d of $q-1$, $d \neq 1, 2$. Hence

$$\sum_{a \in \mathcal{C},\ \mathcal{C} \text{ type 1}} \frac{1}{\text{ord}_d(a)} = \frac{q^2+q}{2}(N(a, C_{q-1}) - 1 - 1_{2\nmid a}).$$

Similarly for type 2, we note that the elements of $\mathbb{F}_{q^2}$ satisfying $x^{q+1} = 1$ form a cyclic subgroup of the multiplicative group. Therefore

$$\sum_{a \in \mathcal{C},\ \mathcal{C} \text{ type 2}} \frac{1}{\text{ord}_d(a)} = \frac{q^2-q}{2}(N(a, C_{q-1}) - 1 - 1_{2\nmid a}).$$

For type 3, the contribution is $1 + 1_{2\nmid a}$.

For type 4, each element with eigenvalue 1 has order p, and each element with eigenvalue -1 has order $2p$. Hence,

$$\sum_{a \in \mathcal{C},\ \mathcal{C} \text{ type 4}} \frac{1}{\text{ord}_d(a)} = \frac{q^2-1}{\text{ord}_p(a)} + 1_{2\nmid a}\frac{q^2-1}{\text{ord}_{2p}(a)} = \frac{q^2-1}{\text{ord}_p(a)}(1 + 1_{2\nmid a}),$$

since $\text{ord}_{2p}(a) = \text{ord}_p(a)$ for a odd. Summing over the 4 types of conjugacy classes gives the result. □

Theorem 1 allows us to bound the normal and extremal order of $N(a, SL_2(\mathbb{F}_p))$, using the fact that $N(a, SL_2(\mathbb{F}_p)) \gg p^2 N(a, \mathbb{F}_p^*)$.

Corollary 1. *There exist infinitely many primes p such that*

$$N(a, SL_2(\mathbb{F}_p)) \geq p^{29/12+o(1)}.$$

We also have

$$\frac{1}{\pi(x)} \sum_{p \leq x} N(a, SL_2(\mathbb{F}_p)) \gg x^{2.293}.$$

4. On the Minimal Size of $N(a, G)$ Among Groups of a Fixed Order

We now prove Theorem 2. Our strategy is to show that, for a group G of order n, the sum $\sum_{g \in G,\, \gcd(|g|, a)=1} \frac{1}{\text{ord}_{|g|}(a)}$ majorizes $\sum_{g \in C_n,\, \gcd(|g|, a)=1} \frac{1}{\text{ord}_{|g|}(a)}$ for any nilpotent group G. Then, Lemma 1 immediately implies Theorem 2. Before proving Theorem 2, we prove a lemma. For a group G, let $B_G(n)$ denote the number of elements of order at least n in G.

Lemma 13. *Let G be a group of order p^k. Then for all n, $B_G(n) \le B_{C_{p^k}}(n)$.*

Proof. First observe that the number of elements of order n in any finite group is a multiple of $\varphi(n)$. Suppose G is a counterexample to the lemma, then choose ℓ such that $B_G(p^\ell) > B_{C_{p^k}}(p^\ell)$. Since $B_G(1) = B_{C_{p^k}}(1)$, there must be fewer than $\varphi(p^b)$ elements of order p^b for some $b < \ell$. Hence there are no elements of order p^b for some b. But if a group has an element of order p^c, then it also has an element of order p^b for every $b < c$. □

Proof of Theorem 2. We first prove Theorem 2 for p-groups. Note that $\mathrm{ord}_{p^b}(a) \le \mathrm{ord}_{p^c}(a)$ if $b \le c$. But then Lemma 13 and Lemma 1 immediately imply that $N(a, G) \ge N(a, C_{|G|})$ for any p-group G.

Recall that a group is nilpotent if and only if it is a direct product of p-groups. Let $G = P_1 \times \cdots \times P_k$ be a nilpotent group, and let $P_1, \ldots, P_k$ be p-groups with orders $p_i^{e_i}$ for distinct primes $p_1, \ldots, p_k$. Let $n = |G|$. We may assume that $\gcd(a, n) = 1$, as factors of p-group with g not relatively prime a do not affect the result. We need to show that

$$\sum_{d|n} \frac{w(d)}{\mathrm{ord}_d(a)} \ge \sum_{d|n} \frac{\varphi(d)}{\mathrm{ord}_d(a)}.$$

Observe that, for a nilpotent group G, w_G is a multiplicative function, i.e.,

$$w_G(p_1^{j_1} p_2^{j_2} \cdots p_k^{j_k}) = w_G(p_1^{j_1}) w_G(p_2^{j_2}) \cdots w_G(p_k^{j_k}).$$

We claim that for any set of ℓ primes, $p_{i_1}, \ldots, p_{i_\ell}$, we have that

$$\sum_{\substack{d|n \\ d = p_{i_1}^{b_1} \cdots p_{i_\ell}^{b_\ell}}} \frac{w(d)}{\mathrm{ord}_d(a)} \ge \sum_{\substack{d|n \\ d = p_{i_1}^{b_1} \cdots p_{i_\ell}^{b_\ell}}} \frac{\varphi(d)}{\mathrm{ord}_d(a)}.$$

This would clearly imply the result by summing over all subsets of the primes dividing n. We prove the claim by induction on ℓ. The base case is the case of p-groups. Fix $b_1, \ldots, b_{\ell-1}$ such that $p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1} \mid n$. Then

$$\begin{aligned}\sum_{k=0}^{j_{i_\ell}} \frac{w(p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1} p_{i_\ell}^k)}{\mathrm{ord}_{p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1} p_{i_\ell}^k}(a)} &= w(p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1}) \sum_{k=0}^{j_{i_\ell}} \frac{w(p_{i_\ell}^k)}{\mathrm{ord}_{p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1} p_{i_\ell}^k}(a)} \\ &\ge \frac{w(p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1})}{\mathrm{ord}_{p_{i_1}^{b_1} \cdots p_{i_{\ell-1}}^{b_\ell - 1}}(a)} \sum_{k=0}^{j_{i_\ell}} \frac{w(p_{i_\ell}^k)}{\mathrm{ord}_{p_{i_\ell}^k}(a)},\end{aligned}$$

where we use Lemma 3 in the inequality. The result follows from summing over all choices of $b_1, \ldots, b_{\ell-1}$ and the inductive hypothesis. □

5. Discussion

In addition to proving a better upper bound on $N(a, S_n)$ and proving Conjecture 1, we pose several open problems.

Since the map $x \mapsto x^a$ is eventually periodic, the orbit $x, x^a, x^{a^2}, \ldots$ consists of a tail which does not repeat followed by a cycle. If x has no tail, then we say that x is *purely periodic*. Thus in $G(a, H)$, every purely periodic element has a rooted tree of tails leading into it. In [6, Theorem 1], Chou and Shparlinski showed that if H is cyclic, then all of the tails coming off the purely periodic elements in H are isomorphic. In particular, every purely periodic element has tails of the same size. This enabled Chou and Shparlinski to give a simple expression for the average length of the period over all elements of C_n. Let $C(a, G)$ denote the average period of an element in G. Then

Theorem 11 ([6, Theorem 1])**.** *If ρ is the largest divisor of n coprime to a, then*

$$C(a, C_n) = \frac{1}{\rho} \sum_{d|\rho} \varphi(d) \operatorname{ord}_d(a).$$

For general groups, the tails coming off a purely periodic vertex are not the same size. It would be interesting to compute or bound $C(a, G)$ for various families of groups.

By analogy with the power graph, it would be interesting to determine what set of invariants is determined by $G(a, H)$ for some fixed a or for all a. Groups H of prime exponent and the same order clearly have the same $G(a, H)$ for every a. Using the example of Cameron and Ghosh in [5], we see that, if $H = \langle x, y \mid x^3 = y^3 = [x, y]^3 = 1\rangle$, the smallest non-abelian group of exponent 3, then $G(a, C_3 \times C_3 \times C_3) \cong G(a, H)$ for every a. This raises the following question.

Question 1. Are there groups H and K such that the power graph of H is isomorphic to the power graph of K, but $G(a, H)$ is not isomorphic to $G(a, K)$ for some a?

It would be interesting to compute the asymptotics of $N(a, SL_n(\mathbb{F}_q))$ as n grows, in analogy with the symmetric group. As in the case of $N(a, S_n)$, Lemma 2 implies that the sequence $\{N(a, SL_n(\mathbb{F}_q))\}_{n\in\mathbb{N}}$ is non-decreasing since $SL_{n-1}(\mathbb{F}_q)$ embeds into $SL_n(\mathbb{F}_q)$.

One could also allow a to vary. Let exp(G) denote the exponent of G. Then clearly $N(a, G) = N(a + \exp(\mathrm{G}), G)$. Then the following question is natural.

Question 2. What $a \in \{2, 3, \ldots, \exp(G) - 1\}$ maximizes $N(a, S_n)$?

Acknowledgments. This research was conducted at the University of Minnesota Duluth REU and was supported by NSF DMS grant 1659047. We thank Igor

Shparlinski for pointing out an oversight in an earlier version of the paper, Joe Gallian for suggesting the subject of the paper, Arsen Yakymiv for discussing his work with us, and Joe Gallian and Phil Matchett Wood for reading the manuscript. We are also grateful to the referee for their helpful comments.

References

[1] J. Abawajy, A. Kelarev, and M. Chowdhury, Power graphs: a survey, *Electron. J. Graph Theory Appl.* **1** (2013), 125-147.

[2] C. Ambrose, Artin's primitive root conjecture and a problem of Rohrlich, *Math. Proc. Cambridge Philos. Soc.* **157** (2014), 79-99.

[3] R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331-361.

[4] L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudo-random number generator, *SIAM J. Comput.* **15** (1986), 364-383.

[5] P. Cameron and S. Ghosh, The power graph of a finite group, *Discrete Math.* **311** (2011), 1220-1222.

[6] W. Chou and I. Shparlinski, On the cycle structure of repeated exponentiation modulo a prime, *J. Number Theory* **107** (2004), 345-356.

[7] P. Erdős and M. R. Murty. On the order of a (mod p), Number theory (Ottawa, ON, 1996), CRM Proc. Lecture Notes **19**, Amer. Math. Soc., Providence, RI (1999), 8797.

[8] P. Erdős, C. Pomerance, and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 363-385.

[9] J. Friedlander, C. Pomerance, and I. Shparlinski, Period of the power generator and small values of Carmichael's function, *Math. Comp.* **70** (2000), 1591-1605.

[10] W. Fulton and J. Harris, *Representation Theory: a First Course*, Springer, New York, 2013.

[11] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 1979.

[12] P. Kurlberg, On the order of unimodular matrices modulo integers, *Acta Arith.* **110** (2003), 141-151.

[13] P. Kurlberg and C. Pomerance, On the periods of the linear congruential and power generators, *Acta Arith.* **119** (2005), 149-169.

[14] A. I. Pavlov, On two classes of permutations on the lengths of the cycles, *Math. Notes* **62** (1998), 739-746.

[15] C. Pomerance and I. Shparlinski, Connected components of the graph generated by power maps in prime finite fields, *Integers* **18** (2017).

[16] W. A. Stein, Sage mathematics software (Version 7.6) (2017).

[17] T. Vasiga and J. Shallit, On the iteration of certain quadratic maps over GF (p), *Disc. Math.* **277** (2004), 219-240.

[18] A. L. Yakymiv, On the Erdős-Turan law for permutations with random cycle weights, *Teor. Veroyatnost. i Primenen.* **63** (2018), 260-283.