Random invariant generation of $\mathrm{SL}_n(\mathbb{F}_q)$ and $\mathrm{Sp}_{2n}(\mathbb{F}_q)$ by a full unipotent Jordan block and a nonscalar element

Corentin Perret-Gentil

Abstract. This note gives a variant of a random invariant generation theorem of Guralnick and Kantor, for SL_n and Sp_{2n} over a finite field of characteristic p, with the element of large order replaced by a regular unipotent element of order p, motivated by a generation result of Gow and Tamburini. This would follow from general bounds of Liebeck and Saxl, but different arguments can be given in this case, leading to improved error terms and not relying on the classification of finite simple groups.

1. Introduction

We start by shortly surveying some of the literature on random (invariant) generation of classical groups, introducing notations and definitions along the way. Henceforth, a finite set X will be equipped with the counting measure, and for a property Φ with n free variables, we will write

$$P\Big(\Phi(\boldsymbol{x}) : \boldsymbol{x} \in X^n\Big) = \frac{|\{\boldsymbol{x} \in X^n : \Phi(\boldsymbol{x}) \text{ holds}\}|}{|X|^n}.$$

Moreover, $\mathbb{F}_q$ will denote a finite field of order q in characteristic p.

1.1. Random generation by two elements.

1.1.1. *Two random elements.* In 1969, Dixon [Dix69] proved Netto's conjecture that two random even permutations generate the alternating group A_n with probability 1 as $n \to \infty$, i.e.

$$P\Big(\langle x, y\rangle = A_n : x, y \in A_n\Big) \to 1.$$

He further conjectured that the same should hold true for any finite simple group G as $|G| \to \infty$, which was shown by Kantor and Lubotzky [KL90a] for a finite classical group, and extended by Liebeck and Shalev [LS95] to all finite simple groups. Their method is based on the classification of maximal subgroups of the finite simple groups by Aschbacher [Asc84], and relies on the classification of finite simple groups.

1.1.2. *One random element, one fixed.* A variant is to fix one of the two elements, as done by Guralnick, Kantor and Saxl [GKS94] for a quasisimple classical group G over $\mathbb{F}_q$ (see also [Sha98] and [MSW94]): for any $x \in G$,

$$P\Big(\langle x, y\rangle = G : y \in G\Big) \to 1 \text{ as } q \to \infty.$$

Date: May 6, 2018.

1.2. **Invariant generation.** A stronger condition on a set of group generators is that any conjugates of the generators remain generators; these are called *invariant generators*.

Usually, a generating set will *not* generate the group invariably. Actually, any generating set generates the group invariably if and only if the group is nilpotent (see [KLS11, Proposition 2.4]).

Kantor, Lubotzky and Shalev [KLS11] have shown that every finite (resp. nonabelian finite simple) group G is invariably generated (resp. invariably generated with respect to $\mathrm{Aut}(G)$) by $\leqslant \log_2 |G|$ (resp. 2) elements. This uses Singer cycles and the results of [MSW94] on the classification of maximal subgroups containing such elements. In the case of simple groups, see also [GS03, Theorem 1.3].

1.2.1. *Invariant generation by random elements.* This notion is particularly relevant when one tries to determine Galois groups (say of the splitting field of an integer polynomial) from conjugacy classes.

As explained in [KZ12], this leads to the definition of the *Chebotarev invariant* of a finite group G: the expected minimal size of a random subset that generates G invariably. Kantor, Lubotzky and Shalev [KLS11] showed that this invariant is $\ll (|G| \log |G|)^{1/2}$, with an absolute implied constant.

By Fulman and Guralnick [FG03, Theorem 5.3] that if G is a fixed type of simple algebraic group, a large enough number of elements of $G(\mathbb{F}_q)$ are almost surely invariants generators.

In the case of only two generators, Niemeier and Praeger [NP98, Theorem 10.1] obtained that for most classical groups G over $\mathbb{F}_q$, a positive proportion of pairs $(x, y) \in G^2$ are "invariant generators modulo obstruction", i.e. for every $g, h \in G$, if $H = \langle x^g, y^h \rangle$ is irreducible, then $H = G$.

1.3. **Invariant generation with a fixed class.** Alternatively, one may fix a (generating) subset and ask how many conjugates remain generators, leading more generally to:

Question 1.1. Given a fixed subset S of a finite group G and $A \subset \mathrm{Aut}(G)$, what is

$$P\Big(\langle f(s)(a) : s \in S\rangle = G : f : S \to A\Big) \quad \text{as } |G| \to \infty \ ?$$

When S has two elements x, y and A is conjugation by the elements of G, this is simply $P(\langle x, y^g\rangle = G : g \in G)$.

1.3.1. *Results with Singer cycles.* Kantor [Kan94] showed that for $n \geqslant 4$, a Singer cycle $s \in G = \mathrm{PSL}_n(\mathbb{F}_q)$ (an element of maximal order $\frac{q^n-1}{q-1}$), and every $1 \neq g \in G$, we have

$$P\Big(\langle g, s^h\rangle = G : h \in G\Big) \geqslant \left(1 - \frac{1}{q} - \frac{1}{q^{n-1}}\right)^2.$$

Earlier, Shalev [Sha98] also proved that a Singer cycle and a random element generate $\mathrm{GL}_n(\mathbb{F}_q)$ invariably with probability tending to 1 when $q \to \infty$.

Kantor's result was in particular extended to any almost simple group G by Guralnick and Kantor [GK00, Theorem I], also with Singer cycles in the

case of classical groups: there exists $s \in G$ such that for any $1 \neq g \in G$,

$$P\Big(\langle g, s^h\rangle = O_\infty(G) : h \in G\Big) \to 1$$

as $|G| \to +\infty$, where $O_\infty(G)$ is the last element in the derived series (G itself for $G = \mathrm{SL}_n(\mathbb{F}_q)$ or $\mathrm{Sp}_n(\mathbb{F}_q)$). The arguments are deep and rely on the classification of finite simple groups, but it is mentioned [GK00, p. 789] that for classical groups, it is possible to proceed by entirely geometric arguments as in [Kan94], by carefully choosing s (of large order).

1.4. **Invariant generation with a regular unipotent.** The goal of this note is to give a variant of the result of Guralnick and Kantor, in the cases $G = \mathrm{SL}_n(\mathbb{F}_q)$ or $\mathrm{Sp}_{2n}(\mathbb{F}_q)$, with the Singer cycle s replaced by a *regular unipotent*, i.e. conjugate to the single unipotent Jordan block

$$u = \begin{pmatrix} 1 & 1 & & \\ & 1 & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}. \tag{1}$$

We note that:

(1) Such an element always exist by [LS12, Corollary 3.6].
(2) If[1] $p \gg_n 1$, such an element in $\mathrm{GL}_n(\mathbb{F}_q)$ has order p by Lucas' theorem on the divisibility of binomial coefficients, which is much smaller than that of a Singer cycle.

1.4.1. *Generation.* This consideration is motivated by the following: As a particular example of Steinberg's result on the generation of finite simple groups of Lie type by two elements [Ste62], Gow and Tamburini [GT92] showed[2] that when n is odd, $\mathrm{SL}_n(\mathbb{F}_p)$ is generated by u and the permutation matrix

$$m = (-1)^{\frac{n-1}{2}} \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

Numerical experiments show that u and m are *not* invariant generators: the pair $(h^{-1}uh, m)$ generates $\mathrm{SL}_3(\mathbb{F}_3)$ for only about 31% of the elements $h \in \mathrm{GL}_3(\mathbb{F}_3)$. However, this proportion increases to about 86% for $\mathrm{SL}_3(\mathbb{F}_{23})$.

1.4.2. *Random invariant generation.* We will show the following:

Theorem 1.2. *Let $k = \mathbb{F}_q$ be a finite field of characteristic p. For $n \geqslant 2$, let*

$$G = \mathrm{SL}_n(k)\ (n \geqslant 2) \quad \textit{or} \quad G = \mathrm{Sp}_n(k)\ (n \geqslant 2 \textit{ even}).$$

[1] In the following, we will write $p \gg_n 1$ (resp. $p \ll_n 1$) for the condition of p being large (resp. small) enough with respect to n.

[2] More generally, they show that u and its transpose generate $\mathrm{SL}_n(\mathbb{F}_p)$ for any $n \geqslant 2$ and p prime, unless $(p, n) = (2, 4)$.

Let $u \in G$ be a unipotent element with a single Jordan block, and let $m \in G$ be nonscalar. Then, if $p \gg_n 1$, the elements u, m invariably generate G with probability 1 as $|k| \to \infty$, that is to say

$$P\Big(\langle m, u^g\rangle = G : g \in G\Big) \quad = \quad 1 - O_n\left(\frac{1}{|k|}\right).$$

If m acts cyclically[3] *on k^n and $n \geqslant 4$, then this can be improved to*

$$1 - O_n\left(\frac{1}{|k|^{n-1}}\right).$$

Remarks 1.3. (1) Even if u, m are defined over $\mathbb{F}_p$, conjugating with elements defined over k allows to generate the full group, and not only a subfield subgroup.

(2) The proof does not depend on the classification of finite simple groups.

2. Bound via maximal subgroups

In the setting of Theorem 1.2, let $G = \mathrm{SL}_n$ ($n \geqslant 2$) or $G = \mathrm{Sp}_n$ ($n \geqslant 2$ even), and

$$\begin{aligned} P_n(k) &= P\Big(\langle m, u^g\rangle = G(k) : g \in G(k)\Big), \\ P_n^c(k) &= 1 - P_n(k). \end{aligned}$$

The goal is to find a lower bound for $P_n^c(k)$ as $|k| \to \infty$.

We use the following classical method: if $\langle m, u^g\rangle$ is a proper subgroup of $G(k)$ for some $g \in G(k)$, then it is contained in a maximal subgroup $H \lneq G(k)$. Hence,

$$P_n^c(k) \leqslant \sum_{\substack{m \in H \lneq G(k) \\ \text{maximal}}} P\Big(u^g \in H : g \in G(k)\Big) \text{ and} \tag{2}$$

$$P_n^c(k) \leqslant \sum_{\substack{u \in H \lneq G(k) \\ \text{maximal}}} P\Big(m^g \in H : g \in G(k)\Big). \tag{3}$$

2.1. **Classification of maximal subgroups.** A major input due to Aschbacher and Kleidman-Liebeck is then that the maximal subgroups of $G(k)$ belong to one of the following classes (see [KL90b]), assuming $p \geqslant 3$:

- Groups in $\mathcal{C}_1$ are subspace stabilizers $\mathrm{Stab}_{G(k)}(W)$ for $0 \neq W \lneq k^n$. If $G = \mathrm{Sp}_n$, W is either nondegenerate or totally isotropic.
- Groups in $\mathcal{C}_2$ (resp. $\mathcal{C}_3$, $\mathcal{C}_4$) are stabilizers of orthogonal (resp. singular, tensor product) decompositions.
- Groups in $\mathcal{C}_5$ are symplectic-type r-subgroups.
- Groups in $\mathcal{C}_6$ are normalizers of classical groups, that only appear if $G = \mathrm{SL}_n$: $N_{G(k)}(\mathrm{Sp}_n(k))$, $N_{G(k)}(\mathrm{SO}_n(k))$, or $N_{G(k)}(\mathrm{SU}(k'))$ for $k' \leqslant k$ a subfield with $|k'| = |k|^{1/2}$.
- Groups $\mathcal{C}_7$ are subfield subgroups: $N_{G(k)}(G(k'))$ for $k' \leqslant k$ of prime index.

[3] i.e. there exists $v \in k^n$ such that $k^n = \mathrm{span}(m^i v : i \geqslant 0)$.

– Groups in $\mathcal{A}(S)$ are maximal subgroups H with

$$\begin{array}{ccccc} S = \pi(T) & \trianglelefteq & \pi(H) & \leqslant & \mathrm{Aut}(S) \\ \uparrow & & \uparrow & & \\ T & \trianglelefteq & H & & \end{array} \tag{4}$$

for a finite simple group S, $\pi : \mathrm{GL}_n(k) \to \mathrm{PGL}_n(k)$ the projection, such that the action of $T \trianglelefteq H \leqslant G(k)$ on $\overline{k}^n$ is irreducible and preserves no nondegenerate bilinear or unitary form.

2.2. **Maximal subgroups containing regular unipotents.** It turns out that some of the classes can be excluded if the subgroup contains a unipotent element with a single Jordan block.

Proposition 2.1. *If* $H \in \bigcup_{i=2}^{5} \mathcal{C}_i$ *and* $p \gg_n 1$*, then*

$$P\Big(u^g \in H : g \in G(k)\Big) = 0. \tag{5}$$

Proof. One can see elementarily (cf. [SS97, pp. 374–375], [Cra17, Section 2] and [PG18, Proposition 6.7]) that if H contains an element with a single Jordan block, then $p \leqslant n$ (if $H \in \mathcal{C}_2 \cup \mathcal{C}_3$), $p \leqslant 3$ (if $H \in \mathcal{C}_4$) or $p \leqslant n^{2\log_2(n)}$ (if $H \in \mathcal{C}_5$). Hence, these classes are excluded if $p \gg_n 1$. □

On the other hand, for the maximal subgroups in class $\mathcal{A}$, we have:

Theorem 2.2. *Let* $S = \pi(T) \in \mathrm{PGL}_n(k)$ *as above be simple and let* $H \in \mathcal{A}(S)$*. If* $p \gg_n$*, then*

$$P\Big(u^g \in H : g \in G(k)\Big) = 0$$

This is either:

– In [Cra17], a classification of irreducible subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$ containing an element with exactly one nontrivial Jordan block is obtained; Theorem 2.2 can be deducted from op. cit. Sections 4–10.
– In [PG18, Section 6.5], using a result of Larsen-Pink [LP11, Theorem 0.2] to reduce to groups of Lie type in the same characteristic, work of Liebeck on minimal dimensions of faithful irreducible modular representations, and the descent of a classification result of Suprunenko through a theorem of Seitz-Testerman.

Thanks to the result of Larsen-Pink, the classification of finite simple groups does not need to be used in either case (in the first one, use [Cra17, Section 5] after applying [LP11, Theorem 0.2]).

2.3. **The bounds of Liebeck and Saxl.** It is a deep result of Liebeck and Saxl [LS91] (see also [GK00, Theorem 2.3]) that if $n \geqslant 3$, then for any $x \in G(k)$ and any maximal subgroup H as above,

$$P\Big(x^g \in H : g \in G(k)\Big) \ll 1/|k|. \tag{6}$$

This is most difficult when H is in class $\mathcal{A}$.

By Equation (3) and (6), it is then clear that $P_n^c(k) \to 0$ as $|k| \to +\infty$ if u is contained in only $o(|k|)$ many maximal subgroups.

The strategy of Guralnick and Kantor in [GK00] for classical groups (see Section 1.3.1 above) is indeed to choose an element that is contained in $O(1)$ maximal subgroups.

2.3.1. *Case of regular unipotents in G.*

Proposition 2.3. *A regular unipotent element u in $G(k)$ is contained in $O_n(\log\log|k|)$ maximal subgroups.*

Proof. By the classification recalled in Section 2, Proposition 2.1 and Theorem 2.2, a regular unipotent u is contained in

$$\begin{aligned} & |\{0 \neq W \lneq k^n : uW = W\}| + \omega([k:\mathbb{F}_p]) + O(1) \\ \ll\ & |\{0 \neq W \lneq k^n : uW = W\}| + \log\log|k| \end{aligned}$$

maximal subgroups when $p \gg_n 1$, where ω denotes the number of prime factors function. Moreover, u has only one invariant subspace per dimension (namely $\mathrm{span}(e_1,\dots,e_d)$ for $0 \leqslant d \leqslant n$ if u is in the basis (1)). □

By Equation (3) and bound (6), this shows that

$$P_n^c(k) \ll_n \frac{\log\log|k|}{|k|},$$

which is Theorem 1.2 with an additional logarithm factor.

However, when x is a regular unipotent element, it is possible to estimate the probabilities (6) easily from the classification reviewed in Section 2.2 and the fact that the centralizers are small. Thus, instead of using (3), we will use (2) to obtain Theorem 1.2 with the smaller error terms.

3. Contribution of classes $\mathcal{C}_6$ and $\mathcal{C}_7$

In what follows, we shall use that for any set $H \subset G(k)$,

$$\begin{aligned} P\Big(u^g \in H : g \in G(k)\Big) &= \sum_{h\in H} P\Big(u^g = h : g \in G(k)\Big) \\ &\leqslant |H|\frac{|C_{G(k)}(u)|}{|G(k)|} \ll_n \frac{|H|}{|k|^{\dim G - n + 1}}, \end{aligned} \tag{7}$$

along with the formulas for the orders of finite groups of Lie type ([KL90b, Chapter 2]).

3.1. Class $\mathcal{C}_6$.

Proposition 3.1. *We have*

$$\begin{aligned} P\Big(u^g \in N_{\mathrm{SL}_n(k)}(\mathrm{Sp}_n(k)) : g \in \mathrm{SL}_n(k)\Big) &\ll_n |k|^{-\frac{n(n-3)}{2}}, \\ P\Big(u^g \in N_{\mathrm{SL}_n(k)}(\mathrm{SO}_n(k)) : g \in \mathrm{SL}_n(k)\Big) &\ll_n |k|^{-\frac{n(n-1)}{2}}, \\ P\Big(u^g \in N_{\mathrm{SL}_n(k)}(\mathrm{SU}_n(k')) : g \in \mathrm{SL}_n(k)\Big) &\ll_n |k|^{-\frac{(n-1)^2}{2}}, \end{aligned}$$

where $k' \leqslant k$ is a subfield with $|k'| = |k|^{1/2}$ in the second case.

Proof. By [KL90b, (2.6.2), (2.3.3), Cor. 2.10.4, Prop. 2.10.6, Prop. 4.8.3, Prop. 4.8.5],

$$\begin{aligned} N_{\mathrm{SL}_n(k)}(\mathrm{Sp}_n(k)) &\cong \mu_n(k) \times \mathrm{Sp}_n(k) \\ N_{\mathrm{SL}_n(k)}(\mathrm{SO}_n(k)) &\cong \mu_n(k) \times \mathrm{SO}_n(k) \\ N_{\mathrm{SL}_n(k)}(\mathrm{SU}_n(k')) &\cong \mu_n(k) \times \mathrm{SU}_n(k'), \end{aligned}$$

if $k' \leqslant k$ is a subfield with $|k'| = |k|^{1/2}$ in the last case. Thus,

$$\begin{aligned} |N_{\mathrm{SL}_n(k)}(\mathrm{Sp}_n(k))| &\ll_n |k|^{\frac{n(n+1)}{2}}, \\ |N_{\mathrm{SL}_n(k)}(\mathrm{SO}_n(k))| &\ll_n |k|^{\frac{n(n-1)}{2}}, \\ |N_{\mathrm{SL}_n(k)}(\mathrm{SU}_n(k'))| &\ll_n |k|^{\frac{n^2-1}{2}}, \end{aligned}$$

which gives the result using (7). □

3.2. **Class $\mathcal{C}_7$.**

Proposition 3.2. *For $k' \leqslant k$ a proper subfield,*

$$P\Big(u^g \in N_{G(k)}(G(k')) : g \in G(k)\Big) \ll_n \begin{cases} |k|^{-\frac{\dim G}{2}+n-1} & n \geqslant 3 \\ 1/|k|^2 & n = 2. \end{cases}$$

Proof. By [KL90b, Prop. 4.5.3–4],

$$N_{G(k)}(G(k')) = \mu_n(k)G(k') \cong \big(\mu_n(k)/\mu_n(k')\big) \times G(k'),$$

so by (7) the probability is

$$\ll_n |k|^{-\dim G\left(1-\frac{1}{[k:k']}\right)+n-1} \leqslant |k|^{-\frac{\dim G}{2}+n-1}.$$

The case $n = 2$ is verified by hand. □

4. Contribution of class $\mathcal{C}_1$

The total contribution to $P_n^c(k)$ of maximal subgroups in class $\mathcal{C}_1$ is

$$\sum_{d=1}^{n-1} |\{0 \neq W \lneq k^n : mW = m\}| P\Big(u^g \in \mathrm{Stab}_{G(k)}(W) : g \in G(k)\Big). \tag{8}$$

4.1. **Upper bound on the probabilities.**

Proposition 4.1. *For $W \leqslant k^n$ a subspace of dimension d and $H = \mathrm{Stab}_{G(k)}(W)$, we have*

$$P\Big(u^g \in H : g \in G(k)\Big) \ll_n \begin{cases} |k|^{-d(n-d)} & : G = \mathrm{SL}_n \\ |k|^{-d(n-d)} & : G = \mathrm{Sp}_n,\ W \text{ nondegenerate} \\ |k|^{\frac{-d(2n+1-3d)}{2}-1} & : G = \mathrm{Sp}_n,\ W \text{ tot. isotropic.} \end{cases}$$

Proof. Let d be the dimension of W. By definition, $u^g \in H = \mathrm{Stab}_{G(k)}(W)$ if and only if $u \in \mathrm{Stab}_{G(k)}(g^{-1}W)$. Since u has exactly one invariant subspace W_d of any dimension $0 \leqslant d \leqslant n$,

$$\begin{aligned} P\Big(u^g \in H : g \in G(k)\Big) &= P\left(g^{-1}W = W_d : g \in G(k)\right) \\ &= \frac{|\{g \in G(k) : g^{-1}W = W_d\}|}{|G(k)|} \end{aligned}$$

If $G = \mathrm{SL}_n$, then

$$P\Big(u^g \in H : g \in G(k)\Big) \ll_n \frac{|k|^{d^2+(n-d)n-1}}{|k|^{n^2-1}} = |k|^{-d(n-d)}.$$

If $G = \mathrm{Sp}_n$, then W is assumed to be nondegenerate or totally isotropic. In the first case, an element $g \in G(k)$ such that $g^{-1}W = W_d$ is determined by an element of $\mathrm{Sp}_d(k) \times \mathrm{Sp}_{n-d}(k)$, so that the probability is

$$\ll_n \frac{|k|^{\dim \mathrm{Sp}_d + \dim \mathrm{Sp}_{n-d}}}{|k|^{\dim \mathrm{Sp}_n}} = |k|^{-d(n-d)}.$$

In the totally isotropic case, $g \in G(k)$ such that $g^{-1}W = W_d$ is determined by an element of $\mathrm{Sp}_{n-d}(k)$ and an element of $\mathrm{SL}_d(k)$, so that the probability is

$$\ll_n \frac{|k|^{\dim \mathrm{SL}_d + \dim \mathrm{Sp}_{n-d}}}{|k|^{\dim \mathrm{Sp}_n}} \leqslant |k|^{\frac{-d(2n+1-3d)}{2}-1}.$$

□

4.2. **Number of invariant subspaces.** The number of subspaces $W \leqslant k^n$ of dimension $0 \leqslant d \leqslant n$ is

$$\binom{n}{d}_{|k|} \leqslant \left(\frac{1}{1-1/|k|}\right)^d |k|^{d(n-d)}.$$

Hence, Proposition 4.1 with the trivial bound for the cardinality in (8) gives a contribution of $O(1)$, and we need to exploit the condition $mW = W$ to obtain a smaller error. This is obtained through the following:

Proposition 4.2. *Let $g \in \mathrm{GL}_n(k)$ and let $\sigma_d(g)$ be the number of g-invariant subspaces of k^n of fixed dimension $1 \leqslant d \leqslant n$.*

(1) If g acts cyclically on k^n, then $\sigma_d(g) \ll_n 1$.
(2) If g is not scalar, then

$$\sigma_d(g) \ll_n |k|^{d(n-d)-1}.$$

Remarks 4.3. (1) Such bounds can be found in [GK00, 3.1–7, 3.15–16], with improved savings when $d > 1$ or when $n \geqslant 6$ if W is supposed to be totally isotropic or nondegenerate for some symplectic form. However, these savings would eventually not improve the error terms in 1.2, so that we seize the opportunity to give an alternative proof of Proposition 4.2 below.

(2) The number of invariant subspaces of given dimension with respect to a fixed linear map was determined in great generality in [Fri11], but it is not easy to derivate upper bounds from there.

4.2.1. *Cyclic case.* If k^n is cyclic under $g \in \mathrm{GL}_n(k)$, then k^n is isomorphic to $k[X]/(\min(\varphi))$ as $k[x]/(\min(g))$-module and g-invariant subspaces correspond to divisors of $\min(g)$. In particular, the number of g-invariant subspaces is $\ll_n 1$.

4.2.2. *Semisimple case.* Let us assume that $g \in \mathrm{GL}_n(k)$ is semisimple, with minimal polynomial $\min(g) = \prod_{i=1}^s f_i$ ($f_i \in k[X]$ irreducible). There are primary and cyclic decomposition

$$k^n = \bigoplus_{i=1}^s V_i \text{ with } V_i = \ker\left(f_i(T)\right) \cong k_i^{r_i} \text{ and } k_i = k[X]/(f_i).$$

Lemma 4.4. *In the above notations,*

$$\sigma_d(g) = \sum_{\substack{d_1+\cdots+d_s=d \\ \deg(f_i)|d_i}} \prod_{i=1}^s \binom{\dim(V_i)/\deg(f_i)}{d_i/\deg(f_i)}_{|k|^{\deg(f_i)}}.$$

Proof. By [BF67, Lemma 1], $\sigma_d(g) = \prod_{i=1}^s \sigma_d(g\mid_{V_i})$. There is a correspondence between g-invariant subspaces and submodules $W \leqslant k_i^{r_i}$, with W corresponding to a subspace of dimension $\dim_{k_i}(W)[k:k_i] = \dim_{k_i}(W)\deg(f_i)$. Hence,

$$\sigma_d(g\mid_{V_i}) = \begin{cases} \binom{r_i}{d/\deg(f_i)}_{|k_i|} & \deg(f_i) \mid d \\ 0 & \text{otherwise.} \end{cases}$$

□

Lemma 4.5. *If g is not scalar, then $\sigma_d(g) \ll_n |k|^{d(n-d)-1}$.*

Proof. Using that

$$\binom{n}{m}_q = \prod_{i=1}^m \frac{q^{n-i+1}}{q^i-1} \leqslant 2^m q^{m(n-m)},$$

we obtain

$$\sigma_d(g) \ll_n \sum_{\substack{d_1+\cdots+d_s=d \\ \deg(f_i)|d_i}} |k|^{\sum_{i=1}^s \frac{d_i}{\deg(f_i)}(\dim(V_i)-d_i)}.$$

Then the conclusion holds as soon as

$$\sum_{i=1}^s d_i \left[(\dim(V_i)-d_i)(\deg(f_i)^{-1}-1) - \sum_{\substack{j=1 \\ j\neq i}}^s (\dim(V_j)-d_j) \right] < 0$$

for all $0 \leqslant d_1, \ldots, d_s \leqslant d$ such that $d_1 + \cdots + d_s = d$ and $\deg(f_i) \mid d_i$. This is verified if there exists $1 \leqslant i \leqslant s$ with $d_i \neq 0$ and either

(1) $\deg(f_i) \geqslant 2$, or
(2) $\deg(f_i) = 1$ and there exists $j \neq i$ with $d_j < \dim(V_j)$.

If $\deg(f_i) = 1$ for every i with $d_i \neq 0$ and $\{i : d_i \neq 0\} = \{j : d_j < \dim(V_j)\}$ is a singleton, then $s = 1$, $k^n = V_1$ is primary, and g has minimal polynomial of degree 1, i.e. it is scalar.

□

4.2.3. *Non-unipotent case.* By the Jordan-Chevalley decomposition, if $g \in \mathrm{GL}_n(k)$ leaves W invariant, then W is also left invariant by the semisimple part of g. If the latter is nontrivial, we can use Section 4.2.2. Thus, it remains to handle the case where g is unipotent.

In this case, there is a decomposition $V = \oplus_{i=1}^r V_i$ such that $g|_{V_i}$ is cyclic, with minimal polynomial $(T-1)^{m_i}$, such that $m_1 \leqslant \cdots \leqslant m_r$. Similarly, an invariant subspace W of dimension d has a cyclic decomposition $W = \oplus_{i=1}^s W_i$, with $\min(g|_{W_i}) = (T-1)^{m_i'}$, and $m_1' \leqslant \cdots \leqslant m_s'$ a subsequence of $m_1 \leqslant \cdots \leqslant m_r$ satisfying $d = \sum_{i=1}^s m_i' \geqslant s$. Thus, there are

$$\ll_n |k|^s \leqslant |k|^d$$

such subspaces. If $2 \leqslant d \leqslant n-1$, or if $n \geqslant 3$, this satisfies the required bound. The case $n = 2$ and $d = 1$ is excluded, since a primary cyclic invariant subspace has an invariant complement.

4.3. **Total contribution.** Thus, we find that the total contribution (8) is:

In the special linear case,

$$\ll_n \sum_{d=1}^{n-1} \sigma_d(m)|k|^{-d(n-d)} \ll_n \frac{1}{|k|},$$

which can be improved to $|k|^{-(n-1)}$ if m acts cyclically.

In the symplectic case (assuming $n \geqslant 4$ even), noting that a totally isotropic subspace is contained in one of the two maximal isotropic subspaces U_1, U_2 of dimension $n/2$,

$$\begin{aligned} &\ll_n \sum_{d=1}^{n-1} \sigma_d(m)|k|^{-d(n-d)} + \sum_{d=1}^{n/2}\sum_{i=1}^{2} \sigma_d(m\,|_{U_i})|k|^{-\frac{d(2n+1-3d)}{2}-1} \\ &\ll_n \sum_{d=1}^{n-1} |k|^{-1} + \sum_{d=1}^{n/2} |k|^{-\frac{d(n+1-d)}{2}-2} \ll_n \frac{1}{|k|} + \frac{1}{|k|^{n/2+2}} \ll \frac{1}{|k|}. \end{aligned}$$

If m acts cyclically, this can be improved to $|k|^{-(n-1)}$.

5. Proof of Theorem 1.2

By (2), Propositions 2.1, 3.1, 3.2, Section 4.3 and Theorem 2.2, we get that for $p \gg_n 1$,

$$\begin{aligned} P_n^c(k) &\ll_n \frac{1}{|k|} + \delta_{G=\mathrm{SL}_n}\left(\frac{\delta_{n\geqslant 4 \text{ even}}}{|k|^{\frac{n(n-3)}{2}}} + \frac{1}{|k|^{\frac{(n-1)^2}{2}}}\right) \\ &\quad + \delta_{k\neq\mathbb{F}_p}\frac{\omega([k:\mathbb{F}_p])}{|k|^{\max(2,\dim G/2-n+1)}} \\ &\ll \frac{1}{|k|}. \end{aligned}$$

If m acts cyclically and $n \geqslant 4$, this can be improved to

$$P_n^c(k) \ll 1/|k|^{n-1}.$$

References

[Asc84] Michael Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones mathematicae*, 76(3):469–514, 1984.

[BF67] Louis Brickman and Peter A. Fillmore. The invariant subspace lattice of a linear transformation. *Canadian Journal of Mathematics*, 19:810–822, 1967.

[Cra17] David A. Craven. Groups with a p-element acting with a single non-trivial Jordan block on a simple module in characteristic p. 2017.

[Dix69] John D. Dixon. The probability of generating the symmetric group. *Mathematische Zeitschrift*, 110:199–205, 1969.

[FG03] Jason Fulman and Robert Guralnick. Derangements in simple and primitive groups. *Groups, Combinatorics and Geometry (Durham, 2001)*, pages 99–121, 2003.

[Fri11] Harald Fripertinger. The number of invariant subspaces under a linear operator on finite vector spaces. *Adv. in Math. of Comm.*, 5(2):407–416, 2011.

[GK00] Robert M. Guralnick and William M. Kantor. Probabilistic Generation of Finite Simple Groups. *Journal of Algebra*, 234(2):743 – 792, 2000.

[GKS94] Robert M. Guralnick, William M. Kantor, and Jan Saxl. The probability of generating a classical group. *Communications in Algebra*, 22(4):1395–1402, 1994.

[GS03] Robert M. Guralnick and Jan Saxl. Generation of finite almost simple groups by conjugates. *Journal of Algebra*, 268(2):519–571, 2003.

[GT92] R. Gow and Maria Chiara Tamburini. Generation of $\mathrm{SL}(n, p)$ by two Jordan block matrices. *Bollettino dell'Unione Matematica Italiana*, 7(6A):346–357, 1992.

[Kan94] William M. Kantor. Finite geometry for a generation. *Bull. Belg. Math. Soc*, 3:423–426, 1994.

[KL90a] William M. Kantor and Alexander Lubotzky. The probability of generating a finite classical group. *Geometriae Dedicata*, 36(1):67–87, 1990.

[KL90b] Peter B. Kleidman and Martin W. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Notes*. Cambridge University Press, 1990.

[KLS11] William M. Kantor, Alexander Lubotzky, and Aner Shalev. Invariable generation and the Chebotarev invariant of a finite group. *Journal of Algebra*, 348(1):302–314, 2011.

[KZ12] Emmanuel Kowalski and David Zywina. The Chebotarev Invariant of a Finite Group. *Experimental Mathematics*, 21(1):38–56, 2012.

[LP11] Michael Larsen and Richard Pink. Finite subgroups of algebraic groups. *Journal of the American Mathematical Society*, 24(4):1105–1158, 2011.

[LS91] Martin W. Liebeck and Jan Saxl. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proceedings of the London Mathematical Society*, 3(2):266–314, 1991.

[LS95] Martin W. Liebeck and Aner Shalev. The probability of generating a finite simple group. *Geometriae dedicata*, 56(1):103–113, 1995.

[LS12] Martin W. Liebeck and Gary M. Seitz. *Unipotent and Nilpotent Classes in Simple Algebraic Groups and Lie Algebras*. Mathematical surveys and monographs. American Mathematical Soc., 2012.

[MSW94] Gunter Malle, Jan Saxl, and Thomas Weigel. Generation of classical groups. *Geometriae Dedicata*, 49(1):85–116, 1994.

[NP98] Alice C. Niemeyer and Cheryl E. Praeger. A Recognition Algorithm for Classical Groups over Finite Fields. *Proc. London Math. Soc*, 3:117–169, 1998.

[PG18] Corentin Perret-Gentil. Integral monodromy groups of Kloosterman sheaves. *Mathematika*, 2018. To appear.

[Sha98] Aner Shalev. A Theorem on Random Matrices and Some Applications. *Journal of Algebra*, 199(1):124 – 141, 1998.

[SS97] Jan Saxl and Gary M. Seitz. Subgroups of algebraic groups containing regular unipotent elements. *Journal of the London Mathematical Society*, 55(02):370–386, 1997.

[Ste62] Robert Steinberg. Generators for simple groups. *Canadian Journal of Mathematics*, 14:277–283, January 1962.

Centre de Recherches Mathématiques, Université de Montréal, Canada
Email address: corentin.perretgentil@gmail.com