Experimental Mathematics, 21(1):38–56, 2012

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2011.565261

Taylor & Francis
Taylor & Francis Group

The Chebotarev Invariant of a Finite Group

Emmanuel Kowalski and David Zywina

CONTENTS

2000 AMS Subject Classification: 20P05, 20Dxx, 20K01, 20F69, 60Bxx
Keywords: Chebotarev density theorem, coupon collector problems, Galois group, conjugacy classes generating a group, probabilistic group theory

We consider invariants of a finite group related to the number of random (independent, uniformly distributed) conjugacy classes that are required to generate it. These invariants are intuitively related to problems of Galois theory. We find group-theoretic expressions for them and investigate their values both theoretically and numerically.

1. INTRODUCTION

A well-known method to compute the Galois group H of a number field (e.g., of the splitting field of a polynomial $P \in \mathbb{Z}[T]$ with integral coefficients) can be described roughly as follows: (1) find a group G that contains H, e.g., of symmetry considerations (such as the fact that the field generated by the ℓ-torsion points of an elliptic curve has Galois group that embeds in $\mathrm{GL}(2, \mathbb{F}_\ell)$); (2) try to prove that $H = G$ by computing the Frobenius automorphisms modulo successive primes, which gives *conjugacy classes* in the Galois group H, and hence conjugacy classes in G. If the guess in (1) was right, and if the conjugacy classes observed in (2) are compatible only with the Galois group being our candidate G, then we have succeeded.

This method is particularly simple when G is "guessed" to be the symmetric group acting on the roots of a polynomial P, since the Frobenius conjugacy class in the symmetric group can be read off quickly from the factorization pattern of P modulo primes.

In practice, however, this is not very efficient; computer algebra systems use other techniques. Still, this method is well suited for certain theoretical investigations, for instance, for probabilistic Galois theory (see, e.g., [Gallagher 73]), and it can be surprisingly efficient even for fairly complicated groups (see our joint works [Jouve et al. 08, Jouve et al. 10] with F. Jouve, involving the Weyl group of a reductive algebraic group; this led to the first explicit examples of integral polynomials with Galois group $W(E_8)$.)

In view of this, it is somewhat surprising that no general study of the efficiency of the underlying algorithm seems to have been performed. Among the very few references we know is [Dixon 92], which considers symmetric groups $\mathfrak{S}_n$ and mentions some earlier work of McKay.[1] On the other hand, there has been a fair amount of interest in the question of determining the probability that a tuple of elements generates a finite group, which is the analogous problem in which conjugacy is ignored; see, for instance, [Kantor and Lubotzky 90]. The paper [Pomerance 01] considers the question for abelian groups, when the conjugacy issue is also irrelevant, and those results do apply to our setting. The current paper provides the beginning of the theoretical analysis of this type of algorithm for general finite groups. Specifically, we prove the following result (Theorem 6.1 gives the precise statement using the definitions of Section 2).

Theorem 1.1. (Boundedness of Chebotarev invariants for symmetric groups.) *There exists a constant $c > 0$ such that for all integers $n \geq 1$, the average number of independently and randomly chosen conjugacy classes*[2] *of the symmetric group $\mathfrak{S}_n$ that one must pick to ensure that any tuple of elements taken from each of these classes generate $\mathfrak{S}_n$ is at most c. In fact, for any $k \geq 1$, there exists $c_k \geq 0$ such that the average of the kth power of this number is bounded by c_k for all n.*

Here is a rough outline of this work: We consider probabilistic models in Section 2 and define invariants, which we call the *Chebotarev invariants*, of a finite group using such a model (the name, based on the Chebotarev density theorem, is justified in Section 8); it makes precise the informal notion in the statement of Theorem 1.1 and takes into account information about mean-square averages.

In Section 3, we indicate how to compute this invariant for abelian groups (based on Pomerance's work), and in Section 4, we consider solvable groups of a certain "extremal" type. In Sections 5, 6, and 7, we consider theoretical and numerical examples for nonabelian, often nonsolvable, groups, in particular alternating and symmetric groups, proving Theorem 1.1. Finally, Section 8 makes some informal remarks concerning the applicability of our results to arithmetic situations (our original motivation). A longer version of this paper is available from arXiv; see [Kowalski and Zywina 11]. It includes more data, questions, and remarks, and details of some computations that are not included in full here.

Notation 1.2. As usual, $|X|$ denotes the cardinality of a set, and $\mathbb{F}_q$ a field with q elements. If G is a finite group and $H \subset G$, we write $\nu_G(H) = \nu(H) = |H|/|G|$. We write $G^\sharp$ for the set of conjugacy classes of G, and for $C \subset G^\sharp$, we also write $\nu_G(C)$ or $\nu(C)$ for $\nu(\tilde{C})$, where $\tilde{C} \subset G$ is the union of all conjugacy classes in C.

We recall that a geometric random variable X with parameter $p \in [0,1]$ on a probability space is a random variable taking values in the set of positive integers almost surely, with

$$\mathbf{P}(X = k) = p(1-p)^{k-1} \tag{1–1}$$

for $k \geq 1$. We then have

$$\begin{aligned} \mathbf{E}(X) &= p \sum_{k \geq 1} k(1-p)^{k-1} = p^{-1}, \\ \mathbf{E}(X^2) &= (2-p)/p^2, \\ \mathbf{V}(X) &= (1-p)/p^2. \end{aligned} \tag{1–2}$$

By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geq 0$ such that $|f(x)| \leq Cg(x)$ for all $x \in X$. The "implied constant" refers to any value of C for which this holds. Similarly, $f \asymp g$ means that $f \ll g$ and $g \ll f$. On the other hand, $f(x) \sim g(x)$ as $x \to x_0$ means that $f(x)/g(x) \to 1$ as $x \to x_0$.

2. THE CHEBOTAREV INVARIANT OF A FINITE GROUP

In this section, we describe a natural probabilistic model for the recognition algorithm described previously. Fix a finite group G. We first remark that whereas it does not make sense to say that a conjugacy class lies in a certain subgroup unless the latter is a normal subgroup, it does make sense to say that it lies in a conjugacy class of subgroups. With that in mind, we make the following definition.

Definition 2.1. Let G be a finite group, and let $C = \{C_1, \ldots, C_m\} \subset G^\sharp$ be a subset of conjugacy classes in G. Then C *generates* G if for any choice of representatives $g_i \in C_i$ for $1 \leq i \leq m$, the elements of the tuple $(g_1, \ldots, g_m)$ generate G. Equivalently, C generates G if

[1] After the first version of this paper appeared as a preprint, some new results appeared in [Kantor et al. 10]; see the remarks at the end of Section 4.

[2] This means distributed in proportion to the size of the conjugacy class.

and only if there is no (proper) maximal subgroup H of G that has nonempty intersection with each of the C_i.[3]

The equivalence of the two definitions is quite clear: if there are $g_i \in C_i$ that generate a proper subgroup H_1, then each C_i intersects any maximal proper subgroup H of G that contains H_1, and conversely. Note also that the second condition can be stated by saying that there is a conjugacy class of maximal subgroups containing C.

The following well-known lemma (due to Jordan; see [Serre 02]) is the basic fact underlying the whole technique.

Lemma 2.2. *Let G be a finite group. Then the set $G^\sharp$ of conjugacy classes generates H. In other words, there is no proper subgroup of G that contains a representative from each conjugacy class.*

Now let $(\Omega, \Sigma, \mathbf{P})$ be a fixed probability space with a sequence $X = (X_n)_{n\geq 1}$ of G-valued random variables

$$X_n : \Omega \to G,$$

and let $X_n^\sharp$ be the conjugacy class of X_n in $G^\sharp$: those are $G^\sharp$-valued random variables.

Intuitively, those $(X_n^\sharp)$ are the conjugacy classes that we see coming "one by one"; the Chebotarev invariant measures the threshold after which one can conclude that those conjugacy classes cannot all belong to some proper subgroup of G.

We now define a random variable $\tau_{X,G}$ (a *waiting time*) by

$$\tau_{X,G} = \min\{n \geq 1 \mid (X_1^\sharp, \ldots, X_n^\sharp) \text{ generate } G\} \\ \in [1, +\infty].$$

This depends on the sequence $X = (X_n)$, and it may always be infinite (e.g., if $X_n = 1$ for all n). But it is, in an intuitive sense, the "finest" invariant in terms of this probabilistic model. To obtain more compact and purely numerical invariants, it is natural to take first the expectation, which takes values in $[1, +\infty]$.

Definition 2.3. Let G be a finite group, $X = (X_n)$ a sequence of G-valued random variables, and $\tau_{X,G}$ the waiting time above. The *Chebotarev invariant* of G with respect to X, denoted by $c(G; X)$, is the expectation $c(G; X) = \mathbf{E}(\tau_{X,G})$ of this random variable.

[3] Alternatively, following [Dixon 92], one says that elements $(g_1, \ldots, g_m)$ *invariably generate* G if their conjugacy classes generate G in the above sense.

To have an unambiguously defined invariant, we must use a specific choice of sequence (X_n). The natural model is that of independent, uniformly distributed elements in G: if (X_n) are independent and identically uniformly distributed G-valued random variables, so that

$$\mathbf{P}(X_n = g) = \frac{1}{|G|} \quad \text{for all } g \in G \text{ and all } n \geq 1,$$

and hence

$$\mathbf{P}(X_n^\sharp = g^\sharp) = \frac{|g^\sharp|}{|G|}, \quad \text{for all } g^\sharp \in G^\sharp \text{ and all } n \geq 1,$$

then we call $c(G; X)$ *the* Chebotarev invariant, and we write simply $c(G)$.

Other numerical invariants may of course be derived from $\tau_{X,G}$, starting from the higher moments $\mathbf{E}(\tau_{X,G}^k)$ for $k \geq 1$. In particular, it is probabilistically most important, when the expectation of a random variable is known, to have control over its second moment as well, since that can be used to control to some extent the "concentration" of the random variable around the average.

Definition 2.4. Let G be a finite group, $X = (X_n)$ a sequence of G-valued random variables, and let $\tau_{X,G}$ be the waiting time above. The *secondary Chebotarev invariant* is the second moment $c_2(G; X) = \mathbf{E}(\tau_{X,G}^2)$. If (X_n) is a sequence of independent uniformly distributed random variables, then we write $c_2(G)$ and call it *the* secondary Chebotarev invariant.

We will now give formulas for the two Chebotarev invariants (in the independent case), which are expressed purely in terms of group-theoretic information.

To state the formulas, we must introduce the following data and notation about G. Let $\max(G)$ be the set of conjugacy classes of (proper) maximal subgroups of G (if G is trivial, this is empty); for a conjugacy class of maximal subgroups $\mathcal{H} \in \max(G)$, let $\mathcal{H}^\sharp$ denote the set of conjugacy classes C of G that "occur in $\mathcal{H}$," i.e., such that $C \cap H_1 \neq \varnothing$ for *some* H_1 in the conjugacy class $\mathcal{H}$.[4] Moreover, if $I \subset \max(G)$ is a set of conjugacy classes of maximal subgroups, we let

$$\mathcal{H}_I^\sharp = \bigcap_{\mathcal{H} \in I} \mathcal{H}^\sharp$$

denote the set of conjugacy classes of G that appear in all subgroups in I.

[4] Note that this depends on the underlying group G.

Proposition 2.5. *Let G be a* nontrivial *finite group. With notation as above, we have*

$$c(G) = \sum_{\substack{I \subset \max(G) \\ I \neq \varnothing}} \frac{(-1)^{|I|+1}}{1-\nu(\mathcal{H}_I^\sharp)} \tag{2–1}$$

and

$$\begin{aligned} c_2(G) &= \sum_{\substack{I \subset \max(G) \\ I \neq \varnothing}} \frac{(-1)^{|I|}}{1-\nu(\mathcal{H}_I^\sharp)} \left(1 - \frac{2}{1-\nu(\mathcal{H}_I^\sharp)}\right) \\ &= \sum_{\substack{I \subset \max(G) \\ I \neq \varnothing}} (-1)^{|I|+1} \frac{1+\nu(\mathcal{H}_I^\sharp)}{(1-\nu(\mathcal{H}_I^\sharp))^2}. \end{aligned} \tag{2–2}$$

Probabilists will have noticed that the first formula (at least) is very similar to that for the expectation of the waiting time for a general coupon collector problem. There is indeed a link, which is provided by the next lemma, where independence of the random elements X_n is not required.

Lemma 2.6. *Let G be a nontrivial finite group and $X = (X_n)$ a sequence of G-valued random variables. The waiting time $\tau_{X,G}$ is equal to*

$$\tau_{X,G} = \max_{\mathcal{H} \in \max G} \hat{\tau}_{\mathcal{H}},$$

where

$$\hat{\tau}_{\mathcal{H}} = \min\left\{n \geq 1 \mid X_n^\sharp \notin \mathcal{H}^\sharp\right\}. \tag{2–3}$$

In other words, $\tau_{X,G}$ is also the maximal n such that we need to look at X_i for i up to n before we witness, for every conjugacy class $\mathcal{H}$ of maximal subgroups, some X_n that is incompatible with the groups in this class $\mathcal{H}$. This is very close to a coupon collector problem (see, for example, [Flajolet et al. 92] for a general description of this type of problem). Because of this, we state and prove the following general abstract result, which may have other applications.

Proposition 2.7. *Let $(\Omega, \Sigma, \mathbf{P})$ be a probability space, D a finite set. Let (Z_n) be a sequence of D-valued random variables. Let $\mathcal{E}$ be a nonempty finite collection of nonempty subsets of D, and let*

$$\tau_{\mathcal{E}} = \min\{n \geq 1 \mid \textit{for all } E \in \mathcal{E}, \textit{ there exists some } m \leq n \textit{ with } Z_m \in E\}$$

be the waiting time before all subsets $E \in \mathcal{E}$ have been witnessed in the sequence (Z_n). For $I \subset \mathcal{E}$ nonempty, let

$$T_I = \min\{n \geq 1 \mid Z_n \in E \textit{ for some subset } E \in I\}.$$

(1) *Assume that $T_I < +\infty$ almost surely for all nonempty subsets $I \subset \mathcal{E}$. Then we have*

$$\tau_{\mathcal{E}} = \sum_{\varnothing \neq I \subset \mathcal{E}} (-1)^{|I|+1} T_I. \tag{2–4}$$

(2) *Assume that the Z_n are independent and identically distributed random variables and let μ be their common law. We have*

$$\mathbf{E}(\tau_{\mathcal{E}}) = \sum_{\substack{I \subset \mathcal{E} \\ I \neq \varnothing}} \frac{(-1)^{|I|+1}}{\mathbf{P}(Z_n \in \bigcup_{E \in I} E)} = \sum_{\substack{I \subset \mathcal{E} \\ I \neq \varnothing}} \frac{(-1)^{|I|+1}}{\mu(\bigcup_{E \in I} E)}. \tag{2–5}$$

(3) *We have*

$$\mathbf{E}(\tau_{\mathcal{E}}^2) = \sum_{\substack{I \subset \mathcal{E} \\ I \neq \varnothing}} \frac{(-1)^{|I|}}{\mu(\bigcup_{E \in I} E)} \left(1 - \frac{2}{\mu(\bigcup_{E \in I} E)}\right). \tag{2–6}$$

When $\mathcal{E}$ is the set of singletons in D, where we have exactly the coupon collector problem, the formulas for the expectation are well known; we have not seen general formulas for the second moment in the literature.

Proof of Proposition 2.7. To simplify notation, define

$$E_I = \bigcup_{E \in I} E \tag{2–7}$$

for each $I \subset \mathcal{E}$. Formula (2–4), which implies in particular that $\tau_{\mathcal{E}}$ is finite almost surely, can be checked easily by inclusion–exclusion.

We can then finish the computation of $\mathbf{E}(\tau_{\mathcal{E}})$ in (2) in the case of independent random variables. Indeed, in that case, the random variable T_I is distributed like a geometric random variable with parameter $p = \mathbf{P}(Z_n \in E_I)$ (see (1–1)) for any nonempty subset $I \subset \mathcal{E}$, so that taking the expectation in (2–4) and applying (1–2), we obtain the result.

Finally, to compute the second moment in the independent case, we start with the same formula (2–4) to get

$$\mathbf{E}(\tau_{\mathcal{E}}^2) = \sum_{\substack{\varnothing \neq I \subset \mathcal{E} \\ \varnothing \neq J \subset \mathcal{E}}} \sum (-1)^{|I|+|J|} \mathbf{E}(T_I T_J).$$

We first transform this by applying the formula

$$\mathbf{E}(T_I T_J) = \frac{1}{\mu(E_{I \cup J})} \left(\frac{1}{\mu(E_I)} + \frac{1}{\mu(E_J)} - 1\right) \tag{2–8}$$

to compute $\mathbf{E}(T_I T_J)$ (this formula is obtained by a straightforward, unenlightening computation; see

[Kowalski and Zywina 11] for details if needed). This gives

$$\mathbf{E}(\tau_{\mathcal{E}}^2) = \sum_{\substack{\varnothing\neq I\subset\mathcal{E}\\ \varnothing\neq J\subset\mathcal{E}}}\sum \frac{(-1)^{|I|+|J|}}{\mu(E_{I\cup J})}\left\{\frac{1}{\mu(E_I)}+\frac{1}{\mu(E_J)}-1\right\}$$
$$= \sum_{\substack{\varnothing\neq I\subset\mathcal{E}\\ \varnothing\neq J\subset\mathcal{E}}}\sum \frac{(-1)^{|I|+|J|}}{\mu(E_{I\cup J})}\left\{\frac{2}{\mu(E_I)}-1\right\} \qquad (2\text{–}9)$$

(by symmetry). To continue, consider more generally arbitrary complex coefficients $\beta(I)$ defined for $I\subset\mathcal{E}$, and the expression

$$W(\beta) = \sum_{\substack{\varnothing\neq I\subset\mathcal{E}\\ \varnothing\neq J\subset\mathcal{E}}}\sum \frac{(-1)^{|I|+|J|}}{\mu(E_{I\cup J})}\beta(I).$$

Note that $\mathbf{E}(\tau_{\mathcal{E}}^2)$ is a simple combination of two such expressions.

We proceed to reduce $W(\beta)$ to a single sum over $I\subset\mathcal{E}$ by rearranging the sum according to the value of $I\cup J$:

$$W(\beta) = \sum_{\varnothing\neq K\subset\mathcal{E}}\frac{1}{\mu(E_K)}\sum_{\substack{\varnothing\neq I,J\subset\mathcal{E}\\ I\cup J=K}}\sum(-1)^{|I|+|J|}\beta(I).$$

The inner sum is rearranged in turn as

$$\sum_{\substack{\varnothing\neq I,J\subset\mathcal{E}\\ I\cup J=K}}\sum(-1)^{|I|+|J|}\beta(I)$$
$$= \sum_{\varnothing\neq I\subset K}(-1)^{|I|}\beta(I)\sum_{\substack{\varnothing\neq J\subset K\\ I\cup J=K}}(-1)^{|J|}$$
$$= \sum_{\varnothing\neq I\subset K}(-1)^{|I|+|K-I|}\beta(I)\sum_{\substack{I'\subset I\\ I'\cup(K-I)\neq\varnothing}}(-1)^{|I'|},$$

since the subsets J with $I\cup J=K$ are parameterized by $I'\subset I$ using the correspondence $I'\mapsto(K-I)\cup I'$ with inverse $J\mapsto J\cap I$.

For fixed I, the last summation condition $I'\cup(K-I)\neq\varnothing$ is always valid, unless $I=K$, in which case it excludes only the set $I'=\varnothing$ from all $I'\subset I$. Since we have, for any finite set X, the binomial relation

$$\sum_{Y\subset X}(-1)^{|Y|}=0,$$

it follows that the double sum is simply given by

$$\sum_{\substack{\varnothing\neq I,J\subset\mathcal{E}\\ I\cup J=K}}\sum(-1)^{|I|+|J|}\beta(I) = (-1)^{|K|+1}\beta(K),$$

and hence

$$W(\beta) = \sum_{\varnothing\neq K\subset\mathcal{E}}\frac{(-1)^{|K|+1}\beta(K)}{\mu(E_K)}.$$

Applied to the expression (2–9), this leads precisely to (2–6). □

To deduce Proposition 2.5, we apply this proposition with

$$Z_n = X_n^\sharp,\quad D=G^\sharp,\quad \mathcal{E}=\{G^\sharp-\mathcal{H}^\sharp \mid \mathcal{H}\in\max(G)\},$$

in the case that the (X_n) are independent and uniformly distributed on G, so that the common distribution is $\mu=\nu$. Since for $I\subset\max G$, we have

$$\nu\Big(\bigcup_{\mathcal{H}\in I}(G^\sharp-\mathcal{H}^\sharp)\Big) = 1-\nu\Big(\bigcap_{\mathcal{H}\in I}\mathcal{H}^\sharp\Big),$$

the formulas (2–5) and (2–6) give exactly the claimed formulas (2–1) and (2–2).

Remark 2.8. As explained in [Serre 02, Theorem 5], we have

$$\nu(\mathcal{H}^\sharp)\le 1-\frac{1}{|G/H|} \qquad (2\text{–}10)$$

for any conjugacy class of a maximal subgroup of G (this is due to Cameron and Cohen).

We now present some easy formal properties of the Chebotarev invariants that can be useful for theoretical purposes.

Lemma 2.9. *Let G be a finite group and $\Phi(G)$ the* Frattini subgroup *of G, i.e., the intersection of all maximal subgroups of G. Then for any normal subgroup $N\triangleleft G$ such that $N\subset\Phi(G)$, in particular for $N=\Phi(G)$, we have*

$$c(G)=c(G/N),\quad c_2(G)=c_2(G/N).$$

Proof. Let $H=G/N$. We have $\Phi(H)=\Phi(G)/N$ and hence $H/\Phi(H)\simeq G/\Phi(G)$. This means that we need only prove the result when $N=\Phi(G)$, the general case following by applying this to H.

Let $\pi: G\to G/\Phi(G)$ be the quotient map. If (X_n) is a sequence of independent random variables uniformly distributed on G, then the $Y_n=\pi(X_n)$ are independent and uniformly distributed on $G/\Phi(G)$. Moreover, for any $n\ge 1$, the elements $(X_1^\sharp,\dots,X_n^\sharp)$ generate G if and only if the elements $(Y_1^\sharp,\dots,Y_n^\sharp)$ generate $G/\Phi(G)$. Indeed, this follows from the basic fact that a subset $S\subset G$ generates G if and only if $\pi(S)$ generates $G/\Phi(G)$ (this is applied to all sets $S=\{x_1,\dots,x_n\}$ where x_i is conjugate to X_i). This gives the result immediately from the definition of the waiting times. □

Proposition 2.10. *Let G_1, G_2 be finite groups such that the only subgroup $H \subset G_1 \times G_2 = G$ that surjects by projection to both factors is $H = G$. Then we have*

$$c(G_1 \times G_2) \leq c(G_1) + c(G_2) - 1.$$

For example, one can take G_1, G_2 to be nonisomorphic simple groups.

Proof. With $G = G_1 \times G_2$ and $X_n = (Y_n, Z_n) \in G_1 \times G_2$ a sequence of independent uniformly distributed random variables, it is clear that $(Y_n), (Z_n)$ are similarly independent and uniformly distributed on G_1 and G_2 respectively. We then have the inequality

$$\tau_G \leq \max(\tau_1, \tau_2) \leq \tau_1 + \tau_2 - 1$$

(since $\tau_i \geq 1$ and $\max(m, n) \leq n + m - 1$ for integers n, $m \geq 1$), with

$$\tau_1 = \min\{n \geq 1 : (Y_1^\sharp, \ldots, Y_n^\sharp) \text{ generate } G_1\}$$

and

$$\tau_2 = \min\{n \geq 1 : (Z_1^\sharp, \ldots, Z_n^\sharp) \text{ generate } G_2\},$$

which are distributed like τ_{G_1}, τ_{G_2} (indeed, if $n \geq \max(\tau_1, \tau_2)$, then the group generated by any elements in $X_n^\sharp = (Y_n^\sharp, Z_n^\sharp)$ surjects to G_1 and G_2; hence it must be equal to G by assumption). Taking the expectation, we get the inequality stated. □

The next result gives upper and lower estimates for the Chebotarev invariant using smaller sets of maximal subgroups than $\max(G)$.

Proposition 2.11. *Let G be a finite group, and let $M \subset \max(G)$ be an arbitrary nonempty finite subset of maximal subgroups. Let*

$$\tilde{\tau}_M = \max_{\mathcal{H} \in M} \hat{\tau}_{\mathcal{H}},$$

with notation as in (2–3) *and*

$$p_M = \nu\Big(G^\sharp - \bigcup_{\mathcal{H} \in \max(G) - M} \mathcal{H}^\sharp\Big). \tag{2–11}$$

We then have

$$\begin{aligned}\mathbf{E}(\tilde{\tau}_M) = \sum_{\varnothing \neq I \subset M} \frac{(-1)^{|I|+1}}{1 - \nu(\bigcap_{\mathcal{H} \in I} \mathcal{H}^\sharp)} &\leq c(G) \\ &\leq \mathbf{E}(\tilde{\tau}_M) - 1 + p_M^{-1}\end{aligned}$$

and

$$\mathbf{E}(\tilde{\tau}_M^2) \leq c_2(G) \leq \mathbf{E}(\tilde{\tau}_M^2) + \frac{2 - p_M}{p_M^2} - 1.$$

Proof. Define the additional waiting time

$$\tau^* = \min\Big\{n \geq 1 \mid X_n \notin \bigcup_{\mathcal{H} \notin M} \mathcal{H}^\sharp\Big\}.$$

We then note the inequalities

$$\tilde{\tau}_M \leq \tau_G \leq \max(\tilde{\tau}_M, \tau^*) \leq \tilde{\tau}_M + \tau^* - 1,$$

where the first inequality is obvious, while the second follows because for $n = \max(\tilde{\tau}_M, \tau^*)$, we know that the group generated by $(X_1^\sharp, \ldots, X_n^\sharp)$ is not contained in any subgroup in a conjugacy class of maximal subgroups $\mathcal{H} \in M$, and that this group also contains one element that is not conjugate to any element in a subgroup not in M.

Now we take expectations on both sides. Observing that by independence, τ^* is distributed like a geometric random variable with parameter p_m given by (2–11), we obtain the first inequalities, using Proposition 2.7 and (1–2).

Similarly, for the secondary invariant, we use the inequalities

$$\tilde{\tau}_M^2 \leq \tau_G^2 \leq \max(\tilde{\tau}_M, \tau^*)^2 \leq \tilde{\tau}_M^2 + (\tau^*)^2 - 1,$$

and get

$$\begin{aligned}\mathbf{E}(\hat{\tau}_M^2) \leq c_2(G) &\leq \mathbf{E}(\hat{\tau}_M^2) + \mathbf{E}((\tau^*)^2) - 1 \\ &= \mathbf{E}(\hat{\tau}_M^2) + \frac{2 - p_M}{p_M^2} - 1.\end{aligned}$$

The proof is complete. □

We have immediately the following corollary.

Corollary 2.12. *Let (G_n) be a sequence of nontrivial finite groups, and let ν_n denote the corresponding density. For each $n \geq 1$, let M_n be a nonempty subset of $\max(G_n)$, and assume that*

$$\lim_{n \to +\infty} \nu_n\Big(\bigcup_{\mathcal{H} \in \max(G_n) - M_n} \mathcal{H}^\sharp\Big) = 0, \tag{2–12}$$

i.e., the proportion of elements represented by a conjugacy class in some subgroup in M_n goes to zero. Then we have

$$\begin{aligned}c(G_n) &= \mathbf{E}(\tilde{\tau}_{M_n}) + o(1), \\ c_2(G_n) &= \mathbf{E}(\tilde{\tau}_{M_n}^2) + o(1),\end{aligned}$$

as $n \to +\infty$, with notation as in Proposition 2.11.

3. ABELIAN AND NILPOTENT GROUPS

In this section, we look at finite *abelian* and nilpotent groups G. In fact, because nilpotent groups have the (characteristic) property that $[G,G] \subset \Phi(G)$ (see, e.g., [Rose 94, Theorem 11.3,(v)]), Lemma 2.9 shows that if G is a nilpotent group, we have

$$c(G) = c(G/[G,G]), \quad c_2(G) = c_2(G/[G,G]),$$

which are Chebotarev and secondary Chebotarev invariants of abelian groups.

We will not use the formula from Proposition 2.5, because abelian groups tend to have many maximal subgroups up to conjugacy. We follow [Pomerance 01] in using another description of the Chebotarev waiting time in the case of abelian groups.

Theorem 3.1. (Pomerance.) *Let G be a finite abelian group, and for any prime number p dividing $|G|$, let $r_p(G) = \dim_{\mathbb{F}_p}(G/pG)$ be the p-rank of G. Let $\delta(G) = \max r_p(G)$ be the minimal cardinality of a generating set of G. Then we have*

$$c(G) = \delta(G) + \sum_{j\geq 1}\Big(1 - \prod_{p\|G|}\prod_{1\leq i\leq r_p(G)}(1-p^{-(\delta(G)+j-i)})\Big).$$

In particular, for $G = \mathbb{Z}/n\mathbb{Z}$ with $n \geq 2$, we have

$$c(G) = -\sum_{\substack{d|n\\ d\neq 1}}\frac{\mu(d)}{1-d^{-1}},$$

and for $G = \mathbb{F}_p^k$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with p prime and $k \geq 1$, we have

$$c(G) = k + \sum_{1\leq j\leq k}\frac{1}{p^j - 1}.$$

This is [Pomerance 01, theorem] and immediate corollaries of it.

Here are the results for the secondary Chebotarev invariant that are not computed by Pomerance.

Theorem 3.2. *Let G be a finite abelian group. With notation as in Theorem 3.1, we have*

$$\begin{aligned}c_2(G) &= \delta(G)^2 + \sum_{j\geq 1}(2j + 2\delta(G) - 1)\Big(1 - \prod_{p\|G|}\\ &\quad\times\prod_{1\leq i\leq r_p(G)}(1-p^{-(\delta(G)+j-i)})\Big).\end{aligned}$$

In particular, we have

$$c_2(\mathbb{Z}/n\mathbb{Z}) = -\sum_{2\leq d|n}\mu(d)\frac{1+d^{-1}}{(1-d^{-1})^2}$$

for $n \geq 1$ and

$$c_2(\mathbb{F}_p^k) = c(\mathbb{F}_p^k)^2 + \sum_{1\leq j\leq k}\frac{p^j}{(p^j-1)^2},$$

for p prime and $k \geq 1$.

Proof. The first result is obtained by reasoning as in [Pomerance 01, p. 195], with r and $(r+j)$ there replaced by r^2 and $(r+j)^2$. The point is that Pomerance shows that

$$\begin{aligned}&\mathbf{P}((X_1,\ldots,X_{\delta(G)+j}) \text{ generate } G)\\ &\quad= \prod_{p\|G|}\prod_{1\leq i\leq r_p(G)}(1-p^{-(\delta(G)-r_p(G)+j+i)}).\end{aligned}$$

To deduce the values for $G = \mathbb{Z}/p^k\mathbb{Z}$, it is simpler to use the description

$$\tau_G = \sum_{j=1}^{k} G_j,$$

where the G_j are independent geometric random variables with parameters $p_j = 1 - p^{-j}$. Concretely, they can be defined as follows:

$$\begin{aligned}G_k &= \min\{n \geq 1 \mid X_n \neq 0\},\\ G_{k-1} &= \min\{n \geq 1 \mid \dim_{\mathbb{F}_p}\langle X_{G_k+n}, X_{G_k}\rangle = 2\},\\ &\cdots\\ G_1 &= \min\{n \geq 1 \mid \dim_{\mathbb{F}_p}\langle X_{G_2+n}, X_{G_2},\ldots,X_{G_k}\rangle = k\},\end{aligned}$$

which, by independence of the (X_n), are easily checked to be indeed independent geometric variables with the stated parameters.

This decomposition leads to the formula for $c_2(G)$ immediately, using (1–2) and additivity of the variance of independent random variables. ☐

The formula of Pomerance gives a quick way to understand the limit values of Chebotarev invariants for abelian groups with a given rank $\delta(G)$.

Corollary 3.3. (Pomerance.) *For any fixed integer $k \geq 1$ and any abelian finite group G with $\delta(G) = k$, we have*

$$\begin{aligned}k \leq c(G) &\leq \limsup_{\substack{|G|\to+\infty\\ \delta(G)=k}} c(G)\\ &= k + 1 + \sum_{j\geq 1}\Big(1 - \prod_{1\leq j\leq k}\zeta(j+k)^{-1}\Big).\end{aligned}$$

In particular, the Chebotarev invariants for cyclic groups are bounded.

Corollary 3.4. *For any fixed k, we have*

$$c(\mathbb{F}_p^k) = k + O(p^{-1}), \quad c_2(\mathbb{F}_p^k) = k^2 + O(p^{-1}),$$

and

$$\mathbf{P}(\tau_{\mathbb{F}_p^k} \neq k) \ll p^{-1},$$

where the implied constants depend only on k.

This last result shows that for vector spaces over a finite field, the Chebotarev invariant is strongly peaked around the average, which is itself close to the dimension.

Proof. Only the last inequality needs (maybe) a bit of explanation. Since $\tau_{\mathbb{F}_p^k}$ takes positive integer values greater than or equal to k, we have

$$|\tau_{\mathbb{F}_p^k} - k| \geq 1$$

if $\tau_{\mathbb{F}_p^k} \neq k$. Hence if $\tau_{\mathbb{F}_p^k} \neq k$, we have

$$\begin{aligned}|\tau_{\mathbb{F}_p^k} - c(\mathbb{F}_p^k)| &\geq |\tau_{\mathbb{F}_p^k} - k| - |c(\mathbb{F}_p^k) - k| \\ &\geq 1 - |c(\mathbb{F}_p^k) - k|,\end{aligned}$$

and if furthermore, we have $p \geq p_0$, where p_0 (depending on k) is chosen so that

$$k \leq c(\mathbb{F}_p^k) \leq k + \frac{1}{2}$$

for all $p \geq p_0$, it follows that

$$\{\tau_{\mathbb{F}_p^k} \neq k\} \subset \left\{|\tau_{\mathbb{F}_p^k} - c(\mathbb{F}_p^k)| \geq \frac{1}{2}\right\}$$

for such p, and then the Chebyshev inequality gives

$$\mathbf{P}(\tau_{\mathbb{F}_p^k} \neq k) \leq 4\mathbf{V}(\tau_{\mathbb{F}_p^k}) \ll p^{-1}$$

for $p \geq p_0$, where the implied constant depends on k. Increasing this constant if needed (e.g., taking it to be at least p_0), we can also claim that this inequality holds for $p \geq 2$. □

Remark 3.5. In particular, for cyclic groups, the Chebotarev invariant is at most, and its lim sup is, the constant

$$2 + \sum_{k \geq 2} \left(1 - \frac{1}{\zeta(k)}\right) = 2.705211140105367764\ldots.$$

This asymptotic behavior is not without interest (and some surprise). On the one hand, we see that $c(\mathbb{Z}/n\mathbb{Z})$ remains absolutely bounded, despite the existence of cyclic groups with many subgroups, and on the other hand, we see that it is not always close to the minimal number of generators.

4. A SOLVABLE EXAMPLE

The results of the previous section, as well as those we will see in the next one, reveal (or suggest) rather small values of the Chebotarev invariants in comparison with the size of the groups. The following example in the solvable case exhibits very different behavior.

Proposition 4.1. *For q a power of a prime, let*

$$H_q = \left\{ \begin{pmatrix} a & t \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_q^\times,\ t \in \mathbb{F}_q \right\}$$

be the group of translations and dilations of the affine plane $\mathbb{F}_q^2$ of order $q(q-1)$, isomorphic to a semidirect product $\mathbb{F}_q \rtimes \mathbb{F}_q^\times$.

(1) *We have*

$$c(H_q) = q - q^{-1} \sum_{1 \neq d \mid q-1} \frac{\mu(d)}{(1 - d^{-1})(1 - d^{-1} + q^{-1})} \tag{4–1}$$

and

$$\begin{aligned} c_2(H_q) = q(2q-1) &+ c_2(\mathbb{Z}/(q-1)\mathbb{Z}) \\ &+ \sum_{1 \neq d \mid q-1} \mu(d) \frac{1 + d^{-1} - q^{-1}}{(1 - d^{-1} + q^{-1})^2}. \end{aligned} \tag{4–2}$$

(2) *For $q \geq 2$, we have*

$$\begin{aligned} c(H_q) &= q + O(\tau(q-1)), \\ c_2(H_q) &= q(2q-1) + O(\tau(q-1)), \end{aligned} \tag{4–3}$$

where $\tau(n)$ is the number of positive divisors of n. In particular, $c(H_q) \sim q$ as $q \to +\infty$.

Since we have a split exact sequence

$$1 \to \mathbb{F}_q \to H_q \xrightarrow{\det} \mathbb{F}_q^\times \to 1$$

and the two surrounding groups are isomorphic to $\mathbb{F}_p^k$, where $q = p^k$ with p prime, and to a cyclic group $\mathbb{Z}/(q-1)\mathbb{Z}$ with Chebotarev invariants respectively tending to k as p gets large and bounded, this shows in particular that the Chebotarev invariant can jump quite uncontrollably under extensions.

The proof will use Proposition 2.5. We start with an elementary lemma.

Lemma 4.2.

(1) *There are q conjugacy classes in H_q; they are given, with representatives of them, by*

$$g_b = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix}, \quad g_b^\sharp = \{g \in H_q \mid \det(g) = b\}, \quad |g_b^\sharp| = q,$$

where $b \in \mathbb{F}_q^\times - \{1\}$ and

$$\mathrm{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathrm{Id}^\sharp = \{\mathrm{Id}\}, \quad u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$
$$u^\sharp = \{g \in H_q - \{\mathrm{Id}\} \mid \det(g) = 1\}, \quad |u^\sharp| = q - 1.$$

(2) *The conjugacy classes of maximal subgroups of H_q have representatives given by*

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_q^\times \right\}$$

and

$$C_\ell = \left\{ \begin{pmatrix} a & t \\ 0 & 1 \end{pmatrix} \in H_q \mid a \in (\mathbb{F}_q^\times)^\ell \text{ and } t \in \mathbb{F}_q \right\},$$

where ℓ runs over the prime divisors of $q - 1$.

We omit the elementary proof, referring to [Kowalski and Zywina 11] for details.

Proof of Proposition 4.1. First of all, in addition to the maximal subgroups C_ℓ given by Lemma 4.2, there are subgroups C_d for all square-free divisors $d \mid q-1$, the inverse image under the determinant of the subgroup D_d of order $(q-1)/d$ in the cyclic group $\mathbb{F}_q^\times$.

Given a subset $I \subset \max(H_q)$, we compute the density of conjugacy classes in

$$\mathcal{H}_I^\sharp = \bigcap_{\mathcal{H} \in I} \mathcal{H}^\sharp.$$

If $A \in I$, then with $I' = I - \{A\}$ and d the product of those primes ℓ for which $C_\ell \in I'$ (including $d = 1$ when $I' = \varnothing$), we have

$$\nu(\mathcal{H}_I^\sharp) = \frac{1}{d} - q^{-1},$$

and in particular

$$\nu(A^\sharp) = 1 - q^{-1}.$$

Indeed, we have to find the density of those elements of H_q that are diagonalizable with eigenvalues 1 and $a \in D_d$. These are exactly the conjugacy classes $g_b^\sharp$ with $b \in D_d - \{1\}$ and the trivial class, so

$$\nu(\mathcal{H}_I^\sharp) = \frac{1 + ((q-1)/d - 1)q}{q(q-1)} = \frac{q(q-1)/d - (q-1)}{q(q-1)} = \frac{1}{d} - \frac{1}{q}.$$

If, on the other hand, $A \notin I$, then I corresponds to a divisor $d \mid q-1$, $d \neq 1$, and we have

$$\nu(\mathcal{H}_I^\sharp) = \frac{1}{d},$$

since we must now compute the density of elements of H_q that have $\det(g) \in D_d$, and this is

$$\frac{q\left(\frac{q-1}{d} - 1\right) + 1 + q - 1}{q(q-1)} = \frac{1}{d}.$$

Applying (2–1) and isolating the contribution of $I = \{A\}$ leads to (4–1) and to (4–2). To deduce (4–3) for $c(H_q)$, we may assume $q = p^k$ with p an odd prime, since for q even, we have

$$c(H_q) = q + c(\mathbb{Z}/(q-1)\mathbb{Z}) = q + O(1)$$

by Corollary 3.4. So for q odd, we write

$$c(H_q) = q + c(\mathbb{Z}/(q-1)\mathbb{Z}) - \Delta(q) = q - \Delta(q) + O(1),$$

where

$$\Delta(q) = \sum_{1 \neq d \mid q-1} \frac{\mu(d)}{1 - d^{-1} + q^{-1}}.$$

Since $1 - d^{-1} + q^{-1} \geq 1 - d^{-1} > 0$, we can bound this from above by

$$|\Delta(q)| \leq \sum_{1 \neq d \mid q-1}^{\flat} \frac{1}{1 - d^{-1}},$$

and then we find easily that

$$\begin{aligned} |\Delta(q)| &\leq \sum_{k \geq 0} \Big(\prod_{p \mid q-1} (1 + p^{-k}) - 1 \Big) \\ &\leq \tau(q-1) + \prod_{p \mid q-1} (1 + p^{-1}) - 2 \\ &\quad + \sum_{k \geq 2} \Big(\frac{\zeta(k)}{\zeta(2k)} - 1 \Big) \\ &= O(\tau(q-1)), \end{aligned}$$

since the series converges absolutely. The asymptotics for $c_2(H_q)$ are obtained by essentially identical arguments. □

The proof confirms the intuitive fact that the large size of $c(H_q)$ is due directly to the existence of a fairly small diagonal subgroup A (of index q) that contains elements conjugate to a very large proportion of elements of H_q. So the waiting time is close to the waiting time until a nondiagonalizable element is obtained, which is a geometric random variable T with

$$\mathbf{P}(T = k) = \frac{1}{q}\left(1 - \frac{1}{q}\right)^{k-1}, \quad \text{for } k \geq 1.$$

This is confirmed by the large second moment $c_2(H_q)$: it corresponds to a standard deviation of the waiting time, which is

$$\sqrt{c_2(H_q) - c(H_q)^2} \sim q, \quad \text{as } q \to +\infty,$$

i.e., very close to the expectation, similar to the fact that $\mathbf{V}(T) = q\sqrt{1 - q^{-1}}$.

The groups $G = H_q$ show that the inequality (2–10) is best possible (with the maximal subgroup $H = A$), as observed also in [Serre 02], so it is not surprising that they lead to high Chebotarev invariants. Indeed, one may wonder whether the upper bound

$$c(G) \ll \sqrt{|G|}$$

might not hold for all finite groups G.[5] In this direction, after the first version of this paper appeared as a preprint, it was shown in [Kantor et al. 10, Theorem 1.2] that

$$c(G) \ll \sqrt{|G|}(\log |G|),$$

which is not far off from this guess. Note, however, that the proof uses the classification of finite simple groups.

In a similar vein, we have in general

$$\tau_G \leq \sum_{\mathcal{H} \in \max(G)} \hat{\tau}_{\mathcal{H}},$$

and hence we obtain

$$c(G) \leq \sum_{\mathcal{H} \in \max(G)} \frac{1}{1 - \nu(\mathcal{H}^\sharp)}$$

from (2–1). Together with (2–10), this gives an upper bound

$$c(G) \leq |G| \sum_{\mathcal{H} \in \max(G)} \frac{1}{|\mathcal{H}|}, \tag{4–4}$$

which is close to being sharp for the groups H_q: indeed, if $q = 2\ell + 1$ is a Sophie Germain prime, then Lemma 4.2 leads to

$$|H_q| \sum_{\mathcal{H} \in \max(H_q)} \frac{1}{|\mathcal{H}|} = \frac{3(q+1)}{2}.$$

[5] The trivial bound in trying to estimate $c(G)$ in terms of $|G|$ is easily seen to be $c(G) \leq |G|^2$.

5. SOME FINITE GROUPS OF LIE TYPE

For specific complicated nonabelian groups, the Chebotarev invariant may be hard to compute exactly, except numerically using the formulas of Proposition 2.5 when feasible (we will give examples from computer calculations in Section 7). However, if we consider infinite families of nonabelian groups, it may be that the subgroup structure is sufficiently well known, simple, and regular that one can derive asymptotic information. In fact, using results like Proposition 2.11, it is not needed for this purpose to have complete control over all maximal subgroups. We illustrate this first with the simplest family of simple groups of Lie type.

Theorem 5.1.

(1) *For p prime, we have*

$$c(\mathrm{SL}(2, \mathbb{F}_p)) = c(\mathrm{PSL}(2, \mathbb{F}_p)) = 3 + O(p^{-1})$$

and

$$c_2(\mathrm{SL}(2, \mathbb{F}_p)) = c_2(\mathrm{PSL}(2, \mathbb{F}_p)) = 11 + O(p^{-1}).$$

(2) *For all $k \geq 2$, we have*

$$\mathbf{P}(\tau_{\mathrm{PSL}(2,\mathbb{F}_p)} = k) = \frac{1}{2^{k-1}} + O(p^{-1}),$$

where the implied constant depends on k.

Note that the limit of $c(\mathrm{SL}(2, \mathbb{F}_p))$ is not the minimal number of generators of $\mathrm{SL}(2, \mathbb{F}_p)$, which is 2.

For the proof, we will not use the formula of Proposition 2.5, although this could be done at least to prove (1). Instead, we use [Serre 72, Proposition 19].

Lemma 5.2. (Serre.) *Let $p \geq 5$ be a prime number. Assume that $G \subset \mathrm{SL}(2, \mathbb{F}_p)$ is a subgroup such that the following hold:*

(1) *The group G contains an element s such that $\mathrm{Tr}(s)^2 - 4$ is a nonzero square in $\mathbb{F}_p$, and such that $\mathrm{Tr}(s) \neq 0$.*

(2) *The group G contains an element s such that $\mathrm{Tr}(s)^2 - 4$ is not a square in $\mathbb{F}_p$, and such that $\mathrm{Tr}(s) \neq 0$.*

(3) *The group G contains an element s such that $\mathrm{Tr}(s)^2 \in \mathbb{F}_p$ is not in $\{0, 1, 2, 4\}$, and is not a root of $X^2 - 3X + 1$.*

Then we have $G = \mathrm{SL}(2, \mathbb{F}_p)$.

Proof of Theorem 5.1. We first notice that we need only consider the case of $\mathrm{SL}(2, \mathbb{F}_p)$, since $\mathrm{PSL}(2, \mathbb{F}_p)$ has the same invariants, as follows from Lemma 2.9 and the well-known fact that $\{\pm I\}$ is in the Frattini subgroup of $\mathrm{SL}(2,\mathbb{F}_p)$ (see, e.g., [Serre 98, IV-23]).

We assume $p \geq 5$. Let $\tau = \tau_{\mathrm{SL}(2,\mathbb{F}_p)}$ denote the corresponding waiting time, and let τ_1, τ_2, τ_3 denote the waiting times for conjugacy classes satisfying the conditions (1), (2), and (3) in Lemma 5.2, e.g.,

$$\tau_1 = \min\{n \geq 1 : s = X_n^\sharp \text{ has } \mathrm{Tr}(s) \neq 0 \text{ and } \mathrm{Tr}(s)^2 - 4 \text{ is in } (\mathbb{F}_p^\times)^2\}.$$

Let also τ_1^*, τ_2^* be the waiting times for conditions (1) and (2) *without* the condition $\mathrm{Tr}(s) \neq 0$. Note that (1) and (2) are exclusive conditions. Moreover, each τ_i is a geometric random variable with parameters, respectively

$$p_1 = \frac{1}{2} + O(p^{-1}), \quad p_2 = \frac{1}{2} + O(p^{-1}), \quad p_3 = 1 + O(p^{-1}), \tag{5–1}$$

and for τ_1^*, τ_2^*, the parameters are also

$$p_1^* = \frac{1}{2} + O(p^{-1}), \quad p_2^* = \frac{1}{2} + O(p^{-1}),$$

as can be checked by looking at tables of conjugacy classes in $\mathrm{SL}(2,\mathbb{F}_p)$ (e.g., in [Fulton and Harris 91, p. 71]).

We then have

$$\max(\tau_1^*, \tau_2^*) \leq \tau_p \leq \max(\tau_1, \tau_2, \tau_3),$$

where the right-hand inequality comes from Lemma 5.2 and the left-hand inequality is due to the fact that the Borel subgroup

$$B = \left\{ \begin{pmatrix} x & a \\ 0 & x^{-1} \end{pmatrix} \right\} \subset \mathrm{SL}(2,\mathbb{F}_p)$$

intersects every conjugacy class satisfying (1) (so that $\tau_p \geq \tau_2^*$) and the nonsplit Cartan subgroup

$$C_{ns} = \left\{ \begin{pmatrix} a & b \\ \varepsilon b & a \end{pmatrix} \right\} \subset \mathrm{SL}(2,\mathbb{F}_p)$$

intersects every conjugacy class satisfying (2), where $\varepsilon \in \mathbb{F}_p^\times$ is a fixed nonsquare element (so that $\tau_p \geq \tau_1^*$).

By applying Proposition 2.5 to compute the expectation and second moment on the two extreme sides, we obtain the desired asymptotics

$$3 + O(p^{-1}) \leq \mathbf{E}(\tau_p) \leq 3 + O(p^{-1}),$$
$$11 + O(p^{-1}) \leq \mathbf{E}(\tau_p^2) \leq 11 + O(p^{-1}).$$

To prove (2), fix some $k \geq 2$. We define

$$\tau_p^* = \max(\tau_1^*, \tau_2^*), \quad \tau_p' = \max(\tau_1, \tau_2, \tau_3),$$

and notice that we have the equality of events

$$\{\tau_p = k\} = \{\tau_p = \tau_p' = k\} \cup \{\tau_p = k < \tau_p'\},$$

which is of course a disjoint union. Then we note that

$$\mathbf{P}(\tau_p = k < \tau_p') \leq \sum_{1 \leq j \leq k} \mathbf{P}(\tau_p^* = j, \ \tau_p' > j).$$

But clearly, if $\tau_p^* = j$ and $\tau_p^* < \tau_p'$, then either one of the conjugacy classes $(X_1^\sharp, \ldots, X_j^\sharp)$ has trace zero, or otherwise we must have $\tau_p' = \tau_3 > j \geq 2$. In the first case, since all X_n have the same uniform distribution, the probability is at most

$$j\mathbf{P}(\mathrm{Tr}(X_1^\sharp) = 0) \ll jp^{-1}$$

that $p \geq 2$ for all p (again by looking at conjugacy classes, for example). In the second case, we have

$$\mathbf{P}(\tau_3 > j) \leq \mathbf{P}(\tau_3 \geq 2) \ll p^{-2}.$$

Combining this with the equality of events we found, it follows that for k fixed, we have

$$\mathbf{P}(\tau_p = k) = \mathbf{P}(\tau_p = \tau_p' = k) + O(p^{-1}),$$

where the implied constant depends on k.

Next we note that

$$\{\tau_p' = k\} = \{\tau_p = \tau_p' = k\} \cup \{\tau_k' = p, \ \tau_p < k\},$$

again a disjoint union. As above, we find that

$$\mathbf{P}(\tau_k' = p, \ \tau_p < k) \leq \sum_{j=1}^{k-1} \mathbf{P}(\tau_p^* = j < \tau_p') \ll p^{-1},$$

where the implied constant depends on k, and hence we have finally

$$\mathbf{P}(\tau_p = k) = \mathbf{P}(\tau_p' = k) + O(p^{-1}),$$

and the result now follows easily: first, by arguments already used, we have

$$\mathbf{P}(\tau_p' = k) = \mathbf{P}(\max(\tau_1, \tau_2) = k) + O(p^{-1}),$$

and then we are left with a coupon collector problem with two coupons of roughly equal probability by (5–1). This gives

$$\begin{aligned} &\mathbf{P}(\max(\tau_1, \tau_2) = k) \\ &\quad = p_1^{k-1} p_2 + p_2^{k-1} p_1 = 2\left(\frac{1}{2} + O(p^{-1})\right)^k \\ &\quad = \frac{1}{2^{k-1}} + O(p^{-1}) \end{aligned}$$

for $p \geq 2$, the implied constant depending on k. $\square$

Remark 5.3. Recent results (announced in [Fulman and Guralnick 03]) should lead to a similar good understanding of $c(\mathbf{G}(\mathbb{F}_q))$ when $\mathbf{G}$ is a fixed (almost simple) algebraic group over $\mathbb{Q}$. Indeed, the cited results should also be applicable to situations with rank going to infinity, which are analogues of the symmetric and alternating groups that we consider now.

6. SYMMETRIC AND ALTERNATING GROUPS

We now come to the case of the symmetric groups $\mathfrak{S}_n$ and alternating groups A_n. Here we have the following result, which is a precise formulation of a result essentially conjectured by Dixon [Dixon 92, abstract], following McKay.[6]

Theorem 6.1. *For $n \geq 1$, we have*

$$c(\mathfrak{S}_n) \asymp 1, \quad c(A_n) \asymp 1, \quad c_2(\mathfrak{S}_n) \asymp 1, \quad c_2(A_n) \asymp 1.$$

In fact, there exists a constant $c > 1$ such that for all $n \geq 1$, we have

$$\mathbf{E}(c^{\tau_{\mathfrak{S}_n}}) \ll 1, \quad \mathbf{E}(c^{\tau_{A_n}}) \ll 1.$$

The proof is based on the following difficult result from [Łuczak and Pyber 93], improving earlier results in [Dixon 92].

Theorem 6.2. (Łuczak and Pyber.) *For any $\varepsilon > 0$, there exists a constant C depending only on ε such that*

$$\mathbf{P}((X_1^\sharp, \ldots, X_m^\sharp) \text{ generate } \mathfrak{S}_n) > 1 - \varepsilon$$

for all $m \geq C$ and all $n \geq 1$. The same applies to A_n.

Proof of Theorem 6.1. We need only prove that the exponential moments $\mathbf{E}(c^{\tau_n})$ are bounded for some $c > 1$, where $\tau_n = \tau_{G_n}$ with $G_n = \mathfrak{S}_n$ (the A_n case is similar).

From Theorem 6.2, there exists $m \geq 1$ such that

$$\mathbf{P}((Y_1^\sharp, \ldots, Y_m^\sharp) \text{ do not generate } \mathfrak{S}_n) \leq \frac{1}{2} \tag{6–1}$$

for any family of independent, uniformly distributed random variables Y_i on G_n.

Now let $k \geq 1$ be given; we can partition the set $\{1, \ldots, k-1\}$ into $\lfloor (k-1)/m \rfloor \geq 0$ subsets of size m and a remainder, and we observe that if $\tau_n = k$, then for each of these subsets I, we have

$$\mathbf{P}\big((X_i^\sharp),\, i \in I\big) \leq \frac{1}{2},$$

by independence and (6–1). Since all those sets are disjoint, we get

$$\mathbf{P}(\tau_n = k) \leq \left(\frac{1}{2}\right)^{\lfloor (k-1)/m \rfloor} \leq 2^{1-(k-1)/m}$$

for $k \geq 1$, and then, for any $c \geq 1$, we have

$$\mathbf{E}(c^{\tau_n}) = \sum_{k \geq 1} c^k \mathbf{P}(\tau_n = k) \leq 2^{1+1/m} \sum_{k \geq 1} (c 2^{1/m})^k,$$

which converges and is independent of n for every c with $1 < c < 2^{1/m}$. ☐

In view of this, the following question seems natural.

Question 6.3. Is it true that for *all* $c > 1$, we have

$$\mathbf{E}(c^{\tau_{\mathfrak{S}_n}}) \ll 1$$

for $n \geq 1$ (and similarly for A_n)?

Another natural question, also suggested by Dixon, is the following.

Question 6.4. Do the sequences $(c(\mathfrak{S}_n))$ and $(c(A_n))$ converge as $n \to +\infty$? If they do, can their limits be computed?

Our guess is that the answer is positive. In fact, we now present a heuristic model that suggests this and predicts the value of the limit for A_n. We do this by first applying Corollary 2.12 to a suitable "essential" set of maximal subgroups of symmetric groups of A_n. This is again provided by [Łuczak and Pyber 93].

Theorem 6.5. (Łuczak and Pyber.) *For $n \geq 1$, let S_n be the set of $g \in \mathfrak{S}_n$ such that g is contained in a subgroup G of $\mathfrak{S}_n$, distinct from A_n, and such that G acts transitively on $\{1, \ldots, n\}$. Then we have*

$$\lim_{n \to +\infty} \nu_n(S_n) = 0,$$

where $\nu_n(A) = |A|/|\mathfrak{S}_n|$ is the uniform density on the symmetric group.

Corollary 6.6. *For $n \geq 1$ and $1 \leq i < n/2$, let*

$$H_{i,n} = \big\{g \in \mathfrak{S}_n \mid g \cdot \{1, \ldots, i\} = \{1, \ldots, i\}\big\}$$

be the subgroup of $\mathfrak{S}_n$ leaving $\{1, \ldots, i\}$ invariant. Let $H'_{i,n} = H_{i,n} \cap A_n$. Then the $H_{i,n}$, respectively $H'_{i,n}$, are

[6] This conjecture is imprecisely formulated in [Dixon 92], where the "expected number of elements needed to generate $\mathfrak{S}_n$ invariably" seems to mean any $r(n)$ for which $\mathbf{P}(c(\mathfrak{S}_n) > r(n)) \to 0$.

maximal subgroups of $\mathfrak{S}_n$, respectively A_n. Moreover, let

$$M_n = \{A_n\} \cup \{H_{i,n} \mid 1 \le i < n/2\} \subset \max(\mathfrak{S}_n),$$
$$M'_n = \{H'_{i,n} \mid 1 \le i < n/2\} \subset \max(A_n).$$

As in Proposition 2.11, let $\tilde{\tau}_n$, respectively $\tilde{\tau}'_n$, be the waiting time before conjugacy classes in each subgroup of M_n, respectively M'_n, have been observed. Then we have

$$c(\mathfrak{S}_n) = \mathbf{E}(\tilde{\tau}_n) + o(1), \quad c_2(\mathfrak{S}_n) = \mathbf{E}(\tilde{\tau}_n^2) + o(1)$$

as $n \to +\infty$, and similarly

$$c(A_n) = \mathbf{E}(\tilde{\tau}'_n) + o(1), \quad c_2(A_n) = \mathbf{E}((\tilde{\tau}'_n)^2) + o(1).$$

Proof. It is known that the $H_{i,n}$ are (representatives of) the conjugacy classes of maximal intransitive subgroups of $\mathfrak{S}_n$. Thus, we find by the definition of S_n that

$$\bigcup_{\mathcal{H} \in \max(\mathfrak{S}_n) - M_n} \mathcal{H}^\sharp = S_n,$$

and hence the result follows immediately from Corollary 2.12 and Theorem 6.5, which provides us with the assumption (2–12) as required. □

We note now that an element $\sigma \in \mathfrak{S}_n$ is conjugate to an element of $H_{i,n} \subset \mathfrak{S}_n$ if and only if when expressed as a product of disjoint cycles of lengths $\ell_j(\sigma) \ge 1$, $1 \le j \le \varpi(\sigma)$, say, it has the property that a sum of a subset of the lengths is equal to i: for some $J \subset \{1, \ldots, \varpi(\sigma)\}$, we have

$$\sum_{j \in J} \ell_j(\sigma) = i.$$

This applies equally to an element σ in A_n: the element is conjugate to $H'_{i,n} \subset A_n$ if and only if the property above is true for its cycle lengths computed in $\mathfrak{S}_n$ (although these cycle lengths do not always characterize the conjugacy class of σ in A_n).

In particular, conjugacy classes $(\sigma_1^\sharp, \ldots, \sigma_k^\sharp)$ in $\mathfrak{S}_n^\sharp$ or $A_n^\sharp$ generate a transitive subgroup of $\mathfrak{S}_n$ or A_n if and only if n (which is the sum of all lengths) is the only such sum occurring for all σ_j. (Indeed, if $i < n$ occurs as a common subsum, we can assume that $i \le n/2$, and then we can select elements in each conjugacy class all of which belong to $H_{i,n}$, so that the conjugacy classes cannot invariably generate a transitive subgroup, and conversely.)

We come now to the model in which $n \to +\infty$. The distribution of the set of lengths of random permutations is a well-studied subject in probabilistic group theory, and this allows us to make a guess as to the existence and value of the limit. For $i \ge 1$, consider the map

$$\varpi_i : \mathfrak{S}_n \to \{0, 1, \ldots\}$$

sending σ to the number of cycles of length i in its decomposition as a product of disjoint cycles. Let s_n, σ_n be uniformly distributed random variables on $\mathfrak{S}_n$ and A_n, respectively. Well-known results going back to [Goncharov 44] show that for fixed i, as $n \to +\infty$, the random variables $\varpi_i(\sigma_n)$ converge in law to a Poisson random variable with parameter $1/i$, i.e., we have

$$\lim_{n \to +\infty} \mathbf{P}(\varpi_i(\sigma_n) = k) = e^{-1/i} \frac{1}{k! i^k}, \quad \text{for fixed } k \ge 0,$$

and the limits for distinct values of i are independent, i.e., for any fixed finite set I of positive integers, we have

$$\lim_{n \to +\infty} \mathbf{P}(\varpi_i(\sigma_n) = k_i \text{ for all } i \in I) = \prod_{i \in I} e^{-1/i} \frac{1}{i^{k_i}\, k_i!}.$$

More precisely, this is proved (and with much more precise results) for symmetric groups in, e.g., [Arratia and Tavaré 92, Theorem 1] and [Arratia et al. 03, Theorem 1.3]. The case of alternating groups can be deduced from this using methods in [Lloyd and Shepp 66, Section 2]; see [Kowalski and Zywina 11] for details.

It seems therefore reasonable to use a model of Poisson variables to predict the limit of Chebotarev invariants of alternating groups. For this purpose, let $\mathcal{A}$ be the set of sequences $(\ell_i)_{i \ge 1}$ of nonnegative integers; we denote the ith component of $\ell \in \mathcal{A}$ by $\varpi_i(\ell)$. Let $\nu_{\mathcal{A}}$ be the infinite product (probability) measure on $\mathcal{A}$ such that the ith component ℓ_i is distributed like a Poisson random variable with parameter $1/i$. This set $\mathcal{A}$ is meant to be like the set of conjugacy classes of an infinite symmetric group, and indeed, from the above, we see that for any finite set I of positive integers and any $k_i \ge 0$ defined for $i \in I$, we have

$$\lim_{n \to +\infty} \mathbf{P}(\varpi_i(\sigma_n) = k_i \text{ for all } i \in I)$$
$$= \nu_{\mathcal{A}}(\{\ell \in \mathcal{A} \mid \varpi_i(\ell) = k_i,\ i \in I\}).$$

Now consider an infinite sequence $(X_k)_{k \ge 1}$ of $\mathcal{A}$-valued independent random variables, identically distributed according to ν. We look at the following waiting time:

$$\tau_{\mathcal{A}} = \min\Big\{k \ge 1 \mid \bigcap_{1 \le j \le k} S(X_j) = \{+\infty\}\Big\},$$

where for $\ell \in \mathcal{A}$, we denote by $S(\ell) \subset \{0, 1, 2, \ldots, \} \cup \{+\infty\}$ the set of all sums

$$\sum_{i \ge 1} i b_i, \quad \text{where } 0 \le b_i \le \varpi_i(\ell)$$

(note the usual shift of notation from our description of the case of fixed n: the sequence of lengths of cycles

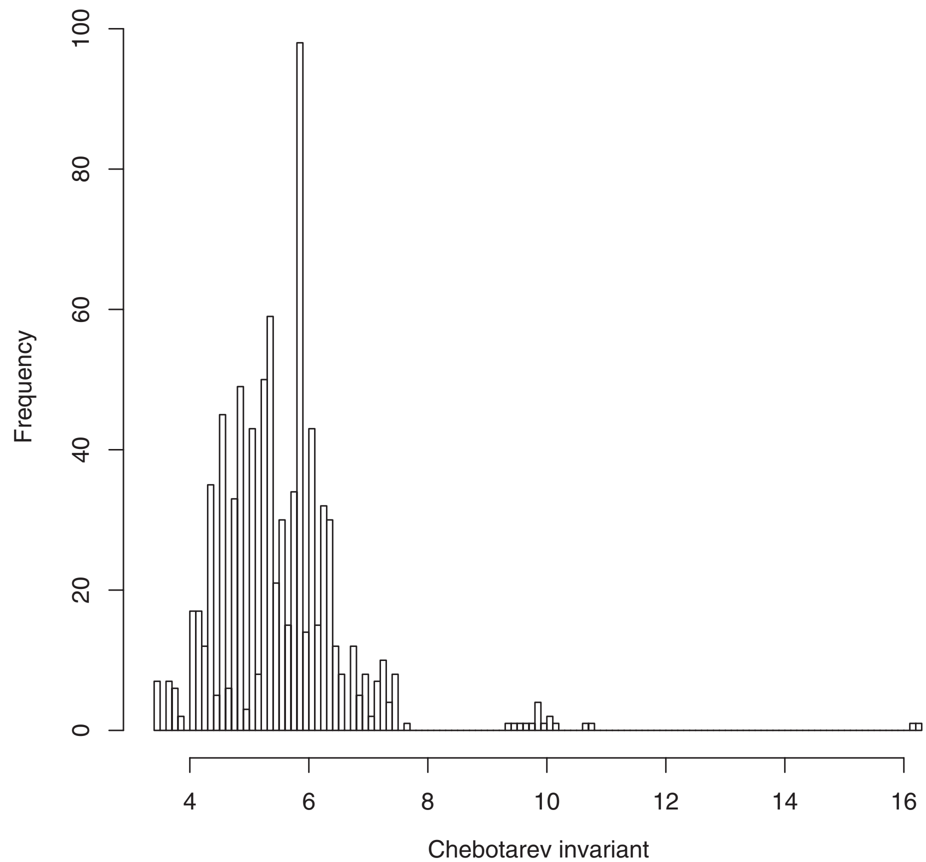

FIGURE 1. Distribution of the Chebotarev invariant for groups of order 720.

occurring in a permutation is replaced by the sequence of multiplicities of each possible length). Then our guess for the limit of $c(A_n)$ is that

$$\lim_{n\to+\infty} c(A_n) = \mathbf{E}(\tau_A).$$

We hope to return to this question in a future work.

7. NONABELIAN GROUPS: NUMERICAL EXPERIMENTS

Some values of the Chebotarev invariants for some nonabelian finite groups are presented in Tables 1 through 5. Figure 1 shows the distribution of the Chebotarev invariant for groups of order 720. The computations are feasible even for fairly large and complicated nonabelian groups, because they may have few conjugacy classes of maximal subgroups and not too many conjugacy classes. For instance, the Weyl group $W(E_8)$ (one of our motivating examples) has 9 conjugacy classes of maximal subgroups and 112 conjugacy classes. However, note that this represents quite deep knowledge about groups, and moreover, to perform the computation in reasonable time, very efficient algorithms must exist to deal with conjugacy classes.

The computations were done with Magma (see [Bosma et al. 97]). More data, as well as the script we used, can be found in the longer version [Kowalski and Zywina 11] of this paper. The names of the “sporadic” groups in the tables should be self-explanatory (e.g., $W(R)$ denotes the Weyl group of a root system of type R; Sz denotes Suzuki groups). The group Rub at the end of the table is the Rubik group (the subgroup of $\mathfrak{S}_{48}$ that gives the possible moves on Rubik’s Cube).

8. ARITHMETIC CONSIDERATIONS

In this short section, we indicate the (expected) number-theoretic connections of our work.

First, let K be a Galois extension of $\mathbb{Q}$ with group G. For each prime p that is unramified in K, we have a well-defined Frobenius conjugacy class $\mathrm{Fr}_{p,K} \in G^\sharp$. For

n	Order	$c(\mathfrak{S}_n)$	$c_2(\mathfrak{S}_n)$
2	2	2.000000...	6.000000...
3	6	3.800000...	19.32000...
4	24	4.498380...	25.91538...
5	120	4.331526...	23.50351...
6	720	5.610738...	37.63260...
7	5040	4.115230...	21.20184...
8	40320	4.626289...	25.71722...
9	362880	4.250355...	22.49197...
10	3628800	4.624666...	25.76898...
11	39916800	4.173683...	21.86294...
12	479001600	4.583705...	25.11338...
13	6227020800	4.213748...	22.21319...
14	87178291200	4.508042...	24.57963...
15	1307674368000	4.365718...	23.39257...
16	20922789888000	4.461633...	24.12713...
17	355687428096000	4.282141...	22.79488...
18	6402373705728000	4.531784...	24.67680...
19	121645100408832000	4.308469...	23.01145...
20	2432902008176640000	4.497047...	24.37207...
21	51090942171709440000	4.391209...	23.61488...
22	1124000727777607680000	4.477492...	24.29632...
23	25852016738884976640000	4.352364...	23.37533...
24	620448401733239439360000	4.523388...	24.57409...

TABLE 1. Chebotarev invariants of $\mathfrak{S}_n$.

Name	Order	$c(G)$	$c_2(G)$
$\mathbb{Z}/17\mathbb{Z}$	17	1.062500...	1.195312...
$C_8 \subset H_{17}$	34	3.094697...	11.81350...
$C_4 \subset H_{17}$	68	4.890000...	35.53580...
$C_2 \subset H_{17}$	136	8.880953...	138.3764...
H_{17}	272	17.21053...	562.3851...
$\mathrm{PSL}(2, \mathbb{F}_{16})$	4080	3.200912...	12.73727...
7	8160	4.055261...	20.84364...
8	16320	4.067118...	20.58582...
A_{17}	177843714048000	4.089704...	21.12890...
$\mathfrak{S}_{17}$	355687428096000	4.282141...	22.79488...

TABLE 2. Chebotarev invariants of transitive groups of degree 17.

n	Order	c $\mathrm{PSL}(n, \mathbb{F}_2)$	c_2 $\mathrm{PSL}(n, \mathbb{F}_2)$
4	20160	4.939097...	31.98434...
5	9999360	4.238182...	25.64374...
6	20158709760	4.456089...	27.20052...
7	163849992929280	4.335957...	26.54874...
8	5348063769211699200	4.465723...	27.53266...
9	699612310033197642547200	4.460433...	27.64706...

TABLE 3. Chebotarev invariants of $\mathrm{PSL}(n, \mathbb{F}_2)$.

simplicity, we write $\mathrm{Fr}_{p,K} = 1$ when p is ramified in K. The *Chebotarev density theorem* says that

$$\lim_{y \to +\infty} \frac{|\{p \leq y : \mathrm{Fr}_{p,K} = C\}|}{\pi(y)} = \frac{|C|}{|G|}, \tag{8–1}$$

where $C \in G^\sharp$ is a fixed conjugacy class of G and $\pi(y)$ is the usual prime-counting function, i.e., the number of primes $p \leq y$.

Now fix a real number y large enough that every conjugacy class of G is of the form $\mathrm{Fr}_{p,K}$ for some $p \leq y$. For each $i \geq 1$, select uniformly and independently a random prime p from the set $\{p : p \leq y\}$ and define $X^\sharp_{i,y} = \mathrm{Fr}_{p,K}$. We thus have a sequence of independent and identically distributed random variables $X(y) = (X^\sharp_{i,y})$ in $G^\sharp$. As

p	Order	$c(B_3(\mathbb{F}_p))$	$c_2(B_3(\mathbb{F}_p))$
7	12348	10.07528...	150.8724...
11	133100	16.38777...	402.7223...
13	316368	18.85106...	551.0363...
17	1257728	25.31072...	978.0196...
19	2222316	27.79352...	1204.483...
23	5888828	34.28491...	1805.763...
29	19120976	43.27249...	2885.634...
31	26811900	45.75644...	3268.081...
37	65646288	54.75057...	4678.007...
41	110273600	61.26132...	5801.515...
43	140250348	63.74680...	6339.956...

TABLE 4. Chebotarev invariants of the Borel subgroup of $\mathrm{SL}(3, \mathbb{F}_p)$.

Name	Order	$c(G)$	$c_2(G)$
$W(G_2) = D_{12}$	12	$4.31\underline{15}\ldots = 717/165$	$23.45407\ldots$
$W(C_4)$	384	$4.864890\ldots$	$29.10488\ldots$
$W(F_4)$	1152	$5.417656\ldots$	$35.12470\ldots$
$\mathrm{GL}(2, \mathbb{F}_7)$	2016	$3.767768\ldots$	$17.29394\ldots$
$A_5 \times A_5$	3600	$5.374156\ldots$	$35.41628\ldots$
$W(C_5)$	3840	$4.863533\ldots$	$28.13517\ldots$
M_{11}	7920	$4.850698\ldots$	$29.72918\ldots$
$\mathrm{GL}(3, \mathbb{F}_3)$	11232	$4.110394\ldots$	$22.77077\ldots$
$G_2(\mathbb{F}_2)$	12096	$5.246204\ldots$	$34.24515\ldots$
$\mathrm{Sz}(8)$	29120	$3.101639\ldots$	$11.92233\ldots$
$W(C_6)$	46080	$5.792117\ldots$	$39.56093\ldots$
$W(E_6)$	51840	$4.470824\ldots$	$23.93050\ldots$
$\mathrm{Sp}(4, \mathbb{F}_3)$	51840	$4.401859\ldots$	$24.03143\ldots$
$\mathrm{PGL}(3, \mathbb{F}_4)$	60480	$3.763384\ldots$	$19.49865\ldots$
M_{12}	95040	$4.953188\ldots$	$29.53947\ldots$
J_1	175560	$3.423739\ldots$	$14.76364\ldots$
M_{22}	443520	$4.164445\ldots$	$22.70981\ldots$
J_2	604800	$4.031298\ldots$	$19.07590\ldots$
$W(C_7)$	645120	$4.632612\ldots$	$25.54504\ldots$
$\mathrm{PSp}(6, \mathbb{F}_2)$	1451520	$5.270439\ldots$	$34.84139\ldots$
$W(E_7)$	2903040	$5.398250\ldots$	$36.04850\ldots$
$G_2(\mathbb{F}_3)$	4245696	$4.511630\ldots$	$24.06106\ldots$
M_{23}	10200960	$4.030011\ldots$	$20.98580\ldots$
$W(C_8)$	10321920	$4.928996\ldots$	$28.53067\ldots$
T	17971200	$4.963701\ldots$	$32.54160\ldots$
$\mathrm{Sz}(32)$	32537600	$2.755449\ldots$	$9.107751\ldots$
HS	44352000	$4.484432\ldots$	$25.68549\ldots$
J_3	50232960	$4.304616\ldots$	$23.42082\ldots$
$W(C_9)$	185794560	$4.716359\ldots$	$26.41344\ldots$
M_{24}	244823040	$4.967107\ldots$	$29.84845\ldots$
$\mathrm{Sp}(4, \mathbb{F}_7)$	276595200	$3.501127\ldots$	$14.83811\ldots$
$\Omega^+(4, \mathbb{F}_{31})$	442828800	$3.829841\ldots$	$17.60003\ldots$
$\Omega^-(4, \mathbb{F}_{31})$	443751360	$3.003133\ldots$	$11.02613\ldots$
$W(E_8)$	696729600	$4.194248\ldots$	$20.79438\ldots$
McL	898128000	$4.561453\ldots$	$27.45649\ldots$
$\mathrm{Sp}(4, \mathbb{F}_9)$	3443212800	$3.409108\ldots$	$14.04475\ldots$
He	4030387200	$3.488680\ldots$	$14.31119\ldots$
$G_2(\mathbb{F}_5)$	5859000000	$3.855868\ldots$	$18.68766\ldots$
$\mathrm{Sp}(6, \mathbb{F}_3)$	9170703360	$3.871692\ldots$	$18.90072\ldots$
Co_3	495766656000	$4.535119\ldots$	$25.99974\ldots$
Co_2	42305421312000	$3.865290\ldots$	$17.74829\ldots$
$\Omega(5, \mathbb{F}_{31})$	409387254681600	$3.277801\ldots$	$12.90986\ldots$
Rub	43252003274489856000	$5.668645\ldots$	$36.78701\ldots$

TABLE 5. Chebotarev invariants of some other groups.

usual, we define the waiting time

$$\tau_{X(y),G} = \min\{n \geq 1 \mid (X^{\sharp}_{1,y}, \dots, X^{\sharp}_{n,y}) \text{ generate } G\} \\ \in [1, +\infty].$$

Using the Chebotarev density theorem, one obtains easily

$$\lim_{y \to +\infty} \mathbf{E}(\tau_{X(y),G}) = c(G).$$

Therefore, in an imprecise way, $c(G)$ can also be thought of as the expected number of "random" primes p needed for $\mathrm{Fr}_{p,K}$ to generate $G = \mathrm{Gal}(K/\mathbb{Q})$. Indeed, this is our motivation for using the name "Chebotarev invariant."

Of course in practice, one usually considers the (nonrandom) sequence $\mathrm{Fr}_{2,K}, \mathrm{Fr}_{3,K}, \mathrm{Fr}_{5,K}, \mathrm{Fr}_{7,K}, \dots$. We now explain, informally, what can be expected to happen in that situation. The deterministic analogue of the Chebotarev waiting time is given by

$$\tau(K) = \min\{k \geq 1 \mid \text{the first } k \text{ conjugacy classes} \\ \mathrm{Fr}_{2,K}, \dots, \mathrm{Fr}_{p_k,K} \text{ generate } G\},$$

where p_k is the kth prime.

However, for a fixed $K/\mathbb{Q}$, the value of $\tau(K)$ might diverge considerably from $c(G)$. So we suppose we have some family $\mathcal{K}$ of finite Galois extensions of $\mathbb{Q}$ (or another base field), all (or almost all) of which have Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ and a fixed finite group, and that for all values of some parameter $x \geq 1$, we have finite subfamilies $\mathcal{K}_x$ (that exhaust $\mathcal{K}$ as $x \to +\infty$) and some averaging process for invariants of the fields in $\mathcal{K}$, denoted by $\mathbf{E}_x$ (for instance, one might take

$$\mathbf{E}_x(\alpha(K)) = \frac{1}{|\mathcal{K}_n|} \sum_{K \in \mathcal{K}_x} \alpha(K),$$

but other weights, involving multiplicities, etc., might be better adapted). Using this, we can define Chebotarev invariants for the family $\mathcal{K}$ by averaging:

$$c(\mathcal{K}_x) = \mathbf{E}_x(\tau(K)), \quad c_2(\mathcal{K}_x) = \mathbf{E}_x(\tau(K)^2).$$

The basic arithmetic question is then this: for a given family, is it true that $c(\mathcal{K}_x)$ is, for x sufficiently large at least, close to $c(G)$ (and similarly for the secondary Chebotarev invariant)? The basic reason one can expect this to be the case is the Chebotarev density theorem (8–1).

We want to point out a few difficulties that definitely arise in trying to make this precise.

First of all, quantifying the Chebotarev density theorem is *hard*: it almost immediately runs into issues related to the generalized Riemann hypothesis; even in the seemingly trivial case in which $G = \mathbb{Z}/2\mathbb{Z}$, the basic question of estimating the size of the smallest nonsplit prime p in terms of the discriminant is unsolved.

This is a problem because if we sum with uniform weight, a single "bad" field K_0 can destroy any chance of approaching the Chebotarev invariant. Indeed, note that in that case,

$$\mathbf{E}_x(\tau(K)) \geq \frac{1}{|\mathcal{K}_x|} k_{\min}(K_0), \tag{8–2}$$

where

$$k_{\min}(K) = \min\{k \geq 1 \mid \mathrm{Fr}_{p,K} \neq 1\}$$

is the index of the first nontrivial Frobenius conjugacy class. In the current state of knowledge, it can be that there exists K_0 with

$$k_{\min}(K_0) > \mathrm{disc}(K_0)^A$$

for some constant $A > 0$ (see [Lagarias et al. 79]); on the other hand, if the family $\mathcal{K}$ is defined as that of splitting fields of monic polynomials of degree n, and the subfamily $\mathcal{K}_x$ is that of polynomials of height $\leq x$, then we know that most $K \in \mathcal{K}$ have Galois group $\mathfrak{S}_n$, that $|\mathcal{K}_x| = (2x+1)^n$ if x is an integer, and that the discriminant is obviously often also *at least* a power of x. Thus (8–2) might already be bad enough to preclude any comparison. On the other hand, on the Riemann hypothesis, we have

$$k_{\min}(K) \ll (\log \mathrm{disc}(K))^2$$

(where the implied constant depends on G), and the problem would then be alleviated.

Another issue is that one cannot expect, as stated, to have

$$\lim_{x \to +\infty} c(\mathcal{K}_x) = c(G)$$

for interesting families for the simple reason that the statistic of small primes is typically not the uniform one, i.e., if we fix a prime p, we cannot expect to have

$$\lim_{x \to +\infty} \mathbf{E}_x(\mathbf{1}_{\{\mathrm{Fr}_{p,K} = c^{\sharp}\}}) = \nu_G(c^{\sharp}),$$

even if we assume that all the fields involved are unramified at p.

On the other hand, it is well known that if p is increasing, the discrepancy between the distribution of the factorization patterns of square-free polynomials modulo p and the density of conjugacy classes disappears: we have

$$\frac{1}{p^n}|\{f \in \mathbb{F}_p[X] \mid f \text{ square-free of degree } n \text{ with } \mathrm{Fr}_f = c^\sharp\}| \sim \nu_G(c^\sharp)$$

uniformly for all conjugacy classes $c^\sharp \in G = \mathfrak{S}_n$.

This suggests that it is likely that one can prove some relevant results: one would consider some increasing starting point $s(x) \geq 2$ and a modified waiting time

$$\tau_x(K) = \min\{k \mid \text{the first } k \text{ conjugacy classes } \mathrm{Fr}_{p,K} \text{ with } p \geq s(x) \text{ generate } G\}$$

and hope to prove (possibly under the generalized Riemann hypothesis, possibly unconditionally after throwing away a few "bad" fields) that

$$\lim_{x\to+\infty} \mathbf{E}_x(\tau_x(K)) = c(G),$$

for suitable $s(x)$.

REFERENCES

[Arratia et al. 03] R. Arratia, A. D. Barbour, and S. Tavaré. *Logarithmic Combinatorial Structures: A Probabilistic Approach*, E.M.S. Monographs. Zurich: European Mathematical Society, 2003.

[Arratia and Tavaré 92] R. Arratia and S. Tavaré. "The Cycle Structure of Random Permutations." *Annals of Prob.* 20 (1992), 1567–1591.

[Bosma et al. 97] W. Bosma, J. Cannon, and C. Playoust. "The Magma Algebra System, I. The User Language." *J. Symbolic Comput.* 24 (1997), 235–265. See also http://magma.maths.usyd.edu.au/magma/.

[Dixon 92] J. D. Dixon: "Random Sets Which Invariably Generate the Symmetric Group." *Discrete Math.* 105 (1992), 25–39.

[Dixon 02] J. D. Dixon. "Probabilistic Group Theory." *C.R. Math. Rep. Acad. Sci. Canada* 24 (2002), 1–15.

[Flajolet et al. 92] P. Flajolet, D. Gardy, and L. Thimonier. "Birthday Paradox, Coupon Collectors, Caching Algorithms and Self-Organizing Search." *Discrete Applied Math.* 39 (1992), 207–229.

[Fulman and Guralnick 03] J. Fulman and R. Guralnick. "Derangements in Simple and Primitive Groups." In *Groups, Combinatorics, and Geometry (Durham, 2001)*, pp. 99–121. River Edge, NJ: World Sci. Publ., 2003.

[Fulton and Harris 91] W. Fulton and J. Harris. *Representation Theory. A First Course*, Grad. Texts in Math. 129. New York: Springer 1991.

[Gallagher 73] P. X. Gallagher. "The Large Sieve and Probabilistic Galois Theory." In *Proc. Sympos. Pure Math.*, vol. XXIV, pp. 91–101. Providence: Amer. Math. Soc., 1973.

[Goncharov 44] V. Goncharov: "Du domaine d'analyse combinatoire." *Bull. Acad. Sci. USSR Ser. Mat. (Izv. Akad. Nauk SSSR)* 8 (1944), 3–48; *Amer. Math. Soc. Transl. (2)* 19 (1962), 1–46.

[Jouve et al. 08] F. Jouve, E. Kowalski, and D. Zywina. "An Explicit Integral Polynomial Whose Splitting Field Has Galois Group $W(E_8)$." *Journal de Théorie des Nombres de Bordeaux* 20 (2008), 761–782.

[Jouve et al. 10] F. Jouve, E. Kowalski, and D. Zywina. "Splitting Fields of Characteristic Polynomials of Random Elements in Arithmetic Groups." arXiv:1008.3662, 2010.

[Kantor and Lubotzky 90] W. M. Kantor and A. Lubotzky. "The Probability of Generating a Finite Classical Group." *Geom. Dedicata* 36 (1990), 67–87.

[Kantor et al. 10] W. M. Kantor, A. Lubotzky, and A. Shalev. "Invariable Generation and the Chebotarev Invariant of a Finite Group." arXiv:1010.5722, 2010.

[Kowalski and Zywina 11] E. Kowalski and D. Zywina. "The Chebotarev Invariant of a Finite Group." arXiv:1008.4909, 2011.

[Lagarias et al. 79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko. "A Bound for the Least Prime Ideal in the Chebotarev Density Theorem." *Inventiones math.* 54 (1979), 271–296.

[Lloyd and Shepp 66] S. P. Lloyd and L. A. Shepp. "Ordered Cycle Lengths in a Random Permutation." *Trans. Amer. Math. Soc.* 121 (1966), 340–357.

[Łuczak and Pyber 93] T. Łuczak and L. Pyber. "On Random Generation of the Symmetric Group." *Combin. Probab. Comput.* 2 (1993), 505–512.

[Pomerance 01] C. Pomerance. "The Expected Number of Random Elements to Generate a Finite Abelian Group." *Period. Math. Hungar.* 43 (2001) 191–198.

[Rose 94] J. S. Rose: *A Course on Group Theory.* New York: Dover, 1994.

[Serre 72] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Invent. math.* 15 (1972), 259–331.

[Serre 98] J.-P. Serre. *Abelian ℓ-adic Representations and Elliptic Curves*, Res. Notes Math. Wellesley: A. K. Peters, 1998.

[Serre 02] J.-P. Serre: "On a Theorem of Jordan." *Math. Medley* 29 (2002), 3–18; also in *Bull. AMS* 40 (2003), 429–440.

Emmanuel Kowalski, ETH Zürich – D-MATH, Rümistrasse 101, 8092 Zürich, Switzerland (kowalski@math.ethz.ch)

David Zywina, Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA (zywina@math.upenn.edu)

Received August 28, 2010; accepted November 22, 2010.