Random character varieties

Emmanuel Breuillard

joint works with O. Becker and with P. Varjú

Banff, August 2022

Plan

I. Random polynomials, mixing times, Lehmer.

II. Height gap, uniform expanders.

III. Random groups, character varieties.

Irreducibility of random polynomials

Odlyzko and Poonen '93 conjectured that most polynomials of the form

$$P = 1 + \sum_{i=1}^{n} a_i X^i$$

where $a_i \in \{0, 1\}$ are irreducible.

Irreducibility of random polynomials

Odlyzko and Poonen '93 conjectured that most polynomials of the form

$$P = 1 + \sum_{i=1}^{n} a_i X^i$$

where $a_i \in \{0, 1\}$ are irreducible.

Recently two approaches have emerged about this question.

Irreducibility of random polynomials

- Konyagin (1999) showed that for $0,1$ polynomials

$$\mathbb{P}(P \text{ is irreducible }) \gg 1/\log n.$$

Irreducibility of random polynomials

• Konyagin (1999) showed that for $0, 1$ polynomials

$$\mathbb{P}(P \text{ is irreducible }) \gg 1/\log n.$$

• Bary-Soroker and Kozma (2017) showed that if the distribution of coefficients is uniform over $[1, H]$ and H is divisible by at least 4 distinct primes, then

$$\mathbb{P}(P \text{ is irreducible }) \to_{n \to +\infty} 1.$$

Irreducibility of random polynomials

• Konyagin (1999) showed that for $0, 1$ polynomials

$$\mathbb{P}(P \text{ is irreducible }) \gg 1/\log n.$$

• Bary-Soroker and Kozma (2017) showed that if the distribution of coefficients is uniform over $[1, H]$ and H is divisible by at least 4 distinct primes, then

$$\mathbb{P}(P \text{ is irreducible }) \to_{n \to +\infty} 1.$$

• B.+ Varju (2018): GRH implies the Odlyzko-Poonen conjecture.

Irreducibility of random polynomials

• Konyagin (1999) showed that for $0, 1$ polynomials

$$\mathbb{P}(P \text{ is irreducible }) \gg 1/\log n.$$

• Bary-Soroker and Kozma (2017) showed that if the distribution of coefficients is uniform over $[1, H]$ and H is divisible by at least 4 distinct primes, then

$$\mathbb{P}(P \text{ is irreducible }) \to_{n\to+\infty} 1.$$

• B.+ Varju (2018): GRH implies the Odlyzko-Poonen conjecture.

• Koukoulopoulos, Bary-Soroker and Kozma (2020) showed that for $0, 1$ polynomials

$$\mathbb{P}(P \text{ is irreducible }) \geq c > 0.$$

Irreducibility of random polynomials

• Koukoulopoulos, Bary-Soroker and Kozma showed much more. In particular they showed that for n large (say $\geq n_H$)

$$\mathbb{P}(P \text{ is irreducible }) \geq 1 - 1/n^{O(1)}$$

under very mild assumptions on the probability measure, e.g. for independent coefficients with uniform distribution on $[-H, H]$, $H \geq 17$ conditionally on $P(0) \neq 0$.

$\rightarrow$ the proof is a remarkable tour-de-force (exploiting recent advances on random permutations, level distribution for integers with missing digits, and more). They also show that the Galois group is large (i.e. at least $Alt(n)$)

Irreducibility of random polynomials

Assume the a_i's are independent and distributed according to a common law on $[-H, H] \subset \mathbb{Z}$ and set:

$$P = \sum_{i=0}^{n} a_i X^i$$

Irreducibility of random polynomials

Assume the a_i's are independent and distributed according to a common law on $[-H, H] \subset \mathbb{Z}$ and set:

$$P = \sum_{i=0}^{n} a_i X^i$$

Theorem (B.-Varjú '18)

Assume GRH. Then with probability at least $1 - \exp(-O(\frac{\sqrt{n}}{\log n}))$

$$P = \Phi \widetilde{P} \text{ where}$$

(i) $\widetilde{P}$ *is irreducible,*
(ii) $\deg(\Phi) = O(\sqrt{n})$ *and* Φ *is a product of cyclotomic factors,*
(iii) moreover the Galois group of P *contains* $Alt(n)$.

Irreducibility of random polynomials: proof method

Step 1

If P is an irreducible polynomial, then as $X \to +\infty$,

$$\mathbb{E}_{p \in [X,2X]}(\# \text{ roots of } P \mod p) = 1 + \text{error}$$

Note: this is an instance of the *Prime Ideal Theorem* as roots of P mod p correspond to prime ideals of $K_P := \mathbb{Q}[X]/(P)$ of norm p: there are roughly as many prime ideals of prime norm $\leqslant X$ as there are rational primes $\leqslant X$.

Note: the quality of the error term depends on the zeroes of the Dedekind zeta function ζ_{K_P}.

In particular, for an arbitrary polynomial P,

$$\mathbb{E}_{p \in [X,2X]}(\# \text{ roots of } P \mod p) = \#\text{irred. factors of } P + \text{error}$$

Irreducibility of random polynomials: proof method

Step 2

On the other hand, for a given prime p, averaging over P yields:

$$\mathbb{E}_P(\#\text{ roots of } P \mod p)) = \sum_{a\in\mathbb{F}_p} \mathbb{P}_P(P(a)=0) \simeq p.\frac{1}{p} \simeq 1$$

provided $\mathbb{P}_P(P(a)=0) \simeq \frac{1}{p}$ for all (most) a's.

Note that the random variable $P(a)$ on $\mathbb{F}_p$ is the n-th step of a random walk/Markov chain $x_{k+1} = ax_k + \mathbf{a_k}$, where the $\mathbf{a_i}$'s are the random coefficients of P.
Showing $\mathbb{P}_P(P(a)=0) \simeq \frac{1}{p}$ amounts to prove that the random walk reaches equilibrium before time n, i.e.

$$\text{mixing time on } \mathbb{F}_p \ll n$$

But Konyagin proved (using Dobrowolski's bound towards Lehmer's conjecture) that the mixing time of the random walk $P \mapsto P(a)$ is at most $(\log p)^{2+o(1)}$, provided $a \in \mathbb{F}_p$ has multiplicative order $\gg (\log p)^{1+o(1)}$.

$\rightarrow$ dividing out the cyclotomic factors and those with small Mahler measure, we can discard the a's in $\mathbb{F}_p$ with small multiplicative order.

$\rightarrow$ putting Steps 1 and 2 together we can take $n \simeq (\log p)^{2+o(1)}$, or equivalently $p \simeq \exp(X^{1/2-o(1)})$. The double averaging (over P and p) of the number $N_P(p)$ of roots mod p yields:

$$\begin{aligned}\mathbb{E}_P(\#\text{irred. factors of } P) &= \mathbb{E}_P\mathbb{E}_{p\in[X,2X]}N_P(p) \\ &= \mathbb{E}_{p\in[X,2X]}\mathbb{E}_P N_P(p) \simeq 1 \text{ QED}\end{aligned}$$

$\rightarrow$ GRH is used in controlling the error term in the Prime Ideal Theorem: $O(X^{\frac{1}{2}+o(1)} \log Disc(P))$ (Stark, Odlyzko)

Irreducibility of random polynomials

Theorem (B.-Varjú '18)

Assume GRH. Then with probability at least $1 - \exp(-O(\frac{\sqrt{n}}{\log n}))$

$$P = \Phi \widetilde{P} \text{ where}$$

(i) $\widetilde{P}$ *is irreducible,*
(ii) $\deg(\Phi) = O(\sqrt{n})$ *and* Φ *is a product of cyclotomic factors,*
(iii) moreover the Galois group of P *contains* $Alt(n)$.

Remark: It is plausible that the error term here can actually be taken to be exponential in n.

Irreducibility of random polynomials

Theorem (B.-Varjú '18)

Assume GRH. Then with probability at least $1 - \exp(-O(\frac{\sqrt{n}}{\log n}))$

$$P = \Phi \widetilde{P} \text{ where}$$

(i) $\widetilde{P}$ *is irreducible,*
(ii) $\deg(\Phi) = O(\sqrt{n})$ *and* Φ *is a product of cyclotomic factors,*
(iii) moreover the Galois group of P *contains* $Alt(n)$.

Remark: It is plausible that the error term here can actually be taken to be exponential in n. But this would imply the Lehmer conjecture.

Lehmer conjecture

The *Mahler measure* of a monic polynomial $P \in \mathbb{Z}[X]$ is defined as the modulus of the product of its roots located outside the unit disc, i.e.

$$M(P) := \prod_{|\theta_i|>1} |\theta_i|,$$

when

$$P(X) := \prod_{i=1}^{n} (X - \theta_i).$$

The *Mahler measure* of a monic polynomial $P \in \mathbb{Z}[X]$ is defined as the modulus of the product of its roots located outside the unit disc, i.e.

$$M(P) := \prod_{|\theta_i|>1} |\theta_i|,$$

when

$$P(X) := \prod_{i=1}^{n} (X - \theta_i).$$

Kronecker: $M(P) = 1$ if and only if all θ_i's are roots of unity.

Conjecture (Lehmer 1930's)

There is an absolute constant $\varepsilon_0 > 0$ such that for every monic polynomial $P \in \mathbb{Z}[X]$, either $M(P) = 1$ or $M(P) \geq 1 + \varepsilon_0$.

Relation with Lehmer's conjecture

Motto: putative counter-examples to Lehmer give rise (in reduction to residue fields) to values of $a \in \mathbb{F}_p$ with *slow* mixing rate.

Relation with Lehmer's conjecture

Motto: putative counter-examples to Lehmer give rise (in reduction to residue fields) to values of $a \in \mathbb{F}_p$ with *slow* mixing rate.

Say that a prime p is δ-bad if there exists $a \in \mathbb{F}_p^\times$ with multiplicative order $\geq (\log p)^2$ such that for some $n \geq \frac{1}{\delta} \log p$

$$|\{P(a) \mod p | P \text{ a } 0,1 \text{ polynomial of deg } n\}| \leqslant p^\delta.$$

Theorem (B.-Varjú '18)

The following are equivalent:

1. *There is $\delta \in (0,1)$ s.t. almost no prime is δ-bad, i.e.*

$$|\{p \leq x | p \text{ is } \delta\text{-bad}\}| = o_{x \to +\infty}(|\{p \leq x\}|).$$

2. *The Lehmer conjecture holds.*

Relation with Lehmer's conjecture

Motto: putative counter-examples to Lehmer give rise (in reduction to residue fields) to values of $a \in \mathbb{F}_p$ with *slow* mixing rate.

Say that a prime p is δ-bad if there exists $a \in \mathbb{F}_p^\times$ with multiplicative order $\geq (\log p)^2$ such that for some $n \geq \frac{1}{\delta} \log p$

$$|\{P(a) \mod p | P \text{ a } 0{,}1 \text{ polynomial of deg } n\}| \leqslant p^\delta.$$

Theorem (B.-Varjú '18)

The following are equivalent:

1. *There is $\delta \in (0,1)$ s.t. almost no prime is δ-bad, i.e.*

$$|\{p \leq x | p \text{ is } \delta\text{-bad}\}| = o_{x \to +\infty}(|\{p \leq x\}|).$$

2. *The Lehmer conjecture holds.*

$\to$ hence mixing in $O(\log p)$ for all a with large order *implies* Lehmer.

II. Height gap, uniform expanders.

Random walks on finite groups of Lie type

The random walk on $\mathbb{F}_p$ considered earlier: $x_{n+1} = ax_n \pm 1$, whose n-th step is distributed exactly as $P(a)$ for a random P, can be seen as a random walk on the (upper triangular) affine group $Aff(\mathbb{F}_p)$:

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_p^{\times}, b \in \mathbb{F}_p \right\}$$

Random walks on finite groups of Lie type

The random walk on $\mathbb{F}_p$ considered earlier: $x_{n+1} = ax_n \pm 1$, whose n-th step is distributed exactly as $P(a)$ for a random P, can be seen as a random walk on the (upper triangular) affine group $Aff(\mathbb{F}_p)$:

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

Similarly, we can consider a random walk on $\mathrm{SL}_2(p)$, or $G(p)$ for a simple group G over $\mathbb{F}_p$.

Mixing time for such walks has been studied a lot in the last twenty years (Bourgain, Gamburd, Sarnak, Helfgott, etc.).

The random walk on $\mathbb{F}_p$ considered earlier: $x_{n+1} = ax_n \pm 1$, whose n-th step is distributed exactly as $P(a)$ for a random P, can be seen as a random walk on the (upper triangular) affine group $Aff(\mathbb{F}_p)$:

$$\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \}$$

Similarly, we can consider a random walk on $\mathrm{SL}_2(p)$, or $G(p)$ for a simple group G over $\mathbb{F}_p$.

Mixing time for such walks has been studied a lot in the last twenty years (Bourgain, Gamburd, Sarnak, Helfgott, etc.).

A finite k-regular graph Γ is an *ε-expander graph* if the random walk on it has mixing time $\ll_{\varepsilon,k} \log|\Gamma|$.

Conjecture (folklore)

For each $k, r \geq 1$ there is $\varepsilon > 0$ s.t. every k-regular Cayley graph of a finite simple group of rank at most r is an ε-expander.

This is open even for the subfamily of groups $\{PSL_2(p), p \text{ prime }\}$.

Remark: the restriction on the rank is necessary. Indeed if $Alt(n) = \langle \tau, \sigma \rangle$, with $\tau = (123), \sigma = (12...n)$, n odd, then the Cayley graph has *diameter* $\gg n^2$, but $\log |Alt(n)| \simeq n \log n$.

Expanders - uniformity

Let $\mathbf{G}(p)$ denote a finite simple group of Lie type over $\mathbb{F}_p$.

Theorem (B+Becker, '22)

for all $\varepsilon > 0$ there is $\mathcal{E}(\varepsilon) \subset \mathcal{P}$ an exceptional set of primes s.t.
(i) $|\mathcal{E}(\varepsilon) \cap [1, T]| \leqslant T^{\varepsilon}$ for all $T \geq 1$
(ii) if $p \notin \mathcal{E}(\varepsilon)$ then every k-regular Cayley graph of $\mathbf{G}(p)$ is an ε-expander. In particular mixing time is $\ll_{\varepsilon} \log p$.

The result generalizes previous joint work of mine with Gamburd ($\sim$ 2010), where we had proved this for $\mathbf{G} = SL(2)$.

The uniformity here (i.e. every generating set) parallels the uniformity (i.e. every a of large multiplicative order) in Konyagin's mixing estimate on $Aff(\mathbb{F}_p)$.

Just as Konyagin's estimate relied on Dobrowolski's bounds, at the heart of the above uniformity for $G(p)$ is a result in diophantine analysis about the height of eigenvalues in Zariski-dense subgroups of semisimple algebraic groups $\mathbf{G}$ (e.g. $\mathbf{G} = \mathrm{SL}_2$):

Theorem (Height gap theorem, B. '08)

There are $\varepsilon_0 = \varepsilon_0(\mathbf{G}) > 0$ and $N_0 = N_0(\mathbf{G})$ s.t. for every $S \subset \mathbf{G}(\overline{\mathbb{Q}})$ with $\langle S \rangle$ Zariski-dense in $\mathbf{G}(\overline{\mathbb{Q}})$ there is $g \in S^{N_0}$ and an eigenvalue λ of g such that

$$h(\lambda) > \varepsilon_0.$$

Here $h(\lambda)$ denotes the (normalized) Weil height of the algebraic number λ.

III: Random groups, character varieties.

Let

$$\Gamma_{\underline{w}} = \langle x_1, \ldots, x_k | w_1 = \ldots = w_r = 1 \rangle$$

be a finitely presented group with k generators and r relators.

Let $G = \mathbf{G}(\mathbb{C})$ be a semisimple algebraic group (defined over $\mathbb{Q}$ say). For example $G = \mathrm{SL}_2(\mathbb{C})$.

Let $X_{\underline{w}} = \mathrm{Hom}(\Gamma_{\underline{w}}, G)$ be the representation variety. It is a closed algebraic set in G^k.

Let $\mathcal{X}_{\underline{w}} = X_{\underline{w}} /\!\!/ G$ be the *character variety*. It is the affine variety with coordinate ring $\mathbb{C}[X_{\underline{w}}]^G$.
Let $\mathcal{X}^Z_{\underline{w}} = X_{\underline{w}} /\!\!/ G$ be the **Zariski dense part** of the *character variety* i.e. $X_{\underline{w}} \cap \Omega /\!\!/ G$, where

$$\Omega := \langle \underline{x} \in G^k, \langle \underline{x} \rangle \text{ is Zariski dense in } G\}$$

<u>Fact:</u> Ω is Zariski open in G^k.

Characters of finitely presented groups - questions

Recall $\mathcal{X}^Z_{\underline{w}} = \mathrm{Hom}(\Gamma_{\underline{w}}, G) \cap \Omega /\!\!/ G$ denotes the 'Zariski-dense character variety'. Some natural questions:

1. $\dim \mathcal{X}^Z_{\underline{w}}$?
2. $\#$ irreducible components?
3. Action of Galois on the components?
4. singularities on $\mathcal{X}^Z_{\underline{w}}$?
5. locus of faithful reps? discrete reps?

Examples:
(a) When $\Gamma_{\underline{w}}$ is a *higher-rank lattice* (e.g. $\mathrm{SL}_n(\mathbb{Z})$ $n \geq 3$), then $\mathcal{X}^Z_{\underline{w}}$ is finite (Margulis' super-rigidity theorem), and even $\mathbb{Q}$-irreducible (the Galois group acts transitively): we say that $\Gamma_{\underline{w}}$ is *Galois rigid*.

Further examples:

(b) $\Gamma_{\underline{w}} = \pi_1(\Sigma_g)$ a surface group of genus $g \geq 2$.

$$\Gamma_w = \langle a_1, \ldots, a_g, b_1, \ldots, b_g | [a_1, b_1] \ldots [a_g, b_g] = 1 \rangle.$$

Then we know (Rapinchuk et al., Liebeck-Shalev) that $\mathcal{X}^Z_{\underline{w}}$ is absolutely irreducible and that

$$\dim \mathcal{X}^Z_{\underline{w}} = (2g-2) \dim G.$$

(c) $\mathcal{X}^Z_{\underline{w}}$ can be empty, for example it is so for $\Gamma_{\underline{w}} = \langle a, b | ba^n b^{-1} a^{-m} = 1 \rangle$ with $\gcd(n, m) = 1$, the Baumslag-Solitar group with $|n| > |m| > 1$.

(d) When $G = \mathrm{SL}_2(\mathbb{C})$ with $k = 2$ generators and $r = 1$ relator we can be very explicit:

Fricke-Klein coordinates: $x = \mathrm{tr}(a), y = \mathrm{tr}(b), z = \mathrm{tr}(ab)$.

<u>Fact:</u> $\forall w \exists P_w \in \mathbb{Z}[x, y, z]$

$$\mathrm{tr}(w(a, b)) = P_w(x, y, z)$$

Moreover $\Omega = G^2 \setminus V_{deg}$ where V_{deg} is the union of:

- the cubic hypersurface $x^2 + y^2 + z^2 - xyz - 4 = 0$ (locus of *reducible* reps)
- 3 lines $x = y = 0$, $x = z = 0$, $y = z = 0$ (dihedral reps),
- a finite set with $x, y, z \in \{0, \pm 1, \pm\sqrt{2}, \phi, 1 - \phi\}$, $\phi =$ golden mean (finite reps).

(d) (continued) We can then find equations for $\mathcal{X}_{\underline{w}}^{Z}$ as follows:

$$\mathcal{X}_{\underline{w}}^{Z} = \{P_w = 2, P_{aw} = x, P_{bw} = y\} \setminus V_{deg}.$$

Computer algebra system (e.g. ‘singular‘) does then compute $\dim \mathcal{X}_{\underline{w}}^{Z}$ and the number of components.

Sage routine for P_w (cf. Ashley-Burelle-Lawton).

<u>Exple:</u> $\langle a, b | [a, u] = 1 \rangle$, $u = [b, a] b^{-1} ab$ is the π_1 of the Whitehead link complement. Then $\mathcal{X}_{\underline{w}}^{Z}$ is open in the hypersurface $x^2 z + y^2 z + z^3 - xy - 2z - xyz^2 = 0$.

Representations of random groups - main theorem

We attempt to answer the above questions for random presentations. Let B_ℓ the set of r-tuples of words of length ℓ in k letters $x_1^{\pm 1}, \dots, x_k^{\pm 1}$. Here k, r are fixed, but ℓ is large.

Theorem (B.+Becker+Varjú)

(under GRH) There is an exceptional set $\mathcal{E}_\ell \subset B_\ell$ with $|\mathcal{E}_\ell| \leqslant e^{-c\ell}|B_\ell|$ for some $c = c(\mathbf{G}) > 0$ s.t. for all $\underline{w} \in B_\ell \setminus \mathcal{E}_\ell$:

1. *if $r \geq k$, $\mathcal{X}_{\underline{w}}^Z$ is empty,*
2. *if $r = k-1$, $\mathcal{X}_{\underline{w}}^Z$ is finite and non-empty and $\mathbb{Q}$-irreducible (Galois-rigid),*
3. *$r \leqslant k-2$, $\mathcal{X}_{\underline{w}}^Z$ is absolutely irreducible and of dimension*

$$\dim \mathcal{X}_{\underline{w}}^Z = (k-r-1)\dim G.$$

Representations of random groups - main theorem

Let B_ℓ the set of r-tuples of words of length ℓ in k letters $x_1^{\pm 1}, \ldots, x_k^{\pm 1}$. Here k, r are fixed, but ℓ is large.

Theorem (B.+Becker+Varjú)

(under GRH) There is an exceptional set $\mathcal{E}_\ell \subset B_\ell$ with $|\mathcal{E}_\ell| \leqslant e^{-c\ell}|B_\ell|$ for some $c = c(\mathbf{G}) > 0$ s.t. for all $\underline{w} \in B_\ell \setminus \mathcal{E}_\ell$:

1. *if $r \geq k$, $\mathcal{X}_{\underline{w}}^{Z}$ is empty,*
2. *if $r = k - 1$, $\mathcal{X}_{\underline{w}}^{Z}$ is finite and non-empty and $\mathbb{Q}$-irreducible (Galois-rigid),*
3. *$r \leqslant k - 2$, $\mathcal{X}_{\underline{w}}^{Z}$ is absolutely irreducible and of dimension*

$$\dim \mathcal{X}_{\underline{w}}^{Z} = (k - r - 1) \dim G.$$

Note that we obtain an exponentially small probability of exceptions. In particular this result is meaningful even if the $\underline{w}$ are constrained to lie in the commutator subgroup $[F_k, F_k]$, or in $D^m(F_k)$ the m-th term of the derived series of the free group.

Representations of random groups - main theorem

Corollary

Fix d and $r \geq k$. For all $\underline{w} \in B_\ell \setminus \mathcal{E}_\ell$, every homomorphism from $\Gamma_{\underline{w}}$ to $\mathrm{GL}_d(\mathbb{C})$ has virtually solvable image.

Our work was motivated by a recent paper of Kozma and Lubotkzy (2019), who proved that if one takes $r \gg \log \ell$ random relators, then, with high probability, every homomorphism from $\Gamma_{\underline{w}}$ to $\mathrm{GL}_d(\mathbb{C})$ has trivial (or $\mathbb{Z}/2\mathbb{Z}$) image.

Representations of random groups - the method

Lang-Weil: X variety over $\mathbb{F}_q$

$$|X(q)| = c(X,q)q^{\dim X} + O(q^{\dim X - 1/2})$$

where
$c(X,q) = \#$geometric components defined over $\mathbb{F}_q$.

strategy: estimate $|X_{\underline{w}}^Z(p)|$ for various primes.

main idea: similar as in Part I: double counting: average $|X_{\underline{w}}^Z(p)|$
- over the primes in a moving window $[\frac{1}{2}T, T]$ with $T \to +\infty$.
- over words of length ℓ.

To get exponential control on the size of the exceptional set of words, we will need to take T to be of size $\exp(C\ell)$ for some $C > 0$, hence the uniform expander results of Part II are essential here.

Representations of random groups - the method

Chebotarev: X variety over $\mathbb{Q}$, then

$$\dim X = \limsup_{p \to +\infty} \frac{\log |X(p)|}{p}$$

$$\mathbb{E}_{p \in [T/2, T]} \frac{|X(p)|}{p^{\dim X}} \to_{T \longrightarrow +\infty} \#\mathbb{Q} - \textit{irred} \text{ components of } X$$

(see Serre's *Lectures on* $N_X(p)$).

This is for fixed X. But we need this for $\underline{X_w}$ for all $\underline{w}$ and the degree of $\underline{X_w}$ grows with $\ell =$ length of $\underline{w}$.

$\to$ we need an *effective version* of all these facts (i.e. Lang-Weil and Chebotarev).
$\to$ need *polynomial* control (in the degree aspect) for Lang-Weil, and the prime ideal theorem (on whose proof Chebotarev is based).

Effective Chebotarev

Let L be a Galois number field with Galois group G, $K \leqslant L$ a subfield, Δ_K its discriminant. For $k \geq 1$, let $N_k^K(T)$ the number of prime ideals of norm p^k in K for p prime in $[T/2, T]$.

Theorem (effective Prime ideal Theorem, under GRH)

$|kN_k^K(T) - P_k N_1^{\mathbb{Q}}(T)| \leqslant CT^{1/2}[K : \mathbb{Q}]^{Ck}(\log \Delta_K + \log T)$

P_k is the k-th *Parker number*, a non-negative integer depending on k and G (and $\sum_1^n P_k = [K : \mathbb{Q}]$) defined by:

$$P_k = \frac{1}{|G|} \sum_{g \in G} kc_k(g)$$

where $c_k(g)$ is the number of k-cycles of g.
$\rightarrow$ proof requires expressing $kc_k(g)$ as an integer combination of *permutation characters* of controlled dimension, and applying the proof of the Prime Ideal Theorem to each.

Representations of random groups - proof idea

Double counting ($\mathbb{E}$ denotes expectation):

$$\mathbb{E}_{p\in[T/2,T]}\mathbb{E}_{\underline{w}}|X_{\underline{w}}(p)| = \mathbb{E}_{\underline{w}}\mathbb{E}_{p\in[T/2,T]}|X_{\underline{w}}(p)|$$

$$\mathbb{E}_{\underline{w}}|X_{\underline{w}}(p)| = \sum_{\underline{x}\in G(p)^k} \mathbb{P}_{\underline{w}}(\underline{w}(\underline{x}) = 1)$$

If $Cay(G(p), \underline{x})$ is an expander, then

$$|\mathbb{P}_{\underline{w}}(\underline{w}(\underline{x}) = 1) - \frac{1}{|G(p)|}| \ll \text{small error}$$

for all $\ell \gg \log p$.
$\longrightarrow$ use of uniform expansion (as in Part II of the talk) is *essential* here.

Representations of random groups - proof idea

When $k = r + 1$, this leads to $\mathbb{E}_{p \in [T/2.T]} |X_{\underline{w}}^{Z}(p)| \simeq 1$ w.o.p in $\underline{w}$, and thus that $X_{\underline{w}}^{Z}$ is finite and $\mathbb{Q}$-irreducible.

When $k > r + 1$, we obtain the right dimension for $X_{\underline{w}}^{Z}$. Absolute irreducibility is obtained by considering the character variety of $\Gamma_{\underline{w}}$ with values in the cartesian product $G \times G$

Galois lower bound, work in progress

Theorem

(under GRH) Suppose $G = \mathrm{SL}_2$. When $k = r + 1$, then away from an exceptional set of words $\underline{w}$ of exponentially small proportion,

$$|\mathcal{X}_{\underline{w}}^{Z}| \gg \ell / \log \ell$$

and the Galois group acts transitively as Alt or Sym.

Note: By Bézout, $|\mathcal{X}_{\underline{w}}^{Z}| = O(\ell^{O(1)})$.
idea: similar counting, but in $G(p^k)$ for k as large as $\ell/\log \ell$. This complicates matters as there can be many subfields subgroups in $G(p^k)$.
We show that w.h.p. $\mathbb{E}_{p \in [T/2, T]} |X_{\underline{w}}^{Z}(p^k)| \simeq \tau(k)$ the number of divisors of k. This will give that $P_k = 1$ for all $k \ll \ell/\log \ell$. This is enough info on the permutation group to conclude.

Thank you!