The Chebotarev invariant of a finite group

Gareth Tracey

Rényi Institute, Budapest

Isaac Newton Institute for Mathematical Sciences
January 14th, 2020

Informal overview

Rough description 1

The Chebotarev invariant $C(G)$ of a finite group G is, roughly speaking, a waiting time to find a certain type of strong generating set [invariable generating set] in G, when choosing elements at random.

Informal overview

Rough description 1

The Chebotarev invariant $C(G)$ of a finite group G is, roughly speaking, a waiting time to find a certain type of strong generating set [invariable generating set] in G, when choosing elements at random.

Rough description 2

The Chebotarev invariant $C(G)$ of a finite Galois group G, is the expected number of random primes required to "generate" G.

Plan for the talk

1. Some practical motivation, and a related invariant.

Plan for the talk

1. Some practical motivation, and a related invariant.
2. Defining invariable generation, and the Chebotarev invariant.

Plan for the talk

1. Some practical motivation, and a related invariant.
2. Defining invariable generation, and the Chebotarev invariant.
3. Motivation from Galois theory.

Plan for the talk

1. Some practical motivation, and a related invariant.
2. Defining invariable generation, and the Chebotarev invariant.
3. Motivation from Galois theory.
4. A conjecture of Kowalski and Zywina; current results; and some ideas from the proofs.

Plan for the talk

1. Some practical motivation, and a related invariant.
2. Defining invariable generation, and the Chebotarev invariant.
3. Motivation from Galois theory.
4. A conjecture of Kowalski and Zywina; current results; and some ideas from the proofs.
5. Closing remarks: Permutation groups.

1. Practical motivation for studying probabilistic generation

Probabilsitic vs Minimal generation

Moral question

Why should we study probabilistic generation [the probability that a random d-tuple of elements of a group generate the group] rather than just minimal generation [the minimal d such that there exists such a d-tuple]?

Probabilsitic vs Minimal generation

Moral question

Why should we study probabilistic generation [the probability that a random d-tuple of elements of a group generate the group] rather than just minimal generation [the minimal d such that there exists such a d-tuple]?

Example ($G := Alt(5)^{19}$)

1. $d(G) = 2$..[$d(X)$ is the minimal number of elements required to generate the finite group X]

Probabilsitic vs Minimal generation

Moral question

Why should we study probabilistic generation [the probability that a random d-tuple of elements of a group generate the group] rather than just minimal generation [the minimal d such that there exists such a d-tuple]?

Example ($G := Alt(5)^{19}$)

1. $d(G) = 2$..[$d(X)$ is the minimal number of elements required to generate the finite group X]
2. ..But the probability that a random 2-tuple (x, y) from $G \times G$ generates G is around $0.000000000010466242223689929832286180403 8..$ (Kantor and Lubotzky, 1990).

Probabilsitic vs Minimal generation

Moral question

Why should we study probabilistic generation [the probability that a random d-tuple of elements of a group generate the group] rather than just minimal generation [the minimal d such that there exists such a d-tuple]?

Example ($G := Alt(5)^{19}$)

1. $d(G) = 2$..[$d(X)$ is the minimal number of elements required to generate the finite group X]
2. ..But the probability that a random 2-tuple (x, y) from $G \times G$ generates G is around 0.000000000010466242223689929832286180403 8.. (Kantor and Lubotzky, 1990).
3. The expected number of elements required to generate G [when one choose elements uniformly at random, with replacement], on the other hand is approx. 4.296971920512335513548518374 43..

"Probabilistic versions" of $d(G)$

There are a few different ways one can study "probabilistic minimal generation"..

"Probabilistic versions" of $d(G)$

There are a few different ways one can study "probabilistic minimal generation"..

For example, Pak (1999) and Holt and Roney-Dougal (2013) have studied the invariant $d^{\epsilon}(G)$: the minimal number k such that the probability $P_G(k)$ that k uniformly-distributed random elements of G generate G with probability at least $1 - \epsilon$.

"Probabilistic versions" of $d(G)$

There are a few different ways one can study "probabilistic minimal generation"..

For example, Pak (1999) and Holt and Roney-Dougal (2013) have studied the invariant $d^{\epsilon}(G)$: the minimal number k such that the probability $P_G(k)$ that k uniformly-distributed random elements of G generate G with probability at least $1 - \epsilon$.

Dixon's conjecture [Dixon (1969); Kantor and Lubotzky (1990); and Liebeck and Shalev (1995)] shows that for all $\epsilon > 0$ there exists $N = N(\epsilon)$ such that $d^{\epsilon}(G) = 2$ for all finite simple groups G with $|G| > N$.

"Probabilistic versions" of $d(G)$

There are a few different ways one can study "probabilistic minimal generation"..

For example, Pak (1999) and Holt and Roney-Dougal (2013) have studied the invariant $d^{\epsilon}(G)$: the minimal number k such that the probability $P_G(k)$ that k uniformly-distributed random elements of G generate G with probability at least $1 - \epsilon$.

Dixon's conjecture [Dixon (1969); Kantor and Lubotzky (1990); and Liebeck and Shalev (1995)] shows that for all $\epsilon > 0$ there exists $N = N(\epsilon)$ such that $d^{\epsilon}(G) = 2$ for all finite simple groups G with $|G| > N$.

In this talk, we will study $E(G)$: the expected number of uniformly-distributed random elements of G required to generate G.

We remark that Chebyshev's Inequality from Probability Theory tells us that $d^{\epsilon}(G) \leq \frac{E(G)}{\epsilon}$, so the invariant $E(G)$ gives information about $d^{\epsilon}(G)$ as well.

Formal definition of $E(G)$

Let G be a finite group, and let $(x_i)_{i \in \mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables.

Formal definition of $E(G)$

Let G be a finite group, and let $(x_i)_{i\in\mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables.

We define a random variable (a waiting time) $\mathcal{T}_G$ by

$$\mathcal{T}_G := \min\{n \in \mathbb{N} : \{x_1, \ldots, x_n\} \text{ generates } G\}.$$

Formal definition of $E(G)$

Let G be a finite group, and let $(x_i)_{i\in\mathbb{N}}$ be a sequence of independent, uniformly distributed G-valued random variables.

We define a random variable (a waiting time) $\mathcal{T}_G$ by

$$\mathcal{T}_G := \min\{n \in \mathbb{N} : \{x_1, \ldots, x_n\} \text{ generates } G\}.$$

$E(G)$ is then defined to be the expected value of this random variable: $E(G) := E(\mathcal{T}_G)$.

What do we know about $E(G)$?

Of course, $d(G) \leq E(G)$.. But how large can $E(G) - d(G)$ be?

What do we know about $E(G)$?

Of course, $d(G) \leq E(G)$.. But how large can $E(G) - d(G)$ be?

The abelian case was done by Pomerance:

What do we know about $E(G)$?

Of course, $d(G) \leq E(G)$.. But how large can $E(G) - d(G)$ be?

The abelian case was done by Pomerance:

Theorem (Pomerance, 2001)

Let G be a finite abelian group. Then

$$d(G) \leq E(G) \leq d(G) + \sigma$$

where $\sigma \sim 2.118456565\ldots$.

What do we know about $E(G)$?

Of course, $d(G) \leq E(G)$.. But how large can $E(G) - d(G)$ be?

The abelian case was done by Pomerance:

Theorem (Pomerance, 2001)

Let G be a finite abelian group. Then

$$d(G) \leq E(G) \leq d(G) + \sigma$$

where $\sigma \sim 2.118456565\ldots$.

Corollary (Pomerance, 2001)

Let G be a finite nilpotent group. Then

$$d(G) \leq E(G) \leq d(G) + \sigma$$

where $\sigma \sim 2.118456565\ldots$.

$d(G)$ vs $E(G)$

Kantor and Lubotzky (1990) have shown that $E(G) - d(G)$ can be arbitrarily large in general..

$d(G)$ vs $E(G)$

Kantor and Lubotzky (1990) have shown that $E(G) - d(G)$ can be arbitrarily large in general..

.. However, the difference has been shown to be "small":

$d(G)$ vs $E(G)$

Kantor and Lubotzky (1990) have shown that $E(G) - d(G)$ can be arbitrarily large in general..

.. However, the difference has been shown to be "small":

Theorem (Detomi and Lucchini, 2003; Lubotzky, 2003)

Let G be a finite group. Then

$$E(G) \leq d(G) + O(\log \log |G|) \leq O(\log |G|).$$

Exact formula for $E(G)$

Furthermore, Lucchini has now given an exact formula for $E(G)$ in terms of a "Mobiüs function on subgroups":

Theorem (Lucchini, 2015)

Let G be a finite group, and define the function μ_G by $\mu_G(G) := 1$, and $\mu_G(H) := -\sum_{H<K} \mu_G(K)$ for any $H < G$. Then

$$E(G) = \sum_{H<G} \frac{\mu_G(H)|G|}{|G| - |H|}.$$

2. Defining invariable generation and the Chebotarev invariant

A related invariant

A related invariant

Definition (Dixon)

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for each choice of $(g_1, \ldots, g_d) \in G^d$.

A related invariant

Definition (Dixon)

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for each choice of $(g_1, \ldots, g_d) \in G^d$.

Example (S_3)

Any 2-cycle and any 3-cycle invariably generate S_3. The set $\{(1,2),(2,3)\}$ is an example of a generating set for S_3 which is not an invariable generating set.

A related invariant

Definition (Dixon)

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for each choice of $(g_1, \ldots, g_d) \in G^d$.

Example (S_3)

Any 2-cycle and any 3-cycle invariably generate S_3. The set $\{(1,2),(2,3)\}$ is an example of a generating set for S_3 which is not an invariable generating set.

Example ($\mathbf{SL}_n(p)$)

If A is a set of transvections with $\mathbf{SL}_n(p) = \langle A \rangle$, then A is not an invariable generating set for $\mathbf{SL}_n(p)$.

A related invariant

Definition (Dixon)

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for each choice of $(g_1, \ldots, g_d) \in G^d$.

Example (S_3)

Any 2-cycle and any 3-cycle invariably generate S_3. The set $\{(1,2),(2,3)\}$ is an example of a generating set for S_3 which is not an invariable generating set.

Example ($\mathbf{SL}_n(p)$)

If A is a set of transvections with $\mathbf{SL}_n(p) = \langle A \rangle$, then A is not an invariable generating set for $\mathbf{SL}_n(p)$.

Example (In general..)

- If p is a fixed prime and G is not a p-group, then a set of p-elements can not be an invariable generating set for G.

A related invariant

Definition (Dixon)

A subset $\{x_1, x_2, \ldots, x_d\}$ of a group G *invariably generates* G if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for each choice of $(g_1, \ldots, g_d) \in G^d$.

Example ($\mathbf{SL}_n(p)$)

If A is a set of transvections with $\mathbf{SL}_n(p) = \langle A \rangle$, then A is not an invariable generating set for $\mathbf{SL}_n(p)$.

Example (In general..)

- If p is a fixed prime and G is not a p-group, then a set of p-elements can not be an invariable generating set for G.
- In fact, if G is a finite group, then G is nilpotent if and only if every generating set for G is an invariable generating set (Kantor, Lubotzky and Shalev, 2011).

Infinite groups: A warning

Of course, one can also speak about invariable generation in infinite groups..

Infinite groups: A warning

Of course, one can also speak about invariable generation in infinite groups..

But here, not only do you have to decide whether or not such a G is finitely invariably generated, but whether it is invariably generated at all: Sometimes, not even G generates G invariably!

Infinite groups: A warning

Of course, one can also speak about invariable generation in infinite groups..

But here, not only do you have to decide whether or not such a G is finitely invariably generated, but whether it is invariably generated at all: Sometimes, not even G generates G invariably!

The easiest way to see this is to take $G = GL_n(\mathbb{C})$, and notice that every invertible matrix over $\mathbb{C}$ is triangularizable (into Jordan normal form). Hence, G does not invariably generate itself.

Invariable generation: Definitions

We can of course now define "invariable generation invariants" in an analogous way to their "generation" equivalents..

Invariable generation: Definitions

We can of course now define "invariable generation invariants" in an analogous way to their "generation" equivalents..

Definition

We write $d_I(G)$ for the minimal number of elements required to invariably generate G.

Invariable generation: Definitions

We can of course now define "invariable generation invariants" in an analogous way to their "generation" equivalents..

Definition

We write $d_I(G)$ for the minimal number of elements required to invariably generate G.

Definition

We write $C(G)$ for the expected number of uniform random elements required to invariably generate G. We call $C(G)$ the *Chebotarev invariant* of G.

Invariable generation: Definitions

We can of course now define "invariable generation invariants" in an analogous way to their "generation" equivalents..

Definition

We write $d_I(G)$ for the minimal number of elements required to invariably generate G.

Definition

We write $C(G)$ for the expected number of uniform random elements required to invariably generate G. We call $C(G)$ the *Chebotarev invariant* of G.

But why do we care?!

3. Motivation from Galois theory

Invariable generation: Why do we care?

Questions on invariable generation go back to the 1930s..

Question (van der Waerden, 1936)

If one chooses elements of the symmetric group S_n uniformly at random, with replacement, then how long will one have to wait before one finds an invariable generating set?

Motivation: Galois theory

Let K be Galois extension over $\mathbb{Q}$.

Motivation: Galois theory

Let K be Galois extension over $\mathbb{Q}$.

For each prime p which is unramified in K, there is a well-defined Frobenius conjugacy class in $G := Gal(K/\mathbb{Q})$. Call it $C_p(K)$.

Motivation: Galois theory

Let K be Galois extension over $\mathbb{Q}$.

For each prime p which is unramified in K, there is a well-defined Frobenius conjugacy class in $G := Gal(K/\mathbb{Q})$. Call it $C_p(K)$.

Example

- Suppose that K is the splitting field of a monic (separable) polynomial f with coefficients in $\mathbb{Z}$.

Motivation: Galois theory

Let K be Galois extension over $\mathbb{Q}$.

For each prime p which is unramified in K, there is a well-defined Frobenius conjugacy class in $G := Gal(K/\mathbb{Q})$. Call it $C_p(K)$.

Example

- Suppose that K is the splitting field of a monic (separable) polynomial f with coefficients in $\mathbb{Z}$.
- Here, the unramified primes are the primes which do not divide the discriminant of f.

Motivation: Galois theory

Let K be Galois extension over $\mathbb{Q}$.

For each prime p which is unramified in K, there is a well-defined Frobenius conjugacy class in $G := Gal(K/\mathbb{Q})$. Call it $C_p(K)$.

Example

- Suppose that K is the splitting field of a monic (separable) polynomial f with coefficients in $\mathbb{Z}$.
- Here, the unramified primes are the primes which do not divide the discriminant of f.
- If p is such a prime and n is the degree of f, then $G \leq S_n$ and $C_p(K)$ has cycle type $(n_1, n_2, \ldots, n_r)$, where $n_1 \geq n_2 \geq \ldots \geq n_k$ are the degrees of the irreducible factors of f modulo p.

Motivation: Galois theory (Continued)

If p is ramified in K, then set $C_p(K) := \{1\}$.

Motivation: Galois theory (Continued)

If p is ramified in K, then set $C_p(K) := \{1\}$.

Theorem (Chebotarev density theorem)

Let C be a conjugacy class in $G = Gal(K/\mathbb{Q})$. Then

$$\lim_{N\to\infty} \frac{|\{p \leq N : C_p(K) = C\}|}{\pi(N)} = \frac{|C|}{|G|}.$$

Motivation: Galois theory (Continued)

If p is ramified in K, then set $C_p(K) := \{1\}$.

Theorem (Chebotarev density theorem)

Let C be a conjugacy class in $G = Gal(K/\mathbb{Q})$. Then

$$\lim_{N\to\infty} \frac{|\{p \leq N : C_p(K) = C\}|}{\pi(N)} = \frac{|C|}{|G|}.$$

Now, let N be a large enough integer so that there exists $p_1, \ldots, p_t \leq N$ such that $\{C_{p_1}(K), \ldots, C_{p_t}(K)\}$ invariably generate G.

Motivation: Galois theory (Continued)

If p is ramified in K, then set $C_p(K) := \{1\}$.

Theorem (Chebotarev density theorem)

Let C be a conjugacy class in $G = Gal(K/\mathbb{Q})$. Then

$$\lim_{N\to\infty} \frac{|\{p \leq N : C_p(K) = C\}|}{\pi(N)} = \frac{|C|}{|G|}.$$

Now, let N be a large enough integer so that there exists $p_1, \ldots, p_t \leq N$ such that $\{C_{p_1}(K), \ldots, C_{p_t}(K)\}$ invariably generate G.

Then choosing a random prime $p_i \leq N$ gives a sequence $C_{p_i}(K)$ of independent identically distributed random variables with values in the set of conjugacy classes of G.

Motivation: Galois theory (Continued)

Define a random variable $\mathcal{T}_{I,G,N}$ by

$$\mathcal{T}_{I,G,N} := \min\{n \in \mathbb{N} : \{C_{p_1}(K), \ldots, C_{p_n}(K)\} \text{ invariably generates } G\}.$$

Motivation: Galois theory (Continued)

Define a random variable $\mathcal{T}_{I,G,N}$ by

$$\mathcal{T}_{I,G,N} := \min\{n \in \mathbb{N} : \{C_{p_1}(K), \ldots, C_{p_n}(K)\} \text{ invariably generates } G\}.$$

Then Chebotarev's Theorem allows one to prove that

$$\lim_{N\to\infty} E(\mathcal{T}_{I,G,N}) = E(\mathcal{T}_{I,G}) = C(G).$$

Theorem (Chebotarev density theorem)

Let C be a conjugacy class in $G = Gal(K/\mathbb{Q})$. Then

$$\lim_{N\to\infty} \frac{|\{p \leq N : C_p(K) = C\}|}{\pi(N)} = \frac{|C|}{|G|}.$$

Motivation: Galois theory (Continued)

Define a random variable $\mathcal{T}_{I,G,N}$ by

$$\mathcal{T}_{I,G,N} := \min\{n \in \mathbb{N} : \{C_{p_1}(K), \ldots, C_{p_n}(K)\} \text{ invariably generates } G\}.$$

Then Chebotarev's Theorem allows one to prove that

$$\lim_{N\to\infty} E(\mathcal{T}_{I,G,N}) = E(\mathcal{T}_{I,G}) = C(G).$$

Theorem (Chebotarev density theorem)

Let C be a conjugacy class in $G = Gal(K/\mathbb{Q})$. Then

$$\lim_{N\to\infty} \frac{|\{p \leq N : C_p(K) = C\}|}{\pi(N)} = \frac{|C|}{|G|}.$$

Hence, $C(G)$ may be seen as the expected number of "random primes" required to generate the Galois group G.

Galois theory: Aside 1

The reason that van der Waerden cared about the case $G = S_n$ is the following result:

Galois theory: Aside 1

The reason that van der Waerden cared about the case $G = S_n$ is the following result:

Theorem (van der Waerden, 1936)

For $b, n \in \mathbb{N}$, let $IrrPol_b(n)$ denote the number of irreducible polynomials $f(X) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ of degree n such that $a_i \in \mathbb{Z}$, $|a_i| \leq b$, and $Gal(f) = S_n$. Let $Pol_b(n)$ be the number of polynomials $f(X) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ of degree n such that $a_i \in \mathbb{Z}$ and $|a_i| \leq b$. Then

$$\frac{IrrPol_b(n)}{Pol_b(n)} \to 1 \text{ as } b \to \infty.$$

Galois theory: Aside 1

The reason that van der Waerden cared about the case $G = S_n$ is the following result:

Theorem (van der Waerden, 1936)

For $b, n \in \mathbb{N}$, let $IrrPol_b(n)$ denote the number of irreducible polynomials $f(X) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ of degree n such that $a_i \in \mathbb{Z}$, $|a_i| \leq b$, and $Gal(f) = S_n$. Let $Pol_b(n)$ be the number of polynomials $f(X) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1} + a_nx^n$ of degree n such that $a_i \in \mathbb{Z}$ and $|a_i| \leq b$. Then

$$\frac{IrrPol_b(n)}{Pol_b(n)} \to 1 \text{ as } b \to \infty.$$

Thus, in some sense most polynomials of degree n over $\mathbb{Z}[X]$ are irreducible with Galois group the full symmetric group S_n.

Galois theory: Aside 2

The case $G = GL_2(\mathbb{F}_p)$ for p prime is also of interest to number theorists, since if K is generated by the p-torsion points of an elliptic curve E over $\mathbb{Q}$, then $Gal(K/\mathbb{Q})$ embeds into $GL_2(\mathbb{F}_p)$ (and by results of Serre, will "almost always" be the full group $GL_2(\mathbb{F}_p)$).

Galois theory: Aside 2

The case $G = GL_2(\mathbb{F}_p)$ for p prime is also of interest to number theorists, since if K is generated by the p-torsion points of an elliptic curve E over $\mathbb{Q}$, then $Gal(K/\mathbb{Q})$ embeds into $GL_2(\mathbb{F}_p)$ (and by results of Serre, will "almost always" be the full group $GL_2(\mathbb{F}_p)$).

In fact, Serre's Uniformity Conjecture says that if E does not have complex multiplication (i.e. $End(E) = \mathbb{Z}$) and $p > 37$, then we should have $Gal(K/\mathbb{Q}) = GL_2(\mathbb{F}_p)$.

Galois theory: Aside 2

The case $G = GL_2(\mathbb{F}_p)$ for p prime is also of interest to number theorists, since if K is generated by the p-torsion points of an elliptic curve E over $\mathbb{Q}$, then $Gal(K/\mathbb{Q})$ embeds into $GL_2(\mathbb{F}_p)$ (and by results of Serre, will "almost always" be the full group $GL_2(\mathbb{F}_p)$).

In fact, Serre's Uniformity Conjecture says that if E does not have complex multiplication (i.e. $End(E) = \mathbb{Z}$) and $p > 37$, then we should have $Gal(K/\mathbb{Q}) = GL_2(\mathbb{F}_p)$.

Serre has also proved that if E does not have complex multiplication, then there exists a positive integer p_E such that $Gal(K/\mathbb{Q}) = GL_2(\mathbb{F}_p)$ for $p > p_E$.

Galois theory: Aside 3

Galois theory: Aside 3

We remark that within the above discussion, there lies a (sort of) algorithm for computing the Galois group of a given number field..

Galois theory: Aside 3

We remark that within the above discussion, there lies a (sort of) algorithm for computing the Galois group of a given number field..

Step 1:

Find a group X such that $Gal(K/\mathbb{Q}) \leq X$: the group X is our guess for $Gal(K/\mathbb{Q})$.

Galois theory: Aside 3

We remark that within the above discussion, there lies a (sort of) algorithm for computing the Galois group of a given number field..

Step 1:

Find a group X such that $Gal(K/\mathbb{Q}) \leq X$: the group X is our guess for $Gal(K/\mathbb{Q})$.

(For example, one may try $X := GL_2(\mathbb{F}_p)$ if we are in the elliptic curve example from the last slide, or $X := S_n$ if K is the splitting field of an integer polynomial of degree n, as in the last slide.)

Galois theory: Aside 3 (Continued)

Step 1:

Find a group X such that $Gal(K/\mathbb{Q}) \leq X$: the group X is our guess for $Gal(K/\mathbb{Q})$.

(For example, one may try $X := GL_2(\mathbb{F}_p)$ if we are in the example at the top of the slide, or $X := S_n$ if K is the splitting field of an integer polynomial of degree n, as in the last slide.)

Step 2:

Computing Frobenius automorphisms modulo p as in the last slide yields conjugacy classes in the Galois group.

Galois theory: Aside 3 (Continued)

Step 1:

Find a group X such that $Gal(K/\mathbb{Q}) \leq X$: the group X is our guess for $Gal(K/\mathbb{Q})$.

(For example, one may try $X := GL_2(\mathbb{F}_p)$ if we are in the example at the top of the slide, or $X := S_n$ if K is the splitting field of an integer polynomial of degree n, as in the last slide.)

Step 2:

Computing Frobenius automorphisms modulo p as in the last slide yields conjugacy classes in the Galois group.

If our guess in Step 1 was correct, and we compute enough conjugacy classes so that the only possibility is $Gal(K/\mathbb{Q}) = X$, then we will have been successful.

Galois theory: Aside 3 (Continued)

The Chebotarev invariant measures the efficiency of this "algorithm".

Galois theory: Aside 3 (Continued)

The Chebotarev invariant measures the efficiency of this "algorithm".

We remark that computer algebra systems have better algorithms for computing the Galois group of a given number field..

Galois theory: Aside 3 (Continued)

The Chebotarev invariant measures the efficiency of this "algorithm".

We remark that computer algebra systems have better algorithms for computing the Galois group of a given number field..

However, theoretically the algorithm described above has proved to be quite useful..

Galois theory: Aside 3 (Continued)

The Chebotarev invariant measures the efficiency of this "algorithm".

We remark that computer algebra systems have better algorithms for computing the Galois group of a given number field..

However, theoretically the algorithm described above has proved to be quite useful..

For example, Jouve, Kowalski and Zywina (2008) used this approach to find the first example of a number field with Galois group the Weyl group of the exceptional algebraic group E_8.

4. A conjecture of Kowalski and Zywina, and some results

Comparing invariants

Clearly we have $d(G) \leq E(G) \leq C(G)$, where $d(G)$ denotes the minimal number of elements required to generate G, and $E(G)$ denotes the expected number of uniform random elements required to generate G.

Comparing invariants

Clearly we have $d(G) \leq E(G) \leq C(G)$, where $d(G)$ denotes the minimal number of elements required to generate G, and $E(G)$ denotes the expected number of uniform random elements required to generate G.

But how large can the difference $C(G) - E(G)$ be?

Comparing invariants

Clearly we have $d(G) \leq E(G) \leq C(G)$, where $d(G)$ denotes the minimal number of elements required to generate G, and $E(G)$ denotes the expected number of uniform random elements required to generate G.

But how large can the difference $C(G) - E(G)$ be?

For context, it has been proven that $d(G) = d_I(G)$ for some important classes of finite groups [for example $d_I(G) = 2$ if G is nonabelian simple Kantor, Lubotzky and Shalev (2011); Guralnick and Malle (2011)].

$E(G)$ vs $C(G)$

If G is abelian, then $E(G) = C(G)$.

$E(G)$ vs $C(G)$

If G is abelian, then $E(G) = C(G)$.

If G is a finite group, then G is nilpotent if and only if every generating set is an invariable generating set (Kantor, Lubotzky and Shalev, 2011).

$E(G)$ vs $C(G)$

If G is abelian, then $E(G) = C(G)$.

If G is a finite group, then G is nilpotent if and only if every generating set is an invariable generating set (Kantor, Lubotzky and Shalev, 2011).

$E(G)$ vs $C(G)$

If G is abelian, then $E(G) = C(G)$.

If G is a finite group, then G is nilpotent if and only if every generating set is an invariable generating set (Kantor, Lubotzky and Shalev, 2011).

Corollary (Pomerance, 2001)

Let G be a finite nilpotent group. Then

$$E(G) = C(G) \leq d(G) + \sigma$$

where $\sigma \sim 2.118456565\ldots$.

$E(G)$ vs $C(G)$

Is the difference between $C(G)$ and $E(G)$ small in general?

$E(G)$ vs $C(G)$

Is the difference between $C(G)$ and $E(G)$ small in general?

NO!

$E(G)$ vs $C(G)$

Is the difference between $C(G)$ and $E(G)$ small in general?

NO!

Theorem (Detomi and Lucchini, 2003; Lubotzky, 2003)

Let G be a finite group. Then

$$E(G) = d(G) + O(\log\log|G|) = O(\log|G|).$$

Proposition (Kowalski and Zywina, 2010)

Let q be a prime power, and consider the affine group $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$. Then $C(G_q) = q - f(q)$, where $f(q) \to 0$ as $q \to \infty$. In particular, $C(G_q) \sim \sqrt{|G_q|}$ as q tends to ∞.

$E(G)$ vs $C(G)$

Is the difference between $C(G)$ and $E(G)$ small in general?

NO!

Theorem (Detomi and Lucchini, 2003; Lubotzky, 2003)

Let G be a finite group. Then

$$E(G) = d(G) + O(\log\log|G|) = O(\log|G|).$$

Proposition (Kowalski and Zywina, 2010)

Let q be a prime power, and consider the affine group $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$. Then $C(G_q) = q - f(q)$, where $f(q) \to 0$ as $q \to \infty$. In particular, $C(G_q) \sim \sqrt{|G_q|}$ as q tends to ∞.

Thus, even in the metabelian case the invariant $C(G)$ behaves wildly differently to $E(G)$.

Kowalski and Zywina's Conjecture

Proposition (Kowalski and Zywina, 2010)

Let q be a prime power, and consider the affine group $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$. Then $C(G_q) = q - f(q)$, where $f(q) \to 0$ as $q \to \infty$. In particular, $C(G_q) \sim \sqrt{|G_q|}$ as q tends to ∞.

Conjecture (Kowalski and Zywina, 2010)

Let G be a finite group. Then $C(G) \leq \frac{5}{3}\sqrt{|G|}$.

Kowalki and Zywina's Conjecture

The bound $C(G) \leq \frac{5}{3}\sqrt{|G|}$ is "best possible"..

Kowalki and Zywina's Conjecture

The bound $C(G) \leq \frac{5}{3}\sqrt{|G|}$ is "best possible"..

Example

Let $G = C_2 \times C_2$. Then $G \neq \langle g_1, g_2, \ldots, g_k \rangle$ if and only if there exists $x \in G$ such that $g_i \in \langle x \rangle$ for all i. Hence

Kowalki and Zywina's Conjecture

The bound $C(G) \leq \frac{5}{3}\sqrt{|G|}$ is "best possible"..

Example

Let $G = C_2 \times C_2$. Then $G \neq \langle g_1, g_2, \ldots, g_k \rangle$ if and only if there exists $x \in G$ such that $g_i \in \langle x \rangle$ for all i. Hence

1. This failure probability is precisely $\frac{3 \times 2^k - 2}{4^k}$.

Kowalki and Zywina's Conjecture

The bound $C(G) \leq \frac{5}{3}\sqrt{|G|}$ is "best possible"..

Example

Let $G = C_2 \times C_2$. Then $G \neq \langle g_1, g_2, \ldots, g_k \rangle$ if and only if there exists $x \in G$ such that $g_i \in \langle x \rangle$ for all i. Hence

1. This failure probability is precisely $\frac{3 \times 2^k - 2}{4^k}$.
2. Hence, $C(G) = 3\sum_{i \geq 0} \frac{1}{2^k} - 2\sum_{i \geq 0} \frac{1}{4^k} = 6 - \frac{8}{3} = \frac{10}{3} = \frac{5}{3}\sqrt{|G|}$.

Possible approaches

For a positive integer k, denote by $P_I(G, k)$ the probability that k randomly chosen elements of G invariably generate G.

Possible approaches

For a positive integer k, denote by $P_I(G, k)$ the probability that k randomly chosen elements of G invariably generate G.

Then $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G, k))$.

Possible approaches

For a positive integer k, denote by $P_I(G,k)$ the probability that k randomly chosen elements of G invariably generate G.

Then $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G,k))$.

For a subgroup H of G, let $\widetilde{H} := \bigcup_{g\in G} H^g$ denote the union of the G-conjugates of H.

Possible approaches

For a positive integer k, denote by $P_I(G,k)$ the probability that k randomly chosen elements of G invariably generate G.

Then $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G,k))$.

For a subgroup H of G, let $\widetilde{H} := \bigcup_{g\in G} H^g$ denote the union of the G-conjugates of H.

A subset $\{x_1, \ldots, x_k\}$ fails to invariably generate G if and only if it is contained in $\widetilde{M}$ for some maximal subgroup M of G.

Possible approaches

For a positive integer k, denote by $P_I(G,k)$ the probability that k randomly chosen elements of G invariably generate G.

Then $C(G) = \sum_{k=0}^{\infty}(1 - P_I(G,k))$.

For a subgroup H of G, let $\widetilde{H} := \bigcup_{g\in G} H^g$ denote the union of the G-conjugates of H.

A subset $\{x_1, \ldots, x_k\}$ fails to invariably generate G if and only if it is contained in $\widetilde{M}$ for some maximal subgroup M of G.

Hence, $1 - P_I(G,k) \leq \sum_{M\in\mathcal{M}} \left(\frac{|\widetilde{M}|}{|G|}\right)^k$, where $\mathcal{M}$ is a set of representatives for the conjugacy classes of maximal subgroups of G.

Results

Results

Theorem (Kantor, Lubotzky and Shalev, 2011)

Let G be a finite group. Then

$$C(G) = O(\log |G| \sqrt{|G|}).$$

Results

Theorem (Kantor, Lubotzky and Shalev, 2011)

Let G be a finite group. Then

$$C(G) = O(\log |G| \sqrt{|G|}).$$

Theorem (Lucchini, 2015)

Let G be a finite group. Then

$$C(G) = O(\sqrt{|G|}).$$

Results

Theorem (Kantor, Lubotzky and Shalev, 2011)

Let G be a finite group. Then

$$C(G) = O(\log |G| \sqrt{|G|}).$$

Theorem (Lucchini, 2015)

Let G be a finite group. Then

$$C(G) = O(\sqrt{|G|}).$$

Theorem (Lucchini and T., 2017)

Let G be a finite group.

1. *For each $\epsilon > 0$, there exists a constant c_ϵ such that $C(G) \leq (1+\epsilon)\sqrt{|G|} + c_\epsilon$.*
2. *If G is soluble, then $C(G) \leq \frac{5}{3}\sqrt{|G|}$.*

Ideas from the proof

Principle: Look at unions of different equivalence classes of maximal subgroups [coarser than conjugacy].

Ideas from the proof

Principle: Look at unions of different equivalence classes of maximal subgroups [coarser than conjugacy].

Let V be a chief factor of G.

Ideas from the proof

Principle: Look at unions of different equivalence classes of maximal subgroups [coarser than conjugacy].

Let V be a chief factor of G.

We say that a maximal subgroup M of G is of *type* V if the primitive permutation group $G/core_G(M)$ has a minimal normal subgroup which is "G-equivalent" to V.

Ideas from the proof

Principle: Look at unions of different equivalence classes of maximal subgroups [coarser than conjugacy].

Let V be a chief factor of G.

We say that a maximal subgroup M of G is of *type* V if the primitive permutation group $G/core_G(M)$ has a minimal normal subgroup which is "G-equivalent" to V.

We say that a subset $\{x_1, \ldots, x_k\}$ *satisfies the* V*-property* in G if it is contained in $\widetilde{M}$ for a maximal subgroup M of G of type V.

Ideas from the proof

Principle: Look at unions of different equivalence classes of maximal subgroups [coarser than conjugacy].

Let V be a chief factor of G.

We say that a maximal subgroup M of G is of *type* V if the primitive permutation group $G/core_G(M)$ has a minimal normal subgroup which is "G-equivalent" to V.

We say that a subset $\{x_1, \ldots, x_k\}$ *satisfies the* V*-property* in G if it is contained in $\widetilde{M}$ for a maximal subgroup M of G of type V.

A subset $\{x_1, \ldots, x_k\}$ fails to invariably generate G if and only if it satisfies the V-property for some chief factor V of G.

"Gathering" the probabilities in a different way

Now, let $P_{G,V}(k)$ denote the probability that a randomly selected k-tuple of elements of G satisfy the V-property in G. Then we have

"Gathering" the probabilities in a different way

Now, let $P_{G,V}(k)$ denote the probability that a randomly selected k-tuple of elements of G satisfy the V-property in G. Then we have

Proposition

Let G be a finite group, and let A be a set of representatives for the non-central chief factors of G. Then

$$C(G) \leq \sum_{V \in A} \sum_{k=0}^{\infty} P_{G,V}(k) + d(G/G') + \sigma,$$

where $\sigma = 2.11\ldots$.

"Gathering" the probabilities in a different way

Now, let $P_{G,V}(k)$ denote the probability that a randomly selected k-tuple of elements of G satisfy the V-property in G. Then we have

Proposition

Let G be a finite group, and let A be a set of representatives for the non-central chief factors of G. Then

$$C(G) \leq \sum_{V \in A} \sum_{k=0}^{\infty} P_{G,V}(k) + d(G/G') + \sigma,$$

where $\sigma = 2.11\ldots$.

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

"Gathering" the probabilities in a different way

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

"Gathering" the probabilities in a different way

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

By using induction on the order of the group to compute $C(G/N)$, our task reduces to computing $\sum_{k=1}^{\infty} P_{G,V}(k)$ for a fixed chief factor V of G.

"Gathering" the probabilities in a different way

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

By using induction on the order of the group to compute $C(G/N)$, our task reduces to computing $\sum_{k=1}^{\infty} P_{G,V}(k)$ for a fixed chief factor V of G.

In fact, an easy exercise shows that this computation can be done inside the "V-crown" of G.

V-crowns

Definition

Define $R_G(V)$ to be the intersection of all maximal subgroups of G of type V. Then $R_G(V) \trianglelefteq G$, and the group $G/R_G(V)$ is called the *V-crown based power* of G.

V-crowns

Definition

Define $R_G(V)$ to be the intersection of all maximal subgroups of G of type V. Then $R_G(V) \trianglelefteq G$, and the group $G/R_G(V)$ is called the *V-crown based power* of G.

It can be shown that if V is abelian, then $G/R_G(V)$ has shape $V^\delta \rtimes H$, where H is the induced linear group on V, and the action of H is diagonal on V^δ.

V-crowns

Definition

Define $R_G(V)$ to be the intersection of all maximal subgroups of G of type V. Then $R_G(V) \trianglelefteq G$, and the group $G/R_G(V)$ is called the *V-crown based power* of G.

It can be shown that if V is abelian, then $G/R_G(V)$ has shape $V^\delta \rtimes H$, where H is the induced linear group on V, and the action of H is diagonal on V^δ.

If V is non-abelian, then $G/R_G(V)$ has shape $V^\delta.H$ (not necessarily a split extension), where H is the group of automorphisms of V induced by G.

Ideas from the proof

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

By using induction on the order of the group to compute $C(G/N)$, our task reduces to computing $\sum_{k=1}^{\infty} P_{G,V}(k)$ for a fixed chief factor V of G.

Ideas from the proof

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

By using induction on the order of the group to compute $C(G/N)$, our task reduces to computing $\sum_{k=1}^{\infty} P_{G,V}(k)$ for a fixed chief factor V of G.

As remarked above, this computation can be done inside the "V-crown" of G.

Ideas from the proof

Lemma (Reduction lemma)

Let G be a finite group. There exists a chief factor V of G and a normal subgroup N of G such that

$$C(G) \leq C(G/N) + \sum_{k=1}^{\infty} P_{G,V}(k).$$

By using induction on the order of the group to compute $C(G/N)$, our task reduces to computing $\sum_{k=1}^{\infty} P_{G,V}(k)$ for a fixed chief factor V of G.

As remarked above, this computation can be done inside the "V-crown" of G.

That is, we may assume that G has shape $V^{\delta}.H$, where $H := G/C_G(V)$.

Ideas from the proof: The abelian case

Suppose that V is abelian, so that $G \cong V^{\delta} \rtimes H$.

Ideas from the proof: The abelian case

Suppose that V is abelian, so that $G \cong V^{\delta} \rtimes H$.

Using a probabilistic argument, we prove the following:

Ideas from the proof: The abelian case

Suppose that V is abelian, so that $G \cong V^{\delta} \rtimes H$.

Using a probabilistic argument, we prove the following:

Lemma (The V abelian case)

Suppose that V is abelian. Then

Ideas from the proof: The abelian case

Suppose that V is abelian, so that $G \cong V^{\delta} \rtimes H$.

Using a probabilistic argument, we prove the following:

Lemma (The V abelian case)

Suppose that V is abelian. Then

1. $C(G) \leq C(G/N) + \left(\delta.\theta + \dim_{End_H(V)} H^1(H, V) + \frac{q}{q-1}\right) \frac{|H|}{|H^*|}$;

Ideas from the proof: The abelian case

Suppose that V is abelian, so that $G \cong V^{\delta} \rtimes H$.

Using a probabilistic argument, we prove the following:

Lemma (The V abelian case)

Suppose that V is abelian. Then

1. $C(G) \leq C(G/N) + \left(\delta.\theta + \dim_{End_H(V)} H^1(H, V) + \frac{q}{q-1}\right) \frac{|H|}{|H^*|}$;
2. $C(G) \leq C(G/N) + \left(\frac{\delta.\theta}{n} + \frac{q^n}{q^n-1}\right) |H|$.

where $H^* = \{h \in H : h \text{ fixes a non-zero vector in } V\}$, and $\theta := 0$ if $\delta = 1$, $\theta := 1$ otherwise.

Ideas from the proof: The abelian case

So we need to bound the cohomology $H^1(H, V)$..

Ideas from the proof: The abelian case

So we need to bound the cohomology $H^1(H, V)$..

If H is soluble, then $H^1(H, V) = 0$.

Ideas from the proof: The abelian case

So we need to bound the cohomology $H^1(H, V)$..

If H is soluble, then $H^1(H, V) = 0$.

In general, there are very few cases when $H^1(H, V) > 0$..

Ideas from the proof: The abelian case

So we need to bound the cohomology $H^1(H, V)$..

If H is soluble, then $H^1(H, V) = 0$.

In general, there are very few cases when $H^1(H, V) > 0$..

Lemma

Suppose that $H^1(H, V) > 0$. Then there exists an absolute constant C such that $|H^*| \geq 2(m+1)^2$ if $|H| \geq C$.

Ideas from the proof: The abelian case

So we need to bound the cohomology $H^1(H, V)$..

If H is soluble, then $H^1(H, V) = 0$.

In general, there are very few cases when $H^1(H, V) > 0$..

Lemma

Suppose that $H^1(H, V) > 0$. Then there exists an absolute constant C such that $|H^*| \geq 2(m+1)^2$ if $|H| \geq C$.

Putting these bounds into the previous lemma yields our theorem in the case where V is abelian.

Ideas from the proof: The non-abelian case

The case where V is non-abelian

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Suppose that the chief factor V of G is non-abelian, that is, $V \cong S^t$ for a non-abelian simple group S.

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Suppose that the chief factor V of G is non-abelian, that is, $V \cong S^t$ for a non-abelian simple group S.
- Then for large enough $|G|$, we have that $\sum_{k=0}^{\infty} P_{\overline{G},V}(k) = O(\log^2 |G|)$.

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Suppose that the chief factor V of G is non-abelian, that is, $V \cong S^t$ for a non-abelian simple group S.
- Then for large enough $|G|$, we have that $\sum_{k=0}^{\infty} P_{\overline{G},V}(k) = O(\log^2 |G|)$.
- Thus, it is certainly not close to $\sqrt{|G|}$, and hence we can discount this case..

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Suppose that the chief factor V of G is non-abelian, that is, $V \cong S^t$ for a non-abelian simple group S.
- Then for large enough $|G|$, we have that $\sum_{k=0}^{\infty} P_{\overline{G},V}(k) = O(\log^2 |G|)$.
- Thus, it is certainly not close to $\sqrt{|G|}$, and hence we can discount this case..
- We remark that this case is closely related to the work of Luczak-Pyber and Fulman-Guralnick on the Boston-Shalev conjecture..

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Suppose that the chief factor V of G is non-abelian, that is, $V \cong S^t$ for a non-abelian simple group S.
- Then for large enough $|G|$, we have that $\sum_{k=0}^{\infty} P_{\overline{G},V}(k) = O(\log^2 |G|)$.
- Thus, it is certainly not close to $\sqrt{|G|}$, and hence we can discount this case..
- We remark that this case is closely related to the work of Luczak-Pyber and Fulman-Guralnick on the Boston-Shalev conjecture..
- This conjecture states that the proportion of fixed point free elements in a finite simple primitive permutation group, is "large" (i.e. bounded away from 0).

Ideas from the proof: The non-abelian case

The case where V is non-abelian

- Then for large enough $|G|$, we have that $\sum_{k=0}^{\infty} P_{\overline{G},V}(k) = O(\log^2 |G|)$.
- Thus, it is certainly not close to $\sqrt{|G|}$, and hence we can discount this case..
- We remark that this case is closely related to the work of Luczak-Pyber and Fulman-Guralnick on the Boston-Shalev conjecture..
- This conjecture states that the proportion of fixed point free elements in a finite simple primitive permutation group, is "large" (i.e. bounded away from 0).
- The link to our work comes from the fact that if G is such a simple group and M is a point stabiliser, then this proportion is precisely $1 - \frac{|\widetilde{M}|}{|G|}$.

A partial converse

A natural question to ask is: If $C(G)$ is "close" to $\sqrt{|G|}$, then does G "look like" the affine example $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ of Kowalski and Zywina?

A partial converse

A natural question to ask is: If $C(G)$ is "close" to $\sqrt{|G|}$, then does G "look like" the affine example $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ of Kowalski and Zywina?

Theorem (Lucchini and T., 2018)

Fix a constant $\epsilon > 0$. There exists constants β_ϵ, γ_ϵ, δ_ϵ and k_ϵ such that if G is a finite group with $C(G) > \epsilon\sqrt{|G|}$, then G has a factor group $\overline{G}$ such that

A partial converse

A natural question to ask is: If $C(G)$ is "close" to $\sqrt{|G|}$, then does G "look like" the affine example $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ of Kowalski and Zywina?

Theorem (Lucchini and T., 2018)

Fix a constant $\epsilon > 0$. There exists constants β_ϵ, γ_ϵ, δ_ϵ and k_ϵ such that if G is a finite group with $C(G) > \epsilon\sqrt{|G|}$, then G has a factor group $\overline{G}$ such that

1. *$\overline{G} \cong V \rtimes H$, with $V \cong \mathbb{F}_q^k$, $H \leq \Gamma L_1(q) \wr Sym(k)$, q a prime power, and $k \leq k_\epsilon$;*

A partial converse

A natural question to ask is: If $C(G)$ is "close" to $\sqrt{|G|}$, then does G "look like" the affine example $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ of Kowalski and Zywina?

Theorem (Lucchini and T., 2018)

Fix a constant $\epsilon > 0$. There exists constants β_ϵ, γ_ϵ, δ_ϵ and k_ϵ such that if G is a finite group with $C(G) > \epsilon\sqrt{|G|}$, then G has a factor group $\overline{G}$ such that

1. *$\overline{G} \cong V \rtimes H$, with $V \cong \mathbb{F}_q^k$, $H \leq \Gamma L_1(q) \wr Sym(k)$, q a prime power, and $k \leq k_\epsilon$;*
2. *$|\overline{G}| \geq \delta_\epsilon\sqrt{|G|}$; and*

A partial converse

A natural question to ask is: If $C(G)$ is "close" to $\sqrt{|G|}$, then does G "look like" the affine example $G_q := \mathbb{F}_q \rtimes \mathbb{F}_q^\times$ of Kowalski and Zywina?

Theorem (Lucchini and T., 2018)

Fix a constant $\epsilon > 0$. There exists constants β_ϵ, γ_ϵ, δ_ϵ and k_ϵ such that if G is a finite group with $C(G) > \epsilon\sqrt{|G|}$, then G has a factor group $\overline{G}$ such that

1. $\overline{G} \cong V \rtimes H$, *with* $V \cong \mathbb{F}_q^k$, $H \leq \Gamma L_1(q) \wr Sym(k)$, *$q$ a prime power, and* $k \leq k_\epsilon$;
2. $|\overline{G}| \geq \delta_\epsilon\sqrt{|G|}$; *and*
3. $\beta_\epsilon|V| \leq |H| \leq \gamma_\epsilon|V|$.

5. Closing remarks: Permutation groups

So what about van der Waerden's question?!

Question (van der Waerden, 1936)

What is $C(S_n)$?

So what about van der Waerden's question?!

Question (van der Waerden, 1936)

What is $C(S_n)$?

Theorem (Eberhard, Ford and Green, 2014; Pemantle, Peres and Rivin, 2014)

Let $G = S_n$ or $G = A_n$. Then $P_{l,G}(3)$ tends to 0 as $n \to \infty$, while there exists a constant ϵ such that $P_{l,G}(4) > \epsilon$.

So what about van der Waerden's question?!

Question (van der Waerden, 1936)

What is $C(S_n)$?

Theorem (Eberhard, Ford and Green, 2014; Pemantle, Peres and Rivin, 2014)

Let $G = S_n$ or $G = A_n$. Then $P_{I,G}(3)$ tends to 0 as $n \to \infty$, while there exists a constant ϵ such that $P_{I,G}(4) > \epsilon$.

An easy exercise proves that this means that $C(G)$ is bounded above by an absolute constant in this case, and that $C(G) \geq 4$.

So what about van der Waerden's question?!

Question (van der Waerden, 1936)

What is $C(S_n)$?

Theorem (Eberhard, Ford and Green, 2014; Pemantle, Peres and Rivin, 2014)

Let $G = S_n$ or $G = A_n$. Then $P_{l,G}(3)$ tends to 0 as $n \to \infty$, while there exists a constant ϵ such that $P_{l,G}(4) > \epsilon$.

An easy exercise proves that this means that $C(G)$ is bounded above by an absolute constant in this case, and that $C(G) \geq 4$.

It would also be interesting to see what happens for other almost simple groups..

Closing remarks: Permutation groups in general

Given the motivation from Galois theory, it is also natural to ask:

Closing remarks: Permutation groups in general

Given the motivation from Galois theory, it is also natural to ask:

Question

What can we say about $C(G)$ (in terms of n), where $G \leq S_n$?

Closing remarks: Permutation groups in general

Given the motivation from Galois theory, it is also natural to ask:

Question

What can we say about $C(G)$ (in terms of n), where $G \leq S_n$?

From our results so far, all we can say is that $C(G) = O(\sqrt{|G|}) = \sqrt{n!}$, or that $C(G) = O(24^{\frac{n-1}{6}})$ in the soluble case.

Closing remarks: Permutation groups in general

Given the motivation from Galois theory, it is also natural to ask:

Question

What can we say about $C(G)$ (in terms of n), where $G \leq S_n$?

From our results so far, all we can say is that $C(G) = O(\sqrt{|G|}) = \sqrt{n!}$, or that $C(G) = O(24^{\frac{n-1}{6}})$ in the soluble case.

Reasonable question

Is $C(G)$ polynomial (or even linear) in n in this case?

Closing remarks: Permutation groups in general

Given the motivation from Galois theory, it is also natural to ask:

Question

What can we say about $C(G)$ (in terms of n), where $G \leq S_n$?

From our results so far, all we can say is that $C(G) = O(\sqrt{|G|}) = \sqrt{n!}$, or that $C(G) = O(24^{\frac{n-1}{6}})$ in the soluble case.

Reasonable question

Is $C(G)$ polynomial (or even linear) in n in this case?

Theorem (Lucchini and T., 2019)

If $G \leq S_n$ is either soluble or primitive, then $C(G)$ is polynomial in n.

Closing remarks: Permutation groups in general

Question

What can we say about $C(G)$ (in terms of n), where $G \leq S_n$?

From our results so far, all we can say is that $C(G) = O(\sqrt{|G|}) = \sqrt{n!}$, or that $C(G) = O(24^{\frac{n-1}{6}})$ in the soluble case.

Reasonable question

Is $C(G)$ polynomial (or even linear) in n in this case?

Theorem (Lucchini and T., 2019)

If $G \leq S_n$ is either soluble or primitive, then $C(G)$ is polynomial in n.

Theorem (Lucchini and T., 2020+)

Let $G \leq S_n$, and let r be the maximum of the ranks of the finite groups of Lie type occurring as subsections of G. Then $d(G) \leq n^{c(r)}$, where $c(r)$ is a constant depending only on r.