Can insoluble Galois extensions have Hopf-Galois structures of soluble type?

Nigel Byott

University of Exeter

Omaha, May 2019

Can insoluble Galois extensions have Hopf-Galois structures of soluble type?

Nigel Byott

University of Exeter

Omaha, May 2019

A question I still can't answer!

Given groups G, N with $|G| = |N| < \infty$, we ask

Are there any regular embeddings $\theta : G \to \mathrm{Hol}(N)$?

Given groups G, N with $|G| = |N| < \infty$, we ask

Are there any regular embeddings $\theta : G \to \mathrm{Hol}(N)$?

Equivalently

Given groups G, N with $|G| = |N| < \infty$, we ask

Are there any regular embeddings $\theta : G \to \mathrm{Hol}(N)$?

Equivalently

- Does a Galois extension with group G admit a Hopf-Galois structure of type N?

Given groups G, N with $|G| = |N| < \infty$, we ask

Are there any regular embeddings $\theta : G \to \mathrm{Hol}(N)$?

Equivalently

- Does a Galois extension with group G admit a Hopf-Galois structure of type N?
- Does there exist a left skew brace with multiplicative group G and additive group N?

Given groups G, N with $|G| = |N| < \infty$, we ask

Are there any regular embeddings $\theta : G \to \mathrm{Hol}(N)$?

Equivalently

- Does a Galois extension with group G admit a Hopf-Galois structure of type N?
- Does there exist a left skew brace with multiplicative group G and additive group N?

Specifically, we consider the following conjecture:

Conjecture 1

There is no regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble and N soluble.

What we know:

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).
- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with N nilpotent then G is soluble (NB, 2015).

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).
- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with N nilpotent then G is soluble (NB, 2015).
  We want to replace "nilpotent" by "soluble".

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).
- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with N nilpotent then G is soluble (NB, 2015).
  We want to replace "nilpotent" by "soluble".
- There is no **two-sided** finite skew brace with insoluble multiplicative group and soluble additive group (Nasybullov, 2018).

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).
- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with N nilpotent then G is soluble (NB, 2015).
  We want to replace "nilpotent" by "soluble".
- There is no **two-sided** finite skew brace with insoluble multiplicative group and soluble additive group (Nasybullov, 2018).
- We **can** have a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G **soluble** and N **insoluble**.

What we know:

- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with G nonabelian simple, then $N \cong G$ (NB, 2004).
- If $\theta : G \to \mathrm{Hol}(N)$ is a regular embedding with N nilpotent then G is soluble (NB, 2015).
  We want to replace "nilpotent" by "soluble".
- There is no **two-sided** finite skew brace with insoluble multiplicative group and soluble additive group (Nasybullov, 2018).
- We **can** have a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G **soluble** and N **insoluble**.

  e.g. $G = A_4 \times C_5, \qquad N = A_5 = A_4\, C_5,$

$$\theta(\alpha, \beta) : \sigma \mapsto \alpha\sigma\beta^{-1}.$$

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

(b) *n cannot be of the form $2^r|S|$ when S is one of the following nonabelian simple groups:*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

(b) *n cannot be of the form $2^r|S|$ when S is one of the following nonabelian simple groups:*

   (i) *A_5 of order $2^2 \cdot 3 \cdot 5$;*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

(b) *n cannot be of the form $2^r|S|$ when S is one of the following nonabelian simple groups:*

  (i) *A_5 of order $2^2 \cdot 3 \cdot 5$;*

  (ii) *$\mathrm{PSL}_2(17)$ of order $2^4 \cdot 3^2 \cdot 17$;*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

(a) n *is divisible by* p^3 *for some prime* p*;*

(b) n *cannot be of the form* $2^r|S|$ *when* S *is one of the following nonabelian simple groups:*

   (i) A_5 *of order* $2^2 \cdot 3 \cdot 5$*;*

   (ii) $\mathrm{PSL}_2(17)$ *of order* $2^4 \cdot 3^2 \cdot 17$*;*

   (iii) $\mathrm{Sz}(2^{2m+1})$ *of order* $4^{2m+1}(4^{2m+1}+1)(2^{2m+1}-1)$ *(with a mild extra hypothesis on* m*).*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

(b) *n cannot be of the form $2^r|S|$ when S is one of the following nonabelian simple groups:*

   (i) *A_5 of order $2^2 \cdot 3 \cdot 5$;*

   (ii) *$\mathrm{PSL}_2(17)$ of order $2^4 \cdot 3^2 \cdot 17$;*

   (iii) *$\mathrm{Sz}(2^{2m+1})$ of order $4^{2m+1}(4^{2m+1} + 1)(2^{2m+1} - 1)$ (with a mild extra hypothesis on m).*

(c) *$n > 2000$.*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by p^3 for some prime p;*

(b) *n cannot be of the form $2^r|S|$ when S is one of the following nonabelian simple groups:*

  (i) *A_5 of order $2^2 \cdot 3 \cdot 5$;*

  (ii) *$\mathrm{PSL}_2(17)$ of order $2^4 \cdot 3^2 \cdot 17$;*

  (iii) *$\mathrm{Sz}(2^{2m+1})$ of order $4^{2m+1}(4^{2m+1}+1)(2^{2m+1}-1)$ (with a mild extra hypothesis on m).*

(c) *$n > 2000$.*

Remarks

- *(a) uses Feit-Thompson, (b) uses the Classification of Finite Simple Groups (CFSG), and (c) uses a computer search.*

Theorem 1 (Tsang & Chao, arXiv, March 2019)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

(a) n *is divisible by* p^3 *for some prime* p*;*

(b) n *cannot be of the form* $2^r|S|$ *when* S *is one of the following nonabelian simple groups:*

  (i) A_5 *of order* $2^2 \cdot 3 \cdot 5$*;*

  (ii) $\mathrm{PSL}_2(17)$ *of order* $2^4 \cdot 3^2 \cdot 17$*;*

  (iii) $\mathrm{Sz}(2^{2m+1})$ *of order* $4^{2m+1}(4^{2m+1}+1)(2^{2m+1}-1)$ *(with a mild extra hypothesis on* m*).*

(c) $n > 2000$.

Remarks

- *(a) uses Feit-Thompson, (b) uses the Classification of Finite Simple Groups (CFSG), and (c) uses a computer search.*
- *The Suzuki groups* $\mathrm{Sz}(2^{2m+1})$ *are the only nonabelian simple groups whose order is not divisible by 3.*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

(a) n *is divisible by* 8 *or* p^4 *for some prime* p*;*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by 8 or p^4 for some prime p;*

(b) *n is divisible by one of the following numbers:*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by 8 or p^4 for some prime p;*

(b) *n is divisible by one of the following numbers:*

 (i) $2^3 \cdot 3^3 \cdot 13^4 = 13^3|\mathrm{PSL}_3(3)|$;

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by 8 or p^4 for some prime p;*

(b) *n is divisible by one of the following numbers:*

 (i) $2^3 \cdot 3^3 \cdot 13^4 = 13^3|\mathrm{PSL}_3(3)|$;

 (ii) $(q-1)q^4(q+1) = q^3|\mathrm{PSL}_2(q-1)|$, *where $q = 2^a + 1$ is a Fermat prime, $a \geq 2$ (so $a = 2^c$ for some c), i.e. $q = 5, 17, 257, 65537, ???$*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble,* N *soluble,* $|G| = |N| = n$*, then*

(a) n *is divisible by* 8 *or* p^4 *for some prime* p*;*

(b) n *is divisible by one of the following numbers:*

   (i) $2^3 \cdot 3^3 \cdot 13^4 = 13^3|\mathrm{PSL}_3(3)|$;

   (ii) $(q-1)q^4(q+1) = q^3|\mathrm{PSL}_2(q-1)|$, *where* $q = 2^a + 1$ *is a Fermat prime,* $a \geq 2$ *(so* $a = 2^c$ *for some* c*), i.e.* $q = 5, 17, 257, 65537,$ *???*

   (iii) $\frac{1}{2}p(p-1)(p+1) = |\mathrm{PSL}_2(p)|$, *where* $p = 2^b - 1$ *is a Mersenne prime,* $b \geq 3$ *(so* b *is prime).*

The Main Result of This Talk

Theorem 2 (NB)

If there is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble, N soluble, $|G| = |N| = n$, then

(a) *n is divisible by 8 or p^4 for some prime p;*

(b) *n is divisible by one of the following numbers:*

  (i) $2^3 \cdot 3^3 \cdot 13^4 = 13^3 |\mathrm{PSL}_3(3)|$;

  (ii) $(q-1)q^4(q+1) = q^3 |\mathrm{PSL}_2(q-1)|$, *where $q = 2^a + 1$ is a Fermat prime, $a \geq 2$ (so $a = 2^c$ for some c), i.e. $q = 5, 17, 257, 65537$, ???*

  (iii) $\frac{1}{2} p(p-1)(p+1) = |\mathrm{PSL}_2(p)|$, *where $p = 2^b - 1$ is a Mersenne prime, $b \geq 3$ (so b is prime).*

Moreover, G contains $\mathrm{PSL}_3(3)$, resp. $\mathrm{PSL}_2(q-1)$, resp. $\mathrm{PSL}_2(p)$, as a subquotient.

Remarks

- *(a) marginally improves on Theorem 1(a), but* **does not** *use Feit-Thompson or CFSG.*

Remarks

- *(a) marginally improves on Theorem 1(a), but* **does not** *use Feit-Thompson or CFSG.*
- *It might be possible to replace p^4 by p^{p+1} (see later).*

Remarks

- *(a) marginally improves on Theorem 1(a), but* **does not** *use Feit-Thompson or CFSG.*
- *It might be possible to replace p^4 by p^{p+1} (see later).*
- *(b) does use CFSG.*

Remarks

- *(a) marginally improves on Theorem 1(a), but* **does not** *use Feit-Thompson or CFSG.*
- *It might be possible to replace p^4 by p^{p+1} (see later).*
- *(b) does use CFSG.*
- *Theorem 2 implies all of Theorem 1 except when $n < 2000$ is a multiple of $|\mathrm{PSL}_2(7)| = 168 = 2^3 \cdot 3 \cdot 7$.*

Transitive embeddings

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N. (View $N \subset \mathrm{Hol}(N)$ as left *translations.)*

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N. (View $N \subset \mathrm{Hol}(N)$ as left *translations.)*

The stabiliser G_1 of e_N has index $|N|$ in G, and $\cap_{g \in G} g G_1 g^{-1} = \{e_G\}$.

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N. (View $N \subset \mathrm{Hol}(N)$ as left *translations.)*

The stabiliser G_1 of e_N has index $|N|$ in G, and $\cap_{g \in G} g G_1 g^{-1} = \{e_G\}$.
Also θ is a regular embedding $\Leftrightarrow G_1 = \{e_G\}$.

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N*. (View* $N \subset \mathrm{Hol}(N)$ *as* left *translations.)*

The stabiliser G_1 of e_N has index $|N|$ in G, and $\cap_{g \in G} g G_1 g^{-1} = \{e_G\}$. Also θ is a regular embedding $\Leftrightarrow G_1 = \{e_G\}$.

Starting with the groups G and N, giving a transitive embedding $\theta : G \to \mathrm{Hol}(N)$ is equivalent to giving two functions

$$\theta_a : G \to \mathrm{Aut}(N), \qquad \theta_c : G \to N, \qquad \text{so that}$$

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N. (View $N \subset \mathrm{Hol}(N)$ as left *translations.)*

The stabiliser G_1 of e_N has index $|N|$ in G, and $\cap_{g \in G} g G_1 g^{-1} = \{e_G\}$.
Also θ is a regular embedding $\Leftrightarrow G_1 = \{e_G\}$.

Starting with the groups G and N, giving a transitive embedding $\theta : G \to \mathrm{Hol}(N)$ is equivalent to giving two functions

$$\theta_a : G \to \mathrm{Aut}(N), \qquad \theta_c : G \to N, \qquad \text{so that}$$

θ_a is a homomorphism of groups (i.e. θ_a gives an action of G on N),

Transitive embeddings

Definition

A **transitive embedding** *is an injective group homomorphism*

$$\theta : G \hookrightarrow \mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subseteq \mathrm{Perm}(N)$$

whose image is transitive on N. (View $N \subset \mathrm{Hol}(N)$ as left *translations.)*

The stabiliser G_1 of e_N has index $|N|$ in G, and $\cap_{g \in G} g G_1 g^{-1} = \{e_G\}$.
Also θ is a regular embedding $\Leftrightarrow G_1 = \{e_G\}$.

Starting with the groups G and N, giving a transitive embedding $\theta : G \to \mathrm{Hol}(N)$ is equivalent to giving two functions

$$\theta_a : G \to \mathrm{Aut}(N), \qquad \theta_c : G \to N, \qquad \text{so that}$$

θ_a is a homomorphism of groups (i.e. θ_a gives an action of G on N),
θ_c is a surjective (non-abelian) 1-cocycle for this action:

$$\theta_c(gh) = \theta_c(g)(g \cdot \theta_c(h)) \text{ for all } g, h \in G$$

where $g \cdot n = \theta_a(g)(n)$ for $g \in G$, $n \in N$.

Definition

*A G-**subgroup of** N is a subgroup M such that* $\theta_a(g)(m) \in M$ *for all* $g \in G$, $m \in M$.

Definition

*A G-**subgroup of** N is a subgroup M such that $\theta_a(g)(m) \in M$ for all $g \in G$, $m \in M$.*

Lemma

Let M be a G-subgroup for the transitive embedding $\theta : G \to \mathrm{Hol}(N)$.

Definition

*A G-***subgroup of** *N is a subgroup M such that* $\theta_a(g)(m) \in M$ *for all* $g \in G$, $m \in M$.

Lemma

Let M be a G-subgroup for the transitive embedding $\theta : G \to \mathrm{Hol}(N)$.

(i) *the subset*

$$\begin{aligned} \theta^{-1}M &:= \{g \in G : \theta_c(g) \in M\} \\ &= \{g \in G : g \cdot e_N \in M\}. \end{aligned}$$

is a **subgroup** *of G.*

Definition

*A G-**subgroup of** N is a subgroup M such that $\theta_a(g)(m) \in M$ for all $g \in G$, $m \in M$.*

Lemma

Let M be a G-subgroup for the transitive embedding $\theta : G \to \mathrm{Hol}(N)$.

(i) *the subset*

$$\begin{aligned} \theta^{-1}M &:= \{g \in G : \theta_c(g) \in M\} \\ &= \{g \in G : g \cdot e_N \in M\}. \end{aligned}$$

*is a **subgroup** of G.*

(ii) $\theta|_M : \theta^{-1}M \to \mathrm{Hol}(M)$ *is a transitive embedding.*

Definition

*A G-**subgroup of** N is a subgroup M such that $\theta_a(g)(m) \in M$ for all $g \in G$, $m \in M$.*

Lemma

Let M be a G-subgroup for the transitive embedding $\theta : G \to \mathrm{Hol}(N)$.

(i) *the subset*

$$\begin{aligned} \theta^{-1}M &:= \{g \in G : \theta_c(g) \in M\} \\ &= \{g \in G : g \cdot e_N \in M\}. \end{aligned}$$

*is a **subgroup** of G.*

(ii) $\theta|_M : \theta^{-1}M \to \mathrm{Hol}(M)$ *is a transitive embedding.*

(iii) $\theta|_M$ *is regular if and only if θ is regular.*

Definition

A G-**subgroup of** N *is a subgroup* M *such that* $\theta_a(g)(m) \in M$ *for all* $g \in G$, $m \in M$.

Lemma

Let M *be a* G*-subgroup for the transitive embedding* $\theta : G \to \mathrm{Hol}(N)$.

(i) *the subset*

$$\begin{aligned} \theta^{-1}M &:= \{g \in G : \theta_c(g) \in M\} \\ &= \{g \in G : g \cdot e_N \in M\}. \end{aligned}$$

is a **subgroup** *of* G.

(ii) $\theta|_M : \theta^{-1}M \to \mathrm{Hol}(M)$ *is a transitive embedding.*

(iii) $\theta|_M$ *is regular if and only if* θ *is regular.*

(iv) *If also* $M \lhd N$, *then* θ *induces a transitive embedding* $\overline{\theta} : \overline{G} \to \mathrm{Hol}(N/M)$, *where* $\overline{G} = G/\bigcap_g g(\theta^{-1}M)g^{-1}$.

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*
- *If M is an arbitrary subgroup of N (i.e., not a G-subgroup), $\theta^{-1}M$ is just a* **subset** *of G.*

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*
- *If M is an arbitrary subgroup of N (i.e., not a G-subgroup), $\theta^{-1}M$ is just a* **subset** *of G.*
- *For a G-subgroup M,*

$$M \lhd N \not\Rightarrow \theta^{-1}M \lhd G,$$

so

$$\theta \text{ is regular} \not\Rightarrow \overline{\theta} \text{ is regular.}$$

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*
- *If M is an arbitrary subgroup of N (i.e., not a G-subgroup), $\theta^{-1}M$ is just a* **subset** *of G.*
- *For a G-subgroup M,*

$$M \lhd N \not\Rightarrow \theta^{-1} M \lhd G,$$

so

$$\theta \text{ is regular} \not\Rightarrow \overline{\theta} \text{ is regular.}$$

- *Any characteristic subgroup of N is a normal G-subgroup.*

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*
- *If M is an arbitrary subgroup of N (i.e., not a G-subgroup), $\theta^{-1}M$ is just a* **subset** *of G.*
- *For a G-subgroup M,*

$$M \lhd N \not\Rightarrow \theta^{-1}M \lhd G,$$

so

$$\theta \text{ is regular} \not\Rightarrow \overline{\theta} \text{ is regular.}$$

- *Any characteristic subgroup of N is a normal G-subgroup.*

A new idea for Conjecture 1 . . .

Remarks

- *This gives an isomorphism between the lattice of G-subgroups of N and a certain sublattice of the subgroups of G.*
- *Likewise for normal G-subgroups.*
- *If M is an arbitrary subgroup of N (i.e., not a G-subgroup), $\theta^{-1}M$ is just a* **subset** *of G.*
- *For a G-subgroup M,*

$$M \lhd N \not\Rightarrow \theta^{-1}M \lhd G,$$

so

$$\theta \text{ is regular} \not\Rightarrow \overline{\theta} \text{ is regular.}$$

- *Any characteristic subgroup of N is a normal G-subgroup.*

A new idea for Conjecture 1 . . . Group Theorist's Induction.

Template for Group Theorist's Induction:

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then [. . .], so H doesn't either.

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then $[\dots]$, so H doesn't either.
Contradiction!

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then $[\dots]$, so H doesn't either.
Contradiction!
QED! □

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then [...], so H doesn't either.
Contradiction!
QED! □

This works because G is tacitly assumed to be the minimal counterexample ...

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then [...], so H doesn't either.
Contradiction!
QED! □

This works because G is tacitly assumed to be the minimal counterexample ...

... on some interpretation of "minimal".

Template for Group Theorist's Induction:

Theorem

Every finite group [has some property]

Proof.

Suppose G doesn't.
Let H be [some proper subgroup of G].
Then [. . .], so H doesn't either.
Contradiction!
QED! □

This works because G is tacitly assumed to be the minimal counterexample . . .

. . . on some interpretation of "minimal".

Let's try to apply this to Conjecture 1.

Definition

A **bad regular embedding** *is a regular embedding* $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble and* N *soluble.*

Definition

A **bad regular embedding** *is a regular embedding* $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble and* N *soluble.*

It is a **minimal bad regular embedding** *if* $\theta^{-1}M$ *is soluble for every* G*-subgroup* $M \subsetneq N$.

Definition

A **bad regular embedding** *is a regular embedding $\theta : G \to \mathrm{Hol}(N)$ with G insoluble and N soluble.*

It is a **minimal bad regular embedding** *if $\theta^{-1}M$ is soluble for every G-subgroup $M \subsetneq N$.*

So Conjecture 1 says there are no bad regular embeddings.

Definition

A **bad regular embedding** *is a regular embedding* $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble and* N *soluble.*

It is a **minimal bad regular embedding** *if* $\theta^{-1}M$ *is soluble for every* G*-subgroup* $M \subsetneq N$.

So Conjecture 1 says there are no bad regular embeddings.

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ *be a bad regular embedding. Then there is a* G*-subgroup* M *of* N *so that*

$$\theta|_M : \theta^{-1}M \to \mathrm{Hol}(M)$$

is a minimal bad regular embedding.

Definition

A **bad regular embedding** *is a regular embedding* $\theta : G \to \mathrm{Hol}(N)$ *with* G *insoluble and* N *soluble.*

It is a **minimal bad regular embedding** *if* $\theta^{-1}M$ *is soluble for every* G*-subgroup* $M \subsetneq N$.

So Conjecture 1 says there are no bad regular embeddings.

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ *be a bad regular embedding. Then there is a* G*-subgroup* M *of* N *so that*

$$\theta|_M : \theta^{-1}M \to \mathrm{Hol}(M)$$

is a minimal bad regular embedding.

Any composition factor of $\theta^{-1}M$ *occurs as a subquotient of* G.

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

- V is the vector space $\mathbb{F}_p^r$;

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

- V is the vector space $\mathbb{F}_p^r$;
- $\overline{G} = G / \bigcap_g gHg^{-1}$;

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

- V is the vector space $\mathbb{F}_p^r$;
- $\overline{G} = G/\bigcap_g gHg^{-1}$;
- $H = \theta^{-1}M$, a soluble subgroup of G.

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

- V is the vector space $\mathbb{F}_p^r$;
- $\overline{G} = G / \cap_g gHg^{-1}$;
- $H = \theta^{-1}M$, a soluble subgroup of G.

Since M is maximal, V has no $\overline{G}$-subspaces except $\{0_V\}$ and V,

Now let $\theta : G \to N$ be a minimal bad regular embedding.

Let $M \subsetneq N$ be a maximal normal G-subgroup of N.

Since N is soluble,

$$N/M \cong C_p^r \text{ for some prime } p \text{ and some } r \geq 1.$$

So we have a transitive embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V)$$

where

- V is the vector space $\mathbb{F}_p^r$;
- $\overline{G} = G/\bigcap_g gHg^{-1}$;
- $H = \theta^{-1}M$, a soluble subgroup of G.

Since M is maximal, V has no $\overline{G}$-subspaces except $\{0_V\}$ and V, i.e. V is an irreducible $\mathbb{F}_p[\overline{G}]$-module via $\overline{\theta}_a$.

We give a name to this new situation:

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding $\theta : G \to \mathrm{Hol}(V)$ for some vector space $V = \mathbb{F}_p^r$, with G insoluble, and the stabiliser H of 0_V soluble.*

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding* $\theta : G \to \mathrm{Hol}(V)$ *for some vector space* $V = \mathbb{F}_p^r$*, with* G *insoluble, and the stabiliser* H *of* 0_V *soluble.*

It is **irreducible** *if* V *is an irreducible* $\mathbb{F}_p[G]$*-module via* θ_a*.*

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding* $\theta : G \to \mathrm{Hol}(V)$ *for some vector space* $V = \mathbb{F}_p^r$*, with* G *insoluble, and the stabiliser* H *of* 0_V *soluble.*

It is **irreducible** *if* V *is an irreducible* $\mathbb{F}_p[G]$*-module via* θ_a*.*

Note that H is a soluble subgroup of index p^r in the insoluble group G, and $\cap_g gHg^{-1} = \{e_G\}$.

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding* $\theta : G \to \mathrm{Hol}(V)$ *for some vector space* $V = \mathbb{F}_p^r$*, with* G *insoluble, and the stabiliser* H *of* 0_V *soluble.*

It is **irreducible** *if* V *is an irreducible* $\mathbb{F}_p[G]$*-module via* θ_a*.*

Note that H is a soluble subgroup of index p^r in the insoluble group G, and $\cap_g gHg^{-1} = \{e_G\}$.

If θ is irreducible, the projection $G \to \mathrm{Aut}(V) \subset V \rtimes \mathrm{Aut}(V)$ is injective, i.e. θ is **translation-free**.

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding* $\theta : G \to \mathrm{Hol}(V)$ *for some vector space* $V = \mathbb{F}_p^r$*, with* G *insoluble, and the stabiliser* H *of* 0_V *soluble.*

It is **irreducible** *if* V *is an irreducible* $\mathbb{F}_p[G]$*-module via* θ_a*.*

Note that H is a soluble subgroup of index p^r in the insoluble group G, and $\cap_g gHg^{-1} = \{e_G\}$.

If θ is irreducible, the projection $G \to \mathrm{Aut}(V) \subset V \rtimes \mathrm{Aut}(V)$ is injective,
i.e. θ is **translation-free**.

(By contrast, θ is automorphism-free $\Leftrightarrow$ θ is regular.)

We give a name to this new situation:

Definition

A **bad transitive vectorial embedding** *is a transitive embedding* $\theta : G \to \mathrm{Hol}(V)$ *for some vector space* $V = \mathbb{F}_p^r$*, with* G *insoluble, and the stabiliser* H *of* 0_V *soluble.*

It is **irreducible** *if* V *is an irreducible* $\mathbb{F}_p[G]$*-module via* θ_a*.*

Note that H is a soluble subgroup of index p^r in the insoluble group G, and $\cap_g gHg^{-1} = \{e_G\}$.

If θ is irreducible, the projection $G \to \mathrm{Aut}(V) \subset V \rtimes \mathrm{Aut}(V)$ is injective, i.e. θ is **translation-free**.

(By contrast, θ is automorphism-free $\Leftrightarrow$ θ is regular.)

For a soluble group N, let

$$\mathcal{P}(N) = \{\text{primes } p : N \text{ has a normal subgroup of index } p\}.$$

For a soluble group N, let

$$\mathcal{P}(N) = \{\text{primes } p : N \text{ has a normal subgroup of index } p\}.$$

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal bad regular embedding. For each $p \in \mathcal{P}(N)$ there is a quotient $V \cong \mathbb{F}_p^r$ of N and a quotient $\overline{G}$ of G for which θ induces an irreducible bad transitive vectorial embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V).$$

For a soluble group N, let

$$\mathcal{P}(N) = \{\text{primes } p : N \text{ has a normal subgroup of index } p\}.$$

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal bad regular embedding. For each $p \in \mathcal{P}(N)$ there is a quotient $V \cong \mathbb{F}_p^r$ of N and a quotient $\overline{G}$ of G for which θ induces an irreducible bad transitive vectorial embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V).$$

Moreover, $\overline{G}$ has the same nonabelian composition factors as G (with the same multiplicities).

For a soluble group N, let

$$\mathcal{P}(N) = \{\text{primes } p : N \text{ has a normal subgroup of index } p\}.$$

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal bad regular embedding. For each $p \in \mathcal{P}(N)$ there is a quotient $V \cong \mathbb{F}_p^r$ of N and a quotient $\overline{G}$ of G for which θ induces an irreducible bad transitive vectorial embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V).$$

Moreover, $\overline{G}$ has the same nonabelian composition factors as G (with the same multiplicities).

Potential strategy to prove Conjecture 1:

For a soluble group N, let

$$\mathcal{P}(N) = \{\text{primes } p : N \text{ has a normal subgroup of index } p\}.$$

Lemma

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal bad regular embedding. For each $p \in \mathcal{P}(N)$ there is a quotient $V \cong \mathbb{F}_p^r$ of N and a quotient $\overline{G}$ of G for which θ induces an irreducible bad transitive vectorial embedding

$$\overline{\theta} : \overline{G} \to \mathrm{Hol}(V).$$

Moreover, $\overline{G}$ has the same nonabelian composition factors as G (with the same multiplicities).

Potential strategy to prove Conjecture 1:

Show there are no irreducible bad transitive vectorial embeddings.

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Example

Let $G = \mathrm{PSL}_2(7) = \mathrm{GL}_3(2)$*, the simple group of order* 168*, and* $V = \mathbb{F}_2^3$*.*

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Example

Let $G = \mathrm{PSL}_2(7) = \mathrm{GL}_3(2)$*, the simple group of order* 168*, and* $V = \mathbb{F}_2^3$*.*

Write elements of $\mathrm{Hol}(V)$ *as block matrices in* $\mathrm{GL}_4(2)$*.*

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Example

Let $G = \mathrm{PSL}_2(7) = \mathrm{GL}_3(2)$*, the simple group of order* 168*, and* $V = \mathbb{F}_2^3$*.*

Write elements of $\mathrm{Hol}(V)$ *as block matrices in* $\mathrm{GL}_4(2)$*. Let*

$$A = \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Example

Let $G = \mathrm{PSL}_2(7) = \mathrm{GL}_3(2)$*, the simple group of order* 168*, and* $V = \mathbb{F}_2^3$*.*

Write elements of $\mathrm{Hol}(V)$ *as block matrices in* $\mathrm{GL}_4(2)$*. Let*

$$A = \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $A^4 = B^2 = I \neq A^2$ *and* $BAB^{-1} = A^3$ *so* $\langle A, B \rangle$ *is the image of a regular embedding* $D_4 \to \mathrm{Hol}(V)$*.*

Unfortunately, irreducible bad transitive vectorial embeddings do exist!

Example

Let $G = \mathrm{PSL}_2(7) = \mathrm{GL}_3(2)$*, the simple group of order* 168*, and* $V = \mathbb{F}_2^3$*.*

Write elements of $\mathrm{Hol}(V)$ *as block matrices in* $\mathrm{GL}_4(2)$*. Let*

$$A = \left(\begin{array}{ccc|c} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $A^4 = B^2 = I \neq A^2$ *and* $BAB^{-1} = A^3$ *so* $\langle A, B \rangle$ *is the image of a regular embedding* $D_4 \to \mathrm{Hol}(V)$*.*

It is translation-free but not irreduclble.

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2 S$, *so* $\langle R, S\rangle$ *is a group of order* 21.

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2S$, so $\langle R, S\rangle$ is a group of order 21.

$$AR = R^3A^2B, \qquad AS = S^2A^2B, \qquad BR = RA^3B, \qquad BS = S^2B.$$

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2 S$, *so* $\langle R, S \rangle$ *is a group of order* 21.

$$AR = R^3 A^2 B, \qquad AS = S^2 A^2 B, \qquad BR = RA^3 B, \qquad BS = S^2 B.$$

So

$$\langle A, B, R, S \rangle \cong \mathrm{GL}_3(2)$$

giving us an irreducible bad transitive vectorial embedding.

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2 S$, *so* $\langle R, S\rangle$ *is a group of order* 21.

$$AR = R^3A^2B, \qquad AS = S^2A^2B, \qquad BR = RA^3B, \qquad BS = S^2B.$$

So

$$\langle A, B, R, S\rangle \cong \mathrm{GL}_3(2)$$

giving us an irreducible bad transitive vectorial embedding.

To get some information on minimal bad regular embeddings, we investigate two aspects of translation-free bad transitive vectorial embeddings:

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2 S$, *so* $\langle R, S\rangle$ *is a group of order* 21.

$$AR = R^3 A^2 B, \qquad AS = S^2 A^2 B, \qquad BR = RA^3 B, \qquad BS = S^2 B.$$

So

$$\langle A, B, R, S\rangle \cong \mathrm{GL}_3(2)$$

giving us an irreducible bad transitive vectorial embedding.

To get some information on minimal bad regular embeddings, we investigate two aspects of translation-free bad transitive vectorial embeddings: Sylow p-subgroups,

Example (continued)

$$R = \left(\begin{array}{ccc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \qquad S = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 1 \end{array}\right).$$

Then $R^7 = S^3 = I$, $SR = R^2S$, so $\langle R, S\rangle$ is a group of order 21.

$$AR = R^3A^2B, \qquad AS = S^2A^2B, \qquad BR = RA^3B, \qquad BS = S^2B.$$

So

$$\langle A, B, R, S\rangle \cong \mathrm{GL}_3(2)$$

giving us an irreducible bad transitive vectorial embedding.

To get some information on minimal bad regular embeddings, we investigate two aspects of translation-free bad transitive vectorial embeddings: Sylow p-subgroups, and composition factors.

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Write $V = \mathbb{F}_p^r$, let H be the stabiliser of 0_V, and let P be a Sylow p-subgroup of G.

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Write $V = \mathbb{F}_p^r$, let H be the stabiliser of 0_V, and let P be a Sylow p-subgroup of G.

Then $G = PH$ and P is transitive on V. (In general $P \cap H \neq \{0_V\}$.)

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Write $V = \mathbb{F}_p^r$, let H be the stabiliser of 0_V, and let P be a Sylow p-subgroup of G.

Then $G = PH$ and P is transitive on V. (In general $P \cap H \neq \{0_V\}$.)

So θ restricts to a translation-free transitive embedding $P \to \mathrm{Hol}(V)$.
(It is no longer "bad" since P is soluble, and θ cannot be irreducible.)

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Write $V = \mathbb{F}_p^r$, let H be the stabiliser of 0_V, and let P be a Sylow p-subgroup of G.

Then $G = PH$ and P is transitive on V. (In general $P \cap H \neq \{0_V\}$.)

So θ restricts to a translation-free transitive embedding $P \to \mathrm{Hol}(V)$. (It is no longer "bad" since P is soluble, and θ cannot be irreducible.)

In particular, $|P|$ is divisible by p^r and we have an injection $P \hookrightarrow \mathrm{Aut}(V) = \mathrm{GL}_r(p)$.

Sylow p-subgroups

Let $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$ be a translation-free bad transitive vectorial embedding.

Write $V = \mathbb{F}_p^r$, let H be the stabiliser of 0_V, and let P be a Sylow p-subgroup of G.

Then $G = PH$ and P is transitive on V. (In general $P \cap H \neq \{0_V\}$.)

So θ restricts to a translation-free transitive embedding $P \to \mathrm{Hol}(V)$. (It is no longer "bad" since P is soluble, and θ cannot be irreducible.)

In particular, $|P|$ is divisible by p^r and we have an injection $P \hookrightarrow \mathrm{Aut}(V) = \mathrm{GL}_r(p)$.

This is impossible if $r = 1$ or 2 since then p^r does not divide $|\mathrm{GL}_r(p)|$.

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So, if we had a translation-free transitive embedding $P \to \mathrm{Hol}(\mathbb{F}_p^3)$, it would be regular and WLOG its image would be generated by the matrices

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So, if we had a translation-free transitive embedding $P \to \mathrm{Hol}(\mathbb{F}_p^3)$, it would be regular and WLOG its image would be generated by the matrices

$$A = \left(\begin{array}{ccc|c} 1 & 0 & 1 & u_1 \\ 0 & 1 & 0 & u_2 \\ 0 & 0 & 1 & u_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & v_1 \\ 0 & 1 & 1 & v_2 \\ 0 & 0 & 1 & v_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), C = \left(\begin{array}{ccc|c} 1 & 1 & 0 & w_1 \\ 0 & 1 & 0 & w_2 \\ 0 & 0 & 1 & w_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right),$$

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So, if we had a translation-free transitive embedding $P \to \mathrm{Hol}(\mathbb{F}_p^3)$, it would be regular and WLOG its image would be generated by the matrices

$$A = \left(\begin{array}{ccc|c} 1 & 0 & 1 & u_1 \\ 0 & 1 & 0 & u_2 \\ 0 & 0 & 1 & u_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & v_1 \\ 0 & 1 & 1 & v_2 \\ 0 & 0 & 1 & v_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), C = \left(\begin{array}{ccc|c} 1 & 1 & 0 & w_1 \\ 0 & 1 & 0 & w_2 \\ 0 & 0 & 1 & w_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right),$$

satisfying the relations $BA = AB$, $CA = AC$, $CB = ABC$.

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So, if we had a translation-free transitive embedding $P \to \mathrm{Hol}(\mathbb{F}_p^3)$, it would be regular and WLOG its image would be generated by the matrices

$$A = \left(\begin{array}{ccc|c} 1 & 0 & 1 & u_1 \\ 0 & 1 & 0 & u_2 \\ 0 & 0 & 1 & u_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \; B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & v_1 \\ 0 & 1 & 1 & v_2 \\ 0 & 0 & 1 & v_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \; C = \left(\begin{array}{ccc|c} 1 & 1 & 0 & w_1 \\ 0 & 1 & 0 & w_2 \\ 0 & 0 & 1 & w_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right),$$

satisfying the relations $BA = AB$, $CA = AC$, $CB = ABC$.
These imply $u_3 = v_3 = 0$, $2w_3 = 0$.

Moreover, if $r = 3$, then one Sylow p-subgroup of $\mathrm{GL}_3(p)$ is the group of order p^3 consisting of upper triangular unipotent matrices

$$\left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}.$$

So, if we had a translation-free transitive embedding $P \to \mathrm{Hol}(\mathbb{F}_p^3)$, it would be regular and WLOG its image would be generated by the matrices

$$A = \left(\begin{array}{ccc|c} 1 & 0 & 1 & u_1 \\ 0 & 1 & 0 & u_2 \\ 0 & 0 & 1 & u_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \; B = \left(\begin{array}{ccc|c} 1 & 0 & 0 & v_1 \\ 0 & 1 & 1 & v_2 \\ 0 & 0 & 1 & v_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right), \; C = \left(\begin{array}{ccc|c} 1 & 1 & 0 & w_1 \\ 0 & 1 & 0 & w_2 \\ 0 & 0 & 1 & w_3 \\ \hline 0 & 0 & 0 & 1 \end{array}\right),$$

satisfying the relations $BA = AB$, $CA = AC$, $CB = ABC$.
These imply $u_3 = v_3 = 0$, $2w_3 = 0$.
So if $p \geq 3$, we have $u_3 = v_3 = w_3 = 0$ and the P cannot be transitive.

We conclude

Lemma

If we there is a translation-free bad transitive vectorial embedding $G \to \mathrm{Hol}(\mathbb{F}_p^r)$ then either $r \geq 4$ or $p = 2$, $r = 3$.

The previous Example shows the case $p = 2$, $r = 3$ can occur with $G = \mathrm{PSL}_2(7)$.

Corollary

- *If $\theta : G \to \mathrm{Hol}(N)$ is a minimal bad regular embedding and $p \in \mathcal{P}(N)$ then $|G|$ is divisible by*

$$\begin{cases} p^4 & \text{if } p \geq 3; \\ 2^3 & \text{if } p = 2. \end{cases}$$

- *If $\theta : G \to \mathrm{Hol}(N)$ is any bad regular embedding, then $|G|$ is divisible by either p^4 for a prime $p \geq 3$, or by 8.*

So we have proved Theorem 2(a) without using Feit-Thompson or CFSG.

Remark

If we had a translation-free transitive embedding

$$P \to \mathrm{Hol}(\mathbb{F}_p^r)$$

with P a p-group and $r \leq p$, then P would have exponent p and nilpotency class $< p$.
For $p = 2$ and $p = 3$, we have shown that no such embedding exists. Is the same true for all p?
If so, we could replace p^4 by p^{p+1} in the previous Corollary.

Composition Factors

Suppose we have a bad transitive embedding $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$, with G insoluble and $H = \theta^{-1}\{0_v\}$ soluble of index p^r.

Composition Factors

Suppose we have a bad transitive embedding $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$, with G insoluble and $H = \theta^{-1}\{0_v\}$ soluble of index p^r.

To obtain from this a "bad" action of a normal subgroup or quotient of G, we allow our groups to act just as permutions on a set, rather than via the holomorph of a vector space.

Composition Factors

Suppose we have a bad transitive embedding $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$, with G insoluble and $H = \theta^{-1}\{0_v\}$ soluble of index p^r.

To obtain from this a "bad" action of a normal subgroup or quotient of G, we allow our groups to act just as permutions on a set, rather than via the holomorph of a vector space.

Definition 3

A **bad transitive permutation action** is in injective group homomorphism $\theta : G \hookrightarrow \mathrm{Perm}(X)$, where G acts transitively on X, G is insoluble, the stabiliser H of an element of X is soluble, and $|X| = p^r$ for some prime p and some $r \geq 1$.

Composition Factors

Suppose we have a bad transitive embedding $\theta : G \to \mathrm{Hol}(\mathbb{F}_p^r)$, with G insoluble and $H = \theta^{-1}\{0_v\}$ soluble of index p^r.

To obtain from this a "bad" action of a normal subgroup or quotient of G, we allow our groups to act just as permutions on a set, rather than via the holomorph of a vector space.

Definition 3

A **bad transitive permutation action** is in injective group homomorphism $\theta : G \hookrightarrow \mathrm{Perm}(X)$, where G acts transitively on X, G is insoluble, the stabiliser H of an element of X is soluble, and $|X| = p^r$ for some prime p and some $r \geq 1$.

Then H is a soluble subgroup of index p^r in the insoluble group G, and $\cap_g gHg^{-1} = \{e_G\}$.

Any bad transitive vectorial embedding is an example of a bad transitive permutation action.

Any bad transitive vectorial embedding is an example of a bad transitive permutation action.

We try to find its nonabelian composition factors (ignoring the cyclic composition factors).

Any bad transitive vectorial embedding is an example of a bad transitive permutation action.

We try to find its nonabelian composition factors (ignoring the cyclic composition factors).

If $J \lhd G$ then the orbits of J on X are permuted transitively by G/J.

Any bad transitive vectorial embedding is an example of a bad transitive permutation action.

We try to find its nonabelian composition factors (ignoring the cyclic composition factors).

If $J \lhd G$ then the orbits of J on X are permuted transitively by G/J.

So both J and G/J have permutation actions on sets of p-power size. These have soluble point stabilisers, and become injective after dividing out a soluble subgroup . Thus either J or G/J (or both) gives a bad transitive permutation action.

Any bad transitive vectorial embedding is an example of a bad transitive permutation action.

We try to find its nonabelian composition factors (ignoring the cyclic composition factors).

If $J \lhd G$ then the orbits of J on X are permuted transitively by G/J.

So both J and G/J have permutation actions on sets of p-power size. These have soluble point stabilisers, and become injective after dividing out a soluble subgroup . Thus either J or G/J (or both) gives a bad transitive permutation action.

Repeating, we can break down a bad transitive vectorial embedding of characteristic p into a sequence of bad transitive permutation actions of nonabelian **simple** groups acting on sets of p-power size. This preserves all the nonabelian composition factors of G.

If a nonabelian simple group G has a bad transitive permutation action $G \to \mathrm{Perm}(X)$ with $|X| = p^r$, then G has a soluble subgroup of index p^r.

If a nonabelian simple group G has a bad transitive permutation action $G \to \mathrm{Perm}(X)$ with $|X| = p^r$, then G has a soluble subgroup of index p^r.

Now we use a consequence of CFSG:

If a nonabelian simple group G has a bad transitive permutation action $G \to \mathrm{Perm}(X)$ with $|X| = p^r$, then G has a soluble subgroup of index p^r.

Now we use a consequence of CFSG:

Theorem (Guralnick, 1983)

If G is a nonabelian simple group G with a proper subgroup of prime-power index p^r, then one of the following holds.

(a) $G = A_n$, $H = A_{n-1}$ *with* $n = p^r$;

(b) $G = \mathrm{PSL}_n(q)$, $p^r = (q^n - 1)/(q - 1)$ *and* H *is the stabiliser of a point or a hyperplane in* G;

(c) $G = \mathrm{PSL}_2(11)$ *and* $H = A_5$ *of index* 11;

(d) $G = M_{23}$, $H = M_{22}$ *or* $G = M_{11}$, $H = M_{!0}$;

(e) $G = \mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ *and* H *has index* 27.

Corollary

If G is a nonabelian finite simple group with a **soluble** *subgroup H of prime-power index, then one of the following holds.*

(a) $G = \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, *the simple group of order* 168, *and H has index* 7 *or* 8;

(b) $G = \mathrm{PSL}_3(3)$ *and H has index* 13;

(c) $G = \mathrm{PSL}_2(2^a)$ *where $2^a + 1 = p$ is a Fermat prime, and H has index p;*

(d) $G = \mathrm{PSL}_2(q)$ *where $q = 2^a - 1$ is a Mersenne prime with $q > 7$, and H has index $q + 1 = 2^a$.*

Corollary

If G is a nonabelian finite simple group with a **soluble** *subgroup H of prime-power index, then one of the following holds.*

(a) $G = \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, *the simple group of order* 168, *and H has index* 7 *or* 8;

(b) $G = \mathrm{PSL}_3(3)$ *and H has index* 13;

(c) $G = \mathrm{PSL}_2(2^a)$ *where $2^a + 1 = p$ is a Fermat prime, and H has index p*;

(d) $G = \mathrm{PSL}_2(q)$ *where $q = 2^a - 1$ is a Mersenne prime with $q > 7$, and H has index $q + 1 = 2^a$.*

Case (c) includes the case $\mathrm{PSL}_2(4) \cong A_5$ with a subgroup of index 5. (This group is also isomorphic to $\mathrm{PSL}_2(5)$.)

Corollary

If G is a nonabelian finite simple group with a **soluble** *subgroup H of prime-power index, then one of the following holds.*

(a) $G = \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, *the simple group of order* 168, *and H has index* 7 *or* 8;

(b) $G = \mathrm{PSL}_3(3)$ *and H has index* 13;

(c) $G = \mathrm{PSL}_2(2^a)$ *where* $2^a + 1 = p$ *is a Fermat prime, and H has index* p;

(d) $G = \mathrm{PSL}_2(q)$ *where* $q = 2^a - 1$ *is a Mersenne prime with* $q > 7$, *and H has index* $q + 1 = 2^a$.

Case (c) includes the case $\mathrm{PSL}_2(4) \cong A_5$ with a subgroup of index 5. (This group is also isomorphic to $\mathrm{PSL}_2(5)$.)

We then deduce ...

Theorem

Let $\theta : G \to \mathrm{Hol}(V)$ be a bad transitive vectorial embedding, with $V = \mathbb{F}_p^r$. Then one of the following holds.

(a) *$p = 7$ and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_2(7)$ of order 168;*

(b) *$p = 13$ and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_3(3)$;*

(c) *$p = 2^a + 1$ is a Fermat prime and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_2(2^a)$;*

(d) *$p = 2$ and every nonabelian composition factor of G is of the form $\mathrm{PSL}_2(q)$ for a Mersenne prime $q = 2^a - 1 \geq 7$.*

Theorem

Let $\theta : G \to \mathrm{Hol}(V)$ be a bad transitive vectorial embedding, with $V = \mathbb{F}_p^r$. Then one of the following holds.

(a) *$p = 7$ and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_2(7)$ of order 168;*

(b) *$p = 13$ and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_3(3)$;*

(c) *$p = 2^a + 1$ is a Fermat prime and every nonabelian composition factor of G is isomorphic to $\mathrm{PSL}_2(2^a)$;*

(d) *$p = 2$ and every nonabelian composition factor of G is of the form $\mathrm{PSL}_2(q)$ for a Mersenne prime $q = 2^a - 1 \geq 7$.*

Combining this with the Sylow p-subgroup result, we get ...

Theorem

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal regular embedding. Then one of the following holds.

(a) $\mathcal{P}(N) = \{7\}$ *or* $\{2, 7\}$ *and every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$;

(b) $\mathcal{P}(N) = \{13\}$, *every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_3(3)$, *and* 13^4 *divides* $|G|$;

(c) $\mathcal{P}(N) = \{q\}$ *for some Fermat prime* $q = 2^a + 1$, *every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_2(2^a)$, *and* q^4 *divides* $|G|$;

(d) $\mathcal{P}(N) = \{2\}$ *and each nonabelian composition factor of* G *has the form* $\mathrm{PSL}_2(q)$ *for some Mersenne prime* $q = 2^a - 1 \geq 7$.

Theorem

Let $\theta : G \to \mathrm{Hol}(N)$ be a minimal regular embedding. Then one of the following holds.

(a) $\mathcal{P}(N) = \{7\}$ *or* $\{2, 7\}$ *and every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$*;*

(b) $\mathcal{P}(N) = \{13\}$*, every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_3(3)$*, and* 13^4 *divides* $|G|$*;*

(c) $\mathcal{P}(N) = \{q\}$ *for some Fermat prime* $q = 2^a + 1$*, every nonabelian composition factor of* G *is isomorphic to* $\mathrm{PSL}_2(2^a)$*, and* q^4 *divides* $|G|$*;*

(d) $\mathcal{P}(N) = \{2\}$ *and each nonabelian composition factor of* G *has the form* $\mathrm{PSL}_2(q)$ *for some Mersenne prime* $q = 2^a - 1 \geq 7$*.*

Theorem 2(b) follows.

Thank you for listening!