Automorphisms, commutativity measures and sets of integers without arithmetic progressions

Peter Hegarty

Chalmers University of Technology and University of Gothenburg

11 June, 2011

- **Definition :** An automorphism ϕ of a group G is said to be a *universal power automorphism of degree n* if $\phi(g) = g^n$ for every $g \in G$.

- **Definition :** An automorphism ϕ of a group G is said to be a *universal power automorphism of degree n* if $\phi(g) = g^n$ for every $g \in G$.
- Note that if $n \in \{-1, 2\}$ then

$$(xy)^n = x^n y^n \Rightarrow xy = yx.$$

- **Definition :** An automorphism ϕ of a group G is said to be a *universal power automorphism of degree n* if $\phi(g) = g^n$ for every $g \in G$.
- Note that if $n \in \{-1, 2\}$ then

$$(xy)^n = x^n y^n \Rightarrow xy = yx.$$

- Hence, if G possesses a universal power automorphism of degree -1 or 2, then G is abelian.

- **Definition :** An automorphism ϕ of a group G is said to be a *universal power automorphism of degree n* if $\phi(g) = g^n$ for every $g \in G$.
- Note that if $n \in \{-1, 2\}$ then

$$(xy)^n = x^n y^n \Rightarrow xy = yx.$$

- Hence, if G possesses a universal power automorphism of degree -1 or 2, then G is abelian.
- In fact the same is true for $n = 3$, but not for any $n > 3$ since there exist non-abelian groups of exponent $n - 1$ for every $n > 3$.

- Let G be a finite group. The most natural commutativity measure is the probability that two randomly chosen group elements commute.

- Let G be a finite group. The most natural commutativity measure is the probability that two randomly chosen group elements commute.
- More precisely, let

$$\Pr(G) := \frac{\#\{(x,y) \in G \times G : xy = yx\}}{|G|^2}.$$

- Let G be a finite group. The most natural commutativity measure is the probability that two randomly chosen group elements commute.
- More precisely, let

$$\mathrm{Pr}(G) := \frac{\#\{(x,y) \in G \times G : xy = yx\}}{|G|^2}.$$

- The function Pr assigns to every finite group a rational number in $(0, 1]$. It has the following salient features.

- $\mathrm{Pr}(G) = 1$ if and only if G is abelian.

- $\mathrm{Pr}(G) = 1$ if and only if G is abelian.
- If G is non-abelian, then $\mathrm{Pr}(G)$ is bounded away from one. In fact, $\mathrm{Pr}(G) \leq 5/8$.

- $\Pr(G) = 1$ if and only if G is abelian.
- If G is non-abelian, then $\Pr(G)$ is bounded away from one. In fact, $\Pr(G) \leq 5/8$.
- More generally, groups for which $\Pr(G)$ is *sufficiently large*, say above a certain *threshold*, can be completely classified and have a structure which is clearly *close to abelian*.

- $\Pr(G) = 1$ if and only if G is abelian.
- If G is non-abelian, then $\Pr(G)$ is bounded away from one. In fact, $\Pr(G) \leq 5/8$.
- More generally, groups for which $\Pr(G)$ is *sufficiently large*, say above a certain *threshold*, can be completely classified and have a structure which is clearly *close to abelian*.
- For example, if $\Pr(G) > 1/2$, then G is nilpotent of class 2, $|G'| = 2$ and

$$\Pr(G) = \frac{1}{2}\left(1 + \frac{1}{4^n}\right), \quad \text{for some } n \in \mathbb{N}.$$

- Alternative measures of commutativity have been proposed. One idea is to use universal power automorphisms.

- Alternative measures of commutativity have been proposed. One idea is to use universal power automorphisms.
- Let $n \in \{-1, 2, 3\}$. For a finite group G and $\phi \in \text{Aut}(G)$, set

$$r_n(G, \phi) := \frac{\#\{g \in G : \phi(g) = g^n\}}{|G|}$$

- Alternative measures of commutativity have been proposed. One idea is to use universal power automorphisms.
- Let $n \in \{-1, 2, 3\}$. For a finite group G and $\phi \in \mathrm{Aut}(G)$, set

$$r_n(G, \phi) := \frac{\#\{g \in G : \phi(g) = g^n\}}{|G|}$$

and set

$$r_n(G) := \max_{\phi \in \mathrm{Aut}(G)} r_n(G, \phi).$$

- Alternative measures of commutativity have been proposed. One idea is to use universal power automorphisms.
- Let $n \in \{-1, 2, 3\}$. For a finite group G and $\phi \in \mathrm{Aut}(G)$, set

$$r_n(G, \phi) := \frac{\#\{g \in G : \phi(g) = g^n\}}{|G|}$$

and set

$$r_n(G) := \max_{\phi \in \mathrm{Aut}(G)} r_n(G, \phi).$$

- Thus, the function r_n assigns to a finite group a rational number in $(0, 1]$, and we have already observed that $r_n(G) = 1$ if and only if G is abelian, provided $n \in \{-1, 2, 3\}$.

Theorem *Let G be a finite group. If G is non-abelian, then*

Theorem *Let G be a finite group. If G is non-abelian, then*

- $r_{-1}(G) \leq 3/4$

Theorem *Let G be a finite group. If G is non-abelian, then*

- $r_{-1}(G) \leq 3/4$
- *If* $r_{-1}(G) > 1/2$*, then one of the following possibilities occurs :*

Theorem *Let G be a finite group. If G is non-abelian, then*

- $r_{-1}(G) \leq 3/4$
- *If $r_{-1}(G) > 1/2$, then one of the following possibilities occurs :*

(1) *G has an abelian subgroup of index two and $r_{-1}(G) = \frac{k+1}{2k}$ for some $k \in \mathbb{N}_{\geq 2}$.*

Theorem *Let G be a finite group. If G is non-abelian, then*

- $r_{-1}(G) \leq 3/4$
- *If $r_{-1}(G) > 1/2$, then one of the following possibilities occurs :*

(1) *G has an abelian subgroup of index two and $r_{-1}(G) = \frac{k+1}{2k}$ for some $k \in \mathbb{N}_{\geq 2}$.*

(2) *G is nilpotent of class two, G' is elementary abelian of order 2 or 4, with various explicit commutator relations on the generators of $G/Z(G)$. In this case,*

$$r_{-1}(G) = \frac{2^k + 1}{2^{k+1}}, \quad \text{for some } k \in \mathbb{N}.$$

Theorem *Let G be a finite group. If G is non-abelian, then*

- $r_{-1}(G) \leq 3/4$
- *If* $r_{-1}(G) > 1/2$, *then one of the following possibilities occurs :*

(1) *G has an abelian subgroup of index two and* $r_{-1}(G) = \frac{k+1}{2k}$ *for some* $k \in \mathbb{N}_{\geq 2}$.

(2) *G is nilpotent of class two,* G' *is elementary abelian of order 2 or 4, with various explicit commutator relations on the generators of* $G/Z(G)$. *In this case,*

$$r_{-1}(G) = \frac{2^k + 1}{2^{k+1}}, \quad \textit{for some } k \in \mathbb{N}.$$

- Potter showed that if $r_{-1}(G) > 4/15$, then G is soluble. One has $r_{-1}(A_5, \mathrm{id}) = 16/60 = 4/15$.

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

- $r_2(G) \leq 1/2$.

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

- $r_2(G) \leq 1/2$.
- *If* $r_2(G) \geq 5/12$, *then one of the following possibilities occurs :*

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

- $r_2(G) \leq 1/2$.
- *If* $r_2(G) \geq 5/12$, *then one of the following possibilities occurs :*

(1) *G splits over an abelian, odd-order subgroup of index two and* $r_2(G) = 1/2$.

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

- $r_2(G) \leq 1/2$.
- *If $r_2(G) \geq 5/12$, then one of the following possibilities occurs :*

(1) *G splits over an abelian, odd-order subgroup of index two and $r_2(G) = 1/2$.*

(2) *$Z(G)$ is abelian of odd order, $G/Z(G) \cong A_4$ and $G' \cap Z(G) = \{1\}$. In this case, $r_2(G) = 5/12$.*

Theorem (Zimmerman) *Let G be a finite group. If G is non-abelian, then*

- $r_2(G) \leq 1/2$.
- *If $r_2(G) \geq 5/12$, then one of the following possibilities occurs :*

  (1) *G splits over an abelian, odd-order subgroup of index two and $r_2(G) = 1/2$.*

  (2) *$Z(G)$ is abelian of odd order, $G/Z(G) \cong A_4$ and $G' \cap Z(G) = \{1\}$. In this case, $r_2(G) = 5/12$.*

- Liebeck classified all odd order groups satisfying $r_2(G) = 1/3$, and I classified all even order groups satisfying $r_2(G) \geq 1/6$.

Proposition *If G is non-abelian, then $r_{-1}(G) \leq 3/4$.*

Proposition *If G is non-abelian, then $r_{-1}(G) \leq 3/4$.*

PROOF : Let $\phi \in \mathrm{Aut}(G)$ and set

$$T_{-1,\phi} := \{g \in G : \phi(g) = g^{-1}\}.$$

Proposition *If G is non-abelian, then* $r_{-1}(G) \leq 3/4$.

PROOF : Let $\phi \in \mathrm{Aut}(G)$ and set

$$T_{-1,\phi} := \{g \in G : \phi(g) = g^{-1}\}.$$

Let H be a subgroup of G which is maximal with respect to the condition $H \subseteq T_{-1,\phi}$.

Proposition *If G is non-abelian, then $r_{-1}(G) \leq 3/4$.*

PROOF : Let $\phi \in \text{Aut}(G)$ and set

$$T_{-1,\phi} := \{g \in G : \phi(g) = g^{-1}\}.$$

Let H be a subgroup of G which is maximal with respect to the condition $H \subseteq T_{-1,\phi}$.

Since

$$(xy)^{-1} = x^{-1}y^{-1} \Rightarrow xy = yx,$$

it follows that if $x \in T_{-1,\alpha}$, then

$$\{h \in H : hx \in T_{-1,\phi}\} = C_H(x).$$

By maximality of H, we deduce that if $x \in T_{-1,\phi} \backslash H$, then

$$|Hx \cap T_{-1,\phi}| \leq \frac{1}{2}|H|.$$

By maximality of H, we deduce that if $x \in T_{-1,\phi} \backslash H$, then

$$|Hx \cap T_{-1,\phi}| \leq \frac{1}{2}|H|.$$

Now consider a coset decomposition of G with respect to H, and count !

By maximality of H, we deduce that if $x \in T_{-1,\phi} \backslash H$, then

$$|Hx \cap T_{-1,\phi}| \leq \frac{1}{2}|H|.$$

Now consider a coset decomposition of G with respect to H, and count !

- Since $(xy)^2 = x^2y^2 \Rightarrow xy = yx$, the same basic method works for $n = 2$.

By maximality of H, we deduce that if $x \in T_{-1,\phi} \backslash H$, then

$$|Hx \cap T_{-1,\phi}| \leq \frac{1}{2}|H|.$$

Now consider a coset decomposition of G with respect to H, and count !

- Since $(xy)^2 = x^2y^2 \Rightarrow xy = yx$, the same basic method works for $n = 2$.
- But for $n = 3$ we have a problem. It is no longer true that, if $H \subseteq T_{3,\phi}$ and $x \in T_{3,\phi}$, then

$$\{h \in H : hx \in T_{3,\phi}\} = C_H(x).$$

- However, it is still true that if $H \subseteq T_{3,\phi}$, then H is abelian.

- However, it is still true that if $H \subseteq T_{3,\phi}$, then H is abelian.
- Moreover, if $x \in T_{3,\phi}$, then

$$\{h \in H : hx \in T_{3,\phi}\}$$

is a union of cosets of $C_H(x)$.

- However, it is still true that if $H \subseteq T_{3,\phi}$, then H is abelian.
- Moreover, if $x \in T_{3,\phi}$, then

$$\{h \in H : hx \in T_{3,\phi}\}$$

is a union of cosets of $C_H(x)$.

Hence, this set may be identified with a subset $\mathcal{T}(H, x)$ of the abelian group $H/C_H(x)$.

The Key Lemma *Suppose each of* a, b, ab *and* $a^{-1}b$ *is in* $T_{3,\phi}$*. Then* $[a, b] = 1$*.*

The Key Lemma *Suppose each of a, b, ab and $a^{-1}b$ is in $T_{3,\phi}$. Then $[a, b] = 1$.*

Corollary *If each of a, b, ab and $a^{-2}b$ is in $T_{3,\phi}$, then $[a, b] = 1$.*

The Key Lemma *Suppose each of* a, b, ab *and* $a^{-1}b$ *is in* $T_{3,\phi}$. *Then* $[a, b] = 1$.

Corollary *If each of* a, b, ab *and* $a^{-2}b$ *is in* $T_{3,\phi}$, *then* $[a, b] = 1$.

All of which implies that ...

The Key Lemma *Suppose each of a, b, ab and $a^{-1}b$ is in $T_{3,\phi}$. Then $[a, b] = 1$.*

Corollary *If each of a, b, ab and $a^{-2}b$ is in $T_{3,\phi}$, then $[a, b] = 1$.*

All of which implies that ...

Proposition *If $H \subseteq T_{3,\phi}$ and $x \in T_{3,\phi}$, then the subset $\mathcal{T}(H, x)$ of the abelian group $H/C_H(x)$, written additively, contains no non-trivial solutions to either of the translation invariant linear equations $a + b = 2c$, $a + 2b = 3c$. In particular, it contains no non-trivial 3-term arithmetic progressions.*

To get a feeling for what this is saying, suppose that $H/C_H(x)$ is a cyclic group of order N.

To get a feeling for what this is saying, suppose that $H/C_H(x)$ is a cyclic group of order N.

Roth's theorem (1952) *Let $r_3(N)$ denote the maximum size of a subset of $\mathbb{Z}_N$ containing no non-trivial 3-term arithmetic progressions. Then*

$$r_3(N) = O\left(\frac{N}{\log \log N}\right) = o(N).$$

To get a feeling for what this is saying, suppose that $H/C_H(x)$ is a cyclic group of order N.

Roth's theorem (1952) *Let $r_3(N)$ denote the maximum size of a subset of $\mathbb{Z}_N$ containing no non-trivial 3-term arithmetic progressions. Then*

$$r_3(N) = O\left(\frac{N}{\log \log N}\right) = o(N).$$

Hence, in the group world, the set $T_{3,\phi}$ cannot be too large without forcing a lot of commutativity.