Graphs, groups, and more: Celebrating
Brian Alspach 80th and Dragan Marušič's 65th.
Koper

Invariable generation of alternating groups by prime-power elements

Russ Woodroofe
University of Primorska
russ.woodroofe@famnit.upr.si

A problem, from older work

Joint work with Bob Guralnick and John Shareshian.

Joint work with Bob Guralnick and John Shareshian.

Binomial Question. Given $n > 1$, can you find primes p, r so that every nontrivial binomial coef. is divisible by at least one of p, r?

Example:

For $n = 1{,}000{,}000$, we can take $p = 5$ and $r = 999{,}983$.

$\binom{n}{k}$ is divisible by r if $k > 999{,}983$ or $k < 17$.

$\binom{n}{k}$ is divisible by $p = 5$ unless k is divisible by 5^6,

as $(1+x)^{2^6 \cdot 5^6} \equiv (1 + x^{5^6})^{2^6} \mod 5$.

Similar tricks plus some brute force computation give a "yes" answer out to $n = 1$ billion. (Shareshian and me, 2016)

Motivation

Q: $\forall n$, $\exists ?\, p, r$ s.t. $\forall 0 < k < n$, p divides $\binom{n}{k}$ or r divides $\binom{n}{k}$.

Q: $\forall n$, $\exists ?\, p, r$ s.t. $\forall 0 < k < n$, p divides $\binom{n}{k}$ or r divides $\binom{n}{k}$.

Motivation is from group theory.

Let $\mathcal{C}(G) =$ all cosets of all proper subgroups G.

Problem: When possible, find uncomplicated groups that act fixed-point-freely on $\mathcal{C}(G)$.

For P a p-group, R an r-group (p, r primes), and C a cyclic group:

1. An action by $P \rtimes C \rtimes R$ is good.
2. An action by $C \rtimes R$ is better.

Higher motivation: show that the "universal vertex-transitive G-geometry" $\mathcal{C}(G)$ is not contractible. (Smith-Oliver Theory)

$\mathcal{C}(G) =$ all cosets of all proper s.g.'s of G

How to act on $\mathcal{C}(G)$?

- multiply on left by $L \subseteq G$.
- multiply on right by $R \subseteq G$.
- act by automorphism of G, that is, by $A \subseteq \mathrm{Aut}\, G$.
- exchange left and right.

Indeed, $\mathrm{Aut}\, \mathcal{C}(G) \cong ((G \times G) \rtimes \mathrm{Aut}\, G) \rtimes \mathbb{Z}_2 \,/\, \mathrm{Kernel}$.

What cosets are fixed by $L \times R$ left/right multiplication action?

$$\begin{aligned}
&LHxR = Hx && \iff \\
&LHxRx^{-1}x = Hx && \iff \\
&LHR^{x^{-1}}x = Hx && \iff \\
&L, R^{x^{-1}} \subseteq H. &&
\end{aligned}$$

Thus, $L \times R$ acts fpf-ly on proper cosets $\iff \forall x, \langle L, R^x \rangle = G$.

In this situation, we say that L, R *invariably generate* G.

$L \times R$ acts fpfly on $\mathcal{C}(G) \iff L, R$ *invariably generate* G.
$\iff \forall x$, L and R^x generate G.

Theorem (Shareshian and me, 2016).
If S is a Lie-type or sporadic simple group, then S is invariably generated by a Sylow 2-subgroup and some other Sylow subgroup.

Recall the Classification of Finite Simple Groups says that a simple group is Lie-type (matrix group), sporadic, or alternating.

The direct analog for alternating is false – consider A_{31}, or A_{2^n-1}.

But it is reasonable to ask the following.

Open Question 1. For each alternating group A_n, can you find primes p, r so that A_n is invbly generated by Sylow p-, r-subgroups?

$L \times R$ acts fpfly on $\mathcal{C}(G) \iff L, R$ *invariably generate* G.
$\iff \forall x$, L and R^x generate G.

At this point, we've considered two questions:

Binomial Question. Given $n > 1$, can you find primes p, r so that every nontrivial binomial coef. is divisible by at least one of p, r?

Open Question 1. For each alternating group A_n, can you find primes p, r so that A_n is invbly generated by Sylow p-, r-subgroups?

The two questions turn out to be completely equivalent!
(Shareshian and me, 2016)

E.g.: $A_{1000000}$ is invariably generated by Sylow 999983- and 5-sgs.

Ongoing work

$L \times R$ acts fpfly on $\mathcal{C}(G) \iff L, R$ *invariably generate G.*
$\iff \forall x$, L and R^x generate G.

Right after acceptance of our paper, we saw how to improve it:

Invariable generation by a cyclic subgroup and a Sylow subgroup gives a stronger version of noncontractibility of $\mathcal{C}(G)$.

After some more work, and subject to finishing checking details:

Theorem-in-progress (Guralnick, Shareshian and me 2019+).
If S is a Lie-type or sporadic simple group, then S is invariably generated by two elements of prime order. (up to finitely? many exceptions)

What about alternating groups?

L, R *invariably generate* G if $\forall x$, L and R^x generate G.

Which alternating groups are invariably generated by two elements of prime order?

- Most of them – asymptotic density 1. (assuming RH)
- Not all of them. Fails for $A_8, A_{16}, A_{32}, \ldots$.

But it's reasonable to ask the following:

Open Question 2 (harder).
Is every alternating group invariably generated by two elements of prime power order?

The answer is "yes" out to 90 million.
(We expect to be able to check out to 1 billion or greater.)

Work on the harder question has yielded insight on the easier one!

Computationally checking invariable generation of A_n by Sylow sgs

Q1: Is A_n always invariably generated by two Sylow sgs?
Q2: Is A_n always invariably generated by two elts of pp order?

Strategy for checking inv. gen. of A_n by Sylow: (older)

1. Reduce to binomial divisibility (pure number theory). Now it's enough to find $p \mid n$ and r dividing every $\binom{n}{k}$.
2. Take p so that p^a be largest prime-power divisor of n.
3. If $\exists$ prime r between $n - p^a$ and n, then done! (completely similar to $n = 1,000,000$ example)
4. Otherwise, apply brute force to find an r that "works".

This strategy fails for 22 numbers up to 1 billion.
For these, apply more brute force with a prime other than p.

Computing out to 1 billion took 2 weeks on my MacBook.

Computationally checking invariable generation of A_n by pp elts

Q1: Is A_n always invariably generated by two Sylow sgs?
Q2: Is A_n always invariably generated by two elts of pp order?

As before, let p^a be large(st) pp divisor of n, and
r be some other prime.

To avoid primitive proper subgroups of A_n, we need to have
$r > \sqrt{n}$, and the r-power element to be the product of
r-cycles. Wlog, $\left\lfloor \frac{n}{r} \right\rfloor$ r-cycles.
(Using results of Praeger; Liebeck and Saxl)

We take the p-power element to have cycle structure corresponding
to the base-p representation of n.

To get transitive subgroup, we must have $\left\lfloor \frac{n}{r} \right\rfloor \cdot r + p^a > n$.
(When $\left\lfloor \frac{n}{r} \right\rfloor > 1$, there are additional "cheap" checks to make.)

Computing to 90 million takes a few hours on my MacBook.

Example: Find pp elements that invariably generate A_{31416}.

31416 factorizes as $2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 17$.

Largest pp divisor is $p = p^1 = 17$. (2nd largest is 11.)

Unfortunately there are no primes between 31399 and 31416.
But 7853 is prime, and $31416 = 4 \cdot 7853 + 4$.

Unfortunately, $31416 = 6 \cdot 17^3 + 6 \cdot 17^2 + 12 \cdot 17$, so
$$15708 = 3 \cdot 17^3 + 3 \cdot 17^2 + 6 \cdot 17.$$
So 17 fails a "cheap check" for transitivity.

However, A_{31416} is generated by the product of 4 7853-cycles and an 11-power element.


Happy Birthday
Brian and Dragan

-Advertisement-

If you use GAP on a Mac, you need Gap.app!

- includes latest version of GAP (built-in)
- drag-and-drop install
- Mac-like editing, command completion
- graphics – draw subgroup lattices (and more)

Available at cocoagap.sourceforge.io for the low price of **free**!