Group theory and the Bateman–Horn Conjecture

Celebrating the 70th birthday of Nikolai Vavilov

Gareth Jones,
jointly with Alexander Zvonkin (LaBRI, Bordeaux),
with computational assistance from
Jean Bétréma (LaBRI, Bordeaux).

University of Southampton, UK

September 21, 2022

Introduction

In group theory and other areas of mathematics, the existence of interesting finite objects often depends on certain finite sets of polynomials $f_i(t) \in \mathbb{Z}[t]$ simultaneously taking prime values.

Schinzel's Hypothesis asserts that they do so for infinitely many $t \in \mathbb{N}$ provided they satisfy a few obviously necessary conditions.

The Bateman–Horn Conjecture (BHC) gives an estimate $E(x)$ for the number of such $t \leq x$, in all known cases agreeing closely with the actual number $Q(x)$, and satisfying $E(x) \to \infty$ as $x \to \infty$.

I will show how the BHC gives strong evidence that various families of groups and related objects, some appearing in very old group-theoretic problems, others in more recent work, are infinite.

Permutation groups of prime degree

One of the oldest problems in Group Theory (Lagrange) is to classify the permutation groups of prime degree, originally studied in terms of the solution of polynomial equations of prime degree.

Let G be a transitive permutation group of prime degree p.

Galois (1831) proved that G is solvable if and only if G is (up to isomorphism) a subgroup of the 1-dimensional affine group

$$\mathrm{AGL}_1(p) = \{t \mapsto at + b \mid a, b \in \mathbb{F}_p, a \neq 0\} \cong \mathrm{C}_p \rtimes \mathrm{C}_{p-1}$$

containing the translation subgroup $\{t \mapsto t + b\} \cong \mathrm{C}_p$.

There is one such group G for each d dividing $p - 1$, namely

$$\{t \mapsto at + b \mid a, b \in \mathbb{F}_p, a^d = 1\} \cong \mathrm{C}_p \rtimes \mathrm{C}_d.$$

Nonsolvable groups of degree p

Burnside (1911) proved that if G is nonsolvable then

- G is 2-transitive;
- the commutator subgroup G' is simple (and also 2-transitive);
- $G/G' \cong \mathrm{C}_d$ where d divides $p-1$;
- $C_G(G') = 1$, so $G \leq \mathrm{Aut}\, G'$ (i.e. G is almost simple).

This reduces the problem to studying simple groups S of degree p and their automorphism groups.

The classification of finite simple groups (announced around 1980) implies a classification of finite 2-transitive groups. Most have composite degree; those of prime degree are as follows:

Nonsolvable groups of prime degree (S simple, $G \leq \mathrm{Aut}\, S$)

a) $S = \mathrm{A}_p$, $G = \mathrm{A}_p$ or S_p, for primes $p \geq 5$;

b) $S = \mathrm{PSL}_2(11)$, M_{11} and M_{23} for $p = 11, 11$ and 23;

c) $S = \mathrm{PSL}_n(q) \leq G \leq \mathrm{P\Gamma L}_n(q) = \mathrm{PGL}_n(q) \rtimes \mathrm{Gal}\, \mathbb{F}_q$ in cases where their natural degree $d = (q^n - 1)/(q - 1)$ is a prime p.

In (b), $\mathrm{PSL}_2(11)$, of order 660, acts on the 11 cosets of a subgroup $H \cong \mathrm{A}_5$ (two conjugacy classes, so two actions); M_{11} and M_{23} are Mathieu groups, acting on Steiner systems with 11 and 23 points.

In (c) the groups act on the d points (or d points and hyperplanes if $n \geq 3$) of the projective geometry $\mathbb{P}^{n-1}(\mathbb{F}_q)$ for a prime power q.

Open Problem: In (c), is the degree

$$d = \frac{q^n - 1}{q - 1} = 1 + q + q^2 + \cdots + q^{n-1} \quad (q \text{ a prime power})$$

prime (a 'projective prime') in finitely or infinitely many cases?

Examples of projective primes $p = (q^n - 1)/(q - 1)$

a) For $n = 2$ the primes p are the Fermat primes $1 + 2^e$, $e = 2^f$; the only known examples are $3, 5, 17, 257, 65\,537$ for $f \leq 4$.

b) For $q = 2$ the primes p are the Mersenne primes $2^n - 1$, n prime; 51 examples $3, 7, 31, \ldots, 2^{82\,589\,933} - 1$ are known.

c) Others, e.g. $1 + 2^{59} + 2^{2 \cdot 59} + \cdots + 2^{58 \cdot 59}$ (1031 decimal digits).

It is widely conjectured that there are no further Fermat primes, but infinitely many Mersenne primes. To avoid these difficult problems, assume from now on that $n, q \geq 3$.

Easy lemma: If $\frac{q^n - 1}{q - 1} = 1 + q + \cdots + q^{n-1}$ is prime then n is prime.

Aim: Take the simplest and most frequent case $n = 3$, q prime, and try to show there are infinitely many primes $p = 1 + q + q^2$.

Examples: $1 + 3 + 3^2 = 13$, $1 + 5 + 5^2 = 31$, $1 + 17 + 17^2 = 307$,

$1 + 99\,999\,999\,977 + 99\,999\,999\,977^2 = 9\,999\,999\,995\,500\,000\,000\,507$.

Number-theoretic conjectures

Can polynomials $f_i(t) \in \mathbb{Z}[t]$ $(i = 1, \ldots, k)$ simultaneously take prime values for infinitely many $t \in \mathbb{N}$? Necessary conditions are:

- each f_i is irreducible;
- each f_i has a positive leading coefficient;
- $f := f_1 \ldots f_k$ is not identically zero modulo any prime.

Schinzel's Hypothesis (1958) conjectures that these are sufficient.

Bunyakovsky's Conjecture (1857) was the case $k = 1$,

Examples:
$f_1(t) = t^2 + 1$ gives the Euler–Landau problem;
$f_i(t) = t, t + 2$ gives the twin primes conjecture;
$f_i(t) = t, 2t + 1$ gives the Sophie Germain primes conjecture;
$f_i(t) = t, 1 + t + t^2$ gives our problem with $n = 3$ and q prime.

Schinzel's Hypothesis is proved only for $k = 1$ and $\deg f_1 = 1$:
this is Dirichlet's Theorem for primes $at + b$ with a and b coprime.

The Bateman–Horn Conjecture, generalising work by Hardy and Littlewood on twin primes, estimates the number $Q(x)$ of positive integers $t \leq x \in \mathbb{R}$ such that each $f_i(t)$ is prime. It claims that

$$Q(x) \sim E(x) := C \int_a^x \frac{dt}{\prod_{i=1}^k \ln f_i(t)} \quad \text{as} \quad x \to \infty,$$

where a is chosen to avoid singularities where $\ln f_i(t) = 0$, and

$$C = C(f_1, \ldots, f_k) := \prod_{r \text{ prime}} \left(1 - \frac{1}{r}\right)^{-k} \left(1 - \frac{\omega_f(r)}{r}\right)$$

where $\omega_f(r)$ is the number of distinct roots of $f = f_1 \ldots f_k$ in $\mathbb{Z}_r$.

Now $C > 0$ and $\int_a^x \ldots$ diverges as $x \to \infty$, so $E(x) \to \infty$.
If BHC is true then $Q(x) \to \infty$, so the $f_i(t)$ are prime for infinitely many t; in particular, there are infinitely many projective primes.

Heuristic argument for the BHC

$$Q(x) \sim E(x) := C \int_a^x \frac{dt}{\prod_{i=1}^k \ln f_i(t)} \quad \text{as} \quad x \to \infty,$$

$$C = C(f_1, \ldots, f_k) := \prod_{r \text{ prime}} \left(1 - \frac{1}{r}\right)^{-k} \left(1 - \frac{\omega_f(r)}{r}\right).$$

Prime Number Theorem: $\pi(x) \sim \int_2^x \frac{dt}{\ln t}$ (much better than $\frac{x}{\ln x}$).
One might guess (wrongly) that the number of $t \leq x$ with $f(t)$ prime is asymptotic to $\int_a^x \frac{dt}{\ln f(t)}$, and hence the number of $t \leq x$ with $f_i(t)$ prime for $i = 1, \ldots, k$ is asymptotic to $\int_a^x \frac{dt}{\prod_i \ln f_i(t)}$, assuming that the $f_i(t)$ behave independently.

Of course they don't, and C is a product of correction factors, one for each prime r, replacing the probability $\left(1 - \frac{1}{r}\right)^k$ that k random elements of $\mathbb{Z}_r$ are $\neq 0$ with the probability $1 - \frac{\omega_f(r)}{r}$ that $f(t) \not\equiv 0$.

Computational aspects

Maple can evaluate the definite integral $\int_a^x \ldots$ almost instantly.

(In the 1960s, without tools such as Maple, the programming was done 'from scratch', so Bateman and Horn simplified each $\ln f_i(t)$ to $\deg(f_i) \cdot \ln t$, losing some accuracy.)

The infinite product $C = \prod_{\text{prime } r} \ldots$ converges, but very slowly; by taking the product over the primes $r < 10^9$ we got good approximations, to C and hence $E(x)$, usually after several hours.

Maple can determine $Q(x)$, for $x \approx 10^{11}$, by evaluating the polynomials $f_i(t)$ for $t = 1, 2, \ldots$, and testing each for primality by the Rabin–Miller test. This test is probabilistic, but the chances of an error are negligible (and in our case unimportant).

Example: projective primes $1 + q + q^2$ with q prime

Take $f_1(t) = t$ and $f_2(t) = 1 + t + t^2$ in the BHC.

Compare $Q(x) = |\{t \leq x \mid f_1(t), f_2(t) \text{ are prime}\}|$, obtained by computer search, with the BHC (+Maple) estimate $E(x)$ for $Q(x)$:

x	$Q(x)$	$E(x)$	$E(x)/Q(x)$
10^{10}	15 801 827	1.579642126×10^7	0.9996579044
$2 \cdot 10^{10}$	29 684 763	2.968054227×10^7	0.9998578150
$3 \cdot 10^{10}$	42 963 858	4.296235691×10^7	0.9999650617
$4 \cdot 10^{10}$	55 877 571	5.587447496×10^7	0.9999445924
$5 \cdot 10^{10}$	68 522 804	6.852175590×10^7	0.9999847043
$6 \cdot 10^{10}$	80 962 422	8.096382889×10^7	1.0000173771
$7 \cdot 10^{10}$	93 236 613	9.323905289×10^7	1.0000261688
$8 \cdot 10^{10}$	105 372 725	1.053741048×10^8	1.0000130940
$9 \cdot 10^{10}$	117 383 505	1.173885689×10^8	1.0000431394
10^{11}	129 294 308	1.292974079×10^8	1.0000239757

We feel that this is strong evidence for the existence of infinitely many projective primes $1 + q + q^2$ with q prime (and that it also adds to the substantial evidence for the correctness of the BHC).

There is similar evidence for primes $n > 3$ and for prime powers q (but rather weaker, since $1 + q + \cdots + q^{n-1}$ grows faster out of our computable range), so we propose the following:

Conjecture

For each prime $n \geq 3$ there are infinitely many projective primes $p = 1 + q + \cdots + q^{n-1}$ (where q is a prime power), and hence infinitely many permutation groups $\mathrm{PSL}_n(q)$ of prime degree p.

Other applications to group theory

We have similar evidence for analogous problems in other areas. Here are two more from group theory.

Dixon and Zalesskii (1998) classified the finite primitive linear groups of prime degree d, i.e. finite subgroups of $\mathrm{SL}_d(\mathbb{C})$, in terms of the socle S of their image in $\mathrm{PSL}_d(\mathbb{C})$.

There are several possibly infinite families, such as $S = \mathrm{PSU}_n(q)$ (the simple unitary group) of prime degree

$$d = \frac{q^n + 1}{q + 1} = 1 - q + q^2 - \cdots + q^{n-1},$$

and also $\mathrm{PSL}_2(q)$ for q and $d = (q-1)/2$ prime, and $\mathrm{PSp}_{2n}(q)$ for $d = (q^n + 1)/2$ prime.

Using the BHC we have strong evidence that they are all infinite.

In the 1890s, Hölder, Frobenius and Burnside proved that the non-abelian simple groups of order a product of at most five primes (counting repetitions) are $\mathrm{PSL}_2(q)$ for $q = 5, 7, 11, 13$, of orders

$$2^2 \cdot 3 \cdot 5, \quad 2^3 \cdot 3 \cdot 7, \quad 2^2 \cdot 3 \cdot 5 \cdot 11, \quad 2^2 \cdot 3 \cdot 7 \cdot 13.$$

Peter Neumann asked: are there infinitely many with six primes?

By inspection of the known orders of simple groups, they must be $\mathrm{PSL}_2(q)$ for $q = 8, 9$ or p, of orders

$$2^3 \cdot 3^2 \cdot 7, \quad 2^3 \cdot 3^2 \cdot 5 \quad \text{or} \quad (p-1)p(p+1)/2$$

for primes p such that $p^2 - 1$ is a product of six primes.

Problem: are there infinitely many such primes p?

The BHC gives strong evidence that for each $k \geq 6$ there are infinitely many primes p such that $p^2 - 1$ is a product of k primes.

Problem: Prove this for some $k \geq 6$.

A few recent applications related to group theory

Amarrra, Devillers and Praeger have recently constructed families of block designs with interesting symmetry properties.

Cameron, Manna and Mehatari have recently characterized the nonabelian finite simple groups whose power graph is a cograph.

Hujdorović, Kutnar, Marušič et al. have recently constructed sets of intersecting permutations with interesting symmetry properties.

The constructions or definitions of these objects require certain polynomials to take prime or prime power values.

The BHC gives strong evidence that they do so for infinitely many $t \in \mathbb{N}$, and hence that these families of objects are all infinite.

In conclusion

We also have similar applications in areas such as cryptography, difference sets, elliptic curves, error-correcting codes, expander graphs, fast integer multiplication, intersecting sets, ...

In all these cases, the BHC gives strong evidence of the existence of infinitely many objects of the required type.

The only cases where it fails are those where the values of the polynomials (related to the size of the objects) grow too rapidly for our computing facilities (a modest laptop running Maple) to cope.

In each application, the point is not so much that we find many examples (often millions) of the required objects, but that the distribution of examples predicted by the BHC agrees very closely with what is found by computer search.

This strengthens the evidence for the BHC, and emphasises the desirability of its proof.

More details can be found in the following:

J. and A. K. Zvonkin, Klein's ten planar dessins of degree 11, and beyond, arxiv.math:2104.12015, to appear.

—, Groups of prime degree and the Bateman–Horn Conjecture, arxiv.math:2106.00346, to appear

—, Block designs and prime values of polynomials, arxiv.math:2105.03915, submitted.

—, Orders of simple groups and the Bateman–Horn Conjecture, arXiv.math:2209.06510.

—, The Bateman–Horn Conjecture and some applications, in preparation.

THANK YOU FOR LISTENING,
and
HAPPY BIRTHDAY, NIKOLAI!