Solving semidecidable problems in group theory

Giles Gardam

University of Münster

SMRI – Algebra and Geometry Online
5 October 2021

Mathematics Münster
Cluster of Excellence

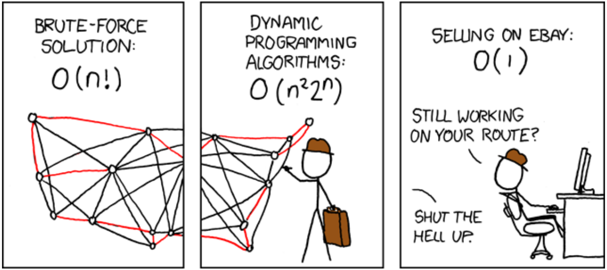
CRC 1442 GEOMETRY: DEFORMATIONS AND RIGIDITY

SPP 2026 GEOMETRY AT INFINITY

Computational complexity 101

The most famous problem in computational complexity theory is

P versus NP: can every decision problem for which `YES` answers can be *checked* in polynomial time in fact be *solved* in polynomial time.



xkcd.com/399

Computational complexity 101

Many problems in group theory lie way beyond classes like NP or EXP, in fact even beyond decidability.

A decision problem is *semidecidable* if there is an algorithm that

- terminates with answer `YES` when given a `YES` input, but
- will run forever (or answer `NO`) otherwise.

Equivalently, the language of `YES` inputs is *recursively enumerable*.

Classical undecidable problems in group theory

- The word problem for groups (Novikov–Boone).

  There exists a finitely presented group $G = \langle X \mid R \rangle$ such that deciding if a word $w \in F(X)$ represents the trivial element or not is undecidable.

  It is however semidecidable: $w =_G 1$ if and only if we can write it as

  $$w = \prod_{i=1}^{n} u_i^{-1} r_i u_i \quad \text{for } r_i \in R \cup R^{-1}, u_i \in F(X)$$

  and such expressions are recursively enumerable.

- The triviality problem for group presentations.

- The profinite triviality problem for group presentations (Bridson–Wilton).

  Non-triviality is semidecidable: you will eventually find a non-trivial finite quotient if one exists.

More semidecidable problems in group theory

It is worth asking yourself: is my question semidecidable? Could I put a computer to work on it? Often "yes", especially if you restrict focus.

The unit conjecture (Higman 1940, Kaplansky 1970)

Let G be a torsion-free group and let K be a field. Then the only units in the group ring $K[G]$ are the trivial units, i.e., kg for $k \in K \setminus \{0\}$ and $g \in G$.

Recall: $K[G]$ has multiplication $(\sum r_g g) \cdot (\sum s_h h) := \sum (r_g s_h)(gh)$.

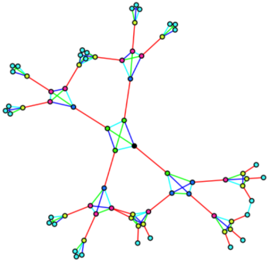
For simplicity, say K is finite. If G has solvable word problem then the set of non-trivial units in $K[G]$ is recursively enumerable. The existence of non-trivial units is semidecidable *modulo the word problem*.

Lots of interesting sets are recursively enumerable, but so is $\emptyset$!

Enumerating recursively enumerable sets

A good first step to find a needle in an infinite haystack: turn the infinite haystack into an infinite sequence of finite haystacks.

For example, for groups we could look the ball $B(n)$ of radius n in the Cayley graph (all words of length at most n in the generators) for increasing values of n.



Source: `okuluma`, imgur.com/gallery/Ozf1bWO

NP

Taking as input the multiplication table for subsets $A, B \subset G$ and deciding if they support a non-trivial solution to $\alpha\beta = 1$ over $\mathbb{F}_q$ is in NP.

The smallest $A = B = B(n)$ in the Hantzsche–Wendt crystallographic group

$$P = \langle\, a, b \mid b^{-1}a^2b = a^{-2},\, a^{-1}b^2a = b^{-2} \,\rangle$$

that works over $\mathbb{F}_2$ is for $n = 5$. It has 147 elements and $2^{147} \approx 10^{44}$.

It's not just pure mathematicians who want answers to problems in NP! Optimization, hardware and software verification, ...

There are industrial tools to solve NP-complete problems. Is there a nice reduction of our problem to one of them?

Boolean satisfiability

SAT was the first NP-complete problem (Cook–Levin, early 1970's). It asks:

> Given a Boolean formula in propositional logic, is there an assignment of the variables to `true` and `false` that makes the formula evaluate to `true` (i.e., that *satisfies* the formula)?

Note that the size of the formula is relevant, not just the number of variables (there are 2^{2^n} functions $\{0,1\}^n \to \{0,1\}$).

The standard encoding used is *conjunctive normal form*: a big AND of ORs. For variables x, y, z we could have something like

$$(x \vee \overline{y}) \wedge (\overline{x} \vee y \vee z) \wedge (y \vee \overline{z})$$

Terminology: $x \vee \overline{y}$ is a *clause* on the *literals* x and $\overline{y}$.

The Tseytin transformation turns an arbitrary formula into CNF of linear size but with auxiliary variables introduced.

Existence of non-trivial units in SAT

For simplicity, $K = \mathbb{F}_2$ (other finite fields possible). Let $\alpha = \sum_{g \in B(n)} a_g g$ and $\beta = \sum_{g \in B(n)} b_g g$. We can assert non-triviality with the clauses

$$a_1 \quad \text{and} \quad \bigvee_{g \in B(n) \setminus \{1\}} a_g .$$

We introduce $|B(n)|^2$ variables $x_{g,h} := a_g \cdot b_h$ via

$$(\overline{x}_{g,h} \vee a_g) \wedge (\overline{x}_{g,h} \vee b_h) \wedge (\overline{a_g} \vee \overline{b_h} \vee x_{g,h}), \quad \text{i.e.,}$$
$$(x_{g,h} \to a_g) \wedge (x_{g,h} \to b_h) \wedge ((a_g \wedge b_h) \to x_{g,h}) .$$

Each equation $\sum_{gh=k} x_{g,h} = \delta_{1,k}$ is asserted by breaking it up into smaller sums, introducing auxiliary variables, with each atomic equation asserted exhaustively, for instance $x + y + z = 0$ being

$$(\overline{x} \vee \overline{y} \vee \overline{z}) \wedge (\overline{x} \vee y \vee z) \wedge (x \vee \overline{y} \vee z) \wedge (x \vee y \vee \overline{z}).$$

After fixing $B(n)$, SAT doesn't care how big the support actually is!

SAT solvers

Most modern SAT solvers (e.g. minisat, glucose, cryptominisat, lingeling, ...) build on the Davis–Putnam–Logemann–Loveland algorithm from 1961, which is a backtracking algorithm with some basic deductions (*unit propagation* and *pure literal elimination*). Using sophisticated heuristics and data structures, together with *conflict driven clause learning*, they can handle problems that were unimaginable before 2000.

$$\begin{tikzcd} & (x \vee \overline{y}) \wedge (\overline{x} \vee y \vee z) \wedge (y \vee \overline{z}) \arrow[dl, "x=0"] \arrow[dr, "x=1"'] & \\ \overline{y} \wedge (y \vee \overline{z}) & & (y \vee z) \wedge (y \vee \overline{z}) \end{tikzcd}$$

The 2016 "world's longest proof" (200 terabytes) by Heule–Kullmann–Marek proved that there is no 2-colouring of the positive integers without a monochromatic Pythagorean triple (solution to $a^2 + b^2 = c^2$). The problem is unsatisfiable on $\{1, 2, \ldots, 7825\}$.

Finding non-trivial units with SAT

How hard is the problem? Timescale of minutes to hours to days.

Why is this problem amenable to SAT solving? Helpful property: some parts of the quadratic system are quite sparse. If $a_g b_h + a_{g'} b_{h'} = 0$ then

$$\begin{aligned} a_g b_h = 1 &\implies a_{g'} b_{h'} = 1 \\ &\implies a_g b_{h'} = 1 \text{ and } a_{g'} b_h = 1 \end{aligned}$$

and something needs to cancel with $a_g b_{h'}$ and $a_{g'} b_h$. This could quickly lead to a contradiction.

Can we SAT solve other problems?

Various problems around the existence of non-trivial units admit nice encodings into SAT.

$$
\begin{tikzcd}
\text{left-orderable} \arrow[r, Rightarrow] & \text{diffuse} \arrow[r, Rightarrow] & \text{unique product property} \arrow[dll, Rightarrow] \\
\text{unit conjecture over } \mathbb{F}_q \arrow[r, Rightarrow] & \text{zero-divisor conjecture over } \mathbb{F}_q \arrow[r, Rightarrow] & \text{idempotent conjecture over } \mathbb{F}_q
\end{tikzcd}
$$

Zero divisor conjecture

The difference between the formula asking for a non-trivial unit and for a zero divisor differs in only one bit!

However, compared to the unit conjecture, we have a shortage of candidate groups, and only quite "large" groups are plausible as candidates.

Unique product property

The group G has the *unique product property* if for all finite $A, B \subset G$ there is some $g \in G$ uniquely expressible as $a \cdot b$ for $a \in A, b \in B$. We can formulate the failure of this property using a cardinality constraint (cf. Frisch–Peugniez).

Exploiting some ahead-of-time deductions we can get

Theorem (G. 2021)

The torsion-free group $\langle\, a, b \mid aba^2b^{-1}a^2b^{-2}, ab^3ab^4a^{-1}b \,\rangle$ *does not have the unique product property.*

(This group is an $\widetilde{A}_2$ lattice and thus has property (T).)

$B(4)$ is a tree. We actually need $B(6)$ with 1311 group elements.

Orderability

A group G is *(left-)orderable* if there is a total order $\prec$ on G that is left-invariant: $h \prec k \implies gh \prec gk$.

Folklore fact

Non-orderability is semidecidable modulo the word problem.

Defining an order is equivalent to choosing the *positive cone* $P = \{g : g \succ 1\}$ such that $G = \{1\} \sqcup P \sqcup P^{-1}$ and P is a subsemigroup: $g, h \in P \implies gh \in P$. Letting the variable x_g encode $g \in P$, we have clauses

$$(\overline{x}_g \vee \overline{x}_h \vee x_{gh}) \wedge (x_g \vee x_h \vee \overline{x}_{gh}).$$

This is an instance of 3-SAT, as used by Orlef to show non-orderability of random groups in the triangular model.

More units

Soelberg's Master's thesis introduced a torsion-free polycyclic group

$$S = \langle\, x, y \mid x^{-1}y^2xy^2, x^{-2}yx^{-2}y^3 \,\rangle$$

with two 8-element sets that fail to have a unique product; this is the current world record. S is virtually the Heisenberg group.

Theorem (G. 2021)

There are non-trivial units in $\mathbb{F}_2[S]$. For instance, with support of size 29:

$$\begin{aligned} &1 + y + y^{-1} + x^2 + xy^{-1} + x^{-1}y + x^{-1}y^{-1} + yx + y^{-2} + xyx \\ &+ xy^{-1}x + x^{-2}y + yx^{-1}y + y^{-3} + x^2yx + x^2y^{-1}x + x^2y^{-2} \\ &+ xyx^{-1}y + xy^{-3} + yxyx + yxy^{-2} + yx^{-2}y^{-1} + y^{-4} + x^3y^{-1}x \\ &+ xyxyx + xyxy^{-2} + xyx^{-2}y^{-1} + xy^{-4} + x^{-1}y^{-4} \end{aligned}$$

Questions?