The Complexity of Solving Equations over Finite Groups

A collecion of results by Goldmann and Russell from 1999

Philipp Nuspl in the seminar *Universal Algebra und Computational Complexity*
Johannes Kepler University Linz

March 26, 2019

Introduction

Problem

We will assume that $(G, \cdot)$ is a finite group.

Definition (Horváth and Szabó 2006)

Given polynomials $p_1, \ldots, p_r, q_1, \ldots, q_r$ over G we want to decide if there is an $x = (x_1, \ldots, x_n) \in G^n$ such that

$$p_i(x) = q_i(x), \quad \text{for all } i = 1, \ldots, r.$$

We write $\textsc{PolSysSat}(G)$ for short. If $r = 1$ we write $\textsc{PolSat}(G)$.

What is a polynomial over G? Each polynomial p over G is of the form

$$p = w_1 \cdot w_2 \cdots w_s \text{ where } w_j \in G \cup \{x_1, \ldots, x_n\} \cup \{x_1^{-1}, \ldots, x_n^{-1}\}.$$

Hence we can assume that $q_i(x) = 1$, i.e. our system is given as

$$p_i(x) = 1, \quad \text{for all } i = 1, \ldots, r.$$

We ask: For which groups G is $\textsc{PolSysSat}(G) \in P$ and for which $\textsc{PolSat}(G) \in P$?

Examples

Some examples of polynomial equations include:

- $(\mathbb{Z}_8, +)$:
$$2 + 3x_1 + 5x_2 + 7x_3 = 0,$$
- $(D_4, \cdot)$ with $a^4 = b^2 = 1$ (so $|D_4| = 8$):
$$a \cdot a \cdot x_1 \cdot x_1 \cdot b \cdot x_2^{-1} \cdot b \cdot a = x_3^{-1} \cdot b,$$
- $(S_3, \circ)$:
$$x \circ \begin{pmatrix} 1 & 3 & 2 \end{pmatrix} \circ x^{-1} \circ \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix},$$
- $(S_5, \circ)$:
$$x_1 \circ \begin{pmatrix} 1 & 5 \end{pmatrix} \circ x_2 \circ \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}.$$

Goal of today

Goldmann and Russell proved two important theorems:

Theorem 1 (Goldmann and Russell 1999, Thm. 1+2)

If G is an abelian group, then $\textsc{PolSysSat}(G) \in P$ and $\textsc{PolSysSat}(G) \in NPC$ otherwise.

Theorem 2 (Goldmann and Russell 1999, Thm. 10 + Cor. 12)

If G is a nilpotent group, then $\textsc{PolSat}(G) \in P$ and if G is not solvable then $\textsc{PolSat}(G) \in NPC$.

System of Equations

Solving systems over abelian groups

As a first step we will show:

Theorem 1 (part 1, (Goldmann and Russell 1999, Thm. 1))

If G is an abelian group, then $\textsc{PolSysSat}(G) \in P$.

Proof: Every finite abelian group G can be written as

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}.$$

Want to solve system $p_i(x_1, \ldots, x_n) = 0$ for $i = 1, \ldots, r$ with polynomials p_i over G. Instead of solving the system over G we can rewrite it as l individual systems over $\mathbb{Z}_{n_k}$. Hence we only consider the case $\mathbb{Z}_m$. Over $\mathbb{Z}_m$ we can solve a system using (essentially) Gaussian elimination.

Solving systems over $\mathbb{Z}_m$

For a polynomial $\tilde{p}_i$ over $\mathbb{Z}_m$ we can write:

$$\tilde{p}_i(x_1, \dots, x_n) = p_i^{(1)} x_1 + \dots + p_i^{(n)} x_n - p_i^{(0)}.$$

Hence the system $\tilde{p}_i(x_1, \dots, x_n) = 0$ is equivalent to

$$(a_{ij})_{i,j=1}^{r,n} x := Ax := \begin{pmatrix} p_1^{(1)} & \dots & p_1^{(n)} \\ \vdots & & \vdots \\ p_r^{(1)} & \dots & p_r^{(n)} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} p_1^{(0)} \\ \vdots \\ p_r^{(0)} \end{pmatrix} =: b =: (b_i)_{i=1}^{r}.$$

We do not change the satisfiablity of the system if we:

- Interchange rows of A: Reordering equations.
- Interchange columns of A: Reordering variables.
- Adding multiple of row to different row.
- Adding multiple of column to different column.

Algorithm

For computing a diagonal form of the matrix using these operations do:

1. Find a nonzero minimal entry a_{ij} of A.
2. Reduce all entries in row i and column j.
3. If all entries in row i and column j (except a_{ij}) are zero, then swap row i with row 1 and column j with column 1 and proceed with step 1 with the submatrix arising by removing the first row and first column.
4. Otherwise we have created an element which is smaller than a_{ij}. Again proceed with step 1 with the whole matrix.

The elements in the matrix get strictly smaller, so the algorithm terminates. It has polynomial complexity $\mathcal{O}(rn \min(r, n))$.

Hence in total $\textsc{PolSysSat}(\mathbb{Z}_n) \in P$, so $\textsc{PolSysSat}(G) \in P$ for abelian groups G. $\square$

NP-completeness

The more difficult part of Theorem 1 will be:

Theorem 1 (part 2)

If G is an not abelian, then $\textsc{PolSysSat}(G)$ is NP complete.

How can one show NP-completeness? (Polynomially) reduce a problem which is known to be NP-complete to the problem for which we want to show NP-completeness. Here: Graph-Colorability.

Graph-colorability

Theorem (Karp 1972)

Given a graph G and $k \geq 3$ different colors. The problem of deciding if there is a color for each vertex of G such that two vertices which are connected by an edge do not have the same color is NP-complete.

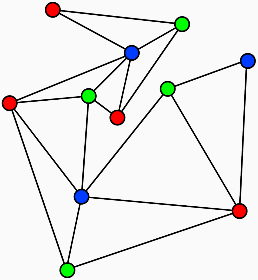


Figure 1: Source: Wikimedia Commons (David Eppstein), *https://commons.wikimedia.org/wiki/File:Triangulation_3-coloring.svg*

Small groups

order	abelian groups	non-abelian groups
1	$\mathbb{Z}_1$	
2	$\mathbb{Z}_2$	
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2$	
5	$\mathbb{Z}_5$	
6	$\mathbb{Z}_6$	$D_3 \cong S_3$
7	$\mathbb{Z}_7$	
8	$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_4, Q_8
9	$\mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3$	
10	$\mathbb{Z}_{10}$	D_5
11	$\mathbb{Z}_{11}$	
12	$\mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6$	D_6, A_4, T
13	$\mathbb{Z}_{13}$	
14	$\mathbb{Z}_{14}$	D_7
15	$\mathbb{Z}_{15}$	

Table 1: Hungerford 2003

PolSysSat(S_3)

To prove that PolSysSat(G) is *NP*-complete for non-abelian groups G we use induction on order of the groups. Smallest non-abelian group is S_3.

Lemma (Goldmann and Russell 1999, Thm. 3)

PolSysSat(S_3) is *NP*-complete.

Proof: We will show that coloring a graph with 6 colors can be reduced to PolSysSat(S_3). Every element in S_3 corresponds to a color (6 colors total). With each vertex i in the graph we associate a variable x_i. For each edge (i, j) in the graph we introduce two variables y_{ij}, z_{ij} and the equation

$$y_{ij}\, x_i\, x_j^{-1}\, z_{ij}\, x_j\, x_i^{-1}\, z_{ij}^{-1}\, y_{ij}^{-1} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}.$$

PolSysSat(S_3)

If the coloring is legal, then for every edge (i, j) we have $\alpha := x_i x_j^{-1} \neq \begin{pmatrix}1\end{pmatrix}$. The equation

$$y_{ij}\, \alpha z_{ij}\, \alpha^{-1}\, z_{ij}^{-1}\, y_{ij}^{-1} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$$

has a solution if and only if α is not the identity:

α	z_{ij}	y_{ij}	α	z_{ij}	y_{ij}
$\begin{pmatrix}1 & 2\end{pmatrix}$	$\begin{pmatrix}1 & 2 & 3\end{pmatrix}$	$\begin{pmatrix}1\end{pmatrix}$	$\begin{pmatrix}1 & 2 & 3\end{pmatrix}$	$\begin{pmatrix}2 & 3\end{pmatrix}$	$\begin{pmatrix}2 & 3\end{pmatrix}$
$\begin{pmatrix}1 & 3\end{pmatrix}$	$\begin{pmatrix}1 & 2 & 3\end{pmatrix}$	$\begin{pmatrix}1\end{pmatrix}$	$\begin{pmatrix}1 & 3 & 2\end{pmatrix}$	$\begin{pmatrix}2 & 3\end{pmatrix}$	$\begin{pmatrix}1\end{pmatrix}$
$\begin{pmatrix}2 & 3\end{pmatrix}$	$\begin{pmatrix}1 & 2 & 3\end{pmatrix}$	$\begin{pmatrix}1\end{pmatrix}$			

Hence we have reduced the problem of coloring a graph to the problem of solving a system of equations over S_3. If we can solve the system of equations over S_3 we can color the graph. Therefore PolSysSat(S_3) $\in NPC$. $\square$

Inducible subgroups

Having the base-case S_3 settled we will introduce some more concepts before we will prove the general result.

Definition (Goldmann and Russell 1999, Def. 1)

A subset $H \subseteq G$ is called inducible if there is a polynomial p over G such that

$$H = \mathrm{Im}(p) = \{p(g_1, \ldots, g_n) \;:\; g_1, \ldots, g_n \in G\}.$$

Inducible subgroups have the nice property that NP completeness carries over to the larger group. Namely:

Lemma (Goldmann and Russell 1999, Lemma 4)

Let H be an inducible subgroup of G.

1. If $\textsc{PolSysSat}(H) \in NPC$, then $\textsc{PolSysSat}(G) \in NPC$.
2. If H is a normal subgroup of G and $\textsc{PolSysSat}(G/H) \in NPC$, then $\textsc{PolSysSat}(G) \in NPC$.

Proof complexity of inducible subgroups

Proof of $\textsc{PolSysSat}(H) \in NPC \implies \textsc{PolSysSat}(G) \in NPC$:

Since H is inducible there exists a polynomial $p(x_1, \ldots, x_n)$ over G such that $H = \mathrm{Im}(p)$. Given an equation

$$w_1 \cdot w_2 \cdots w_s = 1 \text{ over } H \text{ with } w_i \in H \cup \{y_1, \ldots, y_m\} \cup \{y_1^{-1}, \ldots, y_m^{-1}\}$$

we can replace every occurrence of y_i with $p(x_1^{(i)}, \ldots, x_n^{(i)})$ where $x_j^{(i)}$ are new variables over G and every occurrence of y_i^{-1} with $p(x_1^{(i)}, \ldots, x_n^{(i)})^{-1}$. Then we have a new equation over G which can be satisfied if and only if the original one can be satisfied. $\square$

Proof complexity of inducible subgroups

Proof of $\textsc{PolSysSat}(G/H) \in NPC \implies \textsc{PolSysSat}(G) \in NPC$:

Now an equation over G/H looks like

$$(w_1 \cdot w_2 \cdots w_s)H = w_1 H \cdot w_2 H \cdots w_s H = H$$

with $w_i \in G \cup \{y_1, \ldots, y_m\} \cup \{y_1^{-1}, \ldots, y_m^{-1}\}$ which we can rewrite as

$$w_1 \cdot w_2 \cdots w_s = p(x_1, \ldots, x_n)$$

and

$$w_1 \cdot w_2 \cdots w_s \cdot p(x_1, \ldots, x_n)^{-1} = 1$$

over G for new variables $x_1, \ldots, x_n$. $\square$

Commutators

Definition

For two elements $a, b \in G$ we write

$$[a, b] := aba^{-1}b^{-1}$$

and call $[a, b]$ a commutator.

For two subsets $A, B \subseteq G$ we write

$$[A, B] := \{[a, b] = aba^{-1}b^{-1} \ : \ a \in A, b \in B\}$$

and $(A, B) = \langle [A, B] \rangle$ for the group generated by the commutators $[a, b]$ and call (A, B) a commutator subgroup.

In particular (G, G) is the commutator subgroup of G. In fact (G, G) is the smallest subgroup of G such that $G/(G, G)$ is abelian. Furthermore $(G, G) = \{1\}$ if and only if G is abelian.

Commutator subgroup

Lemma (Goldmann and Russell 1999, Lemma 5)

$(G, G) \subseteq G$ is inducible.

Reminder: $[a, b] = aba^{-1}b^{-1}$ and $(G, G) = \langle\{[a, b] \,:\, a, b \in G\}\rangle$.

Proof: Every element $g \in (G, G)$ can be written as

$$g = [a_1, b_1][a_2, b_2] \cdots [a_m, b_m].$$

Since G is finite and $[a, a] = 1$ we have a fixed $m \in \mathbb{N}$ such that

$$(G, G) = \{[a_1, b_1][a_2, b_2] \cdots [a_m, b_m] \,:\, a_i, b_i \in G\}.$$

Hence we can choose the polynomial

$$p(x_1, y_1, \ldots, x_m, y_m) := [x_1, y_1][x_2, y_2] \cdots [x_m, y_m].$$

This p induces (G, G), i.e. $p(G^{2m}) = (G, G)$. $\square$

Commutator facts

Later we will need the commutator subgroups

$$(a, G) := (\{a\}, G) = \{[a, g_1][a, g_2] \cdots [a, g_m] \;:\; g_i \in G\}.$$

Lemma (Goldmann and Russell 1999, Lemma 6)

Let $a \in G$. Then

1. $(a, G) \subseteq (G, G)$,
2. (a, G) is inducible and
3. (a, G) is normal in G.

Proof of $(a, G) \subseteq (G, G)$: For

$$[a, g_1][a, g_2] \cdots [a, g_m] \in (a, G)$$

we also have

$$[a, g_1][a, g_2] \cdots [a, g_m] \in (G, G).$$

Commutator facts

Proof of (a, G) *inducible*: We can choose the polynomial

$$p(x_1, \ldots, x_m) := [a, x_1][a, x_2] \cdots [a, x_m],$$

then $p(G^m) = (a, G)$.

Proof of (a, G) *normal:* Since $(a, G) = \langle \{[a, g] \ : \ g \in G\} \rangle$, it is sufficient to show $b[a, g]b^{-1} \in (a, G)$ for all $g, b \in G$. This follows as

$$\begin{aligned} b[a, g]b^{-1} = b(aga^{-1}g^{-1})b^{-1} &= (ba\,\underbrace{b^{-1}a^{-1})(ab}_{=1}\,ga^{-1}g^{-1}b^{-1}) \\ &= (aba^{-1}b^{-1})^{-1}(abga^{-1}g^{-1}b^{-1}) = [a, b]^{-1}[a, bg]. \end{aligned}$$

As (a, G) is a subgroup $[a, b]^{-1} \in (a, G)$, so $b[a, g]b^{-1} \in (a, G)$ and (a, G) is normal in G. □

Commutator simple

Definition

We call

$$Z(G) := \{g \in G \,:\, gh = hg \text{ for all } h \in G\}$$

the center of G.

Definition (Goldmann and Russell 1999, Def. 3)

We call G commutator simple if for all $a \notin Z(G)$ we have $(G, G) = (a, G)$.

The last Lemma we need before we can finish the proof that $\textsc{PolSysSat}(G) \in NPC$ for non-abelian G:

Lemma (Goldmann and Russell 1999, Lemma 7)

Let G be a non-abelian commutator simple group. Then $\textsc{PolSysSat}(G) \in NPC$.

Commutator simple

Proof: If G is non-abelian, then $G/Z(G)$ is not cyclic. Therefore $G/Z(G)$ contains at least four elements, we will write $k = |G/Z(G)|$. Again we reduce the colorability of a graph with k colors to solving systems over $G/Z(G)$. For every vertex v in the graph we introduce a variable x_v. Then $x_v Z(G) \in G/Z(G)$ will determine the color of v. So two vertices v, w will have the same color if and only if $x_v x_w^{-1} \in Z(G)$.

If $x_v x_w^{-1} \notin Z(G)$, then $(x_v x_w^{-1}, G) = (G, G)$ as G is commutator simple.

Otherwise if $x_v x_w^{-1} \in Z(G)$, then for all $g \in G$ we have

$$[x_v x_w^{-1}, g] = x_v x_w^{-1} g x_w x_v^{-1} g^{-1} = g x_v x_w^{-1} x_w x_v^{-1} g^{-1} = 1,$$

so $(x_v x_w^{-1}, G) = \{1\}$.

Commutator simple

There is a constant $m \in \mathbb{N}$ such that

$$(a, G) = \{[a, g_1][a, g_2] \cdots [a, g_m] \ : \ g_i \in G\}.$$

Let $1 \neq b \in (G, G)$. This b exists as G is not abelian. Than for every edge $e = (v, w)$ in the graph we introduce the equation

$$[x_v x_w^{-1}, s_1^e] \cdots [x_v x_w^{-1}, s_m^e] = b$$

over G where the s_i^e are new variables.

If this system has a solution, then $x_v x_w^{-1} \notin Z(G)$, because if $x_v x_w^{-1} \in Z(G)$, then $b \notin (x_v x_w^{-1}, G) = \{1\}$. So in this case we have legal coloring with $k \geq 4$ colors.

On the other hand, if it has a legal coloring, i.e. $x_v x_w^{-1} \notin Z(G)$, then we can find a solution of the system since in this case $(x_v x_w^{-1}, G) = (G, G)$.

So we have reduced the colorability problem of a graph to the problem of solving a system of equations over G, so $\textsc{PolSysSat}(G) \in NPC$. $\square$

Solving systems over non-abelian groups

Theorem 1 (part 2, Goldmann and Russell 1999, Thm. 2)

If G is an not abelian, then PolSysSat(G) is NP complete.

Proof: By Induction over the group order. For the smallest non-abelian group S_3 we have already shown it.

So assume that the theorem holds for all non-abelian groups of order $n-1$ or less and let G be a non-abelian group of order n. If G is commutator simple, the previous lemma has shown that PolSysSat$(G) \in NPC$.

So we assume that G is not commutator simple. Hence there exists $a \in G - Z(G)$ with $(a, G) \subsetneq (G, G)$. Then (a, G) is nontrivial, because if $[a, g] = 1$ for every $g \in G$, then $a \in Z(G)$, a contradiction.

Then $G/(a, G)$ is non-abelian as $(a, G) \subsetneq (G, G)$. As $|G/(a, G)| < n$ we have PolSysSat$(G/(a, G)) \in NPC$ by induction. Since (a, G) is a normal inducible subgroup of G by a previous Lemma we have PolSysSat$(G) \in NPC$. $\square$

Single Equation

Single equation

Theorem 2

If G is a nilpotent group, then $\textsc{PolSat}(G) \in P$ and if G is not solvable then $\textsc{PolSat}(G) \in NPC$.

Before we can look at the proof we need to understand what nilpotent and solvable groups are.

Nilpotent groups

Definition

Let $G_0 := G$ and

$$G_{i+1} := (G, G_i) = \langle \{[g,h] = ghg^{-1}h^{-1} \;:\; g \in G, h \in G_i\} \rangle$$

for $i \geq 0$. Then G is called nilpotent if $G_n = \{1\}$ for some $n \in \mathbb{N}$.

The groups G_i form the lower central series.

Abelian groups are nilpotent as $G_1 = (G, G) = \{1\}$.

Let $p \in \mathbb{P}$ be a prime. A group of order p^n is nilpotent (and called a p-group). Since $|D_4| = 8 = 2^3$, the group D_4 is nilpotent. However, it is not abelian!

Solvable groups

We have already seen

$$(G, G) = \langle \{[g, h] = ghg^{-1}h^{-1} \ : \ g, h \in G\} \rangle.$$

Definition

Let $G^{(1)} := (G, G)$. By Induction we define

$$G^{(i+1)} := (G^{(i)}, G^{(i)}) := \langle \{[g, h] \ : \ g \in G^{(i)}, h \in G^{(i)}\} \rangle$$

and call $G^{(i)}$ the derived subgroups of G.

If $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}$, then we call G solvable.

Abelian groups are solvable as $G^{(1)} = \{1\}$. Nilpotent groups are solvable.

Groups of order $p^n q^m$ for primes $p, q \in \mathbb{P}$ are solvable (Burnside). Groups of odd order are solvable (Feit-Thompson).

S_3 and S_4 are solvable but not nilpotent. S_n for $n \geq 5$ are not solvable.

Solvable groups

The derived subgroups $G^{(i)}$ form the derived series of G:

$$G \geq G^{(1)} \geq \cdots \geq G^{(n)} \geq \cdots .$$

If G is solvable, there is an $n \in \mathbb{N}$ such that $G^{(n)} = \{1\}$.

If G is not solvable there is (since G is finite) an $n \in \mathbb{N}$ such that

$$G^{(*)} := G^{(n)} = G^{(n+1)} = G^{(n+2)} = \cdots ,$$

i.e. $(G^{(*)}, G^{(*)}) = G^{(*)}$. By a previous Lemma applied inductively $G^{(*)}$ is an inducible subgroup of G.

Lemma

Let H be a normal subgroup of G. Then G is solvable if and only if H and G/H are solvable.

Nilpotent groups solvable

Lemma

A nilpotent group G is solvable.

Proof: We will show first by induction that $G^{(i)} \subseteq G_i$ for all i, i.e. derived series is under the lower central series.

Clearly $G^{(1)} = (G, G) = G_1$ by their definitions.

Now let $G^{(i)} \subseteq G_i$. Then

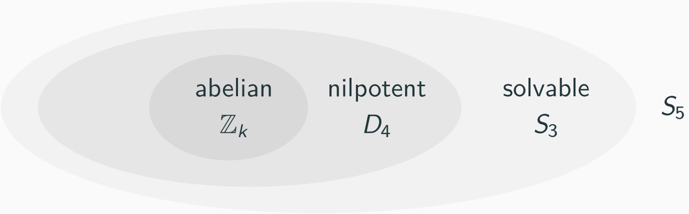
$$G^{(i+1)} = (G^{(i)}, G^{(i)}) \subseteq (G, G^{(i)}) \subseteq (G, G_i) = G_{i+1}.$$

Now if G is nilpotent, then $G_n = \{1\}$ for some $n \in \mathbb{N}$. Then $G^{(n)} \subseteq G_n = \{1\}$, so G is solvable. $\square$

Single equation

Theorem 2

If G is a nilpotent group, then $\textsc{PolSat}(G) \in P$ and if G is not solvable then $\textsc{PolSat}(G) \in NPC$.



Single equation *NPC* for non-solvable groups

Theorem 2, part 1

If G is not solvable then $\textsc{PolSat}(G) \in NPC$.

Again need some preparation.

Lemma (Goldmann and Russell 1999, Lemma 8)

Let H be an inducible subgroup of G.

1. If $\textsc{PolSat}(H) \in NPC$, then $\textsc{PolSat}(G) \in NPC$.
2. If H is normal in G and $\textsc{PolSat}(G/H) \in NPC$, then $\textsc{PolSat}(G) \in NPC$.

Proof : In the same way as for $\textsc{PolSysSat}$. $\square$

Commutator simple non-solvable groups

Reminder: G is commutator simple if $\forall a \notin Z(G)$: $(G,G) = (a,G)$.

Lemma (Goldmann and Russell 1999, Lemma 9)

Let G be a non-solvable group with $G = (G,G)$ and G is commutator simple. Then $\textsc{PolSat}(G) \in NPC$.

Proof : Similar to previous Lemma. $\square$

Single equation

Theorem 2 (part 1, Goldmann and Russell 1999, Thm. 10)

If G is not solvable then $\textsc{PolSat}(G) \in NPC$.

Proof: Again by induction on group order.

Basis: Let G be the smallest non-solvable group (which is A_5 with order 60). Then G must be simple, because otherwise there is a nontrivial normal subgroup H and then G/H as well as H would be solvable as G is chosen with minimal order. Since (G, G) is a normal subgroup and by assumption $(G, G) \neq \{1\}$ we must have $(G, G) = G$. As (a, G) are normal subgroups in G again we have $(a, G) = G$ for $a \notin Z(G)$:

Suppose $(a, G) = \{1\}$, then $[a, g] = aga^{-1}g^{-1} = 1$ for all $g \in G$, so $a \in Z(G)$, a contradiction.

Therefore by the previous Lemma $\textsc{PolSat}(G) \in NPC$ for $G = A_5$.

Single equation

Induction step: Consider arbitrary non-solvable group G. We look at $G^{(*)}$:

If $G^{(*)} \subsetneq G$, then by induction $\textsc{PolSat}(G^{(*)}) \in NPC$. Furthermore $G^{(*)}$ is an inducible subgroup of G, so $\textsc{PolSat}(G) \in NPC$.

If $G^{(*)} = G = (G, G)$ and G is commutator simple, the previous lemma showed $\textsc{PolSat}(G) \in NPC$. So we assume that G is not commutator simple, i.e. there is an $a \in G - Z(G)$ such that $(a, G) \subsetneq (G, G)$. As $a \notin Z(G)$ we have $(a, G) \neq \{1\}$, so $|G/(a, G)| < |G|$. As G is non-solvable either (a, G) or $G/(a, G)$ have to be non-solvable. By the induction hypothesis $\textsc{PolSat}((a, G)) \in NPC$ or $\textsc{PolSat}(G/(a, G)) \in NPC$. Again by a previous lemma $\textsc{PolSat}(G) \in NPC$. $\square$

Theorem 2 (part 2, Goldmann and Russell 1999, Cor. 12)

If G is nilpotent then $\textsc{PolSat}(G) \in P$.

Proof: See Goldman and Russell. $\square$

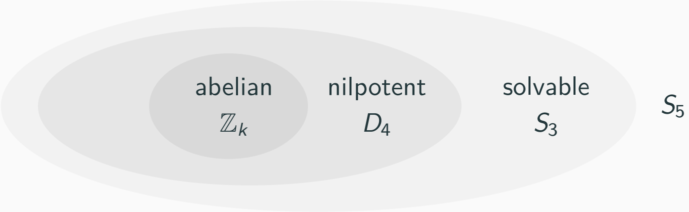
What happened in the last 20 years?

Nilpotent solvable groups

What about the nilpotent non-solvable groups? Goldmann and Russell did not know.

Still, we do not know. Ongoing research.

However, we already have examples of nilpotent non-solvable groups G for which $\textsc{PolSat}(G) \in P$, e.g. groups of order pq for primes p, q (Horváth and Szabó 2006). This shows that $\textsc{PolSat}(S_3) \in P$.



Generalising the results

Goldmann and Russell ”only” considered groups. What about other or more general algebras?

Example Rings

Let R be a finite ring.

- If R is nilpotent (i.e. $R^n = \{0\}$ for some $n \in \mathbb{N}$), then $\textsc{PolSat}(R) \in P$, otherwise $\textsc{PolSat}(R) \in NPC$ (Horváth 2011).
- If R is essentially an abelian group (i.e. $xy = 0$ for all $x, y \in R$), then $\textsc{PolSysSat}(R) \in P$ and $\textsc{PolSysSat}(R) \in NPC$ otherwise (Larose and Zádori 2006).

More general results can be found e.g. in Larose and Zádori 2006, Gorazd and Krzaczkowski 2011, Idziak and Krzaczkowski 2018, Aichinger 2019.

Aichinger, Erhard (2019). “Solving systems of equations in supernilpotent algebras”. In: *arXiv:1901.07862*.

Goldmann, Mikael and Alexander Russell (1999). “The Complexity of Solving Equations over Finite Groups.”. In: *IEEE Conference on Computational Complexity*. IEEE Computer Society, pp. 80–86.

Gorazd, Tomasz A. and Jacek Krzaczkowski (2011). “The complexity of problems connected with two-element algebras”. In: *Reports on Mathematical Logic* 46, pp. 91–108.

Horváth, Gábor (2011). “The complexity of the equivalence and equation solvability problems over nilpotent rings and groups”. In: *Algebra universalis* 66.4, pp. 391–403.

Horváth, Gábor and Csaba A. Szabó (2006). “The Complexity of Checking Identities over Finite Groups”. In: *IJAC* 16.5, pp. 931–940.

Hungerford, Thomas (2003). *Algebra*. Springer.

References ii

Idziak, Pawel M. and Jacek Krzaczkowski (2018). "Satisfiability in multi-valued circuits". In: *LICS*. Ed. by Anuj Dawar and Erich Grädel. ACM, pp. 550–558.

Karp, Richard. M. (1972). "Reducibility among Combinatorial Problems". In: *Complexity of Computer Computations*. Ed. by R.E. Miller and J.W. Thatcher. New York: Plenum Press.

Larose, Benoit and László Zádori (2006). "Taylor Terms, Constraint Satisfaction and the Complexity of Polynomial Equations over Finite Algebras". In: *IJAC* 16.3, pp. 563–582.