Solving equations in groups extended by their commutator

Michael Kompatscher

AAA97 Wien - 03/03/2019

Charles University Prague

Solving equations in groups

The equation solvability problem for groups

$(G, \cdot)$... finite group

Equation solvability $\mathrm{Eq}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) = 0$ have a solution in G?

The equation solvability problem for groups

$(G, \cdot)$... finite group

Equation solvability $\mathrm{Eq}(G, \cdot)$

INPUT: A polynomial $f(x_1, \dots, x_n)$ over G

QUESTION: Does $f(x_1, \dots, x_n) = 0$ have a solution in G?

(Polynomial e.g.: $f(x_1, x_2, x_3) = x_2 \cdot x_1 \cdot c_1 \cdot x_3^{-1} \cdot x_2 \cdot c_2$)

The equation solvability problem for groups

$(G, \cdot)$... finite group

Equation solvability $\mathrm{Eq}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) = 0$ have a solution in G?

(Polynomial e.g.: $f(x_1, x_2, x_3) = x_2 \cdot x_1 \cdot c_1 \cdot x_3^{-1} \cdot x_2 \cdot c_2$)

Identity checking $\mathrm{Id}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) \approx 0$ in G?

The equation solvability problem for groups

$(G, \cdot)$... finite group

Equation solvability $\mathrm{Eq}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) = 0$ have a solution in G?

(Polynomial e.g.: $f(x_1, x_2, x_3) = x_2 \cdot x_1 \cdot c_1 \cdot x_3^{-1} \cdot x_2 \cdot c_2$)

Identity checking $\mathrm{Id}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) \approx 0$ in G?

By finiteness: $\mathrm{Eq}(G, \cdot) \in \mathrm{NP}$, $\mathrm{Id}(G, \cdot) \in \text{co-NP}$

The equation solvability problem for groups

$(G, \cdot)$... finite group

Equation solvability $\mathrm{Eq}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) = 0$ have a solution in G?

(Polynomial e.g.: $f(x_1, x_2, x_3) = x_2 \cdot x_1 \cdot c_1 \cdot x_3^{-1} \cdot x_2 \cdot c_2$)

Identity checking $\mathrm{Id}(G, \cdot)$

INPUT: A polynomial $f(x_1, \ldots, x_n)$ over G

QUESTION: Does $f(x_1, \ldots, x_n) \approx 0$ in G?

By finiteness: $\mathrm{Eq}(G, \cdot) \in \mathrm{NP}$, $\mathrm{Id}(G, \cdot) \in \text{co-NP}$

Question

What are criteria for tractability (P) or hardness (NP-c / coNP-c)?

In groups

Example

$\mathsf{Eq}(\mathbb{Z}_p, +) \in P, \mathsf{Id}(\mathbb{Z}_p, +) \in P.$

In groups

Example

$\mathrm{Eq}(\mathbb{Z}_p, +) \in P, \mathrm{Id}(\mathbb{Z}_p, +) \in P$.

An equation $c_1 \cdot x_1 + c_2 \cdot x_2 + \cdots + c_n \cdot x_n + c = 0$ has a solution, if there is a solution where $\leq d(\mathbb{Z}_p) = 1$ variables are $\neq 0$.

In groups

Example

$\mathrm{Eq}(\mathbb{Z}_p, +) \in P, \mathrm{Id}(\mathbb{Z}_p, +) \in P$.
An equation $c_1 \cdot x_1 + c_2 \cdot x_2 + \cdots + c_n \cdot x_n + c = 0$ has a solution, if there is a solution where $\leq d(\mathbb{Z}_p) = 1$ variables are $\neq 0$.

This $d(G)$ generalizes for nilpotent groups G (Goldmann & Russell '02; Földvári '17: $d(G) \leq \frac{1}{2}|G|^2 \log(|G|)$)

In groups

Example

$\mathrm{Eq}(\mathbb{Z}_p,+) \in P, \mathrm{Id}(\mathbb{Z}_p,+) \in P.$

An equation $c_1 \cdot x_1 + c_2 \cdot x_2 + \cdots + c_n \cdot x_n + c = 0$ has a solution, if there is a solution where $\leq d(\mathbb{Z}_p) = 1$ variables are $\neq 0$.

This $d(G)$ generalizes for nilpotent groups G (Goldmann & Russell '02; Földvári '17: $d(G) \leq \frac{1}{2}|G|^2 \log(|G|)$)

Group G	$\mathrm{Eq}(G,\cdot)$	$\mathrm{Id}(G,\cdot)$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

In groups

Example

$\mathrm{Eq}(\mathbb{Z}_p, +) \in P, \mathrm{Id}(\mathbb{Z}_p, +) \in P$.

An equation $c_1 \cdot x_1 + c_2 \cdot x_2 + \cdots + c_n \cdot x_n + c = 0$ has a solution, if there is a solution where $\leq d(\mathbb{Z}_p) = 1$ variables are $\neq 0$.

This $d(G)$ generalizes for nilpotent groups G (Goldmann & Russell '02; Földvári '17: $d(G) \leq \frac{1}{2}|G|^2 \log(|G|)$)

Group G	$\mathrm{Eq}(G, \cdot)$	$\mathrm{Id}(G, \cdot)$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

Conjectures

The equation solvability problem in solvable groups is decidable in

- polynomial time
  (✓meta-abelian (Horváth), ✓semipattern groups (Földvári))

In groups

Example

$\mathrm{Eq}(\mathbb{Z}_p, +) \in P, \mathrm{Id}(\mathbb{Z}_p, +) \in P$.

An equation $c_1 \cdot x_1 + c_2 \cdot x_2 + \cdots + c_n \cdot x_n + c = 0$ has a solution, if there is a solution where $\leq d(\mathbb{Z}_p) = 1$ variables are $\neq 0$.

This $d(G)$ generalizes for nilpotent groups G (Goldmann & Russell '02; Földvári '17: $d(G) \leq \frac{1}{2}|G|^2 \log(|G|)$)

Group G	$\mathrm{Eq}(G, \cdot)$	$\mathrm{Id}(G, \cdot)$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

Conjectures

The equation solvability problem in solvable groups is decidable in

- polynomial time
  (✓meta-abelian (Horváth), ✓semipattern groups (Földvári))
- quasipolynomial time (open conjecture about CC^0-circuits)

Adding the commutator

The complexity is sensitive to the signature!

Example A_4. (Horváth, Szabó '12)

$\mathrm{Eq}(A_4, \cdot) \in \mathrm{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:

$\mathrm{Eq}(A_4, \cdot, [\cdot, \cdot]) \in$ NP-c, $\mathrm{Id}(A_4, \cdot, [\cdot, \cdot]) \in$ coNP-c

The complexity is sensitive to the signature!

Example A_4. (Horváth, Szabó '12)

$\mathrm{Eq}(A_4, \cdot) \in \mathrm{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:
$\mathrm{Eq}(A_4, \cdot, [\cdot, \cdot]) \in$ NP-c, $\mathrm{Id}(A_4, \cdot, [\cdot, \cdot]) \in$ coNP-c

Proof idea: Encode 3-COLOR

$V = [A_4, A_4] = [V, A_4]$;
$A_4/V = \mathbb{Z}_3$

The complexity is sensitive to the signature!

Example A_4. (Horváth, Szabó '12)

$\text{Eq}(A_4, \cdot) \in \text{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:
$\text{Eq}(A_4, \cdot, [\cdot, \cdot]) \in \text{NP-c}$, $\text{Id}(A_4, \cdot, [\cdot, \cdot]) \in \text{coNP-c}$

Proof idea: Encode 3-COLOR

$V = [A_4, A_4] = [V, A_4]$;
$A_4/V = \mathbb{Z}_3$

$y \mapsto [y, b]$ is 0 if $b \in V$ and a bijective on V if $b \notin V$.

The complexity is sensitive to the signature!

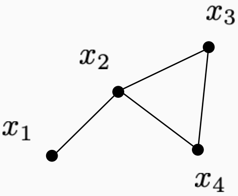
Example A_4. (Horváth, Szabó '12)

$\mathrm{Eq}(A_4, \cdot) \in \mathrm{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:
$\mathrm{Eq}(A_4, \cdot, [\cdot, \cdot]) \in$ NP-c, $\mathrm{Id}(A_4, \cdot, [\cdot, \cdot]) \in$ coNP-c

Proof idea: Encode 3-COLOR

$V = [A_4, A_4] = [V, A_4]$;
$A_4/V = \mathbb{Z}_3$

$y \mapsto [y, b]$ is 0 if $b \in V$ and a bijective on V if $b \notin V$.



$$y \mapsto [[[[y, x_1^{-1}x_2], x_2^{-1}x_3], x_3^{-1}x_4], x_4^{-1}x_2]$$

The complexity is sensitive to the signature!

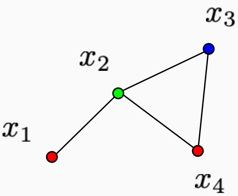
Example A_4. (Horváth, Szabó ’12)

$\mathrm{Eq}(A_4, \cdot) \in \mathrm{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:
$\mathrm{Eq}(A_4, \cdot, [\cdot,\cdot]) \in$ NP-c, $\mathrm{Id}(A_4, \cdot, [\cdot,\cdot]) \in$ coNP-c

Proof idea: Encode 3-COLOR

$V = [A_4, A_4] = [V, A_4]$;
$A_4/V = \mathbb{Z}_3$

$y \mapsto [y, b]$ is 0 if $b \in V$ and a bijective on V if $b \notin V$.



$$y \mapsto [[[[y, x_1^{-1}x_2], x_2^{-1}x_3], x_3^{-1}x_4], x_4^{-1}x_2]$$

The complexity is sensitive to the signature!

Example A_4. (Horváth, Szabó '12)

$\mathrm{Eq}(A_4, \cdot) \in \mathrm{P}$ but adding $[x, y] = x^{-1}y^{-1}xy$:

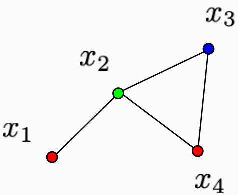
$\mathrm{Eq}(A_4, \cdot, [\cdot, \cdot]) \in$ NP-c, $\mathrm{Id}(A_4, \cdot, [\cdot, \cdot]) \in$ coNP-c

Proof idea: Encode 3-COLOR

$V = [A_4, A_4] = [V, A_4]$;

$A_4/V = \mathbb{Z}_3$

$y \mapsto [y, b]$ is 0 if $b \in V$ and a bijective on V if $b \notin V$.



$$y \mapsto [[[[y, x_1^{-1}x_2], x_2^{-1}x_3], x_3^{-1}x_4], x_4^{-1}x_2]$$

□

Similar: p-COLOR in $G = \mathbb{Z}_p \ltimes (\mathbb{Z}_q^n)$.

Question

Question

What is the complexity of $\mathsf{Eq}(G, \cdot, [\cdot, \cdot])$ and $\mathsf{Id}(G, \cdot, [\cdot, \cdot])$?

Question

Question

What is the complexity of $\mathrm{Eq}(G, \cdot, [\cdot, \cdot])$ and $\mathrm{Id}(G, \cdot, [\cdot, \cdot])$?

Group G	$\mathrm{Eq}(G, [\cdot, \cdot])$	$\mathrm{Id}(G, [\cdot, \cdot])$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

Question

What is the complexity of $\mathrm{Eq}(G, \cdot, [\cdot, \cdot])$ and $\mathrm{Id}(G, \cdot, [\cdot, \cdot])$?

Group G	$\mathrm{Eq}(G, [\cdot, \cdot])$	$\mathrm{Id}(G, [\cdot, \cdot])$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

Theorem (Horváth, Szabó '11)

Every non-nilpotent G has an extension by some term $t(x_1, \ldots, x_n)$ such that $\mathrm{Eq}(G, \cdot, t(x_1, \ldots, x_n)) \in$NP-c and $\mathrm{Id}(G, \cdot, t(x_1, \ldots, x_n)) \in$coNP-c.

Question

What is the complexity of $\mathrm{Eq}(G, \cdot, [\cdot, \cdot])$ and $\mathrm{Id}(G, \cdot, [\cdot, \cdot])$?

Group G	$\mathrm{Eq}(G, [\cdot, \cdot])$	$\mathrm{Id}(G, [\cdot, \cdot])$
Nilpotent	P	P
Solvable, non-nilpotent	?	?
Non-solvable	NP-c	coNP-c

Theorem (Horváth, Szabó '11)

Every non-nilpotent G has an extension by some term $t(x_1, \ldots, x_n)$ such that $\mathrm{Eq}(G, \cdot, t(x_1, \ldots, x_n)) \in$NP-c and $\mathrm{Id}(G, \cdot, t(x_1, \ldots, x_n)) \in$coNP-c.

$\rightarrow$ can one always choose t to be the commutator?

Reducing to 'A_4-like' groups

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \cdots \cdot [x_{n-1}, x_n]$.

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \cdots \cdot [x_{n-1}, x_n]$.

For $V \leq G$ verbal:

$\mathrm{Eq}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$, $\mathrm{Id}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \cdots \cdot [x_{n-1}, x_n]$.

For $V \leq G$ verbal:

$\mathrm{Eq}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot]), \quad \mathrm{Id}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

$\rightarrow$ reduce to smallest non-nilpotent element in derived series.

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \dots \cdot [x_{n-1}, x_n]$.

For $V \leq G$ verbal:

$\mathrm{Eq}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$, $\mathrm{Id}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

$\rightarrow$ reduce to smallest non-nilpotent element in derived series.

$\rightarrow$ wlog G non-nilpotent, G' is nilpotent

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \cdots \cdot [x_{n-1}, x_n]$.

For $V \leq G$ verbal:

$\mathrm{Eq}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$, $\mathrm{Id}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

$\rightarrow$ reduce to smallest non-nilpotent element in derived series.

$\rightarrow$ wlog G non-nilpotent, G' is nilpotent

Lemma (Horváth, Szabó '11)

For $V \leq G$ verbal, normal

- $\mathrm{Eq}(G/V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$
- $\mathrm{Id}(G/C_G(V), \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

Verbal subgroups

A subgroup $V \leq G$ is verbal if $V = t(G, G, \ldots, G)$ for some term t. E.g. G' is verbal: $[x_1, x_2] \cdot \cdots \cdot [x_{n-1}, x_n]$.

For $V \leq G$ verbal:

$\mathrm{Eq}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$, $\mathrm{Id}(V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

$\rightarrow$ reduce to smallest non-nilpotent element in derived series.

$\rightarrow$ wlog G non-nilpotent, G' is nilpotent

Lemma (Horváth, Szabó '11)

For $V \leq G$ verbal, normal

- $\mathrm{Eq}(G/V, \cdot, [\cdot, \cdot]) \leq_p \mathrm{Eq}(G, \cdot, [\cdot, \cdot])$
- $\mathrm{Id}(G/C_G(V), \cdot, [\cdot, \cdot]) \leq_p \mathrm{Id}(G, \cdot, [\cdot, \cdot])$

$\rightsquigarrow$ obtain a reduction of some non-nilpotent $\mathbb{Z}_p \ltimes (\mathbb{Z}_q^n)$ to G.

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) > 2$ then
$\mathrm{Eq}(G, \cdot, [\cdot, \cdot]) \in$ NP-c and $\mathrm{Id}(G, \cdot, [\cdot, \cdot]) \in$ coNP-c.

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) > 2$ then
$\mathrm{Eq}(G, \cdot, [\cdot, \cdot]) \in$ NP-c and $\mathrm{Id}(G, \cdot, [\cdot, \cdot]) \in$ coNP-c.

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) > 2$ then
$\mathrm{Eq}(G, \cdot, [\cdot, \cdot]) \in$ NP-c and $\mathrm{Id}(G, \cdot, [\cdot, \cdot]) \in$ coNP-c.

Problem
If $\exp(G/F(G)) = 2$, there is a reduction from a dihedral $\mathbb{Z}_2 \ltimes \mathbb{Z}_p$ to G.

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) > 2$ then
$\mathrm{Eq}(G, \cdot, [\cdot,\cdot]) \in$ NP-c and $\mathrm{Id}(G, \cdot, [\cdot,\cdot]) \in$ coNP-c.

Problem
If $\exp(G/F(G)) = 2$, there is a reduction from a dihedral $\mathbb{Z}_2 \ltimes \mathbb{Z}_p$ to G.
By our trick we can only encode 2-COLOR in $\mathrm{Eq}(\mathbb{Z}_2 \ltimes \mathbb{Z}_p, \cdot, [\cdot,\cdot])$.

But for $w(y, x_1, x_2, x_3) = y^8[[[y, x_1], x_2], x_3]$:

Result

G ... finite group
$F(G)$ ... Fitting subgroup

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) > 2$ then
$\mathrm{Eq}(G, \cdot, [\cdot, \cdot]) \in$ NP-c and $\mathrm{Id}(G, \cdot, [\cdot, \cdot]) \in$ coNP-c.

Problem
If $\exp(G/F(G)) = 2$, there is a reduction from a dihedral $\mathbb{Z}_2 \ltimes \mathbb{Z}_p$ to G.
By our trick we can only encode 2-COLOR in $\mathrm{Eq}(\mathbb{Z}_2 \ltimes \mathbb{Z}_p, \cdot, [\cdot, \cdot])$.

But for $w(y, x_1, x_2, x_3) = y^8[[[y, x_1], x_2], x_3]$:

Theorem (MK '18)
If $G' \leq F(G) < G$ and $\exp(G/F(G)) = 2$ then
$\mathrm{Eq}(G, \cdot, w)$ is NP-c and $\mathrm{Id}(G, \cdot, w)$ is coNP-c.

Question

Question

What is the complexity of $\mathrm{Eq}(\mathbb{Z}_2 \ltimes \mathbb{Z}_p, \cdot, [\cdot, \cdot])$?

Question

Question

What is the complexity of $\mathrm{Eq}(\mathbb{Z}_2 \ltimes \mathbb{Z}_p, \cdot, [\cdot, \cdot])$?

Equivalent to the following problem:

Question

Question

What is the complexity of $\text{Eq}(\mathbb{Z}_2 \ltimes \mathbb{Z}_p, \cdot, [\cdot, \cdot])$?

Equivalent to the following problem:

Problem

INPUT: Affine subspaces $A_1, \ldots, A_k \leq \mathbb{Z}_2^n$
QUESTION: Is there an $\bar{x} \in \mathbb{Z}_2^n$ that is covered $m \cdot p$ many spaces?