Hardness of equations over finite solvable groups under the exponential time hypothesis

Armin Weiß

Universität Stuttgart, FMI

ICALP 2020

Equations in groups

Equations in $(\mathbb{Z}, +)$:

$$X + X = 1$$

Equations in groups

Armin Weiß

Equations in $(\mathbb{Z}, +)$:

$$X + X = 1$$
$$X + Y = Y + X$$

Equations in groups

Equations in $(\mathbb{Z}, +)$:

$$X + X = 1$$
$$X + Y = Y + X$$
$$X + X + X = 1 + Y + Y$$

Equations in groups

Equations in $(\mathbb{Z}, +)$:

$$X + X = 1$$
$$X + Y = Y + X$$
$$X + X + X = 1 + Y + Y$$

Equations over an arbitrary group G:

$$aXY^{-1} = bXaY$$

Equations in groups

Armin Weiß

Equations in $(\mathbb{Z}, +)$:

$$X + X = 1$$
$$X + Y = Y + X$$
$$X + X + X = 1 + Y + Y$$

Equations over an arbitrary group G:

$$aXY^{-1} = bXaY$$

W. l. o. g. of the form

$$\alpha = 1$$

for an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$ (with variables $\mathcal{X}$).

Equations in groups

The $\mathrm{EQN\text{-}SAT}(G)$ problem:

Constant: The group G

Input: an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$

Question: $\exists$ an assignment $\sigma : \mathcal{X} \to G$ s.t. $\sigma(\alpha) = 1$?

Equations in groups

The $\mathrm{EQN\text{-}SAT}(G)$ problem:

Constant: The group G
Input: an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$
Question: $\exists$ an assignment $\sigma : \mathcal{X} \to G$ s.t. $\sigma(\alpha) = 1$?

The $\mathrm{EQN\text{-}ID}(G)$ problem:

Constant: The group G
Input: an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$
Question: is $\sigma(\alpha) = 1$ $\forall$ assignments $\sigma : \mathcal{X} \to G$?

Equations in groups

The $\mathrm{EQN\text{-}SAT}(G)$ problem:

Constant: The group G
Input: an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$
Question: $\exists$ an assignment $\sigma : \mathcal{X} \to G$ s.t. $\sigma(\alpha) = 1$?

The $\mathrm{EQN\text{-}ID}(G)$ problem:

Constant: The group G
Input: an expression $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$
Question: is $\sigma(\alpha) = 1$ $\forall$ assignments $\sigma : \mathcal{X} \to G$?

In many infinite groups these problems are undecidable!

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Finer classification with respect to complexity?

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Finer classification with respect to complexity?

Observation

$\mathrm{EQN\text{-}ID}(G) \leq_T^{\mathsf{P}} \mathrm{EQN\text{-}SAT}(G)$

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Finer classification with respect to complexity?

Observation

$\mathrm{EQN\text{-}ID}(G) \leq_T^{\mathsf{P}} \mathrm{EQN\text{-}SAT}(G)$

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Finer classification with respect to complexity?

Observation

$\mathrm{EQN\text{-}ID}(G) \leq_T^{\mathsf{P}} \mathrm{EQN\text{-}SAT}(G)$

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each $g \in G \setminus 1$ check whether αg^{-1} is satisfiable,

Complexity of equations in groups

In finite groups $\mathrm{EQN\text{-}SAT}(G)$ is in NP:

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each variable $X \in \mathcal{X}$ that appears in α, guess $\sigma(X) \in G$,
- evaluate $\sigma(\alpha)$.

and $\mathrm{EQN\text{-}ID}(G)$ is in coNP.

Finer classification with respect to complexity?

Observation

$\mathrm{EQN\text{-}ID}(G) \leq_T^{\mathsf{P}} \mathrm{EQN\text{-}SAT}(G)$

- Input: $\alpha \in (G \cup \mathcal{X} \cup \mathcal{X}^{-1})^*$,
- for each $g \in G \setminus 1$ check whether αg^{-1} is satisfiable,
- if yes, then α is not an identity.

Overview: complexity of equations in finite groups

Armin Weiß

Theorem (Goldmann, Russell, 2002)

- *If G is nilpotent, then* $\mathrm{EQN\text{-}SAT}(G) \in \mathrm{P}$.

Overview: complexity of equations in finite groups

Theorem (Goldmann, Russell, 2002)

- *If G is nilpotent, then* $\mathrm{EQN\text{-}SAT}(G) \in \mathsf{P}$.

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)

Overview: complexity of equations in finite groups

Theorem (Goldmann, Russell, 2002)

- *If G is nilpotent, then* $\mathrm{EQN\text{-}SAT}(G) \in \mathsf{P}$.
- *If G is non-solvable, then* $\mathrm{EQN\text{-}SAT}(G)$ *is* NP*-complete.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
non-solvable	NP-complete	

Overview: complexity of equations in finite groups

Theorem (Horváth, Lawrence, Mérai, Szabó, 2007)

If G is non-solvable, then $\mathrm{EQN\text{-}ID}(G)$ is coNP*-complete.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
non-solvable	NP-complete	coNP-complete

Overview: complexity of equations in finite groups

Theorem (Horváth, Lawrence, Mérai, Szabó, 2007)

If G is non-solvable, then $\mathrm{EQN\text{-}ID}(G)$ *is* coNP*-complete.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
solvable, non-nilpotent	in NP	in coNP
non-solvable	NP-complete	coNP-complete

Theorem (Földvári, Horváth 2020)

- $\mathrm{EQN\text{-}SAT}(Q \rtimes A) \in \mathsf{P}$ *for Q a p-group, A abelian.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
solvable, non-nilpotent	in NP *p-group* $\rtimes$ *abelian* in P	in coNP
non-solvable	NP-complete	coNP-complete

Overview: complexity of equations in finite groups

Theorem (Földvári, Horváth 2020)

- $\mathrm{EQN\text{-}SAT}(Q \rtimes A) \in \mathsf{P}$ *for Q a p-group, A abelian.*
- $\mathrm{EQN\text{-}ID}(N \rtimes A) \in \mathsf{P}$ *for N nilpotent, A abelian.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
solvable, non-nilpotent	in NP *p-group* $\rtimes$ *abelian* in P	in coNP *nilpotent* $\rtimes$ *abelian* in P
non-solvable	NP-complete	coNP-complete

Overview: complexity of equations in finite groups

Theorem (Földvári, Horváth 2020)

- $\mathrm{EQN\text{-}SAT}(Q \rtimes A) \in \mathsf{P}$ *for* Q *a* p*-group,* A *abelian.*
- $\mathrm{EQN\text{-}ID}(N \rtimes A) \in \mathsf{P}$ *for* N *nilpotent,* A *abelian.*

	$\mathrm{EQN\text{-}SAT}(G)$	$\mathrm{EQN\text{-}ID}(G)$
nilpotent	in P (actually ACC^0)	in P (actually ACC^0)
solvable, non-nilpotent	in NP *p-group* $\rtimes$ *abelian* in P ???	in coNP *nilpotent* $\rtimes$ *abelian* in P ???
non-solvable	NP-complete	coNP-complete

The role of commutators

For showing NP-completeness: reduce $3\mathrm{SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

The role of commutators

For showing NP-completeness: reduce $\mathrm{3SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

Usually: encode false by 1 and true by $\neq 1 \in G$.

The role of commutators

For showing NP-completeness: reduce $3\mathrm{SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

Usually: encode false by 1 and true by $\neq 1 \in G$.

Consider the following problem:

- There are two nails in the wall.

The role of commutators

For showing NP-completeness: reduce $\mathrm{3SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

Usually: encode false by 1 and true by $\neq 1 \in G$.

Consider the following problem:

- There are two nails in the wall.
- You have a rope and a picture hanging on the rope.

The role of commutators

For showing NP-completeness: reduce $3\mathrm{SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

Usually: encode false by 1 and true by $\neq 1 \in G$.

Consider the following problem:

- There are two nails in the wall.
- You have a rope and a picture hanging on the rope.
- You want to wrap the rope around the nails such that, if you remove one of the nails, the picture falls down.

The role of commutators

For showing NP-completeness: reduce $\mathrm{3SAT}$ to $\mathrm{EQN\text{-}SAT}(G)$

$\rightsquigarrow$ need to encode conjunctions/disjunctions

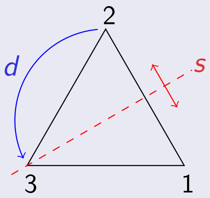
Usually: encode false by 1 and true by $\neq 1 \in G$.

Consider the following problem:

- There are two nails in the wall.
- You have a rope and a picture hanging on the rope.
- You want to wrap the rope around the nails such that, if you remove one of the nails, the picture falls down.

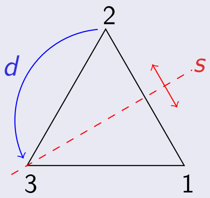
Commutators: $[x, y] = x^{-1}y^{-1}xy = \begin{cases} ?? & \text{if } x \neq 1 \text{ and } y \neq 1 \\ 1 & \text{otherwise.} \end{cases}$

Examples: S_3 and G^*



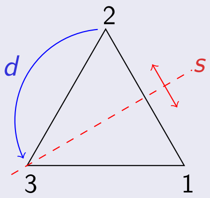
$$\begin{aligned} S_3 &= \text{group of permutations over three elements} \\ &= \text{symmetry group of a regular triangle} \\ &= \{1, \underbrace{(1\,2)}_{s}, (1\,3), (2\,3), \underbrace{(1\,2\,3)}_{d}, (1\,3\,2)\} \end{aligned}$$

Examples: S_3 and G^*

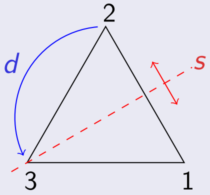


$$
\begin{aligned}
S_3 &= \text{group of permutations over three elements} \\
&= \text{symmetry group of a regular triangle} \\
&= \{1, \underbrace{(1\,2)}_{s}, (1\,3), (2\,3), \underbrace{(1\,2\,3)}_{d}, (1\,3\,2)\} \\
&= C_3 \rtimes C_2
\end{aligned}
$$

Examples: S_3 and G^*



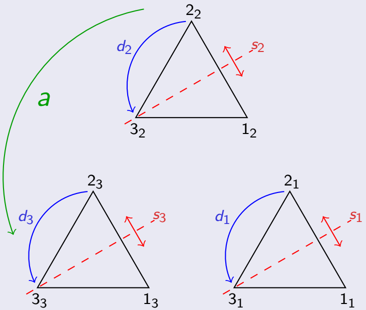
$$
\begin{aligned}
S_3 &= \text{ group of permutations over three elements} \\
&= \text{ symmetry group of a regular triangle} \\
&= \{1, \underbrace{(1\,2)}_{s}, (1\,3), (2\,3), \underbrace{(1\,2\,3)}_{d}, (1\,3\,2)\} \\
&= C_3 \rtimes C_2 \\
&= F(\{\, s, d \,\}) \big/ \{\, s^2 = d^3 = 1, ds = sd^2 \,\}
\end{aligned}
$$



$$
\begin{aligned}
S_3 &= \text{ group of permutations over three elements}\\
&= \text{ symmetry group of a regular triangle}\\
&= \{1, \underbrace{(1\,2)}_{s}, (1\,3), (2\,3), \underbrace{(1\,2\,3)}_{d}, (1\,3\,2)\}\\
&= C_3 \rtimes C_2\\
&= F(\{\, s, d \,\}) \Big/ \{\, s^2 = d^3 = 1, ds = sd^2 \,\}
\end{aligned}
$$

$$\rightsquigarrow \quad [d, s] = d^{-1}s^{-1}ds = d^{-1}d^{-1} = d$$

Examples: S_3 and G^*



$$G^* = G_{648,705} = (S_3 \times S_3 \times S_3) \rtimes C_3$$

with $a(x, y, z) = (z, x, y)a$

Commutators: $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \ldots, x_k] = \bigl[[x_1, \ldots, x_{k-1}], x_k\bigr]$

The Fitting length

Commutators: $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \ldots, x_k] = \big[[x_1, \ldots, x_{k-1}], x_k\big]$

G is nilpotent of class c if $\forall\, x_1, \ldots, x_{c+1} \in G : [x_1, \ldots, x_{c+1}] = 1$.

The Fitting length

Commutators: $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \dots, x_k] = \big[[x_1, \dots, x_{k-1}], x_k\big]$

G is nilpotent of class c if $\forall\, x_1, \dots, x_{c+1} \in G : [x_1, \dots, x_{c+1}] = 1$.

The Fitting length $\mathrm{FitLen}(G)$ (nilpotent length) of G is the smallest k such that there are normal subgroups

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$$

with N_i/N_{i-1} nilpotent for all $i = 1, \dots, k$.

The Fitting length

Commutators: $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \ldots, x_k] = \big[[x_1, \ldots, x_{k-1}], x_k\big]$

G is nilpotent of class c if $\forall\, x_1, \ldots, x_{c+1} \in G : [x_1, \ldots, x_{c+1}] = 1$.

The Fitting length $\mathrm{FitLen}(G)$ (nilpotent length) of G is the smallest k such that there are normal subgroups

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$$

with N_i/N_{i-1} nilpotent for all $i = 1, \ldots, k$.

Example

$\mathrm{FitLen}(S_3) = 2$: $1 \lhd C_3 \lhd S_3$ with $S_3/C_3 = C_2$

The Fitting length

Commutators: $[x, y] = x^{-1}y^{-1}xy$ and $[x_1, \ldots, x_k] = \big[[x_1, \ldots, x_{k-1}], x_k\big]$

G is nilpotent of class c if $\forall\, x_1, \ldots, x_{c+1} \in G : [x_1, \ldots, x_{c+1}] = 1$.

The Fitting length $\mathrm{FitLen}(G)$ (nilpotent length) of G is the smallest k such that there are normal subgroups

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$$

with N_i / N_{i-1} nilpotent for all $i = 1, \ldots, k$.

Example

$\mathrm{FitLen}(S_3) = 2$: $1 \lhd C_3 \lhd S_3$ with $S_3/C_3 = C_2$

$\mathrm{FitLen}(G^*) = 3$: $1 \lhd (C_3 \times C_3 \times C_3) \lhd (S_3 \times S_3 \times S_3) \lhd G^*$

Commutators: $[x,y] = x^{-1}y^{-1}xy$ and $[x_1,\dots,x_k] = \big[[x_1,\dots,x_{k-1}],x_k\big]$

G is nilpotent of class c if $\forall\, x_1,\dots,x_{c+1} \in G : [x_1,\dots,x_{c+1}] = 1$.

The Fitting length $\mathrm{FitLen}(G)$ (nilpotent length) of G is the smallest k such that there are normal subgroups

$$1 = N_0 \lhd N_1 \lhd \cdots \lhd N_k = G$$

with N_i/N_{i-1} nilpotent for all $i = 1,\dots,k$.

Example

$\mathrm{FitLen}(S_3) = 2$: $1 \lhd C_3 \lhd S_3$ with $S_3/C_3 = C_2$

$\mathrm{FitLen}(G^*) = 3$: $1 \lhd (C_3 \times C_3 \times C_3) \lhd (S_3 \times S_3 \times S_3) \lhd G^*$

- $(S_3 \times S_3 \times S_3)/(C_3 \times C_3 \times C_3) = (C_2 \times C_2 \times C_2)$
- $G^*/(S_3 \times S_3 \times S_3) = C_3$

Exponential time hypothesis

Exponential time hypothesis (ETH)

$\exists\delta > 0$ s.t. every algorithm for $3\mathrm{SAT}$ needs time $\Omega(2^{\delta n})$
($n =$ number of variables).

Exponential time hypothesis

Exponential time hypothesis (ETH)

$\exists\delta > 0$ s.t. every algorithm for $3\mathrm{SAT}$ needs time $\Omega(2^{\delta n})$
(n = number of variables).

Sparsification Lemma (Impagliazzo, Paturi, Zane, 2001)

ETH $\implies \exists\epsilon > 0$ s.t. every algorithm for $3\mathrm{SAT}$ needs time $\Omega(2^{\epsilon(m+n)})$
(m = number of clauses).

Exponential time hypothesis

Exponential time hypothesis (ETH)

$\exists \delta > 0$ s.t. every algorithm for $3\mathrm{SAT}$ needs time $\Omega(2^{\delta n})$ ($n =$ number of variables).

Sparsification Lemma (Impagliazzo, Paturi, Zane, 2001)

ETH $\implies$ $\exists \epsilon > 0$ s.t. every algorithm for $3\mathrm{SAT}$ needs time $\Omega(2^{\epsilon(m+n)})$ ($m =$ number of clauses).

$\rightsquigarrow$ no $2^{o(n+m)}$-time algorithm for $3\mathrm{SAT}$ under ETH.

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathrm{FitLen}(G) \geq 4$, *or*

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathrm{FitLen}(G) \geq 4$, *or*
- $\mathrm{FitLen}(G) = 3$ *and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathrm{FitLen}(G) \geq 4$, *or*
- $\mathrm{FitLen}(G) = 3$ *and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Then $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *cannot be decided in time* $2^{o(\log^2 N)}$ *under ETH.*

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathrm{FitLen}(G) \geq 4$, *or*
- $\mathrm{FitLen}(G) = 3$ *and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Then $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *cannot be decided in time* $2^{o(\log^2 N)}$ *under ETH.*

In particular, $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *are not in* P *under ETH.*

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathsf{FitLen}(G) \geq 4$, *or*
- $\mathsf{FitLen}(G) = 3$ *and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Then $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *cannot be decided in time* $2^{o(\log^2 N)}$ *under ETH.*

In particular, $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *are not in* P *under ETH.*

What about other groups of Fitting-length three?

Main result

Theorem

Let G be finite solvable group and assume that either

- $\mathrm{FitLen}(G) \geq 4$, *or*
- $\mathrm{FitLen}(G) = 3$ *and there is no Fitting-length-two normal subgroup whose index is a power of two.*

Then $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *cannot be decided in time* $2^{o(\log^2 N)}$ *under ETH.*

In particular, $\mathrm{EQN\text{-}SAT}(G)$ *and* $\mathrm{EQN\text{-}ID}(G)$ *are not in* P *under ETH.*

What about other groups of Fitting-length three?

Theorem (Idziak, Kawałek, Krzaczkowski, LICS 2020)

$\mathrm{EQN\text{-}SAT}(S_4)$ *and* $\mathrm{EQN\text{-}ID}(S_4)$ *are not in* P *under ETH.*

(S_4 = symmetric group on 4 elements)

C-Coloring

A C-coloring for $C \in \mathbb{N}$ of a graph $\Gamma = (V, E)$ is a map $\chi : V \to [1 \mathinner{..} C]$.
A coloring χ valid if $\chi(u) \neq \chi(v)$ whenever $\{ u, v \} \in E$.

C-Coloring

A C-coloring for $C \in \mathbb{N}$ of a graph $\Gamma = (V, E)$ is a map $\chi : V \to [1 \,..\, C]$.
A coloring χ valid if $\chi(u) \neq \chi(v)$ whenever $\{ u, v \} \in E$.

The C-Coloring problem:

Input: given an undirected graph $\Gamma = (V, E)$
Question: $\exists$ a valid C-coloring of Γ?

C-Coloring

A C-coloring for $C \in \mathbb{N}$ of a graph $\Gamma = (V, E)$ is a map $\chi : V \to [1 .. C]$.
A coloring χ valid if $\chi(u) \neq \chi(v)$ whenever $\{ u, v \} \in E$.

The C-Coloring problem:

Input: given an undirected graph $\Gamma = (V, E)$
Question: $\exists$ a valid C-coloring of Γ?

- NP-complete for $C \geq 3$
- 3-Coloring cannot be solved in time $2^{o(|V|+|E|)}$ unless ETH fails (see e. g. Cygan, Fomin, Kowalik, Lokshtanov, Marx, Pilipczuk, Pilipczuk, Saurabh, Thm. 14.6).
- $\rightsquigarrow$ for every $C \geq 3$, C-Coloring cannot be solved in time $2^{o(|V|+|E|)}$ unless ETH fails.

Reduce 2-Coloring to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

Reduce 2-Coloring to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.

Reduce 2-COLORING to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.

Reduce 2-Coloring to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \left[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\right]$ (recall $d = (1\,2\,3)$).

Reduce 2-Coloring to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \left[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\right]$ (recall $d = (1\,2\,3)$).

Claim

$\beta = d$ is satisfiable $\iff$ Γ is 2-colorable.

Reduce 2-COLORING to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \left[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\right]$ (recall $d = (1\,2\,3)$).

Claim

$\beta = d$ is satisfiable $\iff$ Γ is 2-colorable.

Proof.

Recall: $C_3 \lhd S_3$ and $S_3/C_3 = C_2$. Let $\sigma : \{X_1, \ldots, X_n\} \to G$.

$\square$

Reduce 2-COLORING to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \left[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\right]$ (recall $d = (1\,2\,3)$).

Claim

$\beta = d$ is satisfiable $\iff$ Γ is 2-colorable.

Proof.

Recall: $C_3 \lhd S_3$ and $S_3/C_3 = C_2$. Let $\sigma : \{X_1, \ldots, X_n\} \to G$.

Define a coloring $\chi_\sigma : V \to \{1, 2\}$ by $\chi_\sigma(i) = 1 \iff \sigma(X_i) \in C_3$.

$\square$

Reduce 2-Coloring to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = [\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m]$ (recall $d = (1\,2\,3)$).

Claim

$\beta = d$ is satisfiable $\iff$ Γ is 2-colorable.

Proof.

Recall: $C_3 \triangleleft S_3$ and $S_3/C_3 = C_2$. Let $\sigma : \{X_1, \ldots, X_n\} \to G$.

Define a coloring $\chi_\sigma : V \to \{1, 2\}$ by $\chi_\sigma(i) = 1 \iff \sigma(X_i) \in C_3$.

$$\sigma([d, \alpha_1]) = \begin{cases} 1 & \text{if } \sigma(\alpha_1) \in C_3 \\ d & \text{if } \sigma(\alpha_1) \notin C_3 \end{cases}$$

□

Reduce 2-COLORING to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \left[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\right]$ (recall $d = (1\,2\,3)$).

Claim

$\beta = d$ is satisfiable $\iff$ Γ is 2-colorable.

Proof.

Recall: $C_3 \lhd S_3$ and $S_3/C_3 = C_2$. Let $\sigma : \{X_1, \ldots, X_n\} \to G$.

Define a coloring $\chi_\sigma : V \to \{1, 2\}$ by $\chi_\sigma(i) = 1 \iff \sigma(X_i) \in C_3$.

$$\sigma([d, \alpha_1]) = \begin{cases} 1 & \text{if } \sigma(\alpha_1) \in C_3 \\ d & \text{if } \sigma(\alpha_1) \notin C_3 \iff \chi_\sigma(i_1) \neq \chi_\sigma(j_1) \end{cases}$$

$\square$

Reduce 2-COLORING to EQN-SAT(S_3)

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$
$E = \{e_1, \ldots, e_m\}$ where $e_k = \{i_k, j_k\}$

- For every vertex i introduce a variable X_i.
- For every edge $e_k = \{i_k, j_k\}$ set $\alpha_k = X_{i_k} X_{j_k}^{-1}$.
- Set $\beta = [d, \alpha_1, \ldots, \alpha_m] = \big[\cdots[[d, \alpha_1], \alpha_2], \ldots, \alpha_m\big]$ (recall $d = (1\,2\,3)$).

Length: $|\beta| \approx 2^m$.

$$[d, \alpha_1] = d^{-1}{\alpha_1}^{-1} d\alpha_1$$
$$[d, \alpha_1, \alpha_2] = {\alpha_1}^{-1} d^{-1}\alpha_1 d\alpha_2^{-1} d^{-1}{\alpha_1}^{-1} d\alpha_1\alpha_2$$
$$[d, \alpha_1, \alpha_2, \alpha_3] = \alpha_2^{-1}{\alpha_1}^{-1} d^{-1}\alpha_1 d\alpha_2 d^{-1}{\alpha_1}^{-1} d\alpha_1\,{\alpha_3}^{-1}\,{\alpha_1}^{-1} d^{-1}\alpha_1 d\alpha_2^{-1} d^{-1}{\alpha_1}^{-1} d\alpha_1\alpha_2\,\alpha_3$$

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}] Y_k$ for a new variable Y_k.

Reduce 3-COLORING to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}] Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Reduce 3-COLORING to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Claim

$\gamma = (d, 1, 1)$ is satisfiable $\iff$ Γ is 3-colorable.

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Key Observation

$|\beta_k| \approx 2^\mu \rightsquigarrow |\gamma| \approx 2^\mu \cdot 2^\mu \approx 2^{2\sqrt{m}}$

Reduce 3-COLORING to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Key Observation

$|\beta_k| \approx 2^\mu \rightsquigarrow |\gamma| \approx 2^\mu \cdot 2^\mu \approx 2^{2\sqrt{m}}$

Reduce 3-Coloring to $\mathrm{EQN\text{-}SAT}(G^*)$

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Key Observation

$|\beta_k| \approx 2^\mu \rightsquigarrow |\gamma| \approx 2^\mu \cdot 2^\mu \approx 2^{2\sqrt{m}}$

Assume $\mathrm{EQN\text{-}SAT}(G^*)$ decidable in time $2^{o(\log^2 N)}$ (N = equation length).

Reduce 3-Coloring to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s,1,1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d,1,1), \beta_1, \ldots, \beta_\mu]$.

Key Observation

$|\beta_k| \approx 2^\mu \rightsquigarrow |\gamma| \approx 2^\mu \cdot 2^\mu \approx 2^{2\sqrt{m}}$

Assume EQN-SAT(G^*) decidable in time $2^{o(\log^2 N)}$ (N = equation length).
Then we can solve 3-Coloring in time $2^{o(n+m)}$:
with $N = 2^{2\sqrt{m}}$ we have $2^{o(\log^2 2^{2\sqrt{m}})} = 2^{o(\sqrt{m}^2)} = 2^{o(m)}$

Reduce 3-COLORING to EQN-SAT(G^*)

Recall: $G^* = (S_3 \times S_3 \times S_3) \rtimes C_3$

$\Gamma = (V, E)$ graph with $V = \{1, \ldots, n\}$, $E = \{e_1, \ldots, e_m\}$.

- For every vertex i introduce a variable X_i.
- Group the edges in $\mu \approx \sqrt{m}$ groups of μ edges each.
- For every edge $e_{k,\ell} = \{i_{k,\ell}, j_{k,\ell}\}$ set $\alpha_{k,\ell} = X_{i_{k,\ell}} X_{j_{k,\ell}}^{-1}$.
- Set $\beta_k = Y_k^{-1}[(s, 1, 1), \alpha_{k,1}, \ldots, \alpha_{k,\mu}]Y_k$ for a new variable Y_k.
- Set $\gamma = [(d, 1, 1), \beta_1, \ldots, \beta_\mu]$.

Key Observation

$|\beta_k| \approx 2^\mu \rightsquigarrow |\gamma| \approx 2^\mu \cdot 2^\mu \approx 2^{2\sqrt{m}}$

Assume EQN-SAT(G^*) decidable in time $2^{o(\log^2 N)}$ (N = equation length).

Then we can solve 3-COLORING in time $2^{o(n+m)}$:

with $N = 2^{2\sqrt{m}}$ we have $2^{o(\log^2 2^{2\sqrt{m}})} = 2^{o(\sqrt{m}^2)} = 2^{o(m)}$ contradicting ETH.

Conclusion

- Quasipolynomial lower bound for $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ under ETH if G if of Fitting length 3 and complicated enough.

Conclusion

- Quasipolynomial lower bound for $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ under ETH if G if of Fitting length 3 and complicated enough.
- Generalization to all groups of Fitting length 3 under preparation (in collaboration with Idziak, Kawałek, Krzaczkowski).

Conclusion

- Quasipolynomial lower bound for $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ under ETH if G if of Fitting length 3 and complicated enough.
- Generalization to all groups of Fitting length 3 under preparation (in collaboration with Idziak, Kawałek, Krzaczkowski).
- What about groups of Fitting length two?

Conclusion

- Quasipolynomial lower bound for $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ under ETH if G if of Fitting length 3 and complicated enough.
- Generalization to all groups of Fitting length 3 under preparation (in collaboration with Idziak, Kawałek, Krzaczkowski).

- What about groups of Fitting length two?
- Conjecture: if G is finite solvable, then $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ are decidable in quasipolynomial time.

Conclusion

- Quasipolynomial lower bound for $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ under ETH if G if of Fitting length 3 and complicated enough.
- Generalization to all groups of Fitting length 3 under preparation (in collaboration with Idziak, Kawałek, Krzaczkowski).

- What about groups of Fitting length two?
- Conjecture: if G is finite solvable, then $\mathrm{EQN\text{-}SAT}(G)$ and $\mathrm{EQN\text{-}ID}(G)$ are decidable in quasipolynomial time.

Thank you!