THE COMPLEXITY OF CHECKING QUASI-IDENTITIES OVER FINITE ALGEBRAS WITH A MAL'CEV TERM

Simon Grünbacher and Erhard Aichinger
Institute for Algebra
Austrian Science Fund FWF P33878

JOHANNES KEPLER UNIVERSITY LINZ

Der Wissenschaftsfonds.

THE PROBLEM

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$.

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$.

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$. Is this valid?

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes
- In $\mathbb{Z}_3$: yes

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes
- In $\mathbb{Z}_3$: yes
- In $\mathbb{Z}_2$: no (Counterexample $x = 0, y = 1$)

Example

- Consider the formula $(x = 1 + 1 \land x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes
- In $\mathbb{Z}_3$: yes
- In $\mathbb{Z}_2$: no (Counterexample $x = 0, y = 1$)
- In $\mathbb{Z}_6$: no (Counterexample $x = 2, y = 3$)

Example

- Consider the formula $(x = 1 + 1 \land x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes
- In $\mathbb{Z}_3$: yes
- In $\mathbb{Z}_2$: no (Counterexample $x = 0, y = 1$)
- In $\mathbb{Z}_6$: no (Counterexample $x = 2, y = 3$)

Example

- Consider the formula $(x = 1 + 1 \wedge x \cdot y = 0) \Rightarrow y = 0$. Is this valid?
- In $\mathbb{R}$: yes
- In $\mathbb{Z}_3$: yes
- In $\mathbb{Z}_2$: no (Counterexample $x = 0, y = 1$)
- In $\mathbb{Z}_6$: no (Counterexample $x = 2, y = 3$)

We decide the validity of these quasi-identities in finite algebras.

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n\in\mathbb{N}} A^{A^n}$ is a set of functions over A.

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n\in\mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n\in\mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n \in \mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Example

- Algebra: $(\mathbb{N}, +, \cdot)$, term: $(x \cdot x) + (y \cdot z)$

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n \in \mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Example

- Algebra: $(\mathbb{N}, +, \cdot)$, term: $(x \cdot x) + (y \cdot z)$
- Algebra: $(\mathbb{B}, \vee, \wedge, \top)$, term: $x \wedge \top$

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n \in \mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Example

- Algebra: $(\mathbb{N}, +, \cdot)$, term: $(x \cdot x) + (y \cdot z)$
- Algebra: $(\mathbb{B}, \vee, \wedge, \top)$, term: $x \wedge \top$
- Algebra: $(\mathbb{Z}_3, +, \cdot)$, not a term: $x + 1$

Notation

- An algebra $\mathbf{A}$ is a pair (A, F), where A is a set and $F \subseteq \bigcup_{n \in \mathbb{N}} A^{A^n}$ is a set of functions over A.
- A term over $\mathbf{A}$ is a well-formed expression involving variables and operation symbols representing the functions from F.

Example

- Algebra: $(\mathbb{N}, +, \cdot)$, term: $(x \cdot x) + (y \cdot z)$
- Algebra: $(\mathbb{B}, \vee, \wedge, \top)$, term: $x \wedge \top$
- Algebra: $(\mathbb{Z}_3, +, \cdot)$, not a term: $x + 1$
- Not an algebra: $(\mathbb{R}, +, -, \cdot, /)$ (because $/$ is not total)

Quasi-Identity Validity

Let $\mathbf{A}$ be a finite algebra with finitely many fundamental operations. We are interested in the following decision problem:

Quasi-Identity Validity

Let $\mathbf{A}$ be a finite algebra with finitely many fundamental operations. We are interested in the following decision problem:

$\textsc{QuasiIdVal}(\mathbf{A})$
Given: Terms $s_1, \ldots, s_k, t_1, \ldots, t_k, u, v$ over $\mathbf{A}$

Quasi-Identity Validity

Let $\mathbf{A}$ be a finite algebra with finitely many fundamental operations. We are interested in the following decision problem:

QUASIIDVAL($\mathbf{A}$)

Given: Terms $s_1, \ldots, s_k, t_1, \ldots, t_k, u, v$ over $\mathbf{A}$

Asked: Does

$$\forall \boldsymbol{x} \in A^n : (\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})) \Longrightarrow (u(\boldsymbol{x}) = v(\boldsymbol{x}))$$

hold?

Quasi-Identity Validity

Let $\mathbf{A}$ be a finite algebra with finitely many fundamental operations. We are interested in the following decision problem:

QuasiIdVal($\mathbf{A}$)

Given: Terms $s_1, \ldots, s_k, t_1, \ldots, t_k, u, v$ over $\mathbf{A}$

Asked: Does

$$\forall \boldsymbol{x} \in A^n : (\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})) \Longrightarrow (u(\boldsymbol{x}) = v(\boldsymbol{x}))$$

hold?

Problem is in coNP.

Question: For which $\mathbf{A}$ is QuasiIdVal($\mathbf{A}$) in P or coNP-complete?

RELATION TO STUDIED PROBLEMS

Relation to term equivalence

TermEqv($\mathbf{A}$)

Given: Terms s, t

Relation to term equivalence

TermEqv($\mathbf{A}$)

Given: Terms s, t

Asked: Does $\forall \boldsymbol{x} \in A^n : s(\boldsymbol{x}) = t(\boldsymbol{x})$ hold?

Relation to term equivalence

TermEqv($\mathbf{A}$)

Given: Terms s, t

Asked: Does $\forall \boldsymbol{x} \in A^n : s(\boldsymbol{x}) = t(\boldsymbol{x})$ hold?

The term equivalence

$$\forall \boldsymbol{x} \in A^n : s(\boldsymbol{x}) = t(\boldsymbol{x})$$

is valid iff the quasi-identity

$$\forall \boldsymbol{x} \in A^n : x_1 = x_1 \Rightarrow s(\boldsymbol{x}) = t(\boldsymbol{x})$$

is valid.

Relation to term equivalence

$\textsc{TermEqv}(\mathbf{A})$

Given: Terms s, t

Asked: Does $\forall \boldsymbol{x} \in A^n : s(\boldsymbol{x}) = t(\boldsymbol{x})$ hold?

The term equivalence

$$\forall \boldsymbol{x} \in A^n : s(\boldsymbol{x}) = t(\boldsymbol{x})$$

is valid iff the quasi-identity

$$\forall \boldsymbol{x} \in A^n : x_1 = x_1 \Rightarrow s(\boldsymbol{x}) = t(\boldsymbol{x})$$

is valid.

Hence $\textsc{TermEqv}(\mathbf{A}) \leq_m^{\mathrm{P}} \textsc{QuasiIdVal}(\mathbf{A})$.

Relation to solving systems of polynomial equations

POLSYSSAT($\mathbf{A}$)

Given: $\boldsymbol{a} \in A^r$, terms $s_1, \ldots, s_k, t_1, \ldots, t_k$

Relation to solving systems of polynomial equations

PolSysSat($\mathbf{A}$)

Given: $\boldsymbol{a} \in A^r$, terms $s_1, \dots, s_k, t_1, \dots, t_k$

Asked: Does $\exists \boldsymbol{x} \in A^n : s_1(\boldsymbol{a}, \boldsymbol{x}) = t_1(\boldsymbol{a}, \boldsymbol{x}) \wedge \cdots \wedge s_k(\boldsymbol{a}, \boldsymbol{x}) = t_k(\boldsymbol{a}, \boldsymbol{x})$ hold?

Relation to solving systems of polynomial equations

PolSysSat($\mathbf{A}$)

Given: $\boldsymbol{a} \in A^r$, terms $s_1, \ldots, s_k, t_1, \ldots, t_k$

Asked: Does $\exists \boldsymbol{x} \in A^n : s_1(\boldsymbol{a}, \boldsymbol{x}) = t_1(\boldsymbol{a}, \boldsymbol{x}) \wedge \cdots \wedge s_k(\boldsymbol{a}, \boldsymbol{x}) = t_k(\boldsymbol{a}, \boldsymbol{x})$ hold?

The quasi-identity

$$\Big(\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})\Big) \Rightarrow u(\boldsymbol{x}) = v(\boldsymbol{x})$$

is not valid iff there are $a, b \in A$ with $a \neq b$ such that

$$\Big(\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})\Big) \wedge u(\boldsymbol{x}) = a \wedge v(\boldsymbol{x}) = b$$

has a solution.

Relation to solving systems of polynomial equations

$\textsc{PolSysSat}(\mathbf{A})$

Given: $\boldsymbol{a} \in A^r$, terms $s_1, \dots, s_k, t_1, \dots, t_k$

Asked: Does $\exists \boldsymbol{x} \in A^n : s_1(\boldsymbol{a}, \boldsymbol{x}) = t_1(\boldsymbol{a}, \boldsymbol{x}) \wedge \dots \wedge s_k(\boldsymbol{a}, \boldsymbol{x}) = t_k(\boldsymbol{a}, \boldsymbol{x})$ hold?

The quasi-identity

$$\Big(\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})\Big) \Rightarrow u(\boldsymbol{x}) = v(\boldsymbol{x})$$

is not valid iff there are $a, b \in A$ with $a \neq b$ such that

$$\Big(\bigwedge_{i=1}^{k} s_i(\boldsymbol{x}) = t_i(\boldsymbol{x})\Big) \wedge u(\boldsymbol{x}) = a \wedge v(\boldsymbol{x}) = b$$

has a solution.

Hence $\textsc{TermEqv}(\mathbf{A}) \leq_m^{\mathrm{P}} \textsc{QuasiIdVal}(\mathbf{A}) \leq_{tt}^{\mathrm{P}} \text{co}\textsc{PolSysSat}(\mathbf{A})$.

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).
- $\textsc{PolSysSat}(\mathbf{G}) \in \mathrm{P}$ if $\mathbf{G}$ is abelian (Goldmann, Russel 2002).

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).
- $\textsc{PolSysSat}(\mathbf{G}) \in \mathrm{P}$ if $\mathbf{G}$ is abelian (Goldmann, Russel 2002).
- $\Longrightarrow$ Open cases for $\textsc{QuasiIdVal}(\mathbf{R})$: $\mathbf{R}$ is nilpotent and nonzero.

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).
- $\textsc{PolSysSat}(\mathbf{G}) \in \mathrm{P}$ if $\mathbf{G}$ is abelian (Goldmann, Russel 2002).
- $\Longrightarrow$ Open cases for $\textsc{QuasiIdVal}(\mathbf{R})$: $\mathbf{R}$ is nilpotent and nonzero.
- $\Longrightarrow$ Open cases for $\textsc{QuasiIdVal}(\mathbf{G})$: $\mathbf{G}$ is solvable and nonabelian.

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).
- $\textsc{PolSysSat}(\mathbf{G}) \in \mathrm{P}$ if $\mathbf{G}$ is abelian (Goldmann, Russel 2002).
- $\implies$ Open cases for $\textsc{QuasiIdVal}(\mathbf{R})$: $\mathbf{R}$ is nilpotent and nonzero.
- $\implies$ Open cases for $\textsc{QuasiIdVal}(\mathbf{G})$: $\mathbf{G}$ is solvable and nonabelian.

Known Results

Let $\mathbf{G}$ be a finite group, let $\mathbf{R}$ be a finite ring.

- $\textsc{TermEqv}(\mathbf{R}) \in \mathrm{coNPC}$ if $\mathbf{R}$ is nonnilpotent (Burris, Lawrence 1993).
- $\textsc{TermEqv}(\mathbf{G}) \in \mathrm{coNPC}$ if $\mathbf{G}$ is nonsolvable (Goldmann, Russel 2002).
- $\textsc{PolSysSat}(\mathbf{R}) \in \mathrm{P}$ if $\mathbf{R}$ is a zero ring (Goldmann, Russel 2002; Larose, Zádori 2006).
- $\textsc{PolSysSat}(\mathbf{G}) \in \mathrm{P}$ if $\mathbf{G}$ is abelian (Goldmann, Russel 2002).
- $\implies$ Open cases for $\textsc{QuasiIdVal}(\mathbf{R})$: $\mathbf{R}$ is nilpotent and nonzero.
- $\implies$ Open cases for $\textsc{QuasiIdVal}(\mathbf{G})$: $\mathbf{G}$ is solvable and nonabelian.

Our contribution: coNP-complete in both open cases.

COMPLEXITY FOR MAL'CEV ALGEBRAS

Mal’cev algebras

Mal’cev algebras are a generalization of rings, groups and modules:

Mal'cev algebras

Mal'cev algebras are a generalization of rings, groups and modules:

Definition

A term d is called a Mal'cev term if $d(a,b,b) = a = d(b,b,a)$. We call $\mathbf{A}$ a Mal'cev algebra if it has a Mal'cev term.

Mal’cev algebras

Mal’cev algebras are a generalization of rings, groups and modules:

Definition

A term d is called a Mal’cev term if $d(a, b, b) = a = d(b, b, a)$. We call $\mathbf{A}$ a Mal’cev algebra if it has a Mal’cev term.

Example

- In a group, $d(a, b, c) := ab^{-1}c$ is a Mal’cev term

Mal’cev algebras

Mal’cev algebras are a generalization of rings, groups and modules:

Definition

A term d is called a Mal’cev term if $d(a, b, b) = a = d(b, b, a)$. We call $\mathbf{A}$ a Mal’cev algebra if it has a Mal’cev term.

Example

- In a group, $d(a, b, c) := ab^{-1}c$ is a Mal’cev term
- In a ring, $d(a, b, c) := a - b + c$ is a Mal’cev term

Main Result

Theorem [Aichinger, Grünbacher]

Let $\mathbf{A}$ be a finite Mal'cev algebra. Then $\textsc{QuasiIdVal}(\mathbf{A})$ is in P if $\mathbf{A}$ is abelian and coNP-complete otherwise.

Main Result

Theorem [Aichinger, Grünbacher]

Let $\mathbf{A}$ be a finite Mal'cev algebra. Then $\textsc{QuasiIdVal}(\mathbf{A})$ is in P if $\mathbf{A}$ is abelian and coNP-complete otherwise.

In particular:

Main Result

Theorem [Aichinger, Grünbacher]

Let $\mathbf{A}$ be a finite Mal'cev algebra. Then $\textsc{QuasiIdVal}(\mathbf{A})$ is in P if $\mathbf{A}$ is abelian and coNP-complete otherwise.

In particular:

Corollary

Let $\mathbf{R} = (R, +, -, \cdot)$ be a finite ring. Then $\textsc{QuasiIdVal}(\mathbf{R})$ is in P if $a \cdot b = 0$ for all $a, b \in R$, and coNP-complete otherwise.

Main Result

Theorem [Aichinger, Grünbacher]

Let $\mathbf{A}$ be a finite Mal'cev algebra. Then QUASIIDVAL$(\mathbf{A})$ is in P if $\mathbf{A}$ is abelian and coNP-complete otherwise.

In particular:

Corollary

Let $\mathbf{R} = (R, +, -, \cdot)$ be a finite ring. Then QUASIIDVAL$(\mathbf{R})$ is in P if $a \cdot b = 0$ for all $a, b \in R$, and coNP-complete otherwise.

Corollary

Let $\mathbf{G} = (G, \cdot)$ be a finite group. Then QUASIIDVAL$(\mathbf{G})$ is in P if $\mathbf{G}$ is abelian, and coNP-complete otherwise.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.
- For $z \in \mathbb{Z}_6$, let $\rho_z := \{(a, b) \in R^2 \mid \exists y \in R : y \cdot (a - b) = z\}$.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.
- For $z \in \mathbb{Z}_6$, let $\rho_z := \{(a, b) \in R^2 \mid \exists y \in R : y \cdot (a - b) = z\}$.
- Let $H_z := (\mathbb{Z}_6, \rho_z)$.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.
- For $z \in \mathbb{Z}_6$, let $\rho_z := \{(a, b) \in R^2 \mid \exists y \in R : y \cdot (a - b) = z\}$.
- Let $H_z := (\mathbb{Z}_6, \rho_z)$.
- Let $G = (V, E)$ be any graph.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.
- For $z \in \mathbb{Z}_6$, let $\rho_z := \{(a, b) \in R^2 \mid \exists y \in R : y \cdot (a - b) = z\}$.
- Let $H_z := (\mathbb{Z}_6, \rho_z)$.
- Let $G = (V, E)$ be any graph.
- Let $\Phi(E, z)$ denote the formula $\bigwedge_{(u,v)\in E} y_{(u,v)} \cdot (x_u - x_v) = z$.

Sample case: $(\mathbb{Z}_6, +, -, \cdot, 0)$

- Consider $\mathbf{R} := (\mathbb{Z}_6, +, -, \cdot, 0)$.
- For $z \in \mathbb{Z}_6$, let $\rho_z := \{(a, b) \in R^2 \mid \exists y \in R : y \cdot (a - b) = z\}$.
- Let $H_z := (\mathbb{Z}_6, \rho_z)$.
- Let $G = (V, E)$ be any graph.
- Let $\Phi(E, z)$ denote the formula $\bigwedge_{(u,v)\in E} y_{(u,v)} \cdot (x_u - x_v) = z$.
- Then $c(v) := x_v$ is a homomorphism $G \to H_z$ iff $\Phi(E, z)$ is satisfiable.

Homomorphism problems

For graphs G, H, we write $G \preceq H$ if there is a homomorphism $G \to H$.

Homomorphism problems

For graphs G, H, we write $G \preceq H$ if there is a homomorphism $G \to H$.
The computational problem of H-COLORING asks whether $G \preceq H$ for a given input G.

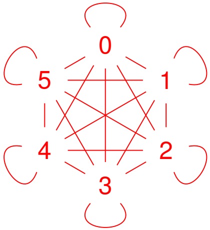
Homomorphism problems

For graphs G, H, we write $G \preceq H$ if there is a homomorphism $G \to H$.
The computational problem of H-COLORING asks whether $G \preceq H$ for a given input G.

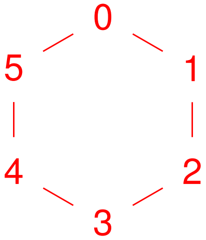
Theorem [Hell, Nešetřil 1990]

Let H be an undirected, loopless non-bipartite graph. Then H-COLORING is NP-complete.

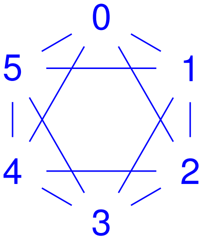
We use this to prove coNP-completeness for QUASIIDVAL.



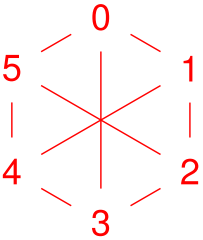
H_0



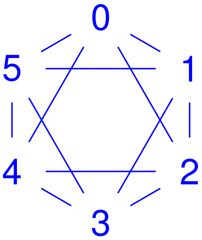
H_1



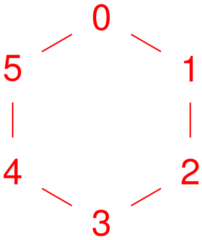
H_2



H_3



H_4



H_5

Restricting z

- H_2-COLORING is NP-complete.

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$ iff $\exists z \neq 0 : G \preceq H_z \wedge H_2 \preceq H_z$

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$
  iff $\exists z \neq 0 : G \preceq H_z \wedge H_2 \preceq H_z$
  iff $\Phi(E, z) \wedge \Phi(\rho_2, z) \wedge z \neq 0$ is satisfiable, where $\Phi(E, z)$ is $\bigwedge_{(u,v)\in E} y_{(u,v)}(x_u - x_v)$

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$
  iff $\exists z \neq 0 : G \preceq H_z \wedge H_2 \preceq H_z$
  iff $\Phi(E, z) \wedge \Phi(\rho_2, z) \wedge z \neq 0$ is satisfiable, where $\Phi(E, z)$ is $\bigwedge_{(u,v) \in E} y_{(u,v)}(x_u - x_v)$
  iff $(\Phi(E, z) \wedge \Phi(\rho_2, z)) \Rightarrow z = 0$ is not valid.

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$
  iff $\exists z \neq 0 : G \preceq H_z \wedge H_2 \preceq H_z$
  iff $\Phi(E, z) \wedge \Phi(\rho_2, z) \wedge z \neq 0$ is satisfiable, where $\Phi(E, z)$ is $\bigwedge_{(u,v) \in E} y_{(u,v)}(x_u - x_v)$
  iff $(\Phi(E, z) \wedge \Phi(\rho_2, z)) \Rightarrow z = 0$ is not valid.

This reduces H_2-COLORING to COQUASIIDVAL$(\mathbb{Z}_6, +, -, \cdot, 0)$.

Restricting z

- H_2-COLORING is NP-complete.
- For all $z \neq 0$, $H_2 \preceq H_z$ implies $H_z \preceq H_2$.
- For $G = (V, E)$ we therefore have $G \preceq H_2$
  iff $\exists z \neq 0 : G \preceq H_z \wedge H_2 \preceq H_z$
  iff $\Phi(E, z) \wedge \Phi(\rho_2, z) \wedge z \neq 0$ is satisfiable, where $\Phi(E, z)$ is $\bigwedge_{(u,v)\in E} y_{(u,v)}(x_u - x_v)$
  iff $(\Phi(E, z) \wedge \Phi(\rho_2, z)) \Rightarrow z = 0$ is not valid.

This reduces H_2-COLORING to COQUASIIDVAL$(\mathbb{Z}_6, +, -, \cdot, 0)$.
Therefore QUASIIDVAL$(\mathbb{Z}_6, +, -, \cdot, 0) \in \mathrm{coNPC}$.

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:
  $\Longrightarrow$ Choose H_a to be $\preceq$-maximal among the possible choices.

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:
  $\Longrightarrow$ Choose H_a to be $\preceq$-maximal among the possible choices.
- To define analogue of $y(a-b) = z$ for Mal'cev algebras:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:
  $\Longrightarrow$ Choose H_a to be $\preceq$-maximal among the possible choices.
- To define analogue of $y(a-b) = z$ for Mal'cev algebras:

Generalization to Mal'cev Algebras

How to make it work in a finite nonabelian Mal'cev algebra $\mathbf{A}$:

- To ensure that we have $z \in A$ with H_z-COLORING $\in \mathrm{NPC}$:
  $\Longrightarrow$ Define ρ_z over A^2 instead ($2^2 \geq 3$ cosets modulo center).
- To ensure that we have $a \in A$ s.t. $\forall z \neq 0 : H_z \preceq H_a \Rightarrow H_a \preceq H_z$:
  $\Longrightarrow$ Choose H_a to be $\preceq$-maximal among the possible choices.
- To define analogue of $y(a - b) = z$ for Mal'cev algebras:
  $\Longrightarrow$ Use commutator theory over Mal'cev algebras. Commutator theory explains what abelian, nilpotent, solvable mean for Mal'cev algebras.

Generalization to Mal'cev Algebras

In particular, for groups and rings we obtain:

Theorem

Let $\mathbf{R} = (R, +, -, \cdot)$ be a finite ring. Then $\textsc{QuasiIdVal}(\mathbf{R})$ is in P if $a \cdot b = 0$ for all $a, b \in R$, and coNP-complete otherwise.

Generalization to Mal'cev Algebras

In particular, for groups and rings we obtain:

Theorem

Let $\mathbf{R} = (R, +, -, \cdot)$ be a finite ring. Then $\textsc{QuasiIdVal}(\mathbf{R})$ is in P if $a \cdot b = 0$ for all $a, b \in R$, and coNP-complete otherwise.

Theorem

Let $\mathbf{G} = (G, \cdot)$ be a finite group. Then $\textsc{QuasiIdVal}(\mathbf{G})$ is in P if $\mathbf{G}$ is abelian, and coNP-complete otherwise.