Submonoid Membership in n-dimensional lamplighter groups

Ruiwen Dong

Magdalen College, University of Oxford

December 2024

MAGDALEN COLLEGE
OXFORD

European Research Council
Established by the European Commission

Let G be an group (infinite, finitely generated, with solvable Word Problem). Consider the following **membership** problems:

Definition (Subgroup Membership)

Input: Elements $g_1, g_2, \ldots, g_n, g \in G$.
Question: Is g in the subgroup $\langle g_1, g_2, \ldots, g_n \rangle_{\text{grp}}$?

Membership problems

Let G be an group (infinite, finitely generated, with solvable Word Problem). Consider the following **membership** problems:

Definition (Subgroup Membership)

Input: Elements $g_1, g_2, \ldots, g_n, g \in G$.
Question: Is g in the subgroup $\langle g_1, g_2, \ldots, g_n \rangle_{\mathrm{grp}}$?

Definition (Submonoid Membership)

Input: Elements $g_1, g_2, \ldots, g_n, g \in G$.
Question: Is g in the sub*monoid* $\langle g_1, g_2, \ldots, g_n \rangle_{\mathrm{mnd}}$?

Membership problems

Let G be an group (infinite, finitely generated, with solvable Word Problem). Consider the following **membership** problems:

Definition (Subgroup Membership)

Input: Elements $g_1, g_2, \dots, g_n, g \in G$.
Question: Is g in the subgroup $\langle g_1, g_2, \dots, g_n \rangle_{\mathrm{grp}}$?

Definition (Submonoid Membership)

Input: Elements $g_1, g_2, \dots, g_n, g \in G$.
Question: Is g in the sub*monoid* $\langle g_1, g_2, \dots, g_n \rangle_{\mathrm{mnd}}$?

Definition (Rational Subset Membership)

Input: A **rational subset** $S \subseteq G$ and an element $g \in G$.
Question: Is g in the rational subset S?

Here, $S \subseteq G$ is called a **rational subset** if there is an alphabet Σ, a monoid homomorphism $\varphi \colon \Sigma^* \to G$, and a regular language $L \subseteq \Sigma^*$, such that $\varphi(L) = S$.
Example: $S = \{g_1\}^*\{g_2\}^* = \{g_1^n g_2^m \mid n, m \in \mathbb{N}\} \subseteq G$.

Classic decidability results

Obviously, Subgroup Mshp. $\leq$ Submonoid Mshp. $\leq$ Rational Subset Mshp.

Theorem (Benois 1969, Grunschlag 1999)

If G is an **abelian** *group or a* **free** *group, then Subgroup Membership, Submonoid Membership and Rational Subset Membership are decidable in G.*

Classic decidability results

Obviously, Subgroup Mshp. $\leq$ Submonoid Mshp. $\leq$ Rational Subset Mshp.

Theorem (Benois 1969, Grunschlag 1999)

If G is an **abelian** *group or a* **free** *group, then Subgroup Membership, Submonoid Membership and Rational Subset Membership are decidable in G.*

Theorem (Malcev 1958, Romanovskii 1974, Roman'kov 2022)

If G is a **nilpotent** *group or a* **metabelian** *group (i.e. $[G, G]$ is abelian), then Subgroup Membership is decidable. But there are nilpotent groups (such as $\mathsf{H}_3(\mathbb{Z})^{10000}$) and metabelian groups where Submonoid Membership and Rational Subset Membership are undecidable.*

Obviously, Subgroup Mshp. $\leq$ Submonoid Mshp. $\leq$ Rational Subset Mshp.

Theorem (Benois 1969, Grunschlag 1999)

*If G is an **abelian** group or a **free** group, then Subgroup Membership, Submonoid Membership and Rational Subset Membership are decidable in G.*

Theorem (Malcev 1958, Romanovskii 1974, Roman'kov 2022)

*If G is a **nilpotent** group or a **metabelian** group (i.e. $[G, G]$ is abelian), then Subgroup Membership is decidable. But there are nilpotent groups (such as $\mathsf{H}_3(\mathbb{Z})^{10000}$) and metabelian groups where Submonoid Membership and Rational Subset Membership are undecidable.*

Theorem (Shafrir 2018, Bodart 2024)

There exists a group G (such as the two-dimensional lamplighter group $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$), where Submonoid Membership is decidable but Rational Subset Membership is undecidable.

Hence, Subgroup Mshp. $\lneq$ Submonoid Mshp. $\lneq$ Rational Subset Mshp.

Decidability under finite extension

Theorem (folklore)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Subgroup Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if H is a f.g. subgroup of G, then $H \cap \widetilde{G}$ is a f.g. subgroup of $\widetilde{G}$.

Decidability under finite extension

Theorem (folklore)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Subgroup Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if H is a f.g. subgroup of G, then $H \cap \widetilde{G}$ is a f.g. subgroup of $\widetilde{G}$.

Theorem (Grunschlag 1999)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Rational Subset Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if S is a rational subset of G, then $S \cap \widetilde{G}$ is a rational subset of $\widetilde{G}$.

Decidability under finite extension

Theorem (folklore)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Subgroup Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if H is a f.g. subgroup of G, then $H \cap \widetilde{G}$ is a f.g. subgroup of $\widetilde{G}$.

Theorem (Grunschlag 1999)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Rational Subset Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if S is a rational subset of G, then $S \cap \widetilde{G}$ is a rational subset of $\widetilde{G}$.

Problem

What about **Submonoid Membership**?

Difficulty: if M is a f.g. submonoid of G, then $M \cap \widetilde{G}$ can be an **infinitely generated** submonoid of $\widetilde{G}$.

Decidability under finite extension

Theorem (folklore)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Subgroup Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if H is a f.g. subgroup of G, then $H \cap \widetilde{G}$ is a f.g. subgroup of $\widetilde{G}$.

Theorem (Grunschlag 1999)

Let G be a group and $\widetilde{G} \leq G$ be a finite index subgroup. Then **Rational Subset Membership** *is decidable in G if and only if it is decidable in $\widetilde{G}$.*

Idea: if S is a rational subset of G, then $S \cap \widetilde{G}$ is a rational subset of $\widetilde{G}$.

Problem

What about **Submonoid Membership**?

Difficulty: if M is a f.g. submonoid of G, then $M \cap \widetilde{G}$ can be an **infinitely generated** submonoid of $\widetilde{G}$.

Theorem (D. 2024 + Shafrir 2024)

There exists a group G and a finite index subgroup $\widetilde{G}$, such that Submonoid Membership is decidable in $\widetilde{G}$ but undecidable in G.

Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Take for example $n = 2$. Each element in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ can be drawn as a $\mathbb{Z}^2$-grid of lamps, each on or off, plus a person in some position.

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$

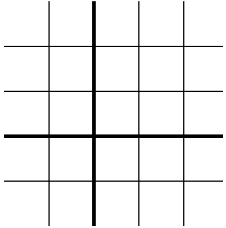
Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Take for example $n = 2$. Each element in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ can be drawn as a $\mathbb{Z}^2$-grid of lamps, each on or off, plus a person in some position.

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$



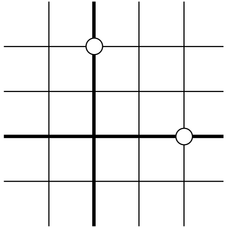
Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \middle| \; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Take for example $n = 2$. Each element in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ can be drawn as a $\mathbb{Z}^2$-grid of lamps, each on or off, plus a person in some position.

$$\begin{pmatrix} X_1^1 X_2^1 & \color{red}{X_1^2 + X_2^2} \\ 0 & 1 \end{pmatrix}$$



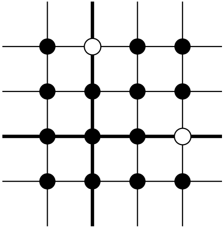
Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Take for example $n = 2$. Each element in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ can be drawn as a $\mathbb{Z}^2$-grid of lamps, each on or off, plus a person in some position.

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$



Definition (n-dimensional lamplighter group)

The *n-dimensional lamplighter group* $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^n$ is defined as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, \underbrace{f \in \mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]}_{\text{Laurent polynomial over } \mathbb{F}_2} \right\}.$$

Take for example $n = 2$. Each element in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ can be drawn as a $\mathbb{Z}^2$-grid of lamps, each on or off, plus a person in some position.

$$\begin{pmatrix} X_1^{1} X_2^{1} & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$

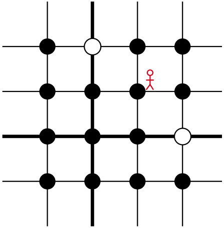


Illustration: multiplication

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$

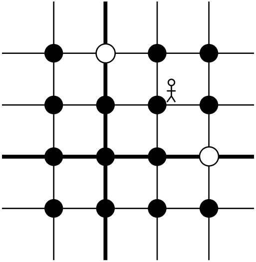


Illustration: multiplication

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix} \quad \times \quad \begin{pmatrix} X_1^1 & 1 \\ 0 & 1 \end{pmatrix}$$

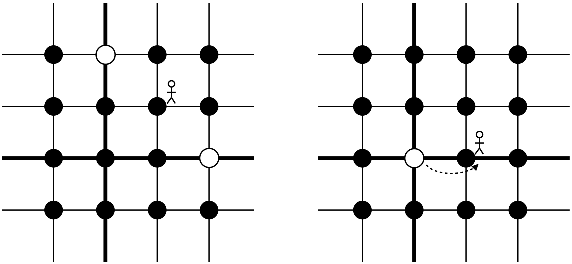
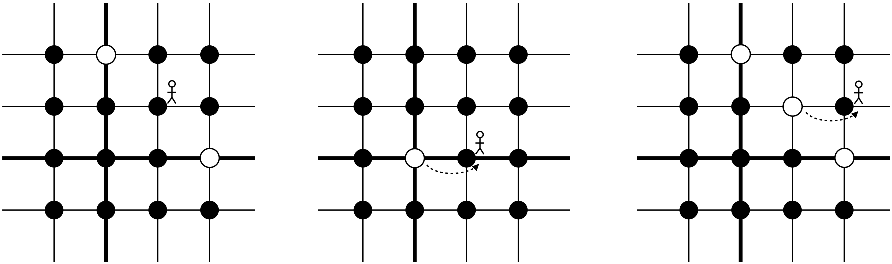


Illustration: multiplication

$$\begin{pmatrix} X_1^1 X_2^1 & X_1^2 + X_2^2 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} X_1^1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} X_1^2 X_2 & X_1^2 + X_1 X_2 + X_2^2 \\ 0 & 1 \end{pmatrix}$$



Constructing the counter-example: semidirect products

Definition (semidirect products)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. One can define a *semidirect product* $\mathcal{Y} \rtimes \mathbb{Z}^n$ as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & y \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, y \in \mathcal{Y} \right\}.$$

Definition (semidirect products)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. One can define a *semidirect product* $\mathcal{Y} \rtimes \mathbb{Z}^n$ as a matrix group

$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & y \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, y \in \mathcal{Y} \right\}.$$

Example:

One can consider $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}]$ as an $\mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]$-module. Then $\mathcal{Y} \rtimes \mathbb{Z}^2$ is simply the direct product of $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$ with $\mathbb{Z}$.

Definition (semidirect products)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. One can define a *semidirect product* $\mathcal{Y} \rtimes \mathbb{Z}^n$ as a matrix group

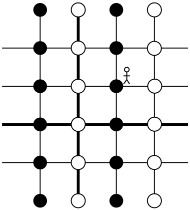
$$\left\{ \begin{pmatrix} X_1^{z_1} X_2^{z_2} \cdots X_n^{z_n} & y \\ 0 & 1 \end{pmatrix} \;\middle|\; z_1, \dots, z_n \in \mathbb{Z}, y \in \mathcal{Y} \right\}.$$

Example:

One can consider $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}]$ as an $\mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]$-module. Then $\mathcal{Y} \rtimes \mathbb{Z}^2$ is simply the direct product of $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$ with $\mathbb{Z}$.

Since $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}] = \mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]/(X_2 - 1)$, the group $\mathcal{Y} \rtimes \mathbb{Z}^2$ can be seen as a quotient of $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ by "wiring" all lamps in the same column together.

$$\begin{pmatrix} X_1^1 X_2^1 & 1 + X_1^2 \\ 0 & 1 \end{pmatrix}$$



Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Rational Subset Membership in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ *is undecidable even for a fixed rational subset.*

Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Rational Subset Membership in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ is undecidable even for a fixed rational subset. (Because it can encode tiling problems on a plane.)

Constructing the counter-example: old and new results

Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Rational Subset Membership in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ is undecidable even for a fixed rational subset. (Because it can encode tiling problems on a plane.)

Theorem (Shafrir 2024)

Let G be a group. Rational Subset Membership (for a fixed rational subset) in G reduces to Submonoid Membership in $G \times H$ for some virtually abelian H.

In particular, for LSZ'15, H can be taken as a finite extension of $\mathbb{Z}^5$.

Constructing the counter-example: old and new results

Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Rational Subset Membership in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ is undecidable even for a fixed rational subset. (Because it can encode tiling problems on a plane.)

Theorem (Shafrir 2024)

Let G be a group. Rational Subset Membership (for a fixed rational subset) in G reduces to Submonoid Membership in $G \times H$ for some virtually abelian H.

In particular, for LSZ'15, H can be taken as a finite extension of $\mathbb{Z}^5$.

Corollary

The direct product $\left((\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2\right) \times \mathbb{Z}^5$ has a finite extension with undecidable Submonoid Membership.

Constructing the counter-example: old and new results

Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Rational Subset Membership in $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ is undecidable even for a fixed rational subset. (Because it can encode tiling problems on a plane.)

Theorem (Shafrir 2024)

Let G be a group. Rational Subset Membership (for a fixed rational subset) in G reduces to Submonoid Membership in $G \times H$ for some virtually abelian H.

In particular, for LSZ'15, H can be taken as a finite extension of $\mathbb{Z}^5$.

Corollary

The direct product $\left((\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2\right) \times \mathbb{Z}^5$ has a finite extension with undecidable Submonoid Membership.

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

But $\left((\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2\right) \times \mathbb{Z}^5 = \mathbb{F}_2[X_1^{\pm}, X_2^{\pm}] \rtimes \mathbb{Z}^7$!!!

Proof of decidability result: submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

Proof of decidability result: submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.

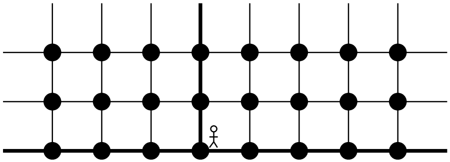
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



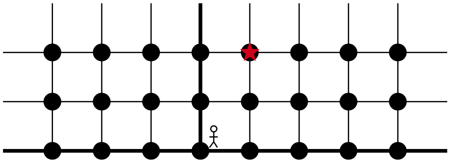
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^{1} X_2^{2} & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



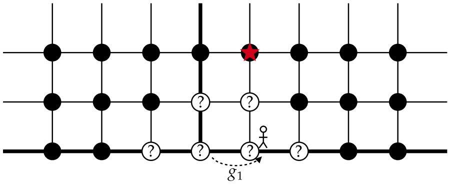
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



Proof of decidability result: submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$

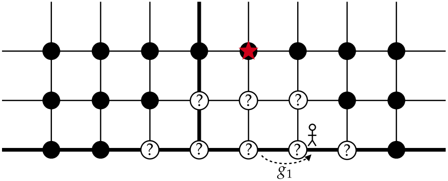
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



Proof of decidability result: submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$

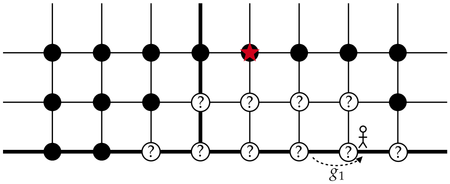
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



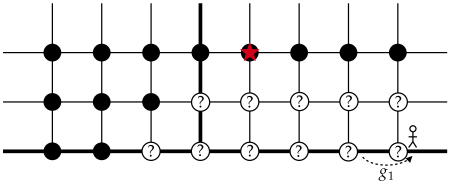
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



Proof of decidability result: submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$

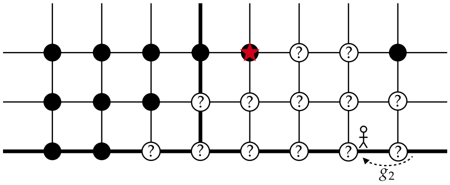
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} {\color{red}X_1^{-1}} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



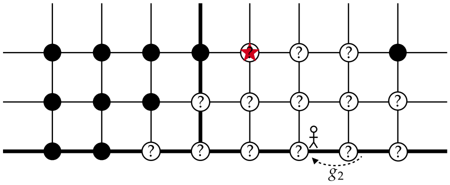
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



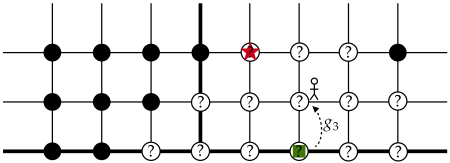
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



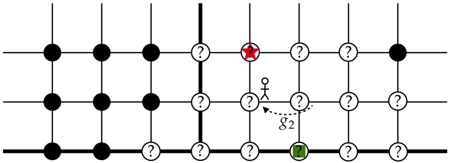
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



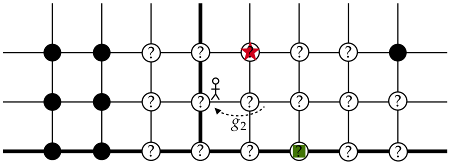
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



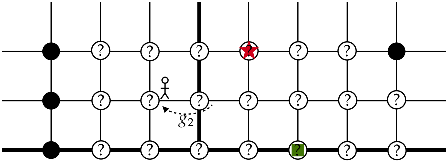
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



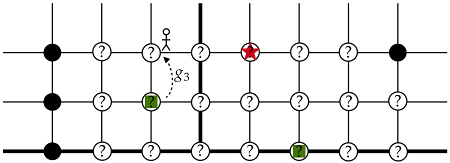
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



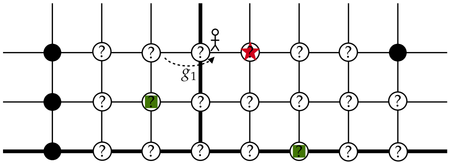
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



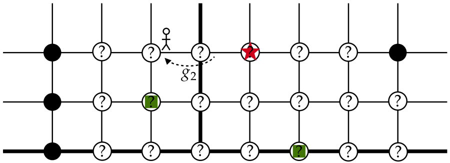
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



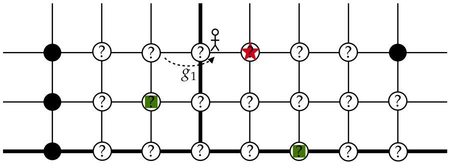
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



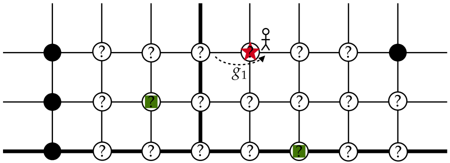
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



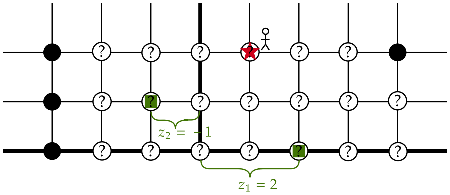
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathrm{mnd}}$.



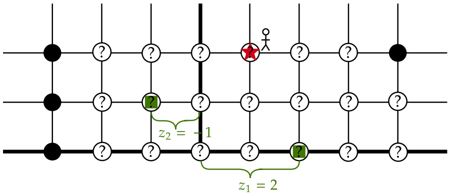
Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

How do submonoids of $\mathcal{Y} \rtimes \mathbb{Z}^n$ look like? Example: $n = 2$, consider the submonoid generated by

$$g_1 = \begin{pmatrix} X_1^1 & ? \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} X_1^{-1} & ? \\ 0 & 1 \end{pmatrix}, g_3 = \begin{pmatrix} X_2^1 & ? \\ 0 & 1 \end{pmatrix}.$$

We want to decide whether $g = \begin{pmatrix} X_1^1 X_2^2 & ? \\ 0 & 1 \end{pmatrix}$ is in the monoid $\langle g_1, g_2, g_3 \rangle_{\mathsf{mnd}}$.



Satisfy: $X_1^{z_1} \cdot m_1 + X_1^{z_2} \cdot m_2 = m_0$ for some $m_1, m_2, m_0 \in \mathcal{Y}/\mathcal{Y}'$.
The quotient by some submodule $\mathcal{Y}'$ accounts for "zigzags".

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

The proof has two steps. **Step 1** is rather elementary:

Proposition (From Submonoid Membership to S-unit equations)

Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ reduces to solving **S-unit equations** *in some finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module $M = \mathcal{Y}/\mathcal{Y}'$.*

Proof of decidability result: from submonoids to S-unit equations

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

The proof has two steps. **Step 1** is rather elementary:

Proposition (From Submonoid Membership to S-unit equations)

Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ reduces to solving **S-unit equations** *in some finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module $M = \mathcal{Y}/\mathcal{Y}'$.*

Definition (S-unit equations in modules)

Input: a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$-module M, and elements $m_1, \dots, m_k, m_0 \in M$.
Question: Does the following equation have solutions $z_{11}, z_{12}, \dots, z_{kn} \in \mathbb{Z}$?

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

For example, if $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$, then we are asking whether

$$X + Y + 1 \mid X^{z_{11}} Y^{z_{12}} m_1 + \cdots + X^{z_{k1}} Y^{z_{k2}} m_k - m_0$$

has integer solutions $z_{11}, z_{12}, \dots, z_{k1}, z_{k2}$.

Proof of decidability result: step 2

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

Proof of decidability result: step 2

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

Example

Let $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$. The following equation in M

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 1$$

is equivalent to the following equation in $\mathbb{F}_2(X)$:

$$X^{z_{11}} (X + 1)^{z_{12}} + X^{z_{21}} (X + 1)^{z_{22}} = 1.$$

Proof of decidability result: step 2

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

Example

Let $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$. The following equation in M

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 1$$

is equivalent to the following equation in $\mathbb{F}_2(X)$:

$$X^{z_{11}} (X+1)^{z_{12}} + X^{z_{21}} (X+1)^{z_{22}} = 1.$$

The solution set is

$$(z_{11}, z_{12}, z_{21}, z_{22}) \in \{(2^k, 0, 0, 2^k) \mid k \in \mathbb{N}\} \cup \{(0, 2^k, 2^k, 0) \mid k \in \mathbb{N}\}.$$

Proof of decidability result: step 2

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \dots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \dots, X_n^{\pm}]$*-module* M*, form an effectively* 2*-automatic subset of* $\mathbb{Z}^{kn}$*.*

Example

Let $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$. The following equation in M

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 1$$

is equivalent to the following equation in $\mathbb{F}_2(X)$:

$$X^{z_{11}} (X+1)^{z_{12}} + X^{z_{21}} (X+1)^{z_{22}} = 1.$$

The solution set is

$$(z_{11}, z_{12}, z_{21}, z_{22}) \in \{(2^k, 0, 0, 2^k) \mid k \in \mathbb{N}\} \cup \{(0, 2^k, 2^k, 0) \mid k \in \mathbb{N}\}.$$

Hint: $(X+1)^{2^k} = X^{2^k} + 1$, so $(X+1)^{2^k} + X^{2^k} = 1$.

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$

$(X + 1)^z + X^z = 1$

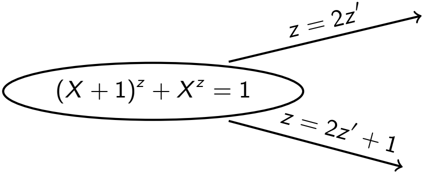
Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$



Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$

$$\begin{tikzcd} & (X+1)^{2z'} + X^{2z'} = 1 \\ (X+1)^z + X^z = 1 \arrow[ur, "z = 2z'"] \arrow[dr, "z = 2z' + 1"'] & \\ & {} \end{tikzcd}$$

Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X+1)^z + X^z = 1.$$

$$\begin{tikzcd}
 & (X^2+1)^{z'} + (X^2)^{z'} = 1 \\
(X+1)^z + X^z = 1 \arrow[ur, "z = 2z'"] \arrow[dr, "z = 2z' + 1"'] & \\
 & {}
\end{tikzcd}$$

Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$

$$\begin{tikzcd}
& (X'+1)^{z'} + (X')^{z'} = 1 \\
(X+1)^z + X^z = 1 \arrow[ur, "z = 2z'"] \arrow[dr, "z = 2z' + 1"'] & \\
& {}
\end{tikzcd}$$

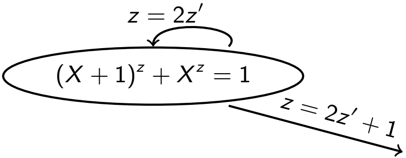
Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X+1)^z + X^z = 1.$$



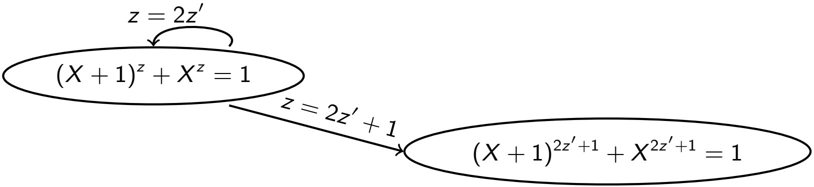
Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$



Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X+Y+1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X+1)^z + X^z = 1.$$

$$\begin{tikzcd} (X+1)^z + X^z = 1 \arrow[loop above, "z = 2z'"] \arrow[r, "z = 2z' + 1"] & z' = 0 \end{tikzcd}$$

Proof of 2-automaticity: Derkson's idea

Let's give the proof idea of step 2.
Instead of an equation with kn integer variables, let's consider a similar equation with one integer variable z.
For example, we want to solve in $M = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/(X + Y + 1)$:

$$Y^z + X^z = 1.$$

That is, we need to solve in $\mathbb{F}_2(X)$:

$$(X + 1)^z + X^z = 1.$$

$$\begin{tikzcd}
\boxed{(X+1)^z + X^z = 1} \arrow[loop above, "z = 2z'"] \arrow[r, "z = 2z' + 1"] & \boxed{z' = 0}
\end{tikzcd}$$

From this automaton, we see directly that $z = 2^k, k \in \mathbb{N}$.

Proof of 2-automaticity: general case

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

Proof of 2-automaticity: general case

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

We can construct an automaton that recognizes the binary expansion of $(z_{11}, z_{12}, \ldots, z_{kn})$ by guessing the parity of each z_{ij} each time.

Proof of 2-automaticity: general case

Proposition (Solution of S-unit equations)

The solutions $(z_{11}, z_{12}, \ldots, z_{kn}) \in \mathbb{Z}^{kn}$ *of an* **S-unit equation**

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} \cdot m_1 + \cdots + X_1^{z_{k1}} X_2^{z_{k2}} \cdots X_n^{z_{kn}} \cdot m_k = m_0.$$

over a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$*-module* M*, form an effectively 2-automatic subset of* $\mathbb{Z}^{kn}$*.*

We can construct an automaton that recognizes the binary expansion of $(z_{11}, z_{12}, \ldots, z_{kn})$ by guessing the parity of each z_{ij} each time.

Some extra difficulty: the module M is not as nice as a field $\mathbb{F}_2(X)$, so can't use "$(X+1)^2 = X^2 + 1$".
Solution: use primary decomposition and Noether Normalization to reduce to case of fields.

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_2[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

Conclusion, future work, and decidability limits

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

(In fact we can replace 2 by any prime p)

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

(In fact we can replace 2 by any prime p)

But can we replace the finite field $\mathbb{F}_p$ by the ring $\mathbb{Z}/k\mathbb{Z}$ for any integer k?

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

(In fact we can replace 2 by any prime p)
But can we replace the finite field $\mathbb{F}_p$ by the ring $\mathbb{Z}/k\mathbb{Z}$ for any integer k?

Conjecture

Let $k \in \mathbb{N}$ and $\mathcal{Y}$ be a finitely presented $(\mathbb{Z}/k\mathbb{Z})[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

(In fact we can replace 2 by any prime p)
But can we replace the finite field $\mathbb{F}_p$ by the ring $\mathbb{Z}/k\mathbb{Z}$ for any integer k?

Conjecture

Let $k \in \mathbb{N}$ and $\mathcal{Y}$ be a finitely presented $(\mathbb{Z}/k\mathbb{Z})[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.
Moreover, let G be a metabelian group with torsion commutator subgroup (i.e. $[G, G]$ is torsion abelian). Then Submonoid Membership is decidable in G.

Conclusion, future work, and decidability limits

Summary: Submonoid Membership $\longrightarrow$ S-unit equations $\longrightarrow$ decidable

Theorem (D. 2024)

Let $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.

(In fact we can replace 2 by any prime p)
But can we replace the finite field $\mathbb{F}_p$ by the ring $\mathbb{Z}/k\mathbb{Z}$ for any integer k?

Conjecture

Let $k \in \mathbb{N}$ and $\mathcal{Y}$ be a finitely presented $(\mathbb{Z}/k\mathbb{Z})[X_1^{\pm}, \dots, X_n^{\pm}]$-module. Then the semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ has decidable Submonoid Membership.
Moreover, let G be a metabelian group with torsion commutator subgroup (i.e. $[G, G]$ is torsion abelian). Then Submonoid Membership is decidable in G.

However we cannot replace the finite field $\mathbb{F}_p$ by $\mathbb{Z}$:

Theorem (Lohrey, Steinberg, and Zetzsche 2015)

Submonoid Membership in $\mathbb{Z} \wr \mathbb{Z} = \mathbb{Z}[X^{\pm}] \rtimes \mathbb{Z}$ is undecidable. (Because it can encode the halting problem for Minsky machines.)