Equations in Wreath Products of Abelian Groups

Jan Philipp **Wächter**

Department of Mathematics
University of Manchester

joint work with
Ruiwen **Dong** and Leon **Pernak**

This research was supported by EPSRC

11 November 2025

Hilbert's 10th Problem

Hilbert's 10th Problem

Is the problem

Input: a polynomial $p \in \mathbb{Z}[X_1, \ldots, X_\ell]$?
Question: are there values $z_1, \ldots, z_\ell \in \mathbb{Z}$ for the variables such that $p(z_1, \ldots, z_\ell) = 0$?

decidable?

Theorem (Matiyasevich; 1970)

The problem is undecidable.

Positive Results

Theorem (Presburger; 1929) Allowed oprations: $\exists, \forall, \wedge, \vee, \neg, +, =, <, \mathbb{N}$

The Presburger arithmetic over the natural numbers/integers is decidable.

No multiplication!

Allowed oprations: $\exists X \in \mathbb{R}, \forall X \in \mathbb{R}, \wedge, \vee, \neg, p = 0, p < 0, \mathbb{Q}$

Theorem (Tarski; 1930s/1948)

The first-order theory of the real numbers (with rational coefficients) is decidable.

Where is the border between decidability and undecidability?

Equations in Groups

Definition

G: group $\mathbb{X}$: finite set of variables $F(\mathbb{X})$: free group over $\mathbb{X}$

An equation over G is an element w of $G \star F(\mathbb{X})$ written as

$$w = 1.$$

A system of equations is simply a set $\{w_1 = 1, \dots\}$ of equations.

For algorithms:

Consider finitely generated groups $G = \langle \Sigma \rangle$ and represent the w_i as words from $(\Sigma^{\pm 1} \cup \mathbb{X}^{\pm 1})^*$.

Definition

An assignment of variables is a function $\sigma\colon \mathbb{X} \to G$.

We may extend it uniquely into a homomorphism $G \star F(\mathbb{X}) \to G$ by letting $\sigma(g) = g\ \forall g \in G$.

It satisfies (is a solution of) a system $\{w_i = 1\}$ if $\sigma(w_i) = 1$ holds in G for all i.

The Diophantine Problem

Definition (Diophantine Problem)

The Diophantine problem DP_1 is the decision problem:

single equation

Constant: the group $G = \langle \Sigma \rangle$

Input: a ~~finite system of equations~~ $\cancel{\{w_1 = 1, \dots, w_\ell = 1\}}$

Question: is the ~~system~~ satisfiable?

equation

Some decidability results:

- DP is decidable in free groups (Makanin 1982, Razborov 1984)
- DP_1 is decidable in the Heisenberg group (Duchin-Liang-Shapiro 2015)
- DP_1 is undecidable in free metabelian groups of rank ≥ 2 (Roman'kov 1979)
- DP_1 is undecidable in non-abelian free nilpotent groups (Truss '95; Duchin-Liang-Shapiro 2015)
- DP is undecidable in $\mathbb{Z} \wr \mathbb{Z}$ (Dong 2024)

Connection: the Word Problem

The word problem is Dehn's first fundamental problem in algorithmic group theory:

Definition (Word Problem)

The word problem of a finitely generated group is the decision problem:

Constant: the group $G = \langle \Sigma \rangle$
Input: a word $w \in (\Sigma \cup \Sigma^{-1})^*$ over the generators
Question: is $w = 1$ in G? i. e. does w represent the identity?

This is a special form of DP_1 where the equation only contains constants.

Connection II: the Conjugacy Problem

Dehn's second fundamental problem in algorithmic group theory is the conjugacy problem:

Definition (Conjugacy Problem)

The conjugacy problem of a finitely generated group is the decision problem:

Constant: the group $G = \langle \Sigma \rangle$
Input: two group elements $g, h \in G$ represented as words from $(\Sigma \cup \Sigma^{-1})^*$
Question: are g and h conjugate in G?

This is equivalent to asking whether $ZgZ^{-1} = h$ has a solution in G and, thus, a special form of DP_1 as well.

Further Variants of the Diophantine Problem

We can…

- …ask about the computational complexity of the problem.
- …compute the full solution set.
- …consider more restricted equations.

For example…

Quadratic Equations

Definition (Quadratic Equation)

An equation $w = 1$ over some group G is quadratic if it contains every variable at most twice where we count each X and X^{-1} as one occurrence of X.

Fact

We only need to consider quadratic equations where every variable appears exactly twice.

Proof.

Suppose: X has one occurrence in w (i. e. $w = uX^{\varepsilon}v$ for $\varepsilon \in \{-1, 1\}$).
Then: $\sigma(w) = 1 \iff \sigma(X)^{\varepsilon} = \sigma(u^{-1}v^{-1})$ and we always have a solution. $\square$

A Normal Form for Quadratic Equations

Proposition (Comerford, Edmunds 1981 (?))

Every quadratic equation $w = 1$ can be normalized into one of following three forms:

1. $\prod_{i=1}^{\ell} Z_i c_i Z_i^{-1} = 1$ "spherical form"
2. $\prod_{j=1}^{d} [X_j, Y_j] \prod_{i=1}^{\ell} Z_i c_i Z_i^{-1} = 1$ "orientable form"
3. $\prod_{j=1}^{d} Y_j^2 \prod_{i=1}^{\ell} Z_i c_i Z_i^{-1} = 1$ "nonorientable form"

(for constants $c_i \in G$)

In fact: The normal form can be efficiently computed.

Goal

Theorem (Dong, Pernak, W.; WIP)

$\textsc{QuadraticDP}_1$ *is decidable in every (restricted) wreath product of abelian groups A and B.*

Theorem (Ushakov, Weiers; 2025)

$\textsc{OrientableQuadraticDP}_1$ *is decidable in every $A \wr B$.*

Proposition

The problem

Constant: any group $A \wr B$ for abelian groups A and B

Input: a nonorientable equation $\prod_{s=1}^{S} Y_s \prod_{k=1}^{K} Z_k c_k Z_k^{-1} = 1$ for $c_k \in A \wr B$

Question: does it have a solution?

is decidable.

Lamplighter Group and Friends

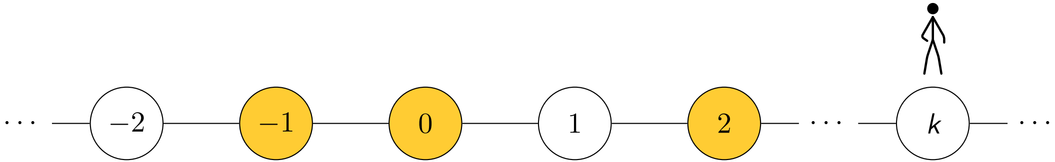
We will solve spherical equations in groups of the form $A \wr B$ where A and B are abelian groups.

For this: We need two views:

1. the geometric view and
2. a view based on rings/Laurent polynomials.

We will start with the classic lamplighter group $L_2 = \mathbb{Z}/2\mathbb{Z} \wr \mathbb{Z}$.

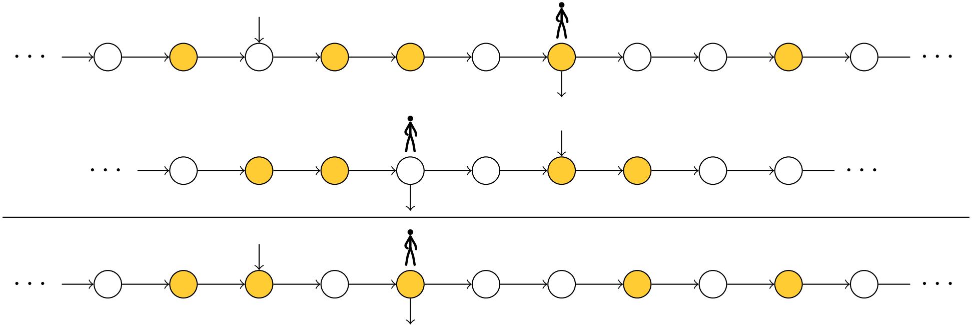
Elements of the Lamplighter Group



An element of the lamplighter group is represented by

- an bi-infinite chain of lamps where
- almost all lamps are off but
- a finite set of lamps may be on and by
- the location of the lamplighter.

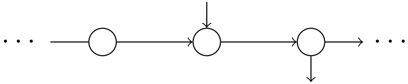
The Product in the Lamplighter Group



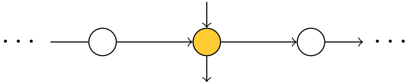
- Consider the first group element.
- Move the 0-lamp of the second element to the lamplighter of the first one.
- Pointwisely, perform an exclusive or.
- Use the position of the lamplighter in the second element.

Generators of the Lamplighter Group

The lamplighter group is generated by the following two elements:

$t =$ 

"move the lamplighter"

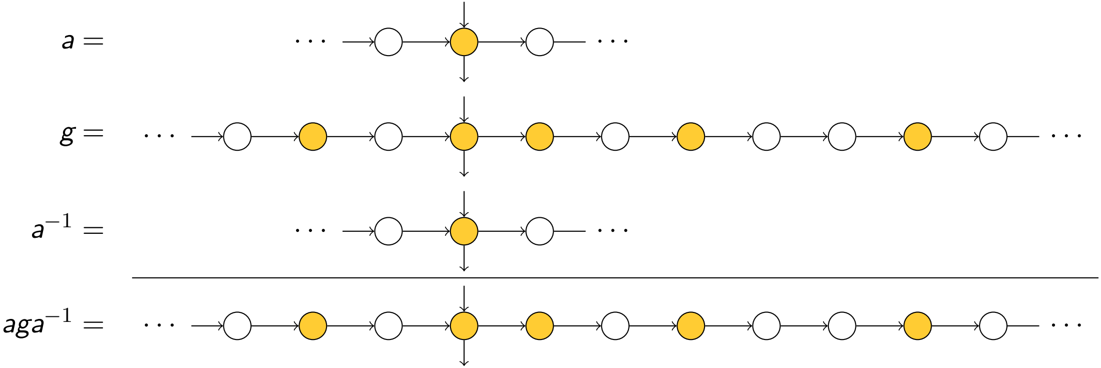
$a =$ 

"toggle the current lamp"

In fact: $L_2 = \langle a, t \mid a^2 = 1, [a, t^\ell a t^{-\ell}] = 1, \ell \in \mathbb{Z} \rangle$.

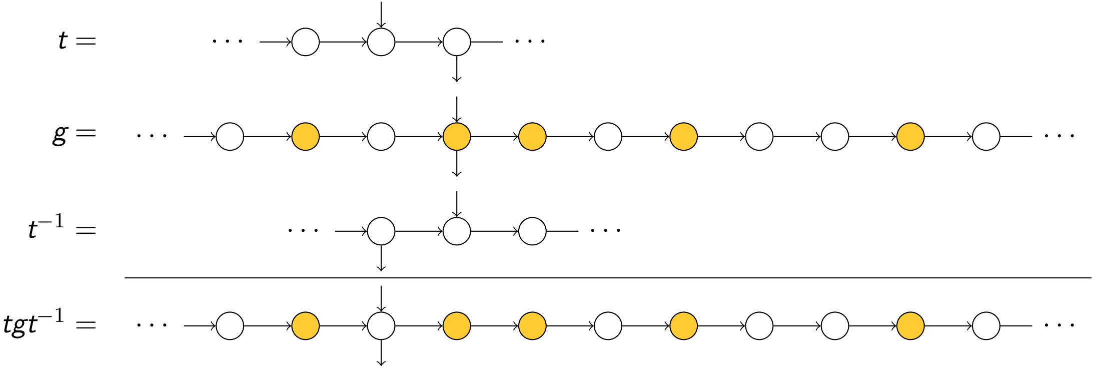
Conjugacy in the Lamplighter Group

- Consider an element g with the lamplighter at 0.
- Conjugate it with $a \rightsquigarrow$ invariant
- Conjugate it with $t \rightsquigarrow$ lamp configuration is translated

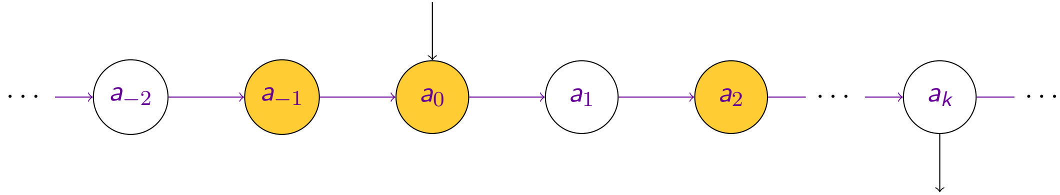


Conjugacy in the Lamplighter Group

- Consider an element g with the lamplighter at 0.
- Conjugate it with $a \rightsquigarrow$ invariant
- Conjugate it with $t \rightsquigarrow$ lamp configuration is translated



Generalized Lamplighter Groups



- Instead of on/off values, we may use values $a_i \in A$.
  The pointwise product then is the product of A.
- The underlying graph is the Cayley graph of $\mathbb{Z} = \langle x \rangle$ and we may replace it by the Cayley graph of B.

$\operatorname{supp} f = \{b \in B \mid f(b) \neq 0\}$

We obtain: functions $B \to A$ with finite support and
an element of B as the lamplighter position

Abelian Groups as Rings

Fact

A: abelian group of rank $r = r_1 + r_2$
Then: $A = \prod_{i=1}^{r_1} \mathbb{Z}/m_i\mathbb{Z} \times \mathbb{Z}^{r_2}$ forms a commutative ring with

$$\mathbb{0}_A = \big(0 + m_1\mathbb{Z}, \ldots, 0 + m_{r_1}\mathbb{Z}, \underbrace{0, \ldots, 0}_{r_2 \text{ many}}\big) \text{ and}$$

$$\mathbb{1}_A = \big(1 + m_1\mathbb{Z}, \ldots, 1 + m_{r_1}\mathbb{Z}, \underbrace{1, \ldots, 1,}_{r_2 \text{ many}}\big)$$

where A is the additive group.

This allows us to define the ring of Laurent polynomials in multiple variables over A...

Laurent Polynomials

Definition (Laurent Polynomial)

Let $\boldsymbol{X} = \{X_1, \dots, X_d\}$ be a set of polynomial variables.
For $\boldsymbol{v} = (v_1, \dots, v_d) \in \mathbb{Z}^d$, write

$$\boldsymbol{X}^{\boldsymbol{v}} = X_1^{v_1} \dots X_d^{v_d}.$$

We let the X_i commute and get $\boldsymbol{X}^{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{v}} = \boldsymbol{X}^{\boldsymbol{u}+\boldsymbol{v}}$.

A Laurent polynomial over A in $\boldsymbol{X}$ is a formal sum

$$\sum_{\boldsymbol{v} \in \mathbb{Z}^d} a_{\boldsymbol{v}} \boldsymbol{X}^{\boldsymbol{v}} \quad \text{where almost all } a_{\boldsymbol{v}} \in A \text{ are } \mathbb{0}_A.$$

The set of all Laurent polynomials is $A[\boldsymbol{X}^{\pm 1}]$.

The Ring of Laurent Polynomials

Definition

The Laurent polynomials over A form the ring $A[\boldsymbol{X}^{\pm 1}]$ with

$$\Big(\sum_{\boldsymbol{v}\in\mathbb{Z}^d} a_{\boldsymbol{v}}\boldsymbol{X}^{\boldsymbol{v}}\Big) + \Big(\sum_{\boldsymbol{v}\in\mathbb{Z}^d} a'_{\boldsymbol{v}}\boldsymbol{X}^{\boldsymbol{v}}\Big) = \sum_{\boldsymbol{v}\in\mathbb{Z}^d} (a_{\boldsymbol{v}} + a'_{\boldsymbol{v}})\boldsymbol{X}^{\boldsymbol{v}} \quad \text{and}$$

$$\Big(\sum_{\boldsymbol{u}\in\mathbb{Z}^d} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}}\Big) \cdot \Big(\sum_{\boldsymbol{v}\in\mathbb{Z}^d} a'_{\boldsymbol{v}}\boldsymbol{X}^{\boldsymbol{v}}\Big) = \sum_{\boldsymbol{u}\in\mathbb{Z}^d} \Big(\sum_{\boldsymbol{v}\in\mathbb{Z}^d} a_{\boldsymbol{u}-\boldsymbol{v}} a'_{\boldsymbol{v}}\Big)\boldsymbol{X}^{\boldsymbol{u}}.$$

We have

$$\mathbb{0} = \sum_{\boldsymbol{b}\in\mathbb{Z}^d} \mathbb{0}_A \boldsymbol{X}^{\boldsymbol{b}} \quad \text{and}$$

$$\mathbb{1} = \mathbb{1}_A\, \boldsymbol{X}^{\boldsymbol{0}}.$$

We write

$$a = a\, \boldsymbol{X}^{\boldsymbol{0}} \quad \text{and}$$

$$X_i = \mathbb{1}_A\, X_i^{\boldsymbol{1}}.$$

Functions $\mathbb{Z}^d \to A$ with finite support and Laurent Polynomials

- Let $A^{(\mathbb{Z}^d)}$ the set of functions $\mathbb{Z}^d \to A$ with finite support.
- We turn $A^{(\mathbb{Z}^d)}$ into an abelian group using pointwise sum.

Fact

There is a natural additive group isomorphism

$$\begin{aligned} A^{(\mathbb{Z}^d)} &\to A[\boldsymbol{X}^{\pm 1}] \\ f &\mapsto \sum_{\boldsymbol{v} \in \mathbb{Z}^d} f(\boldsymbol{v}) \boldsymbol{X}^{\boldsymbol{v}}. \end{aligned}$$

Abelian Groups and Lattices

Definition

A lattice is a finitely generated additive subgroup of $\mathbb{Z}^d$

Note: We may write any abelian group B of rank d as $B = \mathbb{Z}^d / L$ for some lattice L.

Definition

Every lattice L generates an ideal $\mathscr{I}(L) = \langle \boldsymbol{X}^{\ell} - \mathbb{1} \mid \ell \in L \rangle \subseteq A[\boldsymbol{X}^{\pm 1}]$.

Theorem

Let $L = \langle \ell_1, \ldots, \ell_n \rangle \subseteq \mathbb{Z}^d$
Then: $\mathscr{I}(L) = \langle \boldsymbol{X}^{\ell_1} - \mathbb{1}, \ldots, \boldsymbol{X}^{\ell_n} - \mathbb{1} \rangle \subseteq A[\boldsymbol{X}^{\pm 1}]$

"The generating set suffices to obtain the entire ideal."

Abelian Groups and Lattices

Of course: We may view a lattice as an extended lattice!

Definition

An extended lattice is a finitely generated additive subgroup of $\mathbb{Z}^d \times \mathbb{Z}/2\mathbb{Z}$

Note: We may write any abelian group B of rank d as $B = \mathbb{Z}^d/L$ for some lattice L.

Definition

Every extended lattice $\hat{L}$ generates an ideal $\mathscr{I}(L) = \langle \boldsymbol{X}^{\boldsymbol{\ell}} - (-\mathbb{1})^{\sigma} \mid (\boldsymbol{\ell}, \sigma) \in \hat{L} \rangle \subseteq A[\boldsymbol{X}^{\pm 1}]$.

Theorem

Let $L = \langle (\boldsymbol{\ell}_1, \sigma_1), \ldots, (\boldsymbol{\ell}_n, \sigma_n) \rangle \subseteq \mathbb{Z}^d \times \mathbb{Z}/2\mathbb{Z}$
Then: $\mathscr{I}(L) = \langle \boldsymbol{X}^{\boldsymbol{\ell}_1} - (-\mathbb{1})^{\sigma_1}, \ldots, \boldsymbol{X}^{\boldsymbol{\ell}_n} - (-\mathbb{1})^{\sigma_n} \rangle \subseteq A[\boldsymbol{X}^{\pm 1}]$

"The generating set suffices to obtain the entire ideal."

Acting on Laurent Polynomials

Recall: $\mathscr{I}(L) = \langle \boldsymbol{X}^{\ell} = \mathbb{1} \mid \ell \in L \rangle$

The additive group $\mathbb{Z}^d/L = B$ acts on $A[\boldsymbol{X}^{\pm 1}]/\mathscr{I}(L)$:

$\boldsymbol{v} + L \in \mathbb{Z}^d/L$ acts on $f + \mathscr{I}(L) \in A[\boldsymbol{X}^{\pm 1}]/\mathscr{I}(L)$ by $\boldsymbol{X}^{\boldsymbol{v}} f + \mathscr{I}(L)$

This is well-defined: Consider a different representative $\boldsymbol{v} + \boldsymbol{\ell}$. We have:

$$\boldsymbol{X}^{\boldsymbol{v}+\boldsymbol{\ell}} f = \boldsymbol{X}^{\boldsymbol{v}} \underbrace{\boldsymbol{X}^{\boldsymbol{\ell}}}_{=\mathbb{1}} f = \boldsymbol{X}^{\boldsymbol{v}} f \quad \text{in } A[\boldsymbol{X}^{\pm 1}]/\mathscr{I}(L)$$

Again: Lamplighter Groups

Now: $B = \mathbb{Z}^d/L$ acts on $A[\boldsymbol{X}^{\pm 1}]/I$ for $I = \mathscr{I}(L)$ as a group and we may define

$$A[\boldsymbol{X}^{\pm 1}]/I \rtimes \mathbb{Z}^d/L \text{ via } (f + I, \boldsymbol{b} + L) \cdot (g + I, \boldsymbol{c} + L) = (f + \boldsymbol{X}^{\boldsymbol{b}} \cdot g + I, \boldsymbol{b} + \boldsymbol{c} + L).$$

Fact

$$A \wr B \simeq A[\boldsymbol{X}^{\pm 1}]/I \rtimes \mathbb{Z}^d/L$$

Idea:

- f and g are lamp configurations.
- $\boldsymbol{b}$ and $\boldsymbol{c}$ mark the position of the lamplighter.
- Note: g gets shifted by $\boldsymbol{X}^{\boldsymbol{b}}$.

Solving Nonorientable Equations

Magic Lemma 1

$$g_k \in A[\boldsymbol{X}^{\pm 1}],\ \operatorname{supp} g_k \subseteq [-D, D]^d, \quad \boldsymbol{m}_k \in \mathbb{Z}^d$$

$$\prod_{s=1}^{S} Y_s^2 \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, \mathbf{0}) \text{ has a solution in } A[\boldsymbol{X}^{\pm 1}]/\langle \boldsymbol{X}^L = \mathbb{1} \rangle \rtimes \mathbb{Z}^d/L$$

$$\iff \exists \boldsymbol{n}_1, \ldots, \boldsymbol{n}_S \in \mathbb{Z}^d :$$

$$\prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, \sum_{s=1}^{S} 2\boldsymbol{n}_s) \text{ has a solution in } A[\boldsymbol{X}^{\pm 1}]/\langle \boldsymbol{X}^L = \mathbb{1}, \boldsymbol{X}^{\boldsymbol{n}_s} = -\mathbb{1} \rangle \rtimes \mathbb{Z}^d/L$$

Lemma (Magic Lemma 1)

$I \supseteq \mathscr{I}(L)$: *ideal of* $A[\boldsymbol{X}^{\pm 1}]$, $\quad w \in (A \wr B) \star F(\mathbb{X} \setminus \{Y\})$

Then: $Y^2 w = (\mathbb{0}, \mathbf{0})$ *has a solution in* $A[\boldsymbol{X}^{\pm 1}]/I \rtimes \mathbb{Z}^d/L$

$\iff \exists \boldsymbol{n} \in \mathbb{Z}^d : \quad w = (\mathbb{0}, 2\boldsymbol{n})$ *has a solution in* $A[\boldsymbol{X}^{\pm 1}]/\langle I, \boldsymbol{X}^{\boldsymbol{n}} + \mathbb{1} \rangle \rtimes \mathbb{Z}^d/L$

Idea: $\quad (f, \boldsymbol{n})^2 = (f, \boldsymbol{n})\,(f, \boldsymbol{n}) = (f + \boldsymbol{X}^{\boldsymbol{n}} f, 2\boldsymbol{n}) = \big(f(\mathbb{1} + \boldsymbol{X}^{\boldsymbol{n}}), 2\boldsymbol{n}\big)$

Magic Lemma 2

$$\exists \boldsymbol{n}_1, \ldots, \boldsymbol{n}_S : \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, \sum_{s=1}^{S} 2\boldsymbol{n}_s) \text{ sol. in } A[\boldsymbol{X}^{\pm 1}]/\langle \boldsymbol{X}^L = -\boldsymbol{X}^{\boldsymbol{n}_s} = \mathbb{1} \rangle \rtimes \mathbb{Z}^d/L$$

Lemma (Magic Lemma 2)

$I \supseteq \mathscr{I}(L)$: ideal of $A[\boldsymbol{X}^{\pm 1}]$ The above has a solution in $A[\boldsymbol{X}^{\pm 1}]/\langle I, \boldsymbol{X}^{\boldsymbol{n}_s} = -\mathbb{1} \rangle \rtimes \mathbb{Z}^d/L \iff$

$$\exists \boldsymbol{n} \in \mathbb{Z}^d : \sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n} \text{ in } \mathbb{Z}^d/L$$

$$\& \; \exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} \in \mathbb{Z}^d : \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, 2\boldsymbol{n})$$

$$\text{sol. in } A[\boldsymbol{X}^{\pm 1}]/\langle I, \boldsymbol{X}^{\boldsymbol{n}'_s} = -\mathbb{1}, \boldsymbol{X}^{\boldsymbol{n}} = -(-\mathbb{1})^S \rangle \rtimes \mathbb{Z}^d/L$$

Result After Magic Lemma 2

$$\exists \boldsymbol{n} : \sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n} \text{ in } \mathbb{Z}^d/L$$

$$\& \; \exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} : \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, 2\boldsymbol{n})$$

$$\text{has sol. in } A[\boldsymbol{X}^{\pm 1}]/\langle \boldsymbol{X}^L = -\boldsymbol{X}^{\boldsymbol{n}'_s} = (-\mathbb{1})^{S+1}\boldsymbol{X}^{\boldsymbol{n}} = \mathbb{1} \rangle \rtimes \mathbb{Z}^d/L$$

We may swap quantifiers:

$$\exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} \exists \boldsymbol{n} : \sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n} \text{ in } \mathbb{Z}^d/L \text{ and } \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, 2\boldsymbol{n}) \text{ has sol.}$$

Magic Lemma 3

$$\exists \boldsymbol{n}_1', \ldots, \boldsymbol{n}_{S-1}' \exists \boldsymbol{n} : \sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n} \text{ in } \mathbb{Z}^d/L \text{ and } \prod_{k=1}^{K} Z_k(g_k, \overset{\mathbf{0}}{\cancel{\boldsymbol{m}_k}}) Z_k^{-1} = (\mathbb{0}, \overset{\mathbf{0}}{\cancel{2\boldsymbol{n}}}) \text{ has sol. in}$$

$\boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1}$ by Magic Lemma 4

$$A[\boldsymbol{X}^{\pm 1}]/\langle \boldsymbol{X}^L = -\boldsymbol{X}^{\boldsymbol{n}_s'} = (-\mathbb{1})^{S+1}\boldsymbol{X}^{\boldsymbol{n}} = \mathbb{1}\rangle \rtimes \mathbb{Z}^d/\cancel{L}$$

Lemma (Magic Lemma 3)

$I \supseteq \mathscr{I}(L)$: ideal of $A[\boldsymbol{X}^{\pm 1}]$ Then:

$$\prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, \boldsymbol{c}) \textit{ sol. in } A[\boldsymbol{X}^{\pm 1}]/I \rtimes \mathbb{Z}^d/L$$

$$\iff \sum_{k=1}^{K} \boldsymbol{m}_k = \boldsymbol{c} \textit{ in } \mathbb{Z}^d/L \textit{ and } \prod_{k=1}^{K} Z_k(g_k, \mathbf{0}) Z_k^{-1} = (\mathbb{0}, \mathbf{0}) \textit{ sol. in } A[\boldsymbol{X}^{\pm 1}]/\langle I, \boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1}\rangle \rtimes \mathbb{Z}^d/L$$

Where are we now?

$\exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} \exists \boldsymbol{n}:$

1. $\sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n}$ in $\mathbb{Z}^d / L$ and
2. $\prod_{k=1}^{K} Z_k(g_k, \mathbf{0}) Z_k^{-1} = (\mathbb{0}, \mathbf{0})$ has sol. in $A[\boldsymbol{X}^{\pm 1}] / \langle \boldsymbol{X}^L = -\boldsymbol{X}^{\boldsymbol{n}'_s} = (-\mathbb{1})^{S+1} \boldsymbol{X}^{\boldsymbol{n}} = \boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1} \rangle \rtimes \mathbb{Z}^d$

Recall: "Lamplighter at origin $\implies$ conjugation is translation"

Fact

$$\prod_{k=1}^{K} Z_k(g_k, \mathbf{0}) Z_k^{-1} = (\mathbb{0}, \mathbf{0}) \text{ has a solution in } A[\boldsymbol{X}^{\pm 1}]/I \rtimes \mathbb{Z}^d$$

any ideal

$$\iff \exists \boldsymbol{\kappa}_1, \ldots, \boldsymbol{\kappa}_K \in \mathbb{Z}^d : \sum_{k=1}^{K} \boldsymbol{X}^{\boldsymbol{\kappa}_k} g_k = \mathbb{0} \text{ in } A[\boldsymbol{X}^{\pm 1}]/I$$

Some Combinatorics

$\exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} \exists \boldsymbol{n} :$ ❶ $\sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n}$ in $\mathbb{Z}^d / L$ and

❷ $\exists \boldsymbol{\kappa}_1, \ldots, \boldsymbol{\kappa}_K \in \mathbb{Z}^d : \sum_{k=1}^{K} \boldsymbol{X}^{\boldsymbol{\kappa}_k} g_k = \mathbb{0}$ in $A[\boldsymbol{X}^{\pm 1}] / \langle \boldsymbol{X}^L = -\boldsymbol{X}^{\boldsymbol{n}'_s} = (-\mathbb{1})^{S+1} \boldsymbol{X}^{\boldsymbol{n}} = \boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1} \rangle$

Observation: We may move along the lattice $\langle L, \boldsymbol{n}'_s, \boldsymbol{n}, \boldsymbol{m}_k \rangle$ to make the $\boldsymbol{\kappa}_k$ "small"

But: sometimes this creates a $-\mathbb{1}$!

Lemma (Magic Lemma 5)

$L \subseteq \mathbb{Z}^d \times \mathbb{Z}/2\mathbb{Z}$: extended lattice with $\exists \ell : (\ell, 1) \in L$ $\quad g_k \in A[\boldsymbol{X}^{\pm 1}]$ with $\operatorname{supp} g_k \subseteq [-D, D]^d$

Then: $\exists \boldsymbol{\kappa}_1, \ldots, \boldsymbol{\kappa}_K \in \mathbb{Z}^d : \sum_{k=1}^{K} \boldsymbol{X}^{\boldsymbol{\kappa}_k} g_k = \mathbb{0}$ *in* $A[\boldsymbol{X}^{\pm 1}] / \mathscr{I}(L)$

$$\iff \begin{matrix} \exists \boldsymbol{\kappa}'_1, \ldots, \boldsymbol{\kappa}'_K \in [-2KD, 2KD]^d \\ \exists \sigma_1, \ldots, \sigma_K \in \{\pm \mathbb{1}\} \end{matrix} : \sum_{k=1}^{K} \sigma_k \boldsymbol{X}^{\boldsymbol{\kappa}'_k} g_k = \mathbb{0} \text{ in } A[\boldsymbol{X}^{\pm 1}] / \mathscr{I}(L)$$

The Final Result

Summing up and re-ordering quantifiers, we get:

$g_k \in A[\boldsymbol{X}^{\pm 1}]$, $\operatorname{supp} g_k \subseteq [-D, D]^d$, $\quad \boldsymbol{m}_k \in \mathbb{Z}^d$

$$\prod_{s=1}^{S} Y_s^2 \prod_{k=1}^{K} Z_k(g_k, \boldsymbol{m}_k) Z_k^{-1} = (\mathbb{0}, \boldsymbol{0}) \text{ has a solution in } A \wr B$$

$$\iff \boxed{\exists \boldsymbol{\kappa}'_1, \ldots, \boldsymbol{\kappa}'_K \in [-2KD, 2KD]^d \; \exists \sigma_1, \ldots, \sigma_K \in \{\pm \mathbb{1}\}} :$$

finitely many values!

$$\exists \boldsymbol{n} : \; ① \boxed{\sum_{k=1}^{K} \boldsymbol{m}_k = 2\boldsymbol{n} \text{ in } \mathbb{Z}^d / L} \; \cancel{\text{and}}$$

we can check this/find $\boldsymbol{n}$

$$② \; \exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} : \sum_{k=1}^{K} \sigma_k \boldsymbol{X}^{\boldsymbol{\kappa}'_k} g_k = \mathbb{0} \text{ in } A[\boldsymbol{X}^{\pm 1}] / \left(\langle \boldsymbol{X}^L = (-\mathbb{1})^{S+1} \boldsymbol{X}^{\boldsymbol{n}} = \boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1} \rangle + \langle \boldsymbol{X}^{\boldsymbol{n}'_s} = -\mathbb{1} \rangle \right)$$

???

We may treat everything except the $\boldsymbol{n}'_s$ as constants!

The Last Ingredient

$$\exists \boldsymbol{n}'_1, \ldots, \boldsymbol{n}'_{S-1} : \sum_{k=1}^{K} \sigma_k \boldsymbol{X}^{\boldsymbol{\kappa}'_k} g_k = \mathbb{0} \text{ in } A[\boldsymbol{X}^{\pm 1}]/(\langle \boldsymbol{X}^L = (-\mathbb{1})^{S+1} \boldsymbol{X}^{\boldsymbol{n}} = \boldsymbol{X}^{\boldsymbol{m}_k} = \mathbb{1} \rangle + \langle \boldsymbol{X}^{\boldsymbol{n}'_s} = -\mathbb{1} \rangle)$$

Proposition

The problem

Input: $f \in A[\boldsymbol{X}^{\pm 1}]$,
L: extended lattice and
$R \in \mathbb{N}$

Question: $\exists \boldsymbol{k}_1, \ldots, \boldsymbol{k}_R \in \mathbb{Z}^d : f = \mathbb{0}$ in $A[\boldsymbol{X}^{\pm 1}]/(\mathscr{I}(L) + \langle \boldsymbol{X}^{\boldsymbol{k}_i} = -\mathbb{1} \rangle)$?

is decidable.

Thank you!