Submonoid Membership in n-dimensional lamplighter groups and S-unit equations

Ruiwen Dong ✉ 📵
Department of Mathematics, Saarland University, Germany
Magdalen College, University of Oxford, United Kingdom

---- **Abstract** ----

We show that Submonoid Membership is decidable in n-dimensional lamplighter groups $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ for any prime p and integer n. More generally, we show decidability of Submonoid Membership in semidirect products of the form $\mathcal{Y} \rtimes \mathbb{Z}^n$, where $\mathcal{Y}$ is any finitely presented module over the Laurent polynomial ring $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$. Combined with a result of Shafrir (2024), this gives the first example of a group G and a finite index subgroup $\widetilde{G} \leq G$, such that Submonoid Membership is decidable in $\widetilde{G}$ but undecidable in G.

To obtain our decidability result, we reduce Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ to solving S-unit equations over $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-modules. We show that the solution set of such equations is effectively p-automatic, extending a result of Adamczewski and Bell (2012). As an intermediate result, we also obtain that the solution set of the Knapsack Problem in $\mathcal{Y} \rtimes \mathbb{Z}^n$ is effectively p-automatic.

1 Introduction

Algorithmic problems in infinite groups

Algorithmic problems concerning groups are a classical topic in algebra and theoretical computer science. Dating back to the work of Max Dehn from the 1910s, this area has traditionally served as a bridge between geometry, algebra and logic, and has now found numerous applications in automata theory, program analysis and complexity theory [7, 9, 14, 23]. One of the central decision problems on groups is the *Submonoid Membership* problem: given a finite number of elements $g_1, g_2, \ldots, g_k$ in a group G and an element $g \in G$, does g belong to the submonoid generated by $g_1, g_2, \ldots, g_k$? In the seminal work of Markov from the 1950s [31], it was shown that Submonoid Membership is undecidable for a matrix group of dimension six. The undecidability result was later strengthened to the group $\mathsf{SL}(4, \mathbb{Z})$ of 4×4 integer matrices of determinant one [32]. Subsequently, a number of positive decidability results were obtained, such as for commutative matrix groups [2], low-dimensional matrix groups [12, 34], and certain graph groups [27]. See [16, 26] for recent surveys.

A generalization of Submonoid Membership is the *Rational Subset Membership* problem: given a rational subset S of a group G and an element $g \in G$, does g belong to S? Here, a

subset S of a group G is called a *rational subset* if there is a finite alphabet Σ, a monoid homomorphism $\varphi\colon \Sigma^* \to G$, and a regular language $L \subseteq \Sigma^*$, such that $\varphi(L) = S$. In particular, if $L = \Sigma^*$, then we recover the definition of Submonoid Membership. In fact, many decidability results for Submonoid Membership are also proven for the more general Rational Subset Membership, such as in free groups [8], abelian groups [21], and certain wreath products [29]. Nevertheless, Bodart [10] and Shafrir[1] recently provided examples of groups with undecidable Rational Subset Membership but decidable Submonoid Membership.

A longstanding open problem in computational group theory is whether decidability of Submonoid Membership is preserved under finite extension of groups. Grunschlag [21] showed that for any group G and a finite index subgroup $\widetilde{G} \le G$, *Rational Subset Membership* is decidable in $\widetilde{G}$ if and only if it is decidable in G. The same statement is also true for the *Subgroup Membership* problem [21] (given $g_1, g_2, \ldots, g_k, g$, does g belong to the subgroup generated by $g_1, g_2, \ldots, g_k$?). Whether the same holds for *Submonoid Membership* remained open. One of the goals of this paper is to construct a counterexample to this open problem: we construct a group G and a finite index subgroup $\widetilde{G} \le G$, such that Submonoid Membership is decidable in $\widetilde{G}$ but undecidable in G.

n-dimensional lamplighter groups

In this paper, we study Submonoid Membership in *n-dimensional lamplighter groups* as well as their generalizations. The lamplighter groups are well-studied objects in the context of geometric group theory [20, 39]. Given an integer $p \ge 2$ and $n \in \mathbb{N}$, the *n*-dimensional lamplighter group, denoted $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$, can be most easily defined as the (multiplicative) 2×2 upper-triangular matrix group

$$\left\{ \begin{pmatrix} X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} & f \\ 0 & 1 \end{pmatrix} \;\middle|\; a_1, a_2, \ldots, a_n \in \mathbb{Z}, \; f \in (\mathbb{Z}/p\mathbb{Z})[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}] \right\}, \quad (1)$$

where $(\mathbb{Z}/p\mathbb{Z})[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}]$ is the Laurent polynomial ring over n variables, with coefficients in the finite ring $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$. When p is prime, $\mathbb{Z}/p\mathbb{Z}$ is actually the finite field $\mathbb{F}_p$. Intuitively, an element in $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ can be understood as the following configuration: at each position in the lattice $\mathbb{Z}^n$ there is a *lamp*, each lamp has a *state* among $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$, and there is a *pointer* at some position in $\mathbb{Z}^n$. In particular, for the element $\begin{pmatrix} X_1^{a_1} \cdots X_n^{a_n} & f \\ 0 & 1 \end{pmatrix}$, the pointer is at position $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, the lamp at position $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ has state s if the monomial $X_1^{z_1} \cdots X_n^{z_n}$ appearing in f has coefficient s. In particular, all but finitely many lamps have state 0. Multiplication in the group $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$, like matrix multiplication, corresponds to first moving the pointer by a vector $(a_1, \ldots, a_n)$, then additively changing the states of the lamps around the new location.

Owing to this geometric interpretation, the study of lamplighter groups has close connections to automata theory, tiling problems, random walks, and graph theory [3, 4, 24, 28, 30]. Lamplighter groups are also important examples of *metabelian groups*, which are some of the most tractable generalization of abelian groups. Recall that a group G is called *metabelian* if it admits a normal subgroup A such that both A and G/A are abelian. An important amount of research in computational group theory concentrates on metabelian groups, since decision problems in abelian groups are already well-understood. For example, Cadilhac, Chistikov and Zetzsche [11] showed decidability of Rational Subset Membership in the *Baumslag-Solitar*

---

[1] An example appeared in the Bachelor's thesis of Potthast [35], based on an unpublished draft of Shafrir.

groups $\mathsf{BS}(1, p)$; Lohrey, Steinberg and Zetzsche [28] showed decidability of Rational Subset Membership in 1-dimensional lamplighter groups. On the other hand, the 2-dimensional lamplighter groups occupy an interesting position as they have undecidable Rational Subset Membership [28] but decidable Submonoid Membership [35]. The decision algorithm in [35] cannot be generalized to dimensions larger than 2 as it relies on a reduction to Rational Subset Membership in dimension 1. It is thus left as an open problem whether Submonoid Membership is decidable in lamplighter groups of dimension $n \geq 3$.

Contributions of this paper

In this paper, we show that Submonoid Membership is decidable in lamplighter groups $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ of every dimension $n \in \mathbb{N}$ and *prime p*. In fact, we prove a much more general result (Theorem 3.1): Submonoid Membership is decidable for semidirect products $\mathcal{Y} \rtimes \mathbb{Z}^n$, where $\mathcal{Y}$ is a finitely presented module over the Laurent polynomial ring $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$.

An important consequence of the more general Theorem 3.1 is the resolution of a longstanding open problem (Corollary 3.2). Combined with a recent result of Shafrir [38], we show that there exist a group G and a finite index subgroup $\widetilde{G} \leq G$, such that Submonoid Membership decidable in $\widetilde{G}$ but undecidable in G.

Our main strategy to decide Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ is to reduce it to solving *S-unit equations* over modules: these are equations of the form $x_1 c_1 + x_2 c_2 + \cdots + x_m c_m = c_0$, where the variables x_i take value in a multiplicative subgroup of a commutative ring. We show that the solutions of such S-unit equations over an $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-module forms an effectively *p*-automatic set (Theorem 3.3), generalizing a result of Adamczewski and Bell [1] (see also the independent work of Derksen and Masser [15] for a similar result). As an intermediate result, we also obtain effective *p*-automaticity for the solution set of the *Knapsack Problem* in $\mathcal{Y} \rtimes \mathbb{Z}^n$: given $g_1, g_2, \ldots, g_k, g \in \mathcal{Y} \rtimes \mathbb{Z}^n$, find $(z_1, \ldots, z_k) \in \mathbb{Z}^k$ such that $g_1^{z_1} g_2^{z_2} \cdots g_k^{z_k} = g$. We give an example (Example 4.8) where the solution set is *p*-automatic but not semilinear. This shows that the situation in semidirect products is much more complicated than in the wreath product of two abelian groups, as seen in the work of Ganardi, König, Lohrey, and Zetzsche [19].

Note that our decidability results heavily rely on working over the finite ring $\mathbb{Z}/p\mathbb{Z}$ instead of the infinite ring $\mathbb{Z}$. Indeed, Submonoid Membership is known to be undecidable [29] in $\mathbb{Z} \wr \mathbb{Z}^n$ for $n \geq 1$, and solving S-unit equations over $\mathbb{Z}[X_1^{\pm}]$-modules is also known to be undecidable [17]. Nevertheless, it is not clear whether the decidability for $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ can be generalized to non-prime numbers p, for example when $p = p_1 p_2$ for two primes $p_1 \neq p_2$. This is closely related to deciding emptiness of the intersection of a p_1-automatic set and a p_2-automatic set, which to the best of our knowledge remains an open problem (however, see [22, 25] for recent progress). Progress towards a solution for non-prime p will also be the first step towards a classification of metabelian groups with decidable Submonoid Membership, namely by tackling those with torsion commutators.

2 Preliminaries

Laurent polynomial ring and modules

Let p be a prime number, denote by $\mathbb{F}_p$ the finite field of size p. Denote by $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$ the Laurent polynomial ring over $\mathbb{F}_p$ with n variables: this is the set of polynomials over the variables $X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}$, with coefficients in $\mathbb{F}_p$, such that $X_i X_i^{-1} = 1$ for all i. When n is fixed, we denote by $\overline{X}$ the tuple of variables $(X_1, \ldots, X_n)$, and $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$

is written in short as $\mathbb{F}_p[\overline{X}^{\pm}]$.

For a vector $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, denote by $\overline{X}^{\boldsymbol{a}}$ the monomial $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$. When Λ is a subgroup of $\mathbb{Z}^n$, we denote by $\mathbb{F}_p[\overline{X}^{\Lambda}] \subseteq \mathbb{F}_p[\overline{X}^{\pm}]$ the subring of polynomials of the form $\sum_{\boldsymbol{a} \in \Lambda} c_{\boldsymbol{a}} \overline{X}^{\boldsymbol{a}}$.

Since we work in polynomial rings over a finite field $\mathbb{F}_p$, it is worth pointing out a useful equation, folklorishly dubbed "the freshman's dream". For any $f \in \mathbb{F}_p[\overline{X}^{\pm}]$, we have $(f+1)^p = f^p + 1$, and more generally $(f+1)^{p^k} = f^{p^k} + 1$ for all $k \in \mathbb{N}$.

When R is a commutative ring (such as $\mathbb{F}_p[\overline{X}^{\pm}]$), an R-*module* is defined as an abelian group $(M, +)$ along with an operation $\cdot : R \times M \to M$ satisfying $f \cdot (m + m') = f \cdot m + f \cdot m'$, $(f + g) \cdot m = f \cdot m + g \cdot m$, $fg \cdot m = f \cdot (g \cdot m)$ and $1 \cdot m = m$. For example, for any $d \in \mathbb{N}$, $\mathbb{F}_p[\overline{X}^{\pm}]^d$ is an $\mathbb{F}_p[\overline{X}^{\pm}]$-module by $f \cdot (h_1, \ldots, h_d) = (fh_1, \ldots, fh_d)$. We often use a bold symbol $\boldsymbol{h}$ to denote a vector $(h_1, \ldots, h_d) \in \mathbb{F}_p[\overline{X}^{\pm}]^d$.

Given elements $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_k$ in an R-module M, we say that they *generate* the R-module

$$\sum_{i=1}^{k} R \cdot \boldsymbol{h}_i := \left\{ \sum_{i=1}^{k} r_i \cdot \boldsymbol{h}_i \;\middle|\; r_1, \ldots, r_k \in R \right\} \subseteq M.$$

Given submodules M, M' of $\mathbb{F}_p[\overline{X}^{\pm}]^d$ such that $M \supseteq M'$, we define the quotient $M/M' := \{\overline{m} \mid m \in M\}$ where $\overline{m}_1 = \overline{m}_2$ if and only if $m_1 - m_2 \in M'$. This quotient is also an $\mathbb{F}_p[\overline{X}^{\pm}]$-module. We say that an $\mathbb{F}_p[\overline{X}^{\pm}]$-module $\mathcal{Y}$ is *finitely presented* if it can be written as a quotient $\mathbb{F}_p[\overline{X}^{\pm}]^d/M$ for a finitely generated submodule M of $\mathbb{F}_p[\overline{X}^{\pm}]^d$ for some $d \in \mathbb{N}$. We call a *finite presentation* of $\mathcal{Y}$ the generators of such M. Every finitely generated $\mathbb{F}_p[\overline{X}^{\pm}]$-module admits a finite presentation.

Given a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-module $\mathcal{Y}$, we can define the following group using *semidirect product*:

$$\mathcal{Y} \rtimes \mathbb{Z}^n := \{(y, \boldsymbol{a}) \mid y \in \mathcal{Y}, \boldsymbol{a} \in \mathbb{Z}^n\}; \tag{2}$$

multiplication and inversion in this group are defined by

$$(y, \boldsymbol{a}) \cdot (y', \boldsymbol{a}') = (y + \overline{X}^{\boldsymbol{a}} \cdot y', \boldsymbol{a} + \boldsymbol{a}'), \quad (y, \boldsymbol{a})^{-1} = (-\overline{X}^{-\boldsymbol{a}} \cdot y, -\boldsymbol{a}). \tag{3}$$

The neutral element of $\mathcal{Y} \rtimes \mathbb{Z}^n$ is $(0, \boldsymbol{0})$, where $\boldsymbol{0}$ denotes the zero vector in $\mathbb{Z}^n$. Intuitively, the element $(y, \boldsymbol{a})$ can be seen as a 2×2 matrix $\begin{pmatrix} \overline{X}^{\boldsymbol{a}} & y \\ 0 & 1 \end{pmatrix}$, where group multiplication is represented by matrix multiplication. We have the formula $(f, \boldsymbol{a})(y, \boldsymbol{0})(f, \boldsymbol{a})^{-1} = (\overline{X}^{\boldsymbol{a}} \cdot y, \boldsymbol{0})$. Note that $\mathcal{Y} \rtimes \mathbb{Z}^n$ naturally contains the subgroup $\mathcal{Y} \cong \{(y, \boldsymbol{0}) \mid y \in \mathcal{Y}\}$, and there is a projection map $\pi : \mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$, $(y, \boldsymbol{a}) \mapsto \boldsymbol{a}$, such that $\ker(\pi) = \mathcal{Y}$.

In particular, if we take $\mathcal{Y} = \mathbb{F}_p[\overline{X}^{\pm}]$ considered as a $\mathbb{F}_p[\overline{X}^{\pm}]$-module, then we recover the definition (1) of the n-dimensional lamplighter group $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$.

Effective computation in modules

In order to effectively compute in groups of the form $\mathcal{Y} \rtimes \mathbb{Z}^n$, we need to be able to effectively compute in the $\mathbb{F}_p[\overline{X}^{\pm}]$-module $\mathcal{Y}$. The following are some classic problems with effective algorithms that we will make use of. We state the following result over $\mathbb{F}_p[\overline{X}^{\pm}]$, although they hold over polynomial rings over any field.

▶ **Lemma 2.1** ([5, Lemma 2.1, 2.2]). *Let $\mathcal{Y}$ be an $\mathbb{F}_p[\overline{X}^{\pm}]$-module with a given finite presentation. The following problems are effectively solvable:*

   (i) *(Submodule Membership) Given elements $y_1, \ldots, y_k, y \in \mathcal{Y}$, decide whether y is in the submodule generated by $y_1, \ldots, y_k$.*

   (ii) *(Submodule Presentation) Given elements $y_1, \ldots, y_k \in \mathcal{Y}$, compute a finite presentation for the submodule generated by $y_1, \ldots, y_k$.*

   (iii) *(Computing intersection and sum) Given the generators of a submodule $A \subseteq \mathcal{Y}$ and the generators of a submodule $B \subseteq \mathcal{Y}$, compute the generators for the submodule $A \cap B$ and for the submodule $A + B = \{a + b \mid a \in A, b \in B\}$.*

   (iv) *(Computing quotient) Given the generators of a submodule $\mathcal{Y}' \subseteq \mathcal{Y}$, compute a finite presentation of the quotient $\mathcal{Y}/\mathcal{Y}'$.*

Let Λ be a subgroup of $\mathbb{Z}^n$, then any $\mathbb{F}_p[\overline{X}^{\pm}]$-module can be considered as a (possibly infinitely generated) $\mathbb{F}_p[\overline{X}^{\Lambda}]$-module. For example, the $\mathbb{F}_p[X_1^{\pm}, X_2^{\pm}]$-module $\mathbb{F}_p[X_1^{\pm}, X_2^{\pm}]$ can be considered as an $\mathbb{F}_p[X_1^{\pm}]$-module, but it is not finitely generated (it is generated by the infinite set $\{\ldots, X_2^{-2}, X_2^{-1}, 1, X_2, X_2^2, \ldots\}$). However, finitely generated $\mathbb{F}_p[\overline{X}^{\Lambda}]$-submodules of an $\mathbb{F}_p[\overline{X}^{\pm}]$-module are still effectively computable:

▶ **Lemma 2.2** ([5, Theorem 2.14] or [6, Theorem 2.6])**.** *Let Λ be a subgroup of $\mathbb{Z}^n$, and $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module. Given a finite subset S of $\mathcal{Y}$, one can effectively compute the finite presentation of the $\mathbb{F}_p[\overline{X}^{\Lambda}]$-module $\sum_{s \in S} \mathbb{F}_p[\overline{X}^{\Lambda}] \cdot s$.*

p-automatic sets

We recall the standard notion of *p-automatic subsets* of $\mathbb{Z}$, and more generally, *p*-automatic subsets of $\mathbb{Z}^d$.

Let Σ be a finite alphabet. An automaton over Σ is a tuple $\mathcal{A} = (Q, \Sigma, \delta, q_I, F)$, where Q is a finite set of states, $\delta \colon Q \times \Sigma \to Q$ is the transition function, q_I is the initial state, and $F \subseteq Q$ is the set of final states. For a state q in Q and for a finite word $w = w_1 w_2 \cdots w_n$ over the alphabet Σ, we define $\delta(q, w)$ recursively by $\delta(q, w) = \delta(\delta(q, w_1 w_2 \cdots w_{n-1}), w_n)$. The word w is *accepted* by $\mathcal{A}$ if $\delta(q_I, w) \in F$.

Let $p \geq 2$ be an integer, define the alphabet $\Sigma_p := \{+, -, 0, 1, 2, \ldots, p-1\}$. Let $n \geq 0$ be a non-negative integer and let $w_r w_{r-1} \cdots w_1 w_0 \in (\Sigma_p)^{r+1}$ be the base-p expansion of n. That is, $n = \sum_{i=0}^{r} w_i p^i$ with the smallest possible r. We denote by $w(n)$ the word $+w_0 w_1 \cdots w_r$. For example, if $p = 2$, then $w(4) = +001$. Similarly, for a negative integer $-n$, let $w(-n)$ denote the word $-w_0 w_1 \cdots w_r$. A subset S of $\mathbb{Z}$ is called *p-automatic* if there is an automaton over Σ_p that accepts exactly the set $w(S) := \{w(s) \mid s \in S\}$. For example, the set $S = \{2^k \mid k \in \mathbb{N}\}$ is 2-automatic, because $w(S) = \{+1, +01, +001, +0001, \cdots\}$ is accepted by an automaton over $\Sigma_2 = \{+, -, 0, 1\}$.

Let $d \in \mathbb{N}$. The definition of *p*-automatic subsets of $\mathbb{Z}$ can be naturally generalized to *p*-automatic subsets of $\mathbb{Z}^d$. For $(z_1, \ldots, z_d) \in \mathbb{Z}^d$, consider the tuple of words $(w(z_1), \ldots, w(z_d))$ over the alphabet Σ_p. We naturally identify a d-tuple of words $(w(z_1), \ldots, w(z_d))$ over the alphabet Σ_p as a single word $w(z_1, \ldots, z_d)$ over the alphabet Σ_p^d: if the words $w(z_1), \ldots, w(z_d)$ have different lengths, we add a minimal number of zeros at the end so they all have equal lengths. Naturally, a subset S of $\mathbb{Z}^d$ is called *p-automatic* if there is an automaton over Σ_p^d that accepts exactly the set $w(S) := \{w(s) \mid s \in S\}$. For example, the set $S = \{(a, 2a) \mid a < -1\} \subset \mathbb{Z}^2$ is 2-automatic, because

$$w(S) = \{(-,-)(a_1, 0)(a_2, a_1)(a_3, a_2) \cdots (a_k, a_{k-1})(1, a_k)(0, 1) \mid k \in \mathbb{N}, a_1, \ldots, a_k \in \{0, 1\}\}$$

is accepted by an automaton over Σ_2^2. We say a subset $S \subseteq \mathbb{Z}^d$ is *effectively p*-automatic if its accepting automaton is explicitly given. *p*-automatic sets enjoy various closure properties. In this paper, we will use the following:

▶ **Lemma 2.3** ([40]). *Let $p \geq 2$ be an integer.*

(1) *If S and T are effectively p-automatic subsets of $\mathbb{Z}^d$, then $S \cap T$ and $S \cup T$ are also effectively p-automatic.*

(2) *If $S \subseteq \mathbb{Z}^d$ is effectively p-automatic, and $\varphi \colon \mathbb{Z}^d \to \mathbb{Z}^n$ is a linear transformation, then $\varphi(S) \subseteq \mathbb{Z}^n$ is also effectively p-automatic.*

(3) *If $S \subseteq \mathbb{Z}^d$ is effectively p-automatic, and $\phi \colon \mathbb{Z}^N \to \mathbb{Z}^d$ is a linear transformation, then $\phi^{-1}(S) \coloneqq \{v \in \mathbb{Z}^N \mid \phi(v) \in S\}$ is also effectively p-automatic.*

(4) *It is decidable whether a given effectively p-automatic set S is empty.*

3   Main results and consequences

The main result of this paper is the following.

▶ **Theorem 3.1.** *Let p be a prime number, $\overline{X} = (X_1, \ldots, X_n)$ be a tuple of variables and $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module. Then, Submonoid Membership is decidable in the group $\mathcal{Y} \rtimes \mathbb{Z}^n$.*

In particular, taking $\mathcal{Y} = \mathbb{F}_p[\overline{X}^{\pm}]$, we immediately obtain decidability of Submonoid Membership in the n-dimensional lamplighter groups $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ for prime p.

We say a group is *virtually abelian* if it has a finite index subgroup that is abelian. A recent result of Shafrir [38, Theorem 8.1] shows that membership problem in a *fixed* rational subset S of a group L can be reduced to the membership problem in a fixed submonoid M of the group $L \times H$, where H is an explicitly constructed finitely generated virtually abelian group. Combined with Theorem 3.1, this allows us to construct an example where decidability of Submonoid Membership is not preserved under finite extension of groups:

▶ **Corollary 3.2.** *There exist a group G and a finite index subgroup $\widetilde{G} \leq G$, such that Submonoid Membership is decidable in $\widetilde{G}$ but undecidable in G.*

Proof. By [28, Theorem 10], there is a rational subset S of the two-dimensional lamplighter group $L \coloneqq (\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$, whose membership problem (given $g \in L$, whether $g \in S$?) is undecidable. By Shafrir's result [38, Theorem 8.1], the membership problem in S reduces to the membership problem in a finitely generated submonoid of the group $G \coloneqq L \times H$, where H is finitely generated virtually abelian. Therefore, Submonoid Membership is undecidable in $G = L \times H$.

Since H is finitely generated virtually abelian, it has a finite index subgroup $\mathbb{Z}^d \leq H$ for some d. Let $\widetilde{G} \coloneqq L \times \mathbb{Z}^d$, so the index $[G \colon \widetilde{G}] = [H \colon \mathbb{Z}^d]$ is finite. We now show that Submonoid Membership is decidable in $\widetilde{G}$.

Note that $\widetilde{G} = L \times \mathbb{Z}^d = \big((\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2\big) \times \mathbb{Z}^d$ can be written as a semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^{d+2}$, where $\mathcal{Y} \coloneqq \mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]$ is considered as an $\mathbb{F}_2[X_1^{\pm}, X_2^{\pm}, X_3^{\pm} \ldots, X_{d+2}^{\pm}]$-module where the elements $X_3, \ldots, X_{d+2}$ act trivially. That is, $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}, \ldots, X_{d+2}^{\pm}]/\sum_{i=3}^{d+2} \mathbb{F}_2[X_1^{\pm}, \ldots, X_{d+2}^{\pm}] \cdot (X_i - 1)$. So by Theorem 3.1, Submonoid Membership is decidable in $\widetilde{G}$.   ◀

Our proof of Theorem 3.1 is divided into two parts. First, in Section 4, we reduce Submonoid Membership to solving *S-unit equations* over modules. Then, in Section 5, we prove the following result for S-unit equations over modules.

▶ **Theorem 3.3.** *Let p be a prime number, $\overline{X} = (X_1, \ldots, X_n)$ be a tuple of variables, M be a finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module, and let $c_0, c_1, \ldots, c_m \in M$. Then, the set of solutions $(\mathbf{z}_1, \ldots, \mathbf{z}_m) \in (\mathbb{Z}^n)^m$ for the equation*

$$\overline{X}^{\mathbf{z}_1} \cdot c_1 + \cdots + \overline{X}^{\mathbf{z}_m} \cdot c_m = c_0 \tag{4}$$

is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$.

During the reduction in Section 4, we go through an intermediate step involving the *Knapsack Problem* in groups. In particular, we obtain the following intermediate result that is of independent interest:

▶ **Theorem 3.4.** *Let p be a prime number, $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[\overline{X}^\pm]$-module and $G = \mathcal{Y} \rtimes \mathbb{Z}^n$. Let $h_1, \ldots, h_m, g$ be elements of G, then the solution set $(n_1, \ldots, n_m) \in \mathbb{Z}^m$ of*

$$h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g \tag{5}$$

is an effectively p-automatic subset of $\mathbb{Z}^m$.

4 From Submonoid Membership to S-unit equation

In this section we reduce the problem of Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ to solving S-unit equations over $\mathbb{F}_p[\overline{X}^\pm]$-modules. The reduction is done in three steps. In Step 1, we reduce Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ to deciding membership in a product of conjugate groups (Proposition 4.1). In Step 2, we reduce membership in a product of conjugate groups to solving the Knapsack Problem in another semidirect product $\mathcal{Y}' \rtimes \mathbb{Z}^{n'}$ (Proposition 4.4). In Step 3, we show that the solution set of the Knapsack Problem is effectively p-automatic (Theorem 3.4), assuming a theorem on S-unit equations (Theorem 3.3).

Recall that the *rank* of an abelian group A is defined as smallest cardinality of a generating set for A. If $A \leq \mathbb{Z}^n$, then A is a lattice in $\mathbb{Z}^n$, the rank of A is the dimension of this lattice.

Step 1: from Submonoid Membership to Group Product Membership

Given $q \in G$ and a subgroup $H \leq G$, define the conjugate subgroup ${}^qH := \{qhq^{-1} \mid h \in H\}$. For $q_1, q_2, \ldots, q_k \in G$, denote the set

$${}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H := \{h_1 h_2 \cdots h_k \mid h_1 \in {}^{q_1}H, \ldots, h_k \in {}^{q_k}H\}. \tag{6}$$

Note that ${}^qH$ is always a group, but the product ${}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$ is in general not a group. Our first step is the following reduction from Submonoid Membership to the membership problem in sets of the form (6), originally due to Shafrir. We give a proof here for the sake of completeness. Recall that the projection $\pi \colon G = \mathcal{Y} \rtimes \mathbb{Z}^n \to \mathbb{Z}^n$ is surjective and its kernel is $\mathcal{Y}$. A group A is called *torsion* if for all $a \in A$, there exists $t \geq 1$ such that a^t is the neutral element. In particular, an $\mathbb{F}_p[\overline{X}^\pm]$-module $\mathcal{Y}$ considered as an abelian group is torsion, because $py = 0$ for all $y \in \mathcal{Y}$.

▶ **Proposition 4.1** ([35, Theorem 4.3.3]). *Let G be a finitely generated group and $\pi \colon G \to \mathbb{Z}^n$ be a surjective homomorphism with $\ker(\pi)$ being a torsion group. Submonoid Membership in G can be reduced to the following membership problem:*
    __Input:__ elements $g, q_1, \ldots, q_k \in G$ and finitely many generators of a subgroup $H \leq G$.
    __Question:__ whether $g \in {}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$?

Proof. For a subset $T \subseteq G$, denote by $\langle T \rangle$ the submonoid generated by T: this is the set of elements of the form $g_1 g_2 \ldots g_s$ where $s \geq 0$ and $g_i \in T$ for $1 \leq i \leq s$.

Let $g_1, g_2, \ldots, g_m, g \in G$, and suppose we want to decide whether $g \in \langle g_1, g_2, \ldots, g_m \rangle$. Consider the elements $\pi(g_1), \ldots, \pi(g_m), \pi(g) \in \mathbb{Z}^n \subset \mathbb{R}^n$, let $\mathcal{C} \subseteq \mathbb{R}^n$ be the $\mathbb{R}_{\geq 0}$-cone generated by $\pi(g_1), \pi(g_2), \ldots, \pi(g_m)$, and let $\mathcal{C}_0$ be the maximal $\mathbb{R}$-subspace of $\mathcal{C}$. In particular, there exists $v \in \mathbb{R}^n$, such that $v^\top \cdot w = 0$ for all $w \in \mathcal{C}_0$, and $v^\top \cdot w > 0$ for all $w \in \mathcal{C} \setminus \mathcal{C}_0$ (if

$\mathcal{C}_0 = \mathcal{C}$ then we can take $v = \mathbf{0}$). Without loss of generality suppose $\pi(g_1), \ldots, \pi(g_\ell) \in \mathcal{C}_0$ and $\pi(g_{\ell+1}), \ldots, \pi(g_m) \in \mathcal{C} \setminus \mathcal{C}_0$, for some $1 \le \ell \le m$.

If $g \in \langle g_1, g_2, \ldots, g_m \rangle$, then we can write g as a word $g_{i_1} g_{i_2} \cdots g_{i_s}$ over $\{g_1, \ldots, g_m\}$. In this case, $\pi(g) = \pi(g_{i_1}) + \pi(g_{i_2}) + \cdots + \pi(g_{i_s})$, so we must have $v^\top \cdot \pi(g) \ge 0$, and the elements $g_{\ell+1}, \ldots, g_m$ can only be used a bounded number of times (in fact, bounded by $B := v^\top \cdot \pi(g) / \min\{v^\top \cdot \pi(g_{\ell+1}), \ldots, v^\top \cdot \pi(g_m)\}$). Therefore, it suffices to check, for each possible choice of $g_{j_1}, \ldots, g_{j_b} \in \{g_{\ell+1}, \ldots, g_m\}$, $b \le B$, whether g can be written as $h_1 g_{j_1} h_2 g_{j_2} h_3 \cdots g_{j_b} h_{b+1}$ for $h_1, \ldots, h_{b+1} \in \langle g_1, g_2, \ldots, g_\ell \rangle$.

Let $H := \langle g_1, g_2, \ldots, g_\ell \rangle$, we claim that the monoid H is actually a group. It is easy to see that the $\mathbb{R}_{\ge 0}$-cone generated by $\pi(g_1), \ldots, \pi(g_\ell)$ is the linear space $\mathcal{C}_0$. Therefore we can find positive integers $n_1, \ldots, n_\ell > 0$ such that $n_1 \pi(g_1) + \cdots + n_\ell \pi(g_\ell) = \mathbf{0}$. Thus, $\pi(g_1^{n_1} g_2^{n_2} \cdots g_\ell^{n_\ell}) = \mathbf{0}$, so $g_1^{n_1} g_2^{n_2} \cdots g_\ell^{n_\ell} \in \ker(\pi)$. But $\ker(\pi)$ is torsion, so $(g_1^{n_1} g_2^{n_2} \cdots g_\ell^{n_\ell})^t$ is the neutral element for some $t \ge 1$. This yields $g_1^{-1} = g_1^{n_1-1} g_2^{n_2} \cdots g_\ell^{n_\ell} (g_1^{n_1} g_2^{n_2} \cdots g_\ell^{n_\ell})^{t-1} \in H$. Similarly, $g_2^{-1}, \ldots, g_\ell^{-1} \in H$, so the monoid H is actually a group.

By the discussion above, it suffices to check for finitely many instances of $g_{j_1}, \ldots, g_{j_b}$, whether $g \in H g_{j_1} H g_{j_2} H \cdots g_{j_b} H$. But $H g_{j_1} H g_{j_2} H \cdots g_{j_b} H$ is equal to

$$H(g_{j_1} H g_{j_1}^{-1})(g_{j_1} g_{j_2} H g_{j_2}^{-1} g_{j_1}^{-1}) \cdots (g_{j_1} g_{j_2} \cdots g_{j_b} H g_{j_b}^{-1} \cdots g_{j_2}^{-1} g_{j_1}^{-1}) g_{j_1} g_{j_2} \cdots g_{j_b}.$$

So $g \in H g_{j_1} H g_{j_2} H \cdots g_{j_b} H$ is equivalent to

$$g g_{j_b}^{-1} \cdots g_{j_2}^{-1} g_{j_1}^{-1} \in H \cdot {}^{g_{j_1}}H \cdot {}^{g_{j_1} g_{j_2}}H \cdot \ldots \cdot {}^{g_{j_1} g_{j_2} \cdots g_{j_b}}H,$$

which is a product of conjugate groups. This finishes the reduction from Submonoid Membership to membership in products of conjugate groups. ◄

In particular, for the case of $G = \mathcal{Y} \rtimes \mathbb{Z}^n$, Proposition 4.1 is effective, meaning one can explicitly compute the elements $q_1, \ldots, q_k \in G$ and the generators of H.

▶ **Example 4.2.** Let $\mathcal{Y} = \mathbb{F}_2[X_1^\pm, X_2^\pm]$ considered as an $\mathbb{F}_2[X_1^\pm, X_2^\pm]$-module, so $\mathcal{Y} \rtimes \mathbb{Z}^2$ is the 2-dimensional lamplighter group $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$. Let $g_1 = (1 + X_2, (2,0)), g_2 = (1, (-2,0)), g_3 = (1 + X_1, (0,1))$ be the generators of a submonoid, and let $g = (X_2^2, (4,2))$.

We have $\pi(g_1) = (2,0)$, $\pi(g_2) = (-2,0)$, $\pi(g_3) = (0,1)$, so the $\mathbb{R}_{\ge 0}$-cone they generate is $\mathcal{C} = \{(x,y) \in \mathbb{R}^2 \mid y \ge 0\}$. Its maximal subspace is $\mathcal{C}_0 = \{(x,0) \mid x \in \mathbb{R}\}$. We have $\pi(g_1), \pi(g_2) \in \mathcal{C}_0$ and $\pi(g_3) \in \mathcal{C} \setminus \mathcal{C}_0$.

Suppose $g = g_{i_1} g_{i_2} \cdots g_{i_s}$ with $i_1, i_2, \ldots, i_s \in \{1, 2, 3\}$. Let $v = (0, 1)$. Since $v^\top \cdot \pi(g) = v^\top \cdot (4, 2) = 2$, and $v^\top \cdot \pi(g_1) = v^\top \cdot \pi(g_2) = 0$, $v^\top \cdot \pi(g_3) = 1$, the element g_3 must appear exactly twice in the product $g_{i_1} g_{i_2} \cdots g_{i_s}$. Therefore, g must be of the form $w_1 g_3 w_2 g_3 w_3$, where w_1, w_2, w_3 are words over $\{g_1, g_2\}$. Let H be the monoid generated by g_1, g_2: this is actually a group because $(g_1 g_2)^2 = (0, \mathbf{0})$. The above discussion shows $g \in \langle g_1, g_2, g_3 \rangle$ if and only if $g \in H g_3 H g_3 H$: this is equivalent to $g g_3^{-2} \in H \cdot {}^{g_3}H \cdot {}^{g_3^2}H$. ■

▶ **Remark 4.3.** If $G = (\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}^2$ and $\pi(H)$ is of rank one (i.e. $\pi(H) \cong \mathbb{Z}$) as in Example 4.2, then membership problem in the product ${}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$ can be reduced to Rational Subset Membership in the 1-dimensional lamplighter group $(\mathbb{Z}/2\mathbb{Z}) \wr \mathbb{Z}$, which is known to be decidable [29]. In fact, this is the key idea in Shafrir's solution [35] for Submonoid Membership in 2-dimensional lamplighter groups. However, when the dimension n is greater or equal to three, the rank of $\pi(H)$ may be greater or equal to two: in this case, the membership problem in ${}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$ has been open and will be solved in the rest of this paper. Notably, we do *not* want to reduce it to Rational Subset Membership in lamplighter groups of dimension ≥ 2, as it is undecidable [28].

Step 2: from Group Product Membership to Knapsack Problem

The goal of this step is to reduce membership problem in the product $^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$ to a version of the *Knapsack Problem* in groups. Namely, we will prove:

▶ **Proposition 4.4.** *Let $G = \mathcal{Y} \rtimes \mathbb{Z}^n$ where $\mathcal{Y}$ is a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_n^{\pm}]$-module. Let $g, q_1, \ldots, q_k \in G$ and let $H \leq G$ be a finitely generated subgroup. Then, one can effectively find a group $G' = \mathcal{Y}' \rtimes \mathbb{Z}^{n'}$, where $\mathcal{Y}'$ is a finitely presented $\mathbb{F}_p[X_1^{\pm}, \ldots, X_{n'}^{\pm}]$-module, as well as elements $g', h_1, \ldots, h_m \in G'$, such that*

$$g \in {}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$$

if and only if there exist $z_1, \ldots, z_m \in \mathbb{Z}$ satisfying

$$h_1^{z_1} h_2^{z_2} \cdots h_m^{z_m} = g'. \tag{7}$$

We now proceed to prove Proposition 4.4. Recall that $\mathcal{Y}$ can be identified with the subgroup $\mathcal{Y} \times \{\mathbf{0}\} = \ker(\pi)$ of $G = \mathcal{Y} \rtimes \mathbb{Z}^n$. First, we give the following classic result on the structure of subgroups $H \leq G$. Note that $\pi(H) \leq \pi(G) = \mathbb{Z}^n$, let $d \leq n$ be the rank of $\pi(H)$.

▶ **Lemma 4.5** ([6, Theorem 3.3] or [36, Lemma 2]). *Let $G = \mathcal{Y} \rtimes \mathbb{Z}^n$ and $H \leq G$ be a finitely generated subgroup. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d \in \mathbb{Z}^n$ be a $\mathbb{Z}$-basis of $\pi(H)$, and choose elements $h_1, \ldots, h_d \in H$ so that $\pi(h_i) = \boldsymbol{a}_i, i = 1, \ldots, d$. Then, the subgroup $\mathcal{Y} \cap H$ is a finitely generated $\mathbb{F}_p[\overline{X}^{\pi(H)}]$-module, whose finite presentation can be effectively computed. Furthermore, H is generated by $h_1, \ldots, h_d$ and the set $\mathcal{Y} \cap H$.*

▶ **Example 4.2** (continued). As in Example 4.2, let $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]$. Consider the subgroup $H \leq \mathcal{Y} \rtimes \mathbb{Z}^2$ generated by $g_1 = (1 + X_2, (2, 0))$ and $g_2 = (1, (-2, 0))$. Then $\pi(H)$ is the subgroup of $\mathbb{Z}^2$ generated by $\boldsymbol{a}_1 := (2, 0)$, it has rank $d = 1$. We can choose $h_1 := g_1$ in Lemma 4.5.

The subgroup $\mathcal{Y} \cap H$ is an $\mathbb{F}_p[\overline{X}^{\pi(H)}] = \mathbb{F}_p[X_1^2, X_1^{-2}]$-module. We have $g_1 g_2 = (1 + X_2 + X_1^2, \mathbf{0})$. We claim that $1 + X_2 + X_1^2$ is the generator of the $\mathbb{F}_p[X_1^2, X_1^{-2}]$-module $\mathcal{Y} \cap H$: that is, $\mathcal{Y} \cap H = \{F \cdot (1 + X_2 + X_1^2) \mid F \in \mathbb{F}_p[X_1^2, X_1^{-2}]\}$. Indeed, recall the formula $(f, \boldsymbol{a})(y, \mathbf{0})(f, \boldsymbol{a})^{-1} = (\overline{X}^{\boldsymbol{a}} \cdot y, \mathbf{0})$. For each $m \in \mathbb{Z}$, we have $g_1^m (g_1 g_2) g_1^{-m} = g_1^m (1 + X_2 + X_1^2, \mathbf{0}) g_1^{-m} = (X_1^{2m} \cdot (1 + X_2 + X_1^2), \mathbf{0})$. So $X_1^{2m} \cdot (1 + X_2 + X_1^2) \in \mathcal{Y} \cap H$ for all $m \in \mathbb{Z}$. Consequently, $F \cdot (1 + X_2 + X_1^2) \in \mathcal{Y} \cap H$ for all $F \in \mathbb{F}_p[X_1^2, X_1^{-2}]$. It is not difficult to show that $\{F \cdot (1 + X_2 + X_1^2) \mid F \in \mathbb{F}_p[X_1^2, X_1^{-2}]\}$ is indeed all the elements in $\mathcal{Y} \cap H$, but we will omit the details. Note that $\mathcal{Y} \cap H$ is finitely generated as an $\mathbb{F}_p[X_1^2, X_1^{-2}]$-module but not finitely generated *as an abelian group*.

Finally, for any element $h = (f, 2z) \in H$, we have $\pi(h_1^{-z} h) = \mathbf{0}$, so $(y, \mathbf{0}) := h_1^{-z} h \in \mathcal{Y} \cap H$. Consequently, h can actually be written in a "canonical form" $h_1^z (y, \mathbf{0})$, where $z \in \mathbb{Z}$ and $y \in \mathcal{Y} \cap H$. Such canonical forms will be extensively used below. ∎

Define

$$\mathcal{Y}_i := \mathcal{Y} \cap ({}^{q_i}H), \quad i = 1, \ldots, k.$$

Note that for any $q \in G$, we have $\pi({}^q H) = \pi(H)$ because $\mathbb{Z}^n$ is abelian. Therefore $\pi({}^{q_1}H) = \cdots = \pi({}^{q_k}H) = \pi(H)$. So by Lemma 4.5, all the $\mathcal{Y}_i$'s are finitely generated $\mathbb{F}_p[\overline{X}^{\pi(H)}]$-modules. Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d \in \mathbb{Z}^n$ be a $\mathbb{Z}$-basis of $\pi(H)$. For each $1 \leq i \leq k$, choose elements $h_{i,1}, \ldots, h_{i,d} \in {}^{q_i}H$ so that $\pi(h_{i,1}) = \boldsymbol{a}_1, \ldots, \pi(h_{i,d}) = \boldsymbol{a}_d$. Then, ${}^{q_i}H$ is generated by $h_{i,1}, \ldots, h_{i,d}$ and $\mathcal{Y}_i$.

Fix any i. Since $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_d \in \mathbb{Z}^n$ form a $\mathbb{Z}$-basis for $\pi(\,^{q_i}H)$, for each element $h \in \,^{q_i}H$ we can find integers $z_1, \ldots, z_d$ such that

$$\pi(h) = z_1 \boldsymbol{a}_1 + z_2 \boldsymbol{a}_2 + \cdots + z_d \boldsymbol{a}_d = z_1 \pi(h_{i,1}) + z_2 \pi(h_{i,2}) + \cdots + z_d \pi(h_{i,d}).$$

This shows $\pi(h_{i,d}^{-z_{i,d}} \cdots h_{i,2}^{-z_{i,2}} h_{i,1}^{-z_{i,1}} h) = \boldsymbol{0}$, so $h_{i,d}^{-z_{i,d}} \cdots h_{i,2}^{-z_{i,2}} h_{i,1}^{-z_{i,1}} h \in \ker(\pi) \cap \,^{q_i}H = \mathcal{Y}_i$. Consequently, h is equal to $h_{i,1}^{z_{i,1}} h_{i,2}^{z_{i,2}} \cdots h_{i,d}^{z_{i,d}} (y_i, \boldsymbol{0})$ for some $y_i \in \mathcal{Y}_i$.

The form of this product of powers gives us the motivation to reduce membership in group products to the Knapsack Problem. Denote

$$\widetilde{\mathcal{Y}} := \mathcal{Y}_1 + \cdots + \mathcal{Y}_k.$$

Again we identify $\widetilde{\mathcal{Y}}$ with the subgroup $\widetilde{\mathcal{Y}} \times \{\boldsymbol{0}\}$ of $\mathcal{Y} \rtimes \mathbb{Z}^n$. We show the following:

▶ **Lemma 4.6.** *We have $g \in \,^{q_1}H \cdot \,^{q_2}H \cdot \ldots \cdot \,^{q_k}H$, if and only if there exist integers $z_{1,1}, \ldots, z_{1,d}$, $\ldots, z_{k,1}, \ldots, z_{k,d}$, such that*

$$\left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) \cdot g^{-1} \in \widetilde{\mathcal{Y}}. \tag{8}$$

Proof. For the "only if" part, suppose $g \in \,^{q_1}H \cdot \,^{q_2}H \cdot \ldots \cdot \,^{q_k}H$, and write $g = h_1 h_2 \cdots h_k$ with $h_i \in \,^{q_i}H$ for each $1 \leq i \leq k$. As shown above, we can write

$$h_i = h_{i,1}^{z_{i,1}} h_{i,2}^{z_{i,2}} \cdots h_{i,d}^{z_{i,d}} (y_i, \boldsymbol{0})$$

for some $y_i \in \mathcal{Y}_i$, $i = 1, \ldots, k$. Denote $y_i' := \overline{X}^{\sum_{j=1}^d z_{1,j} \boldsymbol{a}_j + \sum_{j=1}^d z_{2,j} \boldsymbol{a}_j + \cdots + \sum_{j=1}^d z_{i,j} \boldsymbol{a}_j} \cdot y_i$, then $y_i' \in \mathcal{Y}_i$. Recall the formula $(f, \boldsymbol{a})(y, \boldsymbol{0})(f, \boldsymbol{a})^{-1} = (\overline{X}^{\boldsymbol{a}} \cdot y, \boldsymbol{0})$, that is $(f, \boldsymbol{a})(y_i, \boldsymbol{0}) = (\overline{X}^{\boldsymbol{a}} \cdot y_i, \boldsymbol{0})(f, \boldsymbol{a})$. Therefore,

$$g = h_1 h_2 \cdots h_k = \left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) (y_1, \boldsymbol{0}) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) (y_k, \boldsymbol{0})$$

$$= (y_k', \boldsymbol{0}) \cdots (y_2', \boldsymbol{0})(y_1', \boldsymbol{0}) \left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right)$$

Therefore

$$\left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) \cdot g^{-1} = (-y_k' - \cdots - y_2' - y_1', \boldsymbol{0}) \in \mathcal{Y}_1 + \cdots + \mathcal{Y}_k = \widetilde{\mathcal{Y}}.$$

For the "if" part, let $z_{1,1}, \ldots, z_{1,d}, \ldots, z_{k,1}, \ldots, z_{k,d}$ be integers that satisfy Equation (8). Since $\widetilde{\mathcal{Y}} := \mathcal{Y}_1 + \cdots + \mathcal{Y}_k$, there exist $y_1 \in \mathcal{Y}_1, \ldots, y_k \in \mathcal{Y}_k$, such that

$$\left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) \cdot g^{-1} = (y_1 + y_2 + \cdots + y_k, \boldsymbol{0}).$$

Denote $y_i' := -\overline{X}^{-\sum_{j=1}^d z_{1,j} \boldsymbol{a}_j - \sum_{j=1}^d z_{2,j} \boldsymbol{a}_j - \cdots - \sum_{j=1}^d z_{i,j} \boldsymbol{a}_j} \cdot y_i$, then $y_i' \in \mathcal{Y}_i$. We have

$$g = (-y_1 - y_2 - \cdots - y_k, \boldsymbol{0}) \left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right)$$

$$= (-y_k, \boldsymbol{0}) \cdots (-y_2, \boldsymbol{0})(-y_1, \boldsymbol{0}) \left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right)$$

$$= \left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) (y_1', \boldsymbol{0}) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) (y_k', \boldsymbol{0}).$$

For each i, we have $(y_i', \boldsymbol{0}) \in \mathcal{Y}_i \leq \,^{q_i}H$, so $\left(h_{i,1}^{z_{i,1}} h_{i,2}^{z_{i,2}} \cdots h_{i,d}^{z_{i,d}} \right) (y_i', \boldsymbol{0}) \in \,^{q_i}H$. Therefore $g \in \,^{q_1}H \cdot \,^{q_2}H \cdot \ldots \cdot \,^{q_k}H$. ◀

Proposition 4.4 then follows from Lemma 4.6:

Proof of Proposition 4.4. By Lemma 4.6, we have $g \in {}^{q_1}H \cdot {}^{q_2}H \cdot \ldots \cdot {}^{q_k}H$ if and only if Equation (8) has integer solutions. Write $h_{i,j}$ as $(f_{i,j}, \boldsymbol{a}_j)$ for $i = 1, \ldots, k$; $j = 1, \ldots, d$, and write g as $(f_0, \boldsymbol{a}_0)$. Let $\mathcal{F}$ denote the $\mathbb{F}_p[\overline{X}^{\pi(H)}]$-submodule of $\mathcal{Y}$ generated by f_0 and $f_{i,j}$, $i = 1, \ldots, k$; $j = 1, \ldots, d$. Notably, $\mathcal{F}$ contains $\mathcal{Y}_i$, $i = 1, \ldots, k$. A finite presentation of $\mathcal{F}$ can be computed (see Lemma 2.2). The group generated by g and all the $h_{i,j}$'s is contained in the subgroup $\mathcal{F} \rtimes \pi(H)$ of $\mathcal{Y} \rtimes \mathbb{Z}^n$. Hence, Equation (8) is equivalent to the following equation in $(\mathcal{F}/\widetilde{\mathcal{Y}}) \rtimes \pi(H)$:

$$\left(h_{1,1}^{z_{1,1}} h_{1,2}^{z_{1,2}} \cdots h_{1,d}^{z_{1,d}} \right) \cdots \left(h_{k,1}^{z_{k,1}} h_{k,2}^{z_{k,2}} \cdots h_{k,d}^{z_{k,d}} \right) = g. \tag{9}$$

Choose the new variables $X_1' := \overline{X}^{\boldsymbol{a}_1}, \ldots, X_d' := \overline{X}^{\boldsymbol{a}_d}$. Then the ring $\mathbb{F}_p[\overline{X}^{\pi(H)}]$ can be written as the polynomial ring $\mathbb{F}_p[X_1'^{\pm}, \ldots, X_d'^{\pm}]$, and $\mathcal{Y}' := \mathcal{F}/\widetilde{\mathcal{Y}}$ is now a finitely presented $\mathbb{F}_p[X_1'^{\pm}, \ldots, X_d'^{\pm}]$-module. We conclude by letting $G' := \mathcal{Y}' \rtimes \mathbb{Z}^d = (\mathcal{F}/\widetilde{\mathcal{Y}}) \rtimes \pi(H)$, and observing that Equation (9) is a Knapsack equation of the form (7). ◀

▶ **Remark 4.7.** Note that even if we only considered the lamplighter group $G = (\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$ by supposing $\mathcal{Y} = \mathbb{F}_p[\overline{X}]$, we would inevitably introduce the quotient by $\widetilde{\mathcal{Y}}$ during our reduction from Submonoid Membership to the Knapsack Problem. Therefore, it is reasonable to directly consider Submonoid Membership in the more general case of semidirect product $\mathcal{Y} \rtimes \mathbb{Z}^n$ with *finitely presented* $\mathcal{Y}$, instead of only the special case of lamplighter groups $(\mathbb{Z}/p\mathbb{Z}) \wr \mathbb{Z}^n$. In other words, it does not appear that the special case of lamplighter groups admits a more direct solution.

Step 3: from Knapsack Problem to S-unit equation

The goal of this step is to solve the Knapsack Problem in groups of the form $\mathcal{Y} \rtimes \mathbb{Z}^n$. Namely, assuming a theorem on S-unit equations (Theorem 3.3), we will prove the following result:

▶ **Theorem 3.4.** *Let p be a prime number, $\mathcal{Y}$ be a finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module and $G = \mathcal{Y} \rtimes \mathbb{Z}^n$. Let $h_1, \ldots, h_m, g$ be elements of G, then the solution set $(n_1, \ldots, n_m) \in \mathbb{Z}^m$ of*

$$h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g \tag{5}$$

is an effectively p-automatic subset of $\mathbb{Z}^m$.

Before we proceed to the formal proof, let us show another example to illustrate the ideas.

▶ **Example 4.8.** Let $p = 2$, $n = 2$. Let $\mathcal{Y} = \mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]/(X_1 + X_2 + 1)$, that is, the quotient of $\mathbb{F}_2[X_1^{\pm}, X_2^{\pm}]$ by the submodule $\mathbb{F}_2[X_1^{\pm}, X_2^{\pm}] \cdot (X_1 + X_2 + 1)$. Let $h_1 = \left(0, (1, 0)\right), h_2 = \left(1 - X_2, (0, 1)\right), h_3 = \left(0, (1, 0)\right), h_4 = \left(0, (0, 1)\right), g = \left(1, (0, 0)\right)$ be elements of $\mathcal{Y} \rtimes \mathbb{Z}^2$. We will to show that the solution set of the equation

$$h_1^{n_1} h_2^{n_2} h_3^{n_3} h_4^{n_4} = g \tag{10}$$

is 2-automatic.

By direct computation, we have $(f, \boldsymbol{a})^z = \left((1 + \overline{X}^{\boldsymbol{a}} + \cdots + \overline{X}^{(z-1)\boldsymbol{a}}) \cdot f, z\boldsymbol{a}\right)$ for $z > 0$ and $(f, \boldsymbol{a})^z = \left((-\overline{X}^{z\boldsymbol{a}} - \overline{X}^{(z+1)\boldsymbol{a}} - \cdots - \overline{X}^{-\boldsymbol{a}}) \cdot f, z\boldsymbol{a}\right)$ for $z < 0$. In either case (and for $z = 0$), we have

$$(f, \boldsymbol{a})^z = \left(\frac{1 - \overline{X}^{z\boldsymbol{a}}}{1 - \overline{X}^{\boldsymbol{a}}} \cdot f, \ z\boldsymbol{a}\right).$$

Hence,

$$
\begin{aligned}
h_1^{n_1} h_2^{n_2} h_3^{n_3} h_4^{n_4} &= \big(0, (1,0)\big)^{n_1} \big(1 - X_2, (0,1)\big)^{n_2} \big(0, (1,0)\big)^{n_3} \big(0, (0,1)\big)^{n_4} \\
&= \big(0, (n_1, 0)\big) \left(\frac{1 - X_2^{n_2}}{1 - X_2} \cdot (1 - X_2), (0, n_2) \right) \big(0, (n_3, 0)\big) \big(0, (0, n_4)\big) \\
&= \big(X_1^{n_1}(1 - X_2^{n_2}), (n_1 + n_3, n_2 + n_4)\big)
\end{aligned}
$$

Since $g = \big(1, (0,0)\big)$, we have $h_1^{n_1} h_2^{n_2} h_3^{n_3} h_4^{n_4} = g$ if and only if

$$
X_1^{n_1}(1 - X_2^{n_2}) = 1, \ n_1 + n_3 = 0, \ n_2 + n_4 = 0.
$$

We now show that the solution set $(n_1, n_2, n_3, n_4) \in \mathbb{Z}^4$ is 2-automatic. Since $n_3 = -n_1$ and $n_4 = -n_2$, it suffices to show that the solution set $(n_1, n_2) \in \mathbb{Z}^2$ of $X_1^{n_1}(1 - X_2^{n_2}) = 1$ is 2-automatic.

The equation $X_1^{n_1}(1 - X_2^{n_2}) = 1$ can be rewritten as

$$
X_1^{-n_1} + X_2^{n_2} = 1 \tag{11}
$$

Therefore, we have reduced the *Knapsack equation* (10) to the *S-unit equation* (11) over the module $\mathbb{F}_2[X_1^\pm, X_2^\pm]/(X_1 + X_2 + 1)$. The 2-automaticity of its solution set can already be deduced from Theorem 3.3 (see below). However, we now prove "by hand" that the solution set of the S-unit Equation (11) is 2-automatic, in order to give an idea of how 2-automaticity can arise from such equations.

Since we work in the module $\mathbb{F}_2[X_1^\pm, X_2^\pm]/(X_1 + X_2 + 1)$, we have $X_2 = -(X_1 + 1) = X_1 + 1$ (we are in characteristic 2). Therefore, Equation (11) is equivalent to $(X_1 + 1)^{n_2} = X_1^{-n_1} + 1$. We claim that its solution set is $(n_1, n_2) \in \{(-2^k, 2^k) \mid k \in \mathbb{N}\}$.

Indeed, since $X_1^{-n_1} + 1 \in \mathbb{F}_2[X_1^\pm]$, we must have $n_2 \geq 0$ so that $(X_1 + 1)^{n_2}$ is also in $\mathbb{F}_2[X_1^\pm]$. Considering the degree of both sides we have $n_1 = -n_2$. Now, in order for $(X_1 + 1)^{n_2} = X_1^{n_2} + 1$ to hold, n_2 must be a power of 2. Indeed, $n_2 = 0$ is not a solution, so suppose $n_2 \geq 1$ and write $n_2 = 2^k + a$ with $0 \leq a < 2^k$. By "freshman's dream", we have

$$
(X_1 + 1)^{n_2} = (X_1 + 1)^{2^k}(X_1 + 1)^a = (X_1^{2^k} + 1)(X_1 + 1)^a = X_1^{2^k}(X_1 + 1)^a + (X_1 + 1)^a.
$$

Every monomial appearing in $X_1^{2^k}(X_1 + 1)^a$ has degree larger than every monomial appearing $(X_1 + 1)^a$. But $(X_1 + 1)^{n_2} = X_1^{n_2} + 1$ has only two monomials. So both $X_1^{2^k}(X_1 + 1)^a$ and $(X_1 + 1)^a$ must be monomials, meaning $a = 0$. Therefore $n_2 = 2^k$, and $n_1 = -n_2 = -2^k$.

In conclusion, the solution set of Equation (10) is $(n_1, n_2, n_3, n_4) \in \{(-2^k, 2^k, 2^k, -2^k) \mid k \in \mathbb{N}\}$, which is 2-automatic. Note that this set is not semilinear, so the situation in semidirect products is more complicated than in the wreath product of two abelian groups [19]. ∎

Example 4.8 shows that there will be two parts in the proof of Theorem 3.4: a (fairly elementary) first part reducing Knapsack Equations to S-unit equations, then a (rather non-trivial) second part showing that S-unit equations have p-automatic solution sets. The second part is summarized as Theorem 3.3 below, which we will prove in Section 5. In the rest of this section, we will focus on the first part of the proof, assuming Theorem 3.3 as a blackbox.

▶ **Theorem 3.3.** *Let p be a prime number, $\overline{X} = (X_1, \ldots, X_n)$ be a tuple of variables, M be a finitely presented $\mathbb{F}_p[\overline{X}^\pm]$-module, and let $c_0, c_1, \ldots, c_m \in M$. Then, the set of solutions $(z_1, \ldots, z_m) \in (\mathbb{Z}^n)^m$ for the equation*

$$
\overline{X}^{z_1} \cdot c_1 + \cdots + \overline{X}^{z_m} \cdot c_m = c_0 \tag{4}
$$

is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$.

Proof of Theorem 3.4 (assuming Theorem 3.3). Write $h_i = (f_i, \boldsymbol{a}_i)$, $i = 1, \ldots, m$, and $g = (f, \boldsymbol{b})$.

Case 1: none of the $\boldsymbol{a}_i$ is $\boldsymbol{0}$ (in fact this case already suffices to solve the Equation (5) arising from the previous step). We have

$$h_i^{n_i} = (f_i, \boldsymbol{a}_i)^{n_i} = \left(\frac{1 - \overline{X}^{n_i \boldsymbol{a}_i}}{1 - \overline{X}^{\boldsymbol{a}_i}} \cdot f_i, \ n_i \boldsymbol{a}_i \right).$$

Computing their product gives

$$h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = \left(\sum_{i=1}^{m} \overline{X}^{n_1 \boldsymbol{a}_1 + \cdots + n_{i-1} \boldsymbol{a}_{i-1}} \cdot \frac{1 - \overline{X}^{n_i \boldsymbol{a}_i}}{1 - \overline{X}^{\boldsymbol{a}_i}} \cdot f_i, \ n_1 \boldsymbol{a}_1 + \cdots + n_m \boldsymbol{a}_m \right).$$

Therefore, writing $\boldsymbol{z}_i := n_1 \boldsymbol{a}_1 + \cdots + n_i \boldsymbol{a}_i$ for $i = 1, \ldots, m$, and $\boldsymbol{z}_0 := \boldsymbol{0}$, we have $h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g$ if and only if

$$\sum_{i=1}^{m} \overline{X}^{\boldsymbol{z}_{i-1}} \cdot \frac{1 - \overline{X}^{\boldsymbol{z}_i - \boldsymbol{z}_{i-1}}}{1 - \overline{X}^{\boldsymbol{a}_i}} \cdot f_i = f, \tag{12}$$

$$\text{and} \quad \boldsymbol{z}_m = \boldsymbol{b}. \tag{13}$$

Write $\mathcal{Y} = \mathbb{F}_p[\overline{X}^{\pm}]^d / N$ for some $N \subseteq \mathbb{F}_p[\overline{X}^{\pm}]^d$. Considering $f_1, \ldots, f_m, f$, as elements in $\mathbb{F}_p[\overline{X}^{\pm}]^d$, Equation (12) is equivalent to

$$\sum_{i=1}^{m} (\overline{X}^{\boldsymbol{z}_{i-1}} - \overline{X}^{\boldsymbol{z}_i}) \prod_{j \neq i} (1 - \overline{X}^{\boldsymbol{a}_j}) \cdot f_i - \prod_{i=1}^{m} (1 - \overline{X}^{\boldsymbol{a}_i}) \cdot f \in \prod_{i=1}^{m} (1 - \overline{X}^{\boldsymbol{a}_i}) \cdot N.$$

Letting $c_0 := -\prod_{j \neq 1} (1 - \overline{X}^{\boldsymbol{a}_j}) \cdot f_1 + \prod_{i=1}^{m} (1 - \overline{X}^{\boldsymbol{a}_i}) \cdot f$, $c_i := \prod_{j \neq (i+1)} (1 - \overline{X}^{\boldsymbol{a}_j}) \cdot f_{i+1} - \prod_{j \neq i} (1 - \overline{X}^{\boldsymbol{a}_j}) \cdot f_i$, $i = 1, \ldots, m-1$ and $c_m := -\prod_{j \neq m} (1 - \overline{X}^{\boldsymbol{a}_j}) \cdot f_m$, the equation above is equivalent to the following equation in $M := \mathbb{F}_p[\overline{X}^{\pm}]^d / \prod_{i=1}^{m} (1 - \overline{X}^{\boldsymbol{a}_i}) N$:

$$\overline{X}^{\boldsymbol{z}_1} \cdot c_1 + \cdots + \overline{X}^{\boldsymbol{z}_m} \cdot c_m = c_0. \tag{14}$$

Therefore, we have $h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g$ if and only if $\boldsymbol{z}_i := n_1 \boldsymbol{a}_1 + \cdots + n_i \boldsymbol{a}_i, i = 1, \ldots, m$ satisfy Equations (13) and (14). By Theorem 3.3, the set $\mathcal{Z}$ of $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \in \mathbb{Z}^{mn}$ satisfying (13) and (14) is p-automatic. Define the map $\varphi \colon \mathbb{Z}^m \to \mathbb{Z}^{mn}, (n_1, \ldots, n_m) \mapsto (n_1 \boldsymbol{a}_1, n_1 \boldsymbol{a}_1 + n_2 \boldsymbol{a}_2, \ldots, n_1 \boldsymbol{a}_1 + \cdots + n_m \boldsymbol{a}_m)$. Then the solution set of $h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g$ is $\varphi^{-1}(\mathcal{Z})$. Since $\mathcal{Z}$ is p-automatic and φ is linear, $\varphi^{-1}(\mathcal{Z})$ is also p-automatic (see Lemma 2.3).

Case 2: some of the $\boldsymbol{a}_i$'s are $\boldsymbol{0}$. We reduce this case to the previous case. Let $i_1, \ldots, i_s$ be the indices where $\boldsymbol{a}_i = \boldsymbol{0}$. We rewrite the equation $h_1^{n_1} h_2^{n_2} \cdots h_m^{n_m} = g$ as

$$\left(h_1^{n_1} \cdots h_{i_1-1}^{n_{i_1-1}} \right) h_{i_1}^{n_{i_1}} \left(h_{i_1+1}^{n_{i_1+1}} \cdots h_{i_2-1}^{n_{i_2-1}} \right) h_{i_2}^{n_{i_2}} \cdots \left(h_{i_s+1}^{n_{i_s+1}} \cdots h_m^{n_m} \right) = g.$$

Since $\boldsymbol{a}_{i_1} = \cdots = \boldsymbol{a}_{i_s} = \boldsymbol{0}$ and $p \cdot f_{i_1} = \cdots = p \cdot f_{i_s} = 0$, we have $h_{i_1}^p = \cdots = h_{i_s}^p = (0, \boldsymbol{0})$. Therefore, the powers $h_{i_1}^{n_{i_1}}, h_{i_2}^{n_{i_2}}, \ldots$, and $h_{i_s}^{n_{i_s}}$ can only take on finitely many different values (at most p each). It suffices to show that for each value $h_{i_1}^{n_{i_1}} = g_1, \ldots, h_{i_s}^{n_{i_s}} = g_s$, the solution set of

$$\left(h_1^{n_1} \cdots h_{i_1-1}^{n_{i_1-1}} \right) g_1 \left(h_{i_1+1}^{n_{i_1+1}} \cdots h_{i_2-1}^{n_{i_2-1}} \right) g_2 \cdots \left(h_{i_s+1}^{n_{i_s+1}} \cdots h_m^{n_m} \right) = g$$

is effectively p-automatic (recall that a union of effectively p-automatic sets is effectively p-automatic, see Lemma 2.3). But the above equation is equivalent to the Knapsack equation

$$h_1^{n_1} \cdots h_{i_1-1}^{n_{i_1-1}} \left(g_1 h_{i_1+1} g_1^{-1}\right)^{n_{i_1+1}} \cdots \left(g_1 h_{i_2-1} g_1^{-1}\right)^{n_{i_2-1}} \left(g_1 g_2 h_{i_2+1} g_2^{-1} g_1^{-1}\right)^{n_{i_2+1}} \cdots$$
$$\cdots \left(g_1 g_2 \ldots g_s h_m g_s^{-1} \cdots g_2^{-1} g_1^{-1}\right)^{n_m} = g g_s^{-1} \cdots g_2^{-1} g_1^{-1}.$$

By Case 1, the solution set of the above equation is indeed effectively p-automatic. ◀

Combining the three steps in this section, we have proven Theorem 3.1:

Proof of Theorem 3.1. By Proposition 4.1, Proposition 4.4 and Theorem 3.4, Submonoid Membership in $\mathcal{Y} \rtimes \mathbb{Z}^n$ reduces to checking whether the solution set of the Knapsack Equation (5) is empty. Since the solution set is effectively p-automatic, its emptiness is decidable (Lemma 2.3). ◀

5 S-unit equation over modules

The purpose of this section is to prove Theorem 3.3 on S-unit equations over modules.

▶ **Theorem 3.3.** *Let p be a prime number, $\overline{X} = (X_1, \ldots, X_n)$ be a tuple of variables, M be a finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module, and let $c_0, c_1, \ldots, c_m \in M$. Then, the set of solutions $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \in (\mathbb{Z}^n)^m$ for the equation*

$$\overline{X}^{\boldsymbol{z}_1} \cdot c_1 + \cdots + \overline{X}^{\boldsymbol{z}_m} \cdot c_m = c_0 \tag{4}$$

is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$.

As a comparison, S-unit equations over *fields* are an intensively studied area in number theory. In the positive characteristic case, Adamczewski and Bell gave the following result. (Independently, Derksen and Masser [15] also proved a similar result.)

▶ **Theorem 5.1** ([1, Theorem 3.1]). *Let K be a field of characteristic $p > 0$, let $c_1, \ldots, c_m \in K^*$, and let $\overline{x} = (x_1, \ldots, x_n) \in (K^*)^n$. Then the set of solutions $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \in (\mathbb{Z}^n)^m$ for the equation*

$$\overline{x}^{\boldsymbol{z}_1} c_1 + \cdots + \overline{x}^{\boldsymbol{z}_m} c_m = 1$$

is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$.

Our objective is to generalize Theorem 5.1 from *fields* to *modules*. Notably, we need to replace the field K by the polynomial ring $\mathbb{F}_p[\overline{X}^{\pm}]$, and replace the elements $c_1, \ldots, c_m$ in K^* by elements in the finitely presented $\mathbb{F}_p[\overline{X}^{\pm}]$-module M. To give a general idea of our approach, consider the following example.

▶ **Example 5.2.** For simplicity, we present this example using regular polynomial rings instead of Laurent polynomial rings. Consider the equation

$$X^a + Y^b = 1 \tag{15}$$

in the $\mathbb{F}_2[X, Y]$-module $\mathbb{F}_2[X, Y]/Y^2(X+Y+1)$. Here, the variables are $a, b \in \mathbb{N}$. (Technically, in order to match the form of the equation in Theorem 3.3, one needs to consider the equation $X^a Y^c + X^d Y^b = 1$ instead of (15). However, to keep this example simple, we only consider the solutions with $c = d = 0$.)

Equation (15) in $\mathbb{F}_2[X, Y]/Y^2(X + Y + 1)$ is equivalent to $Y^2(X + Y + 1) \mid X^a + Y^b + 1$ in $\mathbb{F}_2[X, Y]$, which in turn is equivalent to "$Y^2 \mid X^a + Y^b + 1$ and $X + Y + 1 \mid X^a + Y^b + 1$".

In other words, Equation (15) holds in $\mathbb{F}_2[X,Y]/Y^2(X+Y+1)$ if and only if it holds in both $\mathbb{F}_2[X,Y]/Y^2$ and in $\mathbb{F}_2[X,Y]/(X+Y+1)$.

The $\mathbb{F}_2[X,Y]$-module $\mathbb{F}_2[X,Y]/Y^2$ can be considered as a finitely generated $\mathbb{F}_2[X]$-module $\mathbb{F}_2[X,Y]/Y^2 = \mathbb{F}_2[X] + Y \cdot \mathbb{F}_2[X] \cong \mathbb{F}_2[X]^2$ by $1 \mapsto (1,0)$, $Y \mapsto (0,1)$. Considered as an equation in $\mathbb{F}_2[X]^2$, the equation $X^a + Y^b = 1$ becomes

$$(X^a, 0) = (1,0) \ \text{ if } \ b \geq 2, \quad (X^a, 1) = (1,0) \ \text{ if } \ b = 1, \quad (X^a + 1, 0) = (1,0) \ \text{ if } \ b = 0.$$

So the solution set of $X^a + Y^b = 1$ in $\mathbb{F}_2[X,Y]/Y^2$ is $\mathcal{Z}_1 := \{(a,b) \mid a = 0, \ b \geq 2\}$.

The $\mathbb{F}_2[X,Y]$-module $\mathbb{F}_2[X,Y]/(X+Y+1)$ can be considered as the $\mathbb{F}_2[X]$-module $\mathbb{F}_2[X]$ through the variable substitution $Y = X + 1$. Under this variable substitution, the equation $X^a + Y^b = 1$ becomes $X^a + (X+1)^b = 1$, so its solution set is $\mathcal{Z}_2 := \{(a,b) \mid a = b \in 2^{\mathbb{N}}\}$. This can be shown similar to Example 4.8, or by directly applying Theorem 5.1 on the quotient field $K = \mathbb{F}_2(X)$.

Thus, the solution set of Equation (15) in $\mathbb{F}_2[X,Y]/Y^2(X+Y+1)$ is $\mathcal{Z}_1 \cap \mathcal{Z}_2 = \emptyset$. ∎

Example 5.2 illustrates the idea that, to solve an equation in a module M, we first "decompose" it into several equations in *coprimary modules* $M_1, \ldots, M_l$ (such as $\mathbb{F}_2[X,Y]/Y^2$ and $\mathbb{F}_2[X,Y]/(X+Y+1)$). This will be formalized in Lemma 5.6. Then, for the equation in each coprimary module, we "eliminate" variables to simplify the quotients (for example $\mathbb{F}_2[X,Y]/Y^2 \cong \mathbb{F}_2[X]^2$ and $\mathbb{F}_2[X,Y]/(X+Y+1) \cong \mathbb{F}_2[X]$ both eliminate the variable Y). In general, variable elimination might not be directly possible, and we need to perform a "change of variables" using *Noether Normalization*. This will be formalized in Lemma 5.7 and Lemma 5.8. Finally, we show that each such equation "without quotient" (more precisely, in *torsion-free* modules) has a p-automatic solution set, by reducing to the case of fields (for example, considering equations over $\mathbb{F}_2[X]$ as equations over the quotient field $\mathbb{F}_2(X)$). This will be formalized in Lemma 5.9. Thus, the solution set of the original equation over M is an intersection of effectively p-automatic sets, and is therefore also effectively p-automatic. This approach is inspired by Derkson's proof of the Skolem-Mahler-Lech theorem in modules over positive characteristic [13, Chapter 9].

The starting point of our proof is the following deep theorem by Adamczewski and Bell, generalizing Theorem 5.1.

▶ **Theorem 5.3** ([1, Theorem 4.1]). *Let K be a field of characteristic $p > 0$ and let D be a positive integer. Let V be a Zariski closed subset of $\mathsf{GL}_D(K)$ and let $A_1, \ldots, A_N$ be commuting matrices in $\mathsf{GL}_D(K)$. Then the set $\{(z_1, \ldots, z_N) \in \mathbb{Z}^N \mid A_1^{z_1} A_2^{z_2} \cdots A_n^{z_N} \in V\}$ is effectively p-automatic.*

For effectiveness reasons, we need to suppose K to be an effectively computable field (field where all arithmetic operations are effective): this will be the case in all our applications. We will not give the formal definition of a *Zariski closed subset* because in our application of Theorem 5.3, the set V will be of the form

$$V = \{A \in \mathsf{GL}_D(K) \mid BAv = 0^d\} \tag{16}$$

for some $d \in \mathbb{N}, B \in K^{d \times D}, v \in K^{D \times 1}$. This is a linear subset of $\mathsf{GL}_D(K)$ and hence Zariski closed. For a tuple of commutative matrices $\overline{A} = (A_1, \ldots, A_n) \in (\mathsf{GL}_d(K))^n$ and a vector $\boldsymbol{z} = (z_1, \ldots, z_n) \in \mathbb{Z}^n$, denote

$$\overline{A}^{\boldsymbol{z}} := A_1^{z_1} A_2^{z_2} \cdots A_n^{z_n},$$

similar to our notation for monomials. In the case where V has the form (16), Theorem 5.3 gives the following corollary, which can be considered as a version of Theorem 3.3 where the module M is replaced by a vector space over a field K.

▶ **Corollary 5.4.** *Let K be a field of characteristic $p > 0$ and let $\overline{A} = (A_1, \ldots, A_n) \in (\mathsf{GL}_d(K))^n$ be a tuple of commuting matrices. Let $c_0, c_1, \ldots, c_m$ be elements in the d-dimensional vector space K^d. Then, the set of solutions $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \in (\mathbb{Z}^n)^m$ for the equation*

$$\overline{A}^{\boldsymbol{z}_1} c_1 + \cdots + \overline{A}^{\boldsymbol{z}_m} c_m = c_0 \tag{17}$$

is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$.

Proof. For any $B_1, \ldots, B_{m+1} \in \mathsf{GL}_d(K)$, we denote by $\mathrm{diag}(B_1, \ldots, B_{m+1})$ the block diagonal matrix in $\mathsf{GL}_{(m+1)d}(K)$ whose block diagonal entries are $B_1, \ldots, B_{m+1}$. Let I denote the identity matrix of dimension d and denote $D = (m+1)d$. Consider the following elements in $\mathsf{GL}_D(K)$. For $j = 1, \ldots, n$, let $A_{1j} := \mathrm{diag}(A_j, I, \ldots, I), A_{2j} = \mathrm{diag}(I, A_j, \ldots, I), \ldots, A_{mj} = \mathrm{diag}(I, \ldots, A_j, I)$.

Furthermore, let $v := (c_1^\top, c_2^\top, \ldots, c_m^\top, c_0^\top)^\top \in K^{D \times 1}$, and $B := (I, I, \ldots, I, -I) \in K^{d \times D}$. Then, Equation (17) is equivalent to

$$B\left(\prod_{i=1}^{m}\prod_{j=1}^{n} A_{ij}^{z_{ij}}\right) v = 0^d. \tag{18}$$

We then apply Theorem 5.3 to the set

$$V = \{A \in \mathsf{GL}_D(K) \mid BAv = 0^d\}$$

and the commuting matrices $A_{ij}, i = 1, \ldots, m; j = 1, \ldots, n$. This shows that the set of solutions $(z_{ij})_{1 \le i \le m, 1 \le j \le n}$ for Equation (18) is an effectively p-automatic subset of $\mathbb{Z}^{nm}$. ◀

To pass from vector spaces to modules, we now introduce the *primary decomposition* of a module. First, we recall some standard definitions and tools from commutative algebra [18].

▶ **Definition 5.5.** Let R be a commutative Noetherian ring (for example, $R = \mathbb{K}[\overline{X}^\pm]$ for some field $\mathbb{K}$).

(1) An *ideal* of R is an R-submodule of R. An ideal $I \subseteq R$ is called *prime* if $I \ne R$, and for every $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$. Prime ideals are usually denoted by the Gothic letter $\mathfrak{p}$.

(2) Let M be a finitely generated R-module. The *annihilator* of an element $m \in M$, denoted by $\mathrm{Ann}_R(m)$, is the set $\{r \in R \mid r \cdot m = 0\}$.

(3) An R-module M is called *torsion-free* if for every $r \in R, m \in M$, $r \cdot m = 0$ implies $r = 0$ or $m = 0$. That is, M is torsion-free if and only if $\mathrm{Ann}_R(m) = \{0\}$ for all $m \in M \setminus \{0\}$.

(4) A prime ideal $\mathfrak{p} \subset R$ is called *associated* to M if there exists a non-zero $m \in M$ such that $\mathfrak{p} = \mathrm{Ann}_R(m)$.

(5) Let N be a finitely generated R-module. A submodule N' of N is called *primary* if N/N' has only one associated prime ideal. If we denote this prime ideal by $\mathfrak{p}$, then $N' \subseteq N$ is called $\mathfrak{p}$-*primary*.

(6) Let N' be a submodule of a finitely generated R-module N. The *primary decomposition* of N' is the writing of N' as a finite intersection $\bigcap_{i=1}^{l} N_i$, where N_i is a $\mathfrak{p}_i$-primary submodule of N for some prime ideal $\mathfrak{p}_i \subset R$. A primary decomposition always exists [18, Theorem 3.10]. If $R = \mathbb{F}_p[\overline{X}^\pm]$ and N, N' are finitely generated submodules of R^d for some $d \in \mathbb{N}$, then a primary decomposition of $N' \subseteq N$ can be effectively computed [37].

(7) A finitely generated R-module M is called *coprimary* if the submodule $\{0\}$ is primary, that is, if M has only one associated prime ideal. If we denote this prime ideal by $\mathfrak{p}$, then M is called $\mathfrak{p}$-*coprimary*. If M is $\mathfrak{p}$-coprimary, and m is a non-zero element in M, then $\operatorname{Ann}_R(m) \subseteq \mathfrak{p}$.

Let $M = \mathbb{F}_p[\overline{X}^{\pm}]^d/N$, $N \subseteq \mathbb{F}_p[\overline{X}^{\pm}]^d$ be the finite presentation of M in Theorem 3.3. Let $N = \bigcap_{i=1}^l N_i$ be the primary decomposition of N as a submodule of $\mathbb{F}_p[\overline{X}^{\pm}]^d$, where N_i is $\mathfrak{p}_i$-primary for a prime ideal $\mathfrak{p}_i \subset \mathbb{F}_p[\overline{X}^{\pm}]$, $i = 1, \ldots, l$. Then $M_i := \mathbb{F}_p[\overline{X}^{\pm}]^d/N_i$ is $\mathfrak{p}_i$-coprimary. The finite presentation of N_i, and hence M_i, can be effectively computed (Definition 5.5(6)). Since $N \subseteq N_i$, there is a canonical map $\rho_i \colon M = \mathbb{F}_p[\overline{X}^{\pm}]^d/N \to M_i = \mathbb{F}_p[\overline{X}^{\pm}]^d/N_i$. Since $N = \bigcap_{i=1}^l N_i$, the intersection of kernels $\bigcap_{i=1}^l \ker(\rho_i)$ is $\{0\}$.

▶ **Lemma 5.6.** *For $i = 1, \ldots, l$, let $\mathcal{Z}_i$ denote the set of solutions $(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_m) \in (\mathbb{Z}^n)^m$ of the following equation in M_i:*

$$\overline{X}^{\boldsymbol{z}_1} \cdot \rho_i(c_1) + \cdots + \overline{X}^{\boldsymbol{z}_m} \cdot \rho_i(c_m) = \rho_i(c_0). \tag{19}$$

Then the solution set of Equation (4) is exactly the intersection $\bigcap_{i=1}^l \mathcal{Z}_i$.

Proof. Since $\bigcap_{i=1}^l \ker(\rho_i) = \{0\}$, an element $y \in M$ is zero if and only if $\rho_i(y) = 0$ for all $i = 1, \ldots, l$. Equation (4) is equivalent to $\overline{X}^{\boldsymbol{z}_1} \cdot c_1 + \cdots + \overline{X}^{\boldsymbol{z}_m} \cdot c_m - c_0 = 0$. This holds if and only if $\rho_i\left(\overline{X}^{\boldsymbol{z}_1} \cdot c_1 + \cdots + \overline{X}^{\boldsymbol{z}_m} \cdot c_m - c_0\right) = 0$ for all $i = 1, \ldots, l$. Therefore, Equation (4) holds if and only if Equation (19) holds for all i. Hence, the solution set of Equation (4) is exactly $\bigcap_{i=1}^l \mathcal{Z}_i$. ◀

▶ **Example 5.2** (continued). In Example 5.2, we took R to be the ring $\mathbb{F}_2[X, Y]$, and M to be the finitely presented R-module $\mathbb{F}_2[X, Y]/Y^2(X + Y + 1)$. In this case, we have $M = \mathbb{F}_2[X, Y]/N$ with $N = \mathbb{F}_2[X, Y] \cdot Y^2(X + Y + 1)$, whose primary decomposition is $N = N_1 \cap N_2$, $N_1 = \mathbb{F}_2[X, Y] \cdot Y^2$, $N_2 = \mathbb{F}_2[X, Y] \cdot (X + Y + 1)$. The modules $M_1 = \mathbb{F}_2[X, Y]/N_1 = \mathbb{F}_2[X, Y]/Y^2$ and $M_2 = \mathbb{F}_2[X, Y]/N_2 = \mathbb{F}_2[X, Y]/(X + Y + 1)$ are respectively $\mathfrak{p}_1$ and $\mathfrak{p}_2$-coprimary, where $\mathfrak{p}_1$ is the ideal of R generated by Y, and $\mathfrak{p}_2$ is the ideal of R generated by $X + Y + 1$. The sets $\mathcal{Z}_1, \mathcal{Z}_2$ are respectively solutions of the equation $X^a + Y^b = 1$ in M_1 and M_2. ■

Our next step is to show that each $\mathcal{Z}_i$ is effectively p-automatic. If so, then their intersection $\bigcap_{i=1}^l \mathcal{Z}_i$ will also be p-automatic (see Lemma 2.3). Fix $i \in \{1, \ldots, l\}$. Note that Equation (19) is now an equation over the $\mathfrak{p}_i$-coprimary $\mathbb{F}_p[\overline{X}^{\pm}]$-module M_i. This motivates us to consider the quotient ring $\mathbb{F}_p[\overline{X}^{\pm}]/\mathfrak{p}_i$. We start with the following staple result in commutative algebra, which can be intuitively understood as performing a "change of variable" to simplify $\mathbb{F}_p[\overline{X}^{\pm}]/\mathfrak{p}_i$.

▶ **Lemma 5.7** (Noether Normalization Lemma [33, p.2]). *Let $\mathbb{K}$ be an infinite field and A be a finitely generated $\mathbb{K}$-algebra. Then there exist algebraically independent elements $\widetilde{X}_1, \ldots, \widetilde{X}_s \in A$ such that A is a finitely generated $\mathbb{K}[\widetilde{X}_1, \ldots, \widetilde{X}_s]$-module.*

Ideally we would want to apply the Noether Normalization Lemma to $A = \mathbb{F}_p[\overline{X}^{\pm}]/\mathfrak{p}_i$. Even though $\mathbb{F}_p$ is not an infinite field, we can without loss of generality replace it with its algebraic closure $\mathbb{K}$ (which is infinite). Formally, we replace $\mathfrak{p}_i$ with $\mathfrak{p}_i \otimes_{\mathbb{F}_p} \mathbb{K}$ and M_i with $M_i \otimes_{\mathbb{F}_p} \mathbb{K}$. Now $\mathfrak{p}_i$ and M_i are respectively an ideal and a module over the ring $\mathbb{K}[\overline{X}^{\pm}] = \mathbb{F}_p[\overline{X}^{\pm}] \otimes_{\mathbb{F}_p} \mathbb{K}$. Note that this does not change the solution set $\mathcal{Z}_i$.

The classical proof of Noether Normalization Lemma is constructive [33, p.2]. In our context, this means that given $A = \mathbb{K}[\overline{X}^{\pm}]/\mathfrak{p}_i$, the lemma explicitly gives the expressions for $\widetilde{X}_1, \ldots, \widetilde{X}_s \in A$ as elements in $\mathbb{K}[\overline{X}^{\pm}]/\mathfrak{p}_i$.

Choose $Y_1, \ldots, Y_s \in \mathbb{K}[\overline{X}^\pm]$ such that $Y_i + \mathfrak{p}_i = \widetilde{X}_i$ for all i. Since $\widetilde{X}_1, \ldots, \widetilde{X}_s$ are algebraically independent in $A = \mathbb{K}[\overline{X}^\pm]/\mathfrak{p}_i$, we have $\mathfrak{p}_i \cap \mathbb{K}[Y_1, \ldots, Y_s] = \{0\}$. Any finitely generated $\mathbb{K}[\overline{X}^\pm]$-module M is also a $\mathbb{K}[Y_1, \ldots, Y_s]$-module. However, M might not be finitely generated as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module. However, in case M is also finitely generated as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module, then a finite presentation can be effectively computed. This is summarized in the following rather standard result in effective commutative algebra.

▶ **Lemma 5.8** ([5, Section 2]). *Let $Y_1, \ldots, Y_s \in \mathbb{K}[\overline{X}^\pm]$. Suppose we are given the finite presentation of an $\mathbb{K}[\overline{X}^\pm]$-module M, as well as a finite number of generators $m_1, \ldots, m_t$ of M as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module. Then one can effectively compute the finite presentation of M as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module.*

Proof. Let $M = \mathbb{K}[\overline{X}^\pm]^d/N$ be its finite presentation as a $\mathbb{K}[\overline{X}^\pm]$-module. Let $f_1, \ldots f_s$ be polynomials in $\mathbb{K}[\overline{X}^\pm]$ that correspond to the elements $Y_1, \ldots Y_s$. Then M is also an effectively finitely presented module over the polynomial ring $\mathbb{K}[\overline{X}^\pm, Y_1, \ldots, Y_s]$ by $M \cong \mathbb{K}[\overline{X}^\pm, Y_1, \ldots, Y_s]^d / \big(\mathbb{K}[\overline{X}^\pm, Y_1, \ldots, Y_s] \cdot N + \sum_{i=1}^s (Y_i - f_i) \cdot \mathbb{K}[\overline{X}^\pm, Y_1, \ldots, Y_s]^d \big)$. Then, we can compute the finite presentation of the $\mathbb{K}[Y_1, \ldots, Y_s]$-submodule of M generated by $m_1, \ldots, m_t$ (see [5, Corollary 2.5]). This submodule is exactly M. ◀

▶ **Example 5.2** (continued). Consider the ideal $\mathfrak{p}_1$ of $\mathbb{K}[X, Y]$ generated by Y. Let A be the ring $\mathbb{K}[X, Y]/\mathfrak{p}_1 = \mathbb{K}[X, Y]/Y$. Then in the Noether Normalization Lemma we can let $s = 1$, and $\widetilde{X}_1 = X + \mathfrak{p}_1$. So $\mathbb{K}[X, Y]/Y \cong \mathbb{K}[\widetilde{X}_1]$ is a $\mathbb{K}[\widetilde{X}_1]$-module. Let $Y_1 = X_1$, then the $\mathbb{K}[X, Y]$-module $M_1 = \mathbb{K}[X, Y]/Y^2$ is a finitely presented $\mathbb{K}[Y_1]$-module $\mathbb{K}[Y_1]^2$. ■

▶ **Lemma 5.9.** *The set $\mathcal{Z}_i$ is effectively p-automatic.*

Proof. The main line of our proof follows [13, Lemma 9.7-9.8], with additional remarks given on effectiveness. As above, we can replace the base field $\mathbb{F}_p$ by its algebraic closure $\mathbb{K}$.

Since M_i is $\mathfrak{p}_i$-coprimary, we can compute $t \in \mathbb{N}$ such that $\mathfrak{p}_i^t M_i = 0$ (such t exists by the ascending chain condition [18, Chapter 1.4]). We have $M_i \supseteq \mathfrak{p}_i M_i \supseteq \mathfrak{p}_i^2 M_i \supseteq \cdots \supseteq \mathfrak{p}_i^t M_i = 0$. Because $\mathfrak{p}_i \cdot (\mathfrak{p}_i^j M_i/\mathfrak{p}_i^{j+1} M_i) = 0$, each quotient $\mathfrak{p}_i^j M_i/\mathfrak{p}_i^{j+1} M_i$ is a finitely generated $\mathbb{K}[\overline{X}^\pm]/\mathfrak{p}_i$-module with effectively computable generators, and therefore a finitely generated $\mathbb{K}[Y_1, \ldots, Y_s]$-module with effectively computable generators. It follows that the $\mathbb{K}[\overline{X}^\pm]$-module M_i is also finitely generated as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module, with effectively computable generators. Since the finite presentation of M_i as a $\mathbb{K}[\overline{X}^\pm]$-module is given, we can compute the finite presentation of M_i as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module by Lemma 5.8.

Since M_i is $\mathfrak{p}_i$-coprimary, the annihilator of any non-zero element in M_i as a $\mathbb{K}[Y_1, \ldots, Y_s]$-module is contained in $\mathfrak{p}_i \cap \mathbb{K}[Y_1, \ldots, Y_s] = \{0\}$ (see Definition 5.5(7)). Therefore, M_i is a finitely generated torsion-free $\mathbb{K}[Y_1, \ldots, Y_s]$-module (see Definition 5.5(3)).

Consider the quotient field $K := \mathbb{K}(Y_1, \ldots, Y_s)$ of $\mathbb{K}[Y_1, \ldots, Y_s]$. The localization $\widetilde{M_i} := M_i \otimes_{\mathbb{K}[Y_1, \ldots, Y_s]} K$ is a finite dimensional K-linear space, so $\widetilde{M_i} \cong K^d$ for some integer d. Because M_i is torsion-free, the canonical map $\varphi \colon M_i \to M_i \otimes_{\mathbb{K}[Y_1, \ldots, Y_s]} K$ is injective. The linear transformations $A_j \colon \widetilde{M_i} \to \widetilde{M_i}, y \mapsto X_j \cdot y$, commute for $j = 1, \ldots, n$, and they are respectively inverses of the transformations $A_j^{-1} \colon \widetilde{M_i} \to \widetilde{M_i}, y \mapsto X_j^{-1} \cdot y$. Hence, A_j is in $\mathsf{GL}_d(K)$ for $j = 1, \ldots, n$, for a fixed basis of $\widetilde{M_i} \cong K^d$, and these matrices commute.

Since φ is injective, Equation (19) holds if and only if

$$\overline{A}^{\boldsymbol{z}_1} \cdot \varphi(\rho_i(c_1)) + \cdots + \overline{A}^{\boldsymbol{z}_m} \cdot \varphi(\rho_i(c_m)) = \varphi(\rho_i(c_0)), \tag{20}$$

where $\overline{A} = (A_1, \ldots, A_n)$. So $\mathcal{Z}_i$ is the solution set for Equation (20). Note that $K = \mathbb{K}(Y_1, \ldots, Y_s)$ is an effective field. We now apply Corollary 5.4, and conclude that the solution set for Equation (20) is an effectively p-automatic subset of $(\mathbb{Z}^n)^m \cong \mathbb{Z}^{nm}$. ◀

▶ **Example 5.2** (continued). As above, the $\mathbb{K}[X,Y]$-module $M_1 = \mathbb{K}[X,Y]/Y^2$ is isomorphic to the $\mathbb{K}[X]$-module $\mathbb{K}[X]^2$ by $\mathbb{K}[X,Y]/Y^2 \xrightarrow{\sim} \mathbb{K}[X]^2$, $f_0 + Yf_1 + Y^2f_2 + \cdots \mapsto (f_0, f_1)$, for $f_0, f_1, f_2, \ldots \in \mathbb{K}[X]$.

We would like to solve the equation $X^a + Y^b = 1$ in M_1. Let $\mathbb{K}(X)$ denote the quotient field of $\mathbb{K}[X]$: this is the set of univariate rational functions over the field $\mathbb{K}$. Note that $\varphi : M_1 \cong \mathbb{K}[X]^2 \hookrightarrow \mathbb{K}(X)^2$ is injective. Consider $\mathbb{K}(X)^2$ as a 2-dimensional vector space over $\mathbb{K}(X)$, then the map $\varphi(m) \mapsto \varphi(X \cdot m), m \in M_1$, extends to a linear transformation associated to the matrix $A_X = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$, and the map $\varphi(m) \mapsto \varphi(Y \cdot m), m \in M_1$ extends to a linear transformation associated to the matrix $A_Y = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. (Here, A_Y is not invertible because the variable Y is not invertible in $\mathbb{K}[X,Y]$. However in the proof of Lemma 5.9, we are considering Laurent polynomial rings, so all the associated matrices would be invertible.)

As a result, the equation $X^a + Y^b = 1$ in M_1 is equivalent to the equation $A_X^a \cdot (1,0)^\top + A_Y^b (1,0)^\top = (1,0)^\top$ in the 2-dimensional vector space $\mathbb{K}(X)^2$. Subject to the invertibility of A_Y, we can then use Corollary 5.4 to conclude that the equation admits an effectively 2-automatic solution set. ∎

Combining Lemma 5.6 and Lemma 5.9, we obtain a proof of Theorem 3.3:

Proof of Theorem 3.3. By Lemma 5.6, the solution set of Equation (4) is the intersection $\bigcap_{i=1}^l \mathcal{Z}_i$. Lemma 5.9 shows that each $\mathcal{Z}_i$ is effectively p-automatic, so their intersection is also effectively p-automatic (Lemma 2.3). ◀

─── **References** ───

1   Boris Adamczewski and Jason P. Bell. On vanishing coefficients of algebraic power series over fields of positive characteristic. *Inventiones mathematicae*, 187(2):343–393, 2012.

2   László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. Multiplicative equations over commuting matrices. In *Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 498–507, 1996.

3   Sebastián Barbieri, Jarkko Kari, and Ville Salo. The group of reversible Turing machines. In *Cellular Automata and Discrete Complex Systems: 22nd IFIP WG 1.5 International Workshop, AUTOMATA 2016, Zurich, Switzerland, June 15-17, 2016, Proceedings 22*, pages 49–62. Springer, 2016.

4   Laurent Bartholdi and Ville Salo. Simulations and the lamplighter group. *Groups, Geometry, and Dynamics*, 16(4):1461–1514, 2022.

5   Gilbert Baumslag, Frank B. Cannonito, and Charles F. Miller III. Computable algebra and group embeddings. *Journal of Algebra*, 69(1):186–212, 1981.

6   Gilbert Baumslag, Frank B. Cannonito, and Derek J.S. Robinson. The algorithmic theory of finitely generated metabelian groups. *Transactions of the American Mathematical Society*, 344(2):629–648, 1994.

7   Robert Beals and László Babai. Las Vegas algorithms for matrix groups. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 427–436. IEEE, 1993. `doi:10.1109/SFCS.1993.366844`.

8   Michèle Benois. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris, Sér. A,*, 269:1188–1190, 1969.

9   Vincent D. Blondel, Emmanuel Jeandel, Pascal Koiran, and Natacha Portier. Decidable and undecidable problems about quantum automata. *SIAM Journal on Computing*, 34(6):1464–1473, 2005. `doi:10.1137/S0097539703425861`.

10 Corentin Bodart. Membership problems in nilpotent groups. *arXiv preprint arXiv:2401.15504*, 2024.

11 Michaël Cadilhac, Dmitry Chistikov, and Georg Zetzsche. Rational subsets of Baumslag-Solitar groups. In *47th International Colloquium on Automata, Languages, and Programming, ICALP*, volume 168 of *LIPIcs*, pages 116:1–116:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. `doi:10.4230/LIPICS.ICALP.2020.116`.

12 Thomas Colcombet, Joël Ouaknine, Pavel Semukhin, and James Worrell. On reachability problems for low-dimensional matrix semigroups. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*, volume 132 of *LIPIcs*, pages 44:1–44:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. `doi:10.4230/LIPICS.ICALP.2019.44`.

13 Harm Derksen. A Skolem–Mahler–Lech theorem in positive characteristic and finite automata. *Inventiones mathematicae*, 168(1):175–224, 2007.

14 Harm Derksen, Emmanuel Jeandel, and Pascal Koiran. Quantum automata and algebraic groups. *Journal of Symbolic Computation*, 39(3-4):357–371, 2005. `doi:10.1016/j.jsc.2004.11.008`.

15 Harm Derksen and David Masser. Linear equations over multiplicative groups, recurrences, and mixing I. *Proceedings of the London Mathematical Society*, 104(5):1045–1083, 2012.

16 Ruiwen Dong. Recent advances in algorithmic problems for semigroups. *ACM SIGLOG News*, 10(4):3–23, 2023.

17 Ruiwen Dong. Linear equations with monomial constraints and decision problems in abelian-by-cyclic groups. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1892–1908. SIAM, 2025.

18 David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

19 Moses Ganardi, Daniel König, Markus Lohrey, and Georg Zetzsche. Knapsack problems for wreath products. In *35th Symposium on Theoretical Aspects of Computer Science, STACS 2018, February 28 to March 3, 2018, Caen, France*, volume 96 of *LIPIcs*, pages 32:1–32:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018. `doi:10.4230/LIPICS.STACS.2018.32`.

20 Rostislav Grigorchuk and Andrzej Żuk. The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geometriae Dedicata*, 87(1):209–244, 2001.

21 Zeph Grunschlag. *Algorithms in geometric group theory*. University of California, Berkeley, 1999.

22 Philipp Hieronymi and Christian Schulz. A strong version of Cobham's theorem. *SIAM Journal on Computing*, 51(6):1400–1421, 2022. `doi:10.1137/22M1538065`.

23 Ehud Hrushovski, Joël Ouaknine, Amaury Pouly, and James Worrell. Polynomial invariants for affine programs. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 530–539, 2018. `doi:10.1145/3209108.3209142`.

24 Mark Kambites, Pedro V. Silva, and Benjamin Steinberg. The spectra of lamplighter groups and Cayley machines. *Geometriae Dedicata*, 120(1):193–227, 2006.

25 Toghrul Karimov, Florian Luca, Joris Nieuwveld, Joël Ouaknine, and James Worrell. On the decidability of Presburger arithmetic expanded with powers. In *Proceedings of the 2025 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2755–2778. SIAM, 2025.

26 Markus Lohrey. Membership problems in infinite groups. In *Conference on Computability in Europe*, pages 44–59. Springer, 2024.

27 Markus Lohrey and Benjamin Steinberg. The submonoid and rational subset membership problems for graph groups. *Journal of Algebra*, 320(2):728–755, 2008.

28 Markus Lohrey and Benjamin Steinberg. Tilings and submonoids of metabelian groups. *Theory of Computing Systems*, 48(2):411–427, 2011.

29 Markus Lohrey, Benjamin Steinberg, and Georg Zetzsche. Rational subsets and submonoids of wreath products. *Information and Computation*, 243:191–204, 2015.

30 Russell Lyons, Robin Pemantle, and Yuval Peres. Random walks on the lamplighter group. *The annals of probability*, pages 1993–2006, 1996.

31 A. Markov. On an unsolvable problem concerning matrices. *Doklady Akad. Nauk SSSR*, 78(6):1089–1092, 1951.

32 K. A. Mikhailova. The entrance problem for direct unions of groups. *Doklady Akad. Nauk SSSR*, 119(6):1103–1105, 1958.

33 David Mumford. *The Red Book of Varieties and Schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer, 1999.

34 Igor Potapov and Pavel Semukhin. Decidability of the membership problem for 2×2 integer matrices. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 170–186. SIAM, 2017.

35 Felix Potthast. Submonoid Membership for Wreath Products. Bachelor's thesis, Universität Siegen, 2020. Based on the unpublished draft of Doron Shafrir: *The Submonoid Problem in Torsion-by-$\mathbb{Z}^d$ Groups*, private communication with Markus Lohrey and Benjamin Steinberg. May 2018.

36 N.S. Romanovskii. Some algorithmic problems for solvable groups. *Algebra and Logic*, 13(1):13–16, 1974.

37 Elizabeth W. Rutman. Gröbner bases and primary decomposition of modules. *Journal of symbolic computation*, 14(5):483–503, 1992.

38 Doron Shafrir. Is decidability of the Submonoid Membership Problem closed under finite extensions? *arXiv preprint arXiv:2405.12921*, 2024.

39 Pedro V. Silva and Benjamin Steinberg. On a class of automata groups generalizing lamplighter groups. *International journal of algebra and computation*, 15(05n06):1213–1234, 2005.

40 Pierre Wolper and Bernard Boigelot. On the construction of automata from linear arithmetic constraints. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 1–19. Springer, 2000.