S-unit equations in modules

Ruiwen Dong

Magdalen College, University of Oxford

Based on joint work with Doron Shafrir

Workshop on Loop Invariants and Algebraic Reasoning, ICALP 2025

Consider the three following problems.

Problem 1: the Skolem Problem

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$2^n + 3^n - 13 = 0$$

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) \coloneqq 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$2^n + 3^n - 13 = 0 \iff n = 2.$$

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$\frac{1}{6}\left((-4+7i)^n + (-4-7i)^n\right) + \frac{1}{3}\left((8+i)^n + (8-i)^n\right) = 0$$

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu \colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$\frac{1}{6}\left((-4+7i)^n + (-4-7i)^n\right) + \frac{1}{3}\left((8+i)^n + (8-i)^n\right) = 0 \iff n = ?$$

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu \colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$\frac{1}{6}\left((-4+7i)^n + (-4-7i)^n\right) + \frac{1}{3}\left((8+i)^n + (8-i)^n\right) = 0 \iff n = ?$$

Theorem (Derksen 2007)

The Skolem Problem over a field of characteristic $p > 0$ is decidable.

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) := 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$\frac{1}{6}\left((-4+7i)^n + (-4-7i)^n\right) + \frac{1}{3}\left((8+i)^n + (8-i)^n\right) = 0 \iff n = ?$$

Theorem (Derksen 2007)

The Skolem Problem over a field of characteristic $p > 0$ is decidable.

Example in $\mathbb{K} = \mathbb{F}_2(X)$:

$$\mu(n) := (X+1)^n + X^n - 1$$

Problem 1: the Skolem Problem

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Skolem Problem)

Input: A linear recurrence sequence $\mu\colon \mathbb{N} \to \mathbb{K}$.
Question: Does there exist n such that $\mu(n) = 0$?

Example: $\mu(n) \coloneqq 2^n + 3^n - 13$.

Fact (Tao 2008, Ouaknine, Worrell, etc., since 2014)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem.

$$\frac{1}{6}\left((-4+7i)^n + (-4-7i)^n\right) + \frac{1}{3}\left((8+i)^n + (8-i)^n\right) = 0 \iff n = ?$$

Theorem (Derksen 2007)

The Skolem Problem over a field of characteristic $p > 0$ is decidable.

Example in $\mathbb{K} = \mathbb{F}_2(X)$:

$$\mu(n) \coloneqq (X+1)^n + X^n - 1 = 0 \iff n \text{ is a power of } 2.$$

Problem 2: sparse polynomials in ideals

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Examples:

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 2$.

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Examples:

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 2$.
Answer: Yes, I contains the polynomial $X^3 - 1$.

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Examples:

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 2$.
Answer: Yes, I contains the polynomial $X^3 - 1$.

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 1$.

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Examples:

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 2$.
Answer: Yes, I contains the polynomial $X^3 - 1$.

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 1$.
Answer: No, I does not contain any monomial.

Problem 2: finding sparse polynomial in ideals

Let $\mathbb{K}$ be a field (for example $\mathbb{Q}$).

Definition (Finding sparse polynomial in ideals)

Input: An ideal $I \subset \mathbb{K}[X_1, X_2, \ldots, X_n]$, and a positive number s.
Question: Does I contain a non-zero polynomial with at most s monomials?

Examples:

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 2$.
Answer: Yes, I contains the polynomial $X^3 - 1$.

Input: $I = \langle X^2 + X + 1 \rangle \subset \mathbb{Q}[X]$, and $s = 1$.
Answer: No, I does not contain any monomial.

Theorem (Jensen, Kahle and Katthän 2017)

Finding sparse polynomial in ideals over $\mathbb{Q}$ is decidable for $s = 1, 2$.

For $s \geq 3$, decidability is an open problem.

Problem 3: S-unit equation over fields

Problem 3: S-unit equation over fields

Question: Does $x_1 + 3x_2 = 6$ admit solutions where x_1, x_2 are powers of 2?

Problem 3: S-unit equation over fields

Question: Does $x_1 + 3x_2 = 6$ admit solutions where x_1, x_2 are powers of 2?

Question: Does $x_1 + 3x_2 = 6$ admit solutions x_1, x_2 of the form $2^n 3^m$, $n, m \in \mathbb{Z}$?

Problem 3: S-unit equation over fields

Question: Does $x_1 + 3x_2 = 6$ admit solutions where x_1, x_2 are powers of 2?

Question: Does $x_1 + 3x_2 = 6$ admit solutions x_1, x_2 of the form $2^n 3^m$, $n, m \in \mathbb{Z}$?

Let $\mathbb{K}$ be a field.

Definition (S-unit equation over $\mathbb{K}$)

Input: A finite set $S \subset \mathbb{K} \setminus \{0\}$, and a linear equation

$$x_1 m_1 + \cdots + x_d m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $x_1, \ldots, x_d$ in the multiplicative subgroup generated by S?

Problem 3: S-unit equation over fields

Question: Does $x_1 + 3x_2 = 6$ admit solutions where x_1, x_2 are powers of 2?

Question: Does $x_1 + 3x_2 = 6$ admit solutions x_1, x_2 of the form $2^n 3^m$, $n, m \in \mathbb{Z}$?

Let $\mathbb{K}$ be a field.

Definition (S-unit equation over $\mathbb{K}$)

Input: A finite set $S \subset \mathbb{K} \setminus \{0\}$, and a linear equation

$$x_1 m_1 + \cdots + x_d m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $x_1, \ldots, x_d$ in the multiplicative subgroup generated by S?

Fact (cf. Mahler 1933, Lang 1960, Evertse 1984, Schlickewei 1990, . . .)

Decidability of S-unit equations over $\mathbb{Q}$ is a difficult open problem.

Problem 3: S-unit equation over fields

Question: Does $x_1 + 3x_2 = 6$ admit solutions where x_1, x_2 are powers of 2?

Question: Does $x_1 + 3x_2 = 6$ admit solutions x_1, x_2 of the form $2^n 3^m$, $n, m \in \mathbb{Z}$?

Let $\mathbb{K}$ be a field.

Definition (S-unit equation over $\mathbb{K}$)

Input: A finite set $S \subset \mathbb{K} \setminus \{0\}$, and a linear equation

$$x_1 m_1 + \cdots + x_d m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $x_1, \ldots, x_d$ in the multiplicative subgroup generated by S?

Fact (cf. Mahler 1933, Lang 1960, Evertse 1984, Schlickewei 1990, ...)

Decidability of S-unit equations over $\mathbb{Q}$ is a difficult open problem.

Theorem (Adamczewski and Bell 2012, Derksen and Masser 2012)

S-unit equations over a field of characteristic $p > 0$ is decidable.

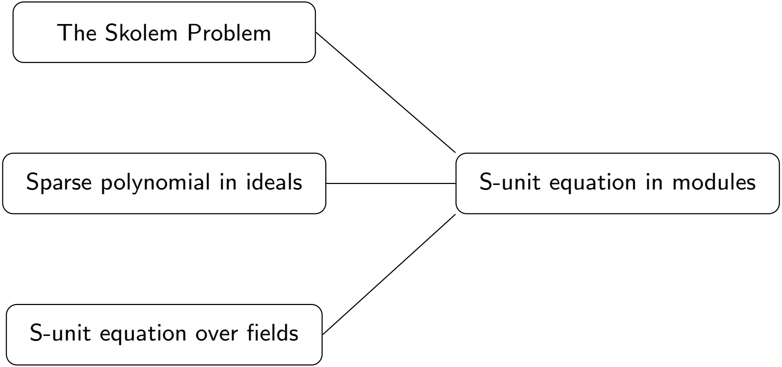
A unified approach?

The Skolem Problem

Sparse polynomial in ideals

S-unit equation over fields

A unified approach?



Motivation: consider the S-unit equation over $\mathbb{Q}$:

$$2^{z_1} + 2^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("powers of 2" solutions)

Motivation: consider the S-unit equation over $\mathbb{Q}$:

$$2^{z_1} + 2^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("powers of 2" solutions)

Equivalently, in the quotient ring $\mathcal{M} := \mathbb{Z}[X^{\pm}]/\langle X - 2\rangle$:

$$X^{z_1} + X^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("monomial" solutions)

Motivation: consider the S-unit equation over $\mathbb{Q}$:

$$2^{z_1} + 2^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("powers of 2" solutions)

Equivalently, in the quotient ring $\mathcal{M} := \mathbb{Z}[X^{\pm}] / \langle X - 2 \rangle$:

$$X^{z_1} + X^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("monomial" solutions)

The quotient $\mathcal{M} = \mathbb{Z}[X^{\pm}] / \langle X - 2 \rangle$ is a **finitely presented module** over $\mathbb{Z}[X^{\pm}]$

Motivation: consider the S-unit equation over $\mathbb{Q}$:

$$2^{z_1} + 2^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("powers of 2" solutions)

Equivalently, in the quotient ring $\mathcal{M} := \mathbb{Z}[X^{\pm}]/\langle X - 2\rangle$:

$$X^{z_1} + X^{z_2} \cdot 3 = 6,$$

where we look for solutions $z_1, z_2 \in \mathbb{Z}$. ("monomial" solutions)

The quotient $\mathcal{M} = \mathbb{Z}[X^{\pm}]/\langle X - 2\rangle$ is a **finitely presented module** over $\mathbb{Z}[X^{\pm}]$

In general, a **finitely presented module** over a ring R is defined as a quotient R^d/N, for an integer d and an R-submodule $N \subset R^d$.

S-unit equation in modules

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

S-unit equation in modules

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

Definition (S-unit equation over a field $\mathbb{K}$)

Input: A finite set $S \subset \mathbb{K} \setminus \{0\}$, and a linear equation over $\mathbb{K}$:

$$x_1 m_1 + \cdots + x_d m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $x_1, \dots, x_d$ in the multiplicative subgroup generated by S?

S-unit equation in modules

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{Sparse polynomial in ideals (over } \mathbb{F}_p\text{)}}$.

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{Sparse polynomial in ideals (over } \mathbb{F}_p)}$.

Input: an ideal $I \subset \mathbb{F}_2[X, Y]$.
Question: Does I contain a polynomial with 2 monomials?

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{Sparse polynomial in ideals (over } \mathbb{F}_p)}$.

Input: an ideal $I \subset \mathbb{F}_2[X, Y]$.
Question: Does I contain a polynomial with 2 monomials?

Equivalently:

Input: the module $\mathcal{M} = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/I$, and equation in $\mathcal{M}$:

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 0 \qquad (*)$$

Question: Does $(*)$ admit solutions $z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z}$?

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \ldots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \ldots, z_{1n}, \ldots, z_{d1}, z_{d2}, \ldots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{Sparse polynomial in ideals (over } \mathbb{F}_p)}$.

Input: an ideal $I \subset \mathbb{F}_2[X, Y]$.
Question: Does I contain a polynomial with 2 monomials?

Equivalently:

Input: the module $\mathcal{M} = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/I$, and equation in $\mathcal{M}$:

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 0 \iff X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} \in I \qquad (*)$$

Question: Does $(*)$ admit solutions $z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z}$?

S-unit equation in modules

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

S-unit equation in modules subsumes S-unit equation over (any) field.

S-unit equation in modules subsumes Sparse polynomial in ideals (over $\mathbb{F}_p$).

Input: an ideal $I \subset \mathbb{F}_2[X, Y]$.
Question: Does I contain a polynomial with 2 monomials?

Equivalently:

Input: the module $\mathcal{M} = \mathbb{F}_2[X^{\pm}, Y^{\pm}]/I = \mathbb{Z}[X^{\pm}, Y^{\pm}]/\langle I, 2\rangle$, and equation in $\mathcal{M}$:

$$X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} = 0 \iff X^{z_{11}} Y^{z_{12}} + X^{z_{21}} Y^{z_{22}} \in I \qquad (*)$$

Question: Does $(*)$ admit solutions $z_{11}, z_{12}, z_{21}, z_{22} \in \mathbb{Z}$?

S-unit equation in modules

Definition (S-unit equation in modules)

Input: A finitely presented $\mathbb{Z}[X_1^{\pm}, \dots, X_n^{\pm}]$-module $\mathcal{M}$, a linear equation in $\mathcal{M}$:

$$X_1^{z_{11}} X_2^{z_{12}} \cdots X_n^{z_{1n}} m_1 + \cdots + X_1^{z_{d1}} X_2^{z_{d2}} \cdots X_n^{z_{dn}} m_d = m_0 \qquad (*)$$

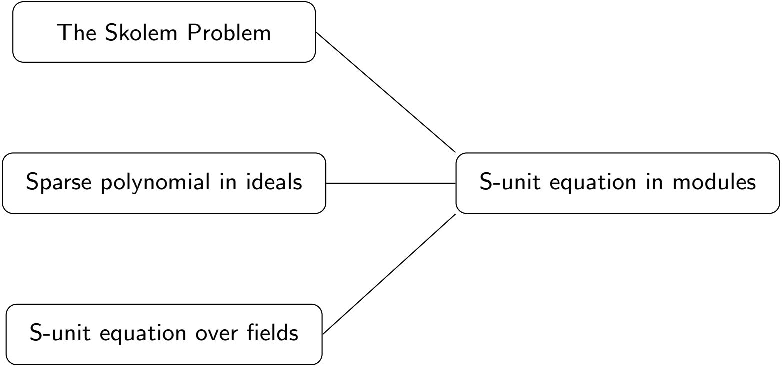
Question: Does $(*)$ have solutions $z_{11}, z_{12}, \dots, z_{1n}, \dots, z_{d1}, z_{d2}, \dots, z_{dn} \in \mathbb{Z}$?

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{S-unit equation over (any) field}}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{Sparse polynomial in ideals (over } \mathbb{F}_p)}$.

$\boxed{\text{S-unit equation in modules}}$ subsumes $\boxed{\text{(bi-)Skolem Problem (in simple LRS)}}$.

A (half-)unified approach



Decidability

Can we decide S-unit equation in modules?

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed* $\mathbb{Z}[X^{\pm}]$*-module* $\mathcal{M}$.

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed $\mathbb{Z}[X^{\pm}]$-module $\mathcal{M}$.*

Proof idea: embed Hilbert's tenth problem.

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed* $\mathbb{Z}[X^{\pm}]$*-module* $\mathcal{M}$.

Proof idea: embed Hilbert's tenth problem.

So what **can** we decide?

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed $\mathbb{Z}[X^{\pm}]$-module $\mathcal{M}$.*

Proof idea: embed Hilbert's tenth problem.

So what **can** we decide?

Fact (folklore, Derksen 2007)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem. But the Skolem Problem over a field of characteristic $p > 0$ is decidable.

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed $\mathbb{Z}[X^{\pm}]$-module $\mathcal{M}$.*

Proof idea: embed Hilbert's tenth problem.

So what **can** we decide?

Fact (folklore, Derksen 2007)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem. But the Skolem Problem over a field of characteristic $p > 0$ is decidable.

Fact (folklore, Adamczewski and Bell 2012, Derksen and Masser 2012)

Decidability of S-unit equations over $\mathbb{Q}$ is a difficult open problem. But S-unit equations over a field of characteristic $p > 0$ is decidable.

Decidability

Can we decide S-unit equation in modules?

Theorem (D., SODA'25)

Solving S-unit equations in finitely presented modules is **undecidable**, *even for a fixed $\mathbb{Z}[X^{\pm}]$-module $\mathcal{M}$.*

Proof idea: embed Hilbert's tenth problem.

So what **can** we decide?

Fact (folklore, Derksen 2007)

Decidability of the Skolem Problem over $\mathbb{Q}$ is a difficult open problem. But the Skolem Problem over a field of characteristic $p > 0$ is decidable.

Fact (folklore, Adamczewski and Bell 2012, Derksen and Masser 2012)

Decidability of S-unit equations over $\mathbb{Q}$ is a difficult open problem. But S-unit equations over a field of characteristic $p > 0$ is decidable.

Recall: a field $\mathbb{K}$ is of characteristic $p > 0$, if $px = 0$ for all $x \in \mathbb{K}$.

p is always prime.

T-torsion modules

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is ***T*-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is **T-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

For example, $\mathbb{Z}[X, Y]/\left\langle 6, X^2 + Y^2 \right\rangle$ is 6-torsion.

T-torsion modules

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is **T-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

For example, $\mathbb{Z}[X, Y]/\left\langle 6, X^2 + Y^2 \right\rangle$ is 6-torsion.

Theorem (D., ICALP'25)

When T is prime, solving S-unit equations in T-torsion modules is decidable.

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is **T-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

For example, $\mathbb{Z}[X, Y]/\left\langle 6, X^2 + Y^2 \right\rangle$ is 6-torsion.

Theorem (D., ICALP'25)

When T is prime, solving S-unit equations in T-torsion modules is decidable.

Theorem (D. and Shafrir, 2025)

When T has at most two different prime divisors (i.e. $T = p^a q^b$ for primes p, q, and $a, b \in \mathbb{N}$), solving S-unit equations in T-torsion modules is decidable.

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is **T-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

For example, $\mathbb{Z}[X, Y]/\left\langle 6, X^2 + Y^2 \right\rangle$ is 6-torsion.

Theorem (D., ICALP'25)

When T is prime, solving S-unit equations in T-torsion modules is decidable.

Theorem (D. and Shafrir, 2025)

When T has at most two different prime divisors (i.e. $T = p^a q^b$ for primes p, q, and $a, b \in \mathbb{N}$), solving S-unit equations in T-torsion modules is decidable.

Theorem (D. and Shafrir, 2025)

Let $T = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be its prime factorization. Solving S-unit equations in T-torsion modules is Turing equivalent to finding solutions to a system of linear equations over $\mathbb{Z}$, where variables can be restricted to powers of p_i.

Example: $T = 3 \times 5 \times 7$ subsumes finding $x_1, x_2, x_3 \in \mathbb{N}$, $3^{x_1} + 5^{x_2} - 7^{x_3} = 11$.

T-torsion modules

Definition

Let $T > 0$ be an integer. A module $\mathcal{M}$ is **T-torsion**, if $Tx = 0$ for all $x \in \mathcal{M}$.

For example, $\mathbb{Z}[X, Y]/\left\langle 6, X^2 + Y^2 \right\rangle$ is 6-torsion.

Theorem (D., ICALP'25)

When T is prime, solving S-unit equations in T-torsion modules is decidable.

Theorem (D. and Shafrir, 2025)

When T has at most two different prime divisors (i.e. $T = p^a q^b$ for primes p, q, and $a, b \in \mathbb{N}$), solving S-unit equations in T-torsion modules is decidable.

Theorem (D. and Shafrir, 2025)

Let $T = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be its prime factorization. Solving S-unit equations in T-torsion modules is Turing equivalent to finding solutions to a system of linear equations over $\mathbb{Z}$, where variables can be restricted to powers of p_i.

Example: $T = 3 \times 5 \times 7$ subsumes finding $x_1, x_2, x_3 \in \mathbb{N}$, $3^{x_1} + 5^{x_2} - 7^{x_3} = 11$.

Difficult open problem for $k \geq 3$.

Main ingredients for our proofs

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $\quad (X+1)^n + X^n = 1 \quad$ over the field $\mathbb{F}_2(X)$.

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

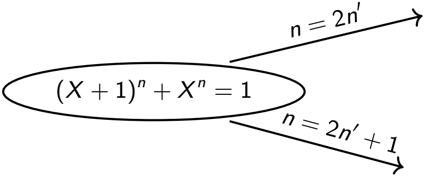
$$(X+1)^n + X^n = 1$$

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.



Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

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

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

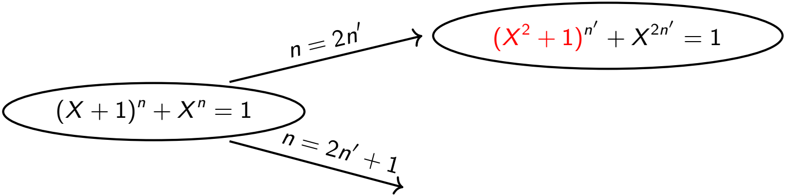
Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

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

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

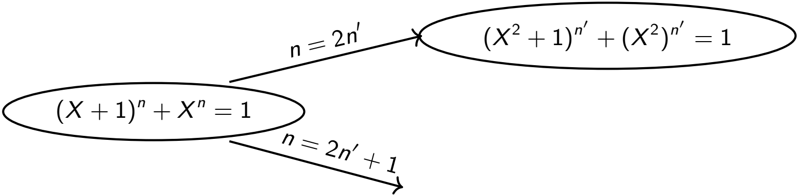


$^*(X+1)^2 = X^2 + 1$

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.



Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

$$(X+1)^n + X^n = 1 \xrightarrow{n = 2n'} (X'+1)^{n'} + (X')^{n'} = 1$$

$$(X+1)^n + X^n = 1 \xrightarrow{n = 2n'+1}$$

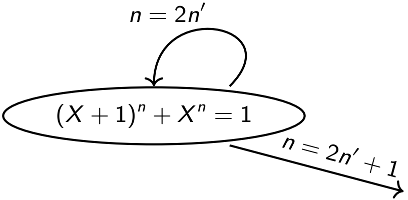
---

*let $X' := X^2$

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

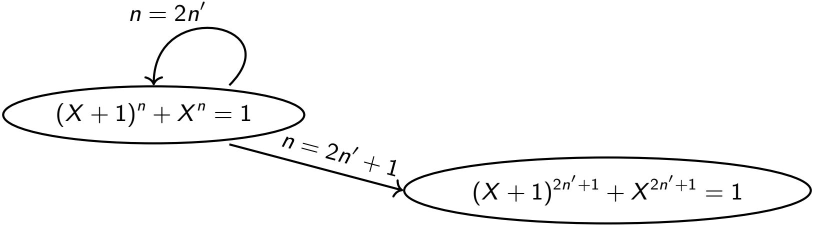


Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

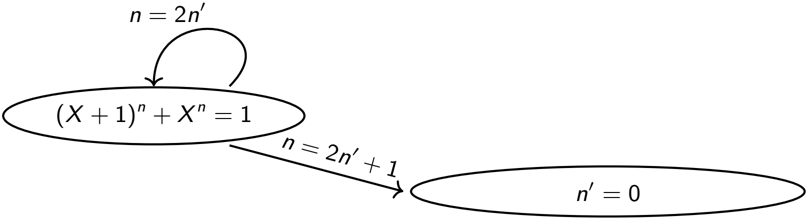


Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.

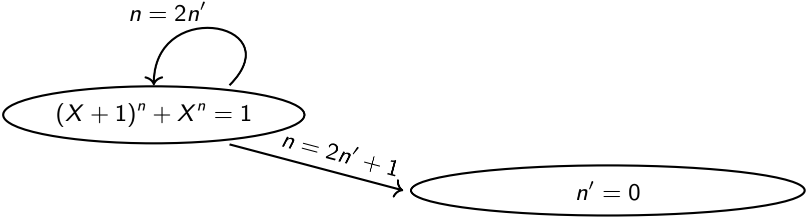


Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.



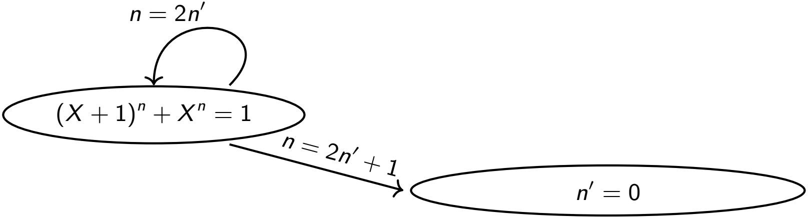
This automaton recognizes the solution set $\{2^k \mid k \in \mathbb{N}\}$.

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ to the Skolem Problem over a field of characteristic $p > 0$ is effectively p-automatic.

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.



This automaton recognizes the solution set $\{2^k \mid k \in \mathbb{N}\}$.

Theorem (Adamczewski and Bell 2012)

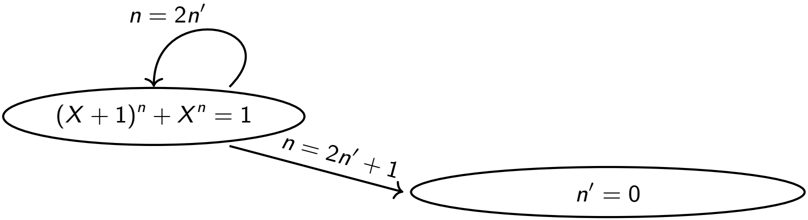
The solution set to an **S-unit equation** *over a field of characteristic $p > 0$ is effectively p-automatic.*

Derksen's approach: p-automata

Theorem (Derksen 2007)

The solution set $\{n \in \mathbb{N} \mid \mu(n) = 0\}$ *to the Skolem Problem over a field of characteristic* $p > 0$ *is effectively* p*-automatic.*

Example: we solve the equation $(X+1)^n + X^n = 1$ over the field $\mathbb{F}_2(X)$.



This automaton, in which no two cycles intersect, recognizes the solution set $\{2^k \mid k \in \mathbb{N}\}$.

Theorem (Adamczewski and Bell 2012, Derksen and Masser 2012)

The solution set to an **S-unit equation** *over a field of characteristic* $p > 0$ *is definable in existential Presburger arithmetic with* p*-power predicate.*

Generalizing from fields to modules:

Theorem (D. and Shafrir, 2025)

The solution set to an S-unit equation **in a p^a-torsion module** *is p-automatic, and definable in existential Presburger arithmetic with p-power predicate.*

Generalizing from fields to modules:

Theorem (D. and Shafrir, 2025)

The solution set to an S-unit equation **in a p^a-torsion module** *is p-automatic, and definable in existential Presburger arithmetic with p-power predicate.*

Proof idea: use primary decomposition to reduce to the case of **local rings**, and generalize Derksen's automata from **fields** to local rings. (very technical)

Generalizing from fields to modules:

Theorem (D. and Shafrir, 2025)

The solution set to an S-unit equation **in a p^a-torsion module** *is p-automatic, and definable in existential Presburger arithmetic with p-power predicate.*

Proof idea: use primary decomposition to reduce to the case of **local rings**, and generalize Derksen's automata from **fields** to local rings. (very technical)

Theorem (Karimov, Luca, Nieuwveld, Ouaknine and Worrell, SODA'25)

Let $p, q \in \mathbb{N}$. Existential Presburger arithmetic with a p-power predicate and a q-power predicate is decidable.

Generalizing to modules

Generalizing from fields to modules:

Theorem (D. and Shafrir, 2025)

The solution set to an S-unit equation **in a p^a-torsion module** *is p-automatic, and definable in existential Presburger arithmetic with p-power predicate.*

Proof idea: use primary decomposition to reduce to the case of **local rings**, and generalize Derksen's automata from **fields** to local rings. (very technical)

Theorem (Karimov, Luca, Nieuwveld, Ouaknine and Worrell, SODA'25)

Let $p, q \in \mathbb{N}$. Existential Presburger arithmetic with a p-power predicate and a q-power predicate is decidable.

Corollary

It is decidable whether an S-unit equation over a $p^a q^b$-torsion module admits a solution.

Generalizing to modules

Generalizing from fields to modules:

Theorem (D. and Shafrir, 2025)

The solution set to an S-unit equation **in a p^a-torsion module** *is p-automatic, and definable in existential Presburger arithmetic with p-power predicate.*

Proof idea: use primary decomposition to reduce to the case of **local rings**, and generalize Derksen's automata from **fields** to local rings. (very technical)

Theorem (Karimov, Luca, Nieuwveld, Ouaknine and Worrell, SODA'25)

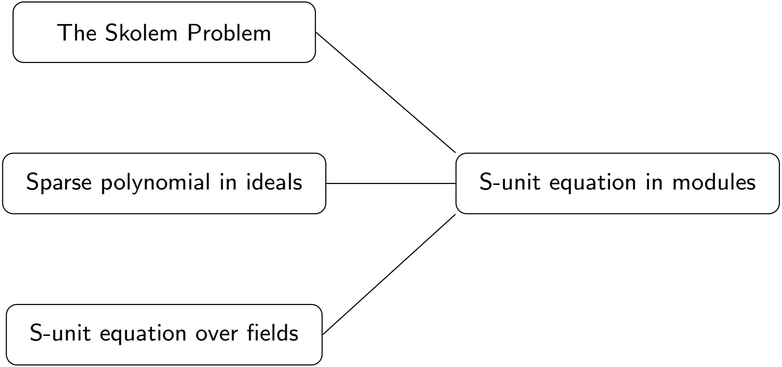
Let $p, q \in \mathbb{N}$. Existential Presburger arithmetic with a p-power predicate and a q-power predicate is decidable.

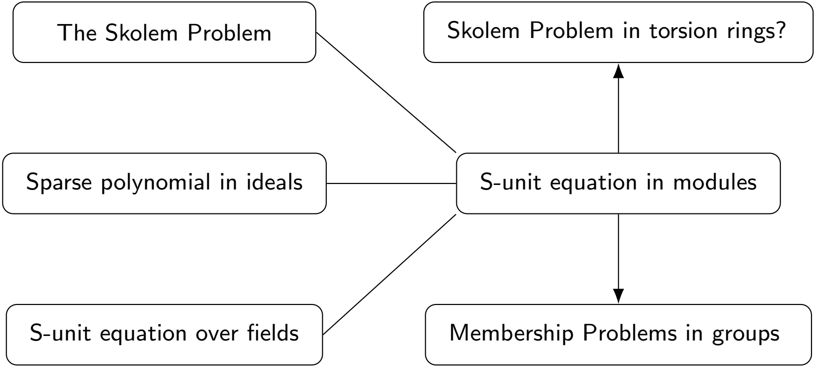
Corollary

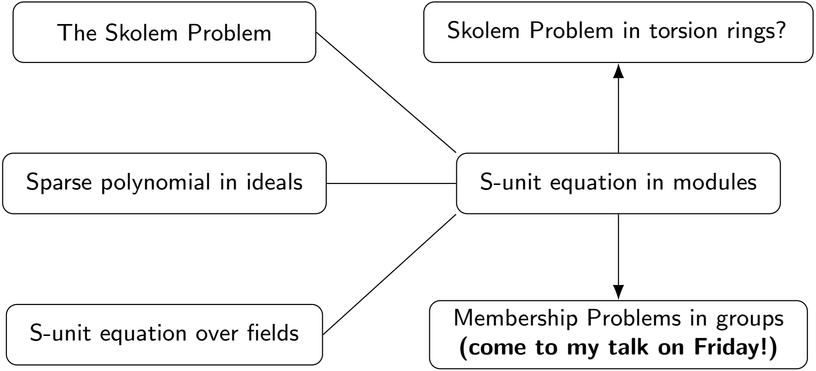
It is decidable whether an S-unit equation over a $p^a q^b$-torsion module admits a solution.

With some more work: hardness result for general T-torsion modules.

Future work and applications




The Skolem Problem
Skolem Problem in torsion rings?
Sparse polynomial in ideals
S-unit equation in modules
S-unit equation over fields
Membership Problems in groups


The Skolem Problem
Skolem Problem in torsion rings?
Sparse polynomial in ideals
S-unit equation in modules
S-unit equation over fields
Membership Problems in groups
(come to my talk on Friday!)