On the Existential Theory of the Reals Enriched with Integer Powers of a Computable Number

Jorge Gallego Hernández, Alessio Mansutti

IMDEA Software

March 4, 2025

Tarski arithmetic + Exponentiation

Tarski arithmetic: First Order theory of $(\mathbb{R}; +, \cdot, \leq)$.

Tarski arithmetic + Exponentiation

Tarski arithmetic: First Order theory of $(\mathbb{R}; +, \cdot, \leq)$.

$\mathbb{R}(e^x)$: extension of Tarski arithmetic with $x \mapsto e^x$.

Tarski arithmetic + Exponentiation

Tarski arithmetic: First Order theory of $(\mathbb{R}; +, \cdot, \leq)$.

$\mathbb{R}(e^x)$: extension of Tarski arithmetic with $x \mapsto e^x$.

Several applications:

- Entropic risk threshold problem for stochastic games
- Containment problem for probabilistic automata
- Reachability problem for Linear Time-Invariant systems
- Verification of Deep Neural Networks
- Deciding accuracy of Differential Privacy Schemes ...

Tarski arithmetic + Exponentiation

Tarski arithmetic: First Order theory of $(\mathbb{R}; +, \cdot, \leq)$.

$\mathbb{R}(e^x)$: extension of Tarski arithmetic with $x \mapsto e^x$.

Several applications:

- Entropic risk threshold problem for stochastic games
- Containment problem for probabilistic automata
- Reachability problem for Linear Time-Invariant systems
- Verification of Deep Neural Networks
- Deciding accuracy of Differential Privacy Schemes ...

Theorem (Macintyre and Wilkie, 1996)

$\mathbb{R}(e^x)$ *is decidable subject to Schanuel's Conjecture.*

Tarski arithmetic + Exponentiation

Goal of our work:

Study variations of $\mathbb{R}(e^x)$ that are **unconditionally decidable** and can be used for some known applications.

Ta

$\mathbb{R}(e$

Sev

- Entropic risk threshold problem for stochastic games
- Containment problem for probabilistic automata
- Reachability problem for Linear Time-Invariant systems
- Verification of Deep Neural Networks
- Deciding accuracy of Differential Privacy Schemes ...

Theorem (Macintyre and Wilkie, 1996)

$\mathbb{R}(e^x)$ *is decidable subject to Schanuel's Conjecture.*

Tarski arithmetic + Exponentiation

Goal of our work:

Study variations of $\mathbb{R}(e^x)$ that are **unconditionally decidable** and can be used for some known applications.

- **Entropic risk threshold problem for stochastic games**
- Containment problem for probabilistic automata
- Reachability problem for Linear Time-Invariant systems
- Verification of Deep Neural Networks

Corollary of our work:

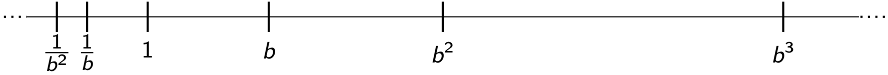
The entropic risk threshold problem for turn-based stochastic games [Baier et al. MFCS 2023] is **unconditionally decidable**.

Our work

We study the existential theory of $(\mathbb{R}; b, +, \cdot, b^{\mathbb{Z}}(x), \leq)$ denoted $\exists\mathbb{R}(b^{\mathbb{Z}})$.

Where:

- $b > 0$ is a fixed computable real number.
- $b^{\mathbb{Z}}(x)$ is a unary predicate, true for integer powers of b.



Our work

We study the existential theory of $(\mathbb{R}; b, +, \cdot, b^{\mathbb{Z}}(x), \leq)$ denoted $\exists\mathbb{R}(b^{\mathbb{Z}})$.

Where:

- $b > 0$ is a fixed computable real number.
- $b^{\mathbb{Z}}(x)$ is a unary predicate, true for integer powers of b.

Theorem

Fix a real number $b > 0$. The satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is

1. *in* EXPSPACE *whenever b is an algebraic number α.*
2. *in* 3EXPTIME *if $b \in \{\pi, e^{\pi}, e^{\alpha}, \alpha^{\beta}, \ln(\alpha), \frac{\ln(\alpha)}{\ln(\beta)} : \alpha, \beta$ algebraic$\}$.*
3. *decidable whenever b is a computable transcendental number.*

(We now also know that $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in EXPTIME for $b \in \mathbb{Q}$)

Our work

We study the existential theory of $(\mathbb{R}; b, +, \cdot, b^{\mathbb{Z}}(x), \leq)$ denoted $\exists\mathbb{R}(b^{\mathbb{Z}})$.

Where:

- $b > 0$ is a fixed computable real number.
- $b^{\mathbb{Z}}(x)$ is a unary predicate, true for integer powers of b.

Theorem

Fix a real number $b > 0$. The satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is

1. *in* EXPSPACE *whenever b is an algebraic number α.*
2. *in* 3EXPTIME *if $b \in \{\pi, e^{\pi}, e^{\alpha}, \alpha^{\beta}, \ln(\alpha), \frac{\ln(\alpha)}{\ln(\beta)} : \alpha, \beta$ algebraic$\}$.*
3. *decidable whenever b is a computable transcendental number.*

(We now also know that $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in EXPTIME for $b \in \mathbb{Q}$)

Our work

WARNING! This theorem needs:

- In ❶ and ❷, representations of α, β (polynomials having these numbers as roots and isolating intervals).
- In ❸ a Turing Machine that computes b.
(For n in unary, the TM returns x_n s.t. $|b - x_n| \leq 2^{-n}$)

Theorem

Fix a real number $b > 0$. *The satisfiability problem* $\exists\mathbb{R}(b^{\mathbb{Z}})$ *is*

① *in* EXPSPACE *whenever* b *is an algebraic number* α.

② *in* 3EXPTIME *if* $b \in \{\pi, e^{\pi}, e^{\alpha}, \alpha^{\beta}, \ln(\alpha), \frac{\ln(\alpha)}{\ln(\beta)} : \alpha, \beta \text{ algebraic}\}$.

③ *decidable whenever* b *is a computable transcendental number.*

(We now also know that $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in EXPTIME for $b \in \mathbb{Q}$)

The theory $\exists\mathbb{R}(b^{\mathbb{Z}})$

Grammar:

$$\varphi, \psi \coloneqq P(b, \boldsymbol{x}) \sim 0 \mid b^{\mathbb{Z}}(x) \mid \top \mid \bot \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \exists x\ \varphi$$

Where $P(b, \boldsymbol{x})$ are **integer polynomials** and $\sim$ belongs to $\{<, =\}$.

Examples:

- $\exists x : x^2 - 5 = 0 \wedge b^{\mathbb{Z}}(x)$
- $\exists x \exists y : b^{\mathbb{Z}}(x) \wedge x \leq y^3 < b^2 x$

The theory $\exists\mathbb{R}(b^{\mathbb{Z}})$

Grammar:

$$\varphi, \psi \coloneqq P(b, \boldsymbol{x}) \sim 0 \mid b^{\mathbb{Z}}(x) \mid \top \mid \bot \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \exists x \ \varphi$$

Where $P(b, \boldsymbol{x})$ are **integer polynomials** and $\sim$ belongs to $\{<, =\}$.

Examples:

- $\exists x : x^2 - 5 = 0 \wedge b^{\mathbb{Z}}(x)$
- $\exists x \exists y : b^{\mathbb{Z}}(x) \wedge x \leq y^3 < b^2 x$

Notation:

- $\deg(P)$: degree of P.
- $\mathrm{h}(P)$: maximum coeff. of P in absolute value (height).

Related work

1986 Van den Dries: FO $\mathbb{R}(2^{\mathbb{Z}})$ is decidable. [Manuscripta Math.]

2007 Avigad and Yin: FO $\mathbb{R}(2^{\mathbb{Z}})$ is in TOWER. [Theor. Comput. Sci.]

2010 Hieronymi: FO $\mathbb{R}(2^{\mathbb{Z}}, 3^{\mathbb{Z}})$ is undecidable. [Proc. Am. Math. Soc.]

2012 Achatz et al.: $\exists x \exists y : y = e^x \wedge \varphi(x, y)$ decidable. [J. Symb. Comp.]

Related work

1986 Van den Dries: FO $\mathbb{R}(2^{\mathbb{Z}})$ is decidable. [Manuscripta Math.]

2007 Avigad and Yin: FO $\mathbb{R}(2^{\mathbb{Z}})$ is in TOWER. [Theor. Comput. Sci.]

2010 Hieronymi: FO $\mathbb{R}(2^{\mathbb{Z}}, 3^{\mathbb{Z}})$ is undecidable. [Proc. Am. Math. Soc.]

2012 Achatz et al.: $\exists x \exists y : y = e^x \wedge \varphi(x, y)$ decidable. [J. Symb. Comp.]

Takeaways from previous work:

- Algebraic numbers allow to establish complexity results.
- Transcendental numbers are difficult to handle complexity-wise.

A way to avoid Schanuel's Conjecture: Root barriers

Problem: For x computable, checking the sign of $P(x)$ is undecidable.

Intuition: Any approximation x_n could yield $P(x_n) \neq 0$ while $P(x) = 0$.

Solution: Suppose to know a number t s.t. either $P(x) = 0$ or $|P(x)| > t$.
Then the problem becomes **decidable**.

A way to avoid Schanuel's Conjecture: Root barriers

Problem: For x computable, checking the sign of $P(x)$ is undecidable.

Intuition: Any approximation x_n could yield $P(x_n) \neq 0$ while $P(x) = 0$.

Solution: Suppose to know a number t s.t. either $P(x) = 0$ or $|P(x)| > t$. Then the problem becomes **decidable**.

Definition (Root barrier)

A function $\sigma : (\mathbb{N}_{\geq 1})^2 \to \mathbb{N}$ is a root barrier of $b \in \mathbb{R}$ if for every integer polynomial $P(x)$, either $P(b) = 0$ or $|P(b)| \geq \frac{1}{2^{\sigma(\deg(P),\mathrm{h}(P))}}$.

A way to avoid Schanuel's Conjecture: Root barriers

Problem: For x computable, checking the sign of $P(x)$ is undecidable.

Intuition: Any approximation x_n could yield $P(x_n) \neq 0$ while $P(x) = 0$.

Solution: Suppose to know a number t s.t. either $P(x) = 0$ or $|P(x)| > t$. Then the problem becomes **decidable**.

Definition (Root barrier)

A function $\sigma : (\mathbb{N}_{\geq 1})^2 \to \mathbb{N}$ is a root barrier of $b \in \mathbb{R}$ if for every integer polynomial $P(x)$, either $P(b) = 0$ or $|P(b)| \geq \frac{1}{2^{\sigma(\deg(P),\mathrm{h}(P))}}$.

Focus on numbers that have a **polynomial root barrier**:

(degree of the root barrier)

$$\sigma(d, h) = c \cdot (d + \lceil \log h \rceil)^{k} \qquad c, k \in \mathbb{N}$$

A general theorem

Theorem

Let $b > 0$ a ptime computable real number with a root barrier of degree k.

1. *If $k = 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 2EXPTIME.*
2. *If $k > 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 3EXPTIME.*

A general theorem

Theorem

Let $b > 0$ *a ptime computable real number with a root barrier of degree* k.

1. *If* $k = 1$, *the satisfiability problem* $\exists\mathbb{R}(b^{\mathbb{Z}})$ *is in 2EXPTIME.*
2. *If* $k > 1$, *the satisfiability problem* $\exists\mathbb{R}(b^{\mathbb{Z}})$ *is in 3EXPTIME.*

Finding k is difficult in general.

- Algebraic numbers have always $k = 1$.

  (2EXPTIME can be improved to EXPSPACE with small tricks.)

- π, e, $\log \alpha$ ... all have $k > 1$.

  (See work of Waldschmidt on transcendence measures.)

Procedure overview

Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \dots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

Procedure overview

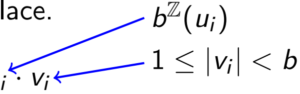
Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \ldots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

1. Guess which variables equal 0 and replace.
2. Replace each x_i with a factorization $u_i \cdot v_i$
3. Eliminate all the v_i with a quantifier elimination procedure for Tarski arithmetic (use, e.g. [Basu, Pollack and Roy, 1996]).

Procedure overview

Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \ldots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

1. Guess which variables equal 0 and replace.
2. Replace each x_i with a factorization $u_i \cdot v_i$
3. Eliminate all the v_i with a quantifier elimination procedure for Tarski arithmetic (use, e.g. [Basu, Pollack and Roy, 1996]).



$b^{\mathbb{Z}}(u_i)$

$1 \leq |v_i| < b$

Procedure overview

Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \ldots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

1. Guess which variables equal 0 and replace.
2. Replace each x_i with a factorization $u_i \cdot v_i$

   $b^{\mathbb{Z}}(u_i)$

   $1 \leq |v_i| < b$
3. Eliminate all the v_i with a quantifier elimination procedure for Tarski arithmetic (use, e.g. [Basu, Pollack and Roy, 1996]).

Remark

At this point we obtained $\psi(u_1, \ldots, u_n)$, an **equisatisfiable** formula to φ where all the variables range over $b^{\mathbb{Z}}$.

Procedure overview

Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \ldots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

1. Guess which variables equal 0 and replace.

$b^{\mathbb{Z}}(u_i)$

$1 \leq |v_i| < b$

2. Replace each x_i with a factorization $u_i \cdot v_i$
3. Eliminate all the v_i with a quantifier elimination procedure for Tarski arithmetic (use, e.g. [Basu, Pollack and Roy, 1996]).
4. Guess a small exponent $g_i \in \mathbb{Z}$ for all u_i (**Small witness property**)
5. Check if $(u_1 = b^{g_1}, \ldots, u_n = b^{g_n})$ is a solution to ψ

Procedure overview

Fixed: $b > 1$ computable number with a polynomial root barrier.
Input: $\varphi(x_1, \ldots, x_n)$, quantifier-free formula from $\exists\mathbb{R}(b^{\mathbb{Z}})$.
Output: **True** if φ is satisfiable, and **False** otherwise.

① Guess which variables equal 0 and replace.

$b^{\mathbb{Z}}(u_i)$

$1 \leq |v_i| < b$

② Replace each x_i with a factorization $u_i \cdot v_i$

③ Eliminate all the v_i with a quantifier elimination procedure for Tarski arithmetic (use, e.g. [Basu, Pollack and Roy, 1996]).

④ Guess a small exponent $g_i \in \mathbb{Z}$ for all u_i (**Small witness property**)

⑤ Check if $(u_1 = b^{g_1}, \ldots, u_n = b^{g_n})$ is a solution to ψ

Small witness property

Proposition (Small Witness Property)

Fix $b > 1$ having a root barrier of degree k.

If a quantifier free formula $\psi(u_1, \dots, u_n)$ over $b^{\mathbb{Z}}$ has a solution then it has one assigning to each variable a number $b^g \in b^{\mathbb{Z}}$ where

$$|g| \leq (2^c \log(\mathrm{h}(\psi)))^{\deg(\psi)^{O(n^2)}} k^{\deg(\psi)^{O(n)}}$$

Small witness property

Proposition (Small Witness Property)

Fix $b > 1$ having a root barrier of degree k.

If a quantifier free formula $\psi(u_1, \dots, u_n)$ over $b^{\mathbb{Z}}$ has a solution then it has one assigning to each variable a number $b^g \in b^{\mathbb{Z}}$ where

$$|g| \leq (2^c \log(\mathrm{h}(\psi)))^{\deg(\psi)^{O(n^2)}} k^{\deg(\psi)^{O(n)}}$$

Theorem

Let $b > 0$ a ptime computable real number with a root barrier of degree k.

1. *If $k = 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 2EXPTIME.*
2. *If $k > 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 3EXPTIME.*

Small witness property

Proposition (Small Witness Property)

Fix $b > 1$ having a root barrier of degree k.

If a quantifier free formula $\psi(u_1, \dots, u_n)$ over $b^{\mathbb{Z}}$ has a solution then it has one assigning to each variable a number $b^g \in b^{\mathbb{Z}}$ where

$$|g| \leq (2^c \log(\mathrm{h}(\psi)))^{\deg(\psi)^{O(n^2)}} \cancel{k^{\deg(\psi)^{O(n)}}}$$

Theorem

Let $b > 0$ a ptime computable real number with a root barrier of degree k.

1. *If $k = 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 2EXPTIME.*
2. *If $k > 1$, the satisfiability problem $\exists\mathbb{R}(b^{\mathbb{Z}})$ is in 3EXPTIME.*

Small witness property

Proposition (Small Witness Property)

Fix $b > 1$ having a root barrier of degree k.

If a quantifier free formula $\psi(u_1, \ldots, u_n)$ over $b^{\mathbb{Z}}$ has a solution then it has one assigning to each variable a number $b^g \in b^{\mathbb{Z}}$ where

$$|g| \leq (2^c \log(\mathrm{h}(\psi)))^{\deg(\psi)^{O(n^2)}} k^{\deg(\psi)^{O(n)}}$$

Done by removing $u_1, \ldots, u_n$, one by one but with a twist.

$$\begin{cases} u_1 = b^{k_1} \cdot z_1^{\ell_1} \cdot z_2^{\ell_2} \\ u_2 = z_1^{j_1} \cdot b^{r_1} \\ u_3 = z_2^{j_1} \cdot b^{r_2} \end{cases} \longrightarrow \begin{cases} z_1 = b^{k_2} \cdot z_3^{\ell_3} \\ z_2 = z_3^{j_2} \cdot b^{r_3} \end{cases} \longrightarrow \begin{cases} z_3 = b^{k_3} \end{cases}$$

elimination of u_1 elimination of z_1 elimination of z_3

Conclusion

We studied the complexity of $\exists\mathbb{R}(b^{\mathbb{Z}})$:

- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ EXPSPACE for b algebraic.
- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ 3EXPTIME for b among e, π and others.
- **Fundamental notion:** polynomial root barriers.
- **Application:** Entropic risk threshold problem for stochastic games is **unconditionally** decidable.

Conclusion

We studied the complexity of $\exists\mathbb{R}(b^{\mathbb{Z}})$:

- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ EXPSPACE for b algebraic.
- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ 3EXPTIME for b among e, π and others.
- **Fundamental notion:** polynomial root barriers.
- **Application:** Entropic risk threshold problem for stochastic games is **unconditionally** decidable.

Future work:

- How far are we from the **exact complexity** of these theories?
- Is $\exists\mathbb{R}(a^{\mathbb{Z}}, b^{\mathbb{Z}})$ decidable for some $a, b \in \mathbb{R}$ with $a^{\mathbb{Z}} \cap b^{\mathbb{Z}} = \{1\}$?
- Can we remove appeals to Schanuel's conjecture in other applications?

Conclusion

We studied the complexity of $\exists\mathbb{R}(b^{\mathbb{Z}})$:

Thank you for your time

- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ EXPSPACE for b algebraic.
- $\exists\mathbb{R}(b^{\mathbb{Z}}) \in$ 3EXPTIME for b among e, π and others.
- **Fundamental notion:** polynomial root barriers.
- **Application:** Entropic risk threshold problem for stochastic games is **unconditionally** decidable.

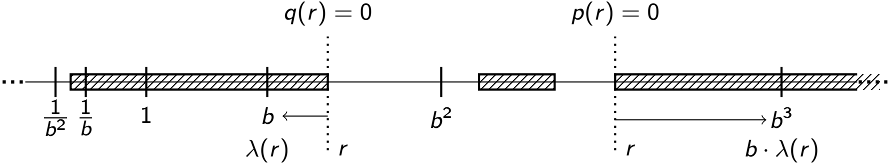
Future work:

- How far are we from the **exact complexity** of these theories?
- Is $\exists\mathbb{R}(a^{\mathbb{Z}}, b^{\mathbb{Z}})$ decidable for some $a, b \in \mathbb{R}$ with $a^{\mathbb{Z}} \cap b^{\mathbb{Z}} = \{1\}$?
- Can we remove appeals to Schanuel's conjecture in other applications?

APPENDIX

Small witness property: Finding the substitutions

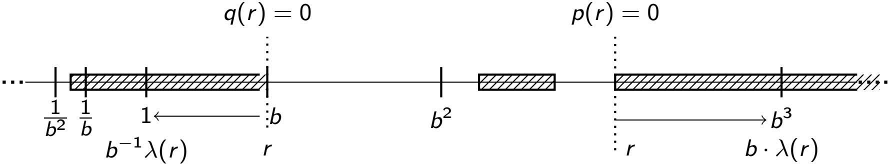
Fix $u_2, \ldots, u_n$. **Over $\mathbb{R}$**, solutions of $\psi(u_1)$ form a **finite set** of intervals.



If an interval contains an element of $b^{\mathbb{Z}}$, then it contains one close to a root r. Hence, we can restrict to $u_1 \in \{b^{-1} \cdot \lambda(r), \lambda(r), b \cdot \lambda(r)\}$.

Small witness property: Finding the substitutions

Fix $u_2, \dots, u_n$. **<u>Over $\mathbb{R}$</u>**, solutions of $\psi(u_1)$ form a **finite set** of intervals.



If an interval contains an element of $b^{\mathbb{Z}}$, then it contains one close to a root r. Hence, we can restrict to $u_1 \in \{b^{-1} \cdot \lambda(r), \lambda(r), b \cdot \lambda(r)\}$.

Small witness property: Key substitutions

We can obtain a finite disjunction equivalent to $\exists u_1 \; \psi$

$$\bigvee \exists u_1 \; : \boxed{\left(u_1^j = b^m \cdot \boldsymbol{u}^{\boldsymbol{\ell}}\right)} \wedge \psi \quad \text{where } \boldsymbol{u}^{\boldsymbol{\ell}} := u_2^{\ell_2} \cdot \dots \cdot u_n^{\ell_n}$$

We would like to perform the substitution right away with

$$u_1 = \sqrt[j]{b^m \cdot u_2^{\ell_2} \cdot \dots \cdot u_n^{\ell_n}} \quad \text{but we have to be careful!}$$

Consider:

$$u_1^5 = b^2 \cdot u_2 \implies u_2 = b^k \wedge 5 | k + 2 \quad \text{for some } k \in \mathbb{Z}$$

Small witness property: Key substitutions

We can obtain a finite disjunction equivalent to $\exists u_1 \ \psi$

$$\bigvee \exists u_1 \ : \boxed{\left(u_1^j = b^m \cdot \boldsymbol{u}^{\boldsymbol{\ell}}\right)} \wedge \psi \quad \text{where } \boldsymbol{u}^{\boldsymbol{\ell}} := u_2^{\ell_2} \cdot \dots \cdot u_n^{\ell_n}$$

We would like to perform the substitution right away with

$$u_1 = \sqrt[j]{b^m \cdot u_2^{\ell_2} \cdot \dots \cdot u_n^{\ell_n}} \quad \text{but we have to be careful!}$$

Conside

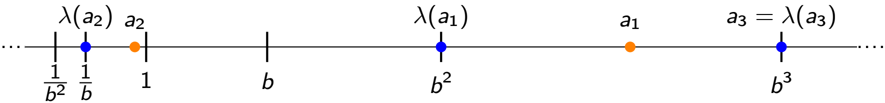
Remember that $u \in \{u_2, \dots, u_n\}$ are integer powers of b,

$$u^{\ell} = b^{\ell \cdot (q \cdot j + r)} = z^j \cdot b^{r \cdot \ell} \quad \text{for } q \in \mathbb{Z},\ r \in [0..j-1],\ z \in b^{\mathbb{Z}}$$

Hence, $m + \sum_{i=2}^{n} r_i \cdot \ell_i$ has to be divisible by j.

Small witness property: Finding the substitutions

We write $\lambda : \mathbb{R}_{>0} \to b^{\mathbb{Z}}$ for the function mapping $a \in \mathbb{R}$ to the largest integer power of b that is less or equal than a.



Sign evaluation

5. Check if $(u_1 = b^{g_1}, \ldots, u_n = b^{g_n})$ is a solution to ψ

$\psi(b^{g_1}, \ldots, b^{g_n})$ is a Boolean combination of $P_i(b) \sim 0$. For each inequality, test $|P(T_n)| \leq 2^{-m}$. Where T is the TM for b, and n and m are obtained via the root barrier.

Finally return true or false depending on the Boolean structure of ψ.

Small witness property: Finding the substitutions

Claim 1

Let $r \in \mathbb{R}$ be a root of a polynomial P. Then, there is a finite characterisation:

$$\lambda(r)^j = b^s \frac{\lambda(Q(b, \boldsymbol{u}))}{\lambda(R(b, \boldsymbol{u}))} \qquad j, s \in \mathbb{Z}$$

With polynomials Q and R computed from P.

Claim 2

The value of $\lambda(Q(b, \boldsymbol{u}))$ is "close" to some monomial $\boldsymbol{u}^\ell$ ocurring in Q:

$$\lambda(Q(b, \boldsymbol{u})) = b^t \boldsymbol{u}^\ell \quad t \in \mathbb{Z}$$

$$[\text{Claim 1}] + [\text{Claim 2}] + \left[u_1 \in \{b^{-1}\lambda(r), \lambda(r), b\lambda(r)\}\right] \rightarrow \boxed{u_1^j = b^m \boldsymbol{u}^\ell}$$