When is Containment Decidable for Probabilistic Automata?

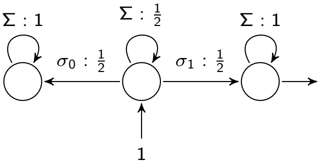
Laure Daviaud[1], Marcin Jurdziński[1], Ranko Lazić[1],
Filip Mazowiecki[2], Guillermo A. Pérez[3], and James Worrell[4]

Warwick University[1], Université de Bordeaux[2]
Université libre de Bruxelles[3], Oxford University[4]

ICALP 2018 @ Prague

Probabilistic automata

A PA $\mathcal{A}$ is a tuple $(\Sigma, Q, \delta, \iota, F)$

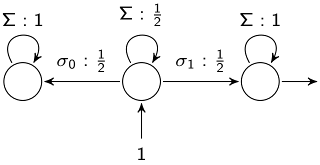


1. $\sum_{p \in Q} \iota(p) \leq 1$
2. for all $p \in Q, \sigma \in \Sigma$

$$\sum_{q \in Q} \delta(p, \sigma, q) \leq 1$$

Probabilistic automata

A PA $\mathcal{A}$ is a tuple $(\Sigma, Q, \delta, \iota, F)$



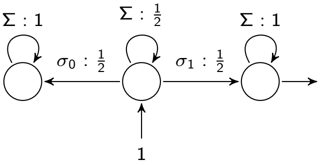
1. $\sum_{p \in Q} \iota(p) \leq 1$
2. for all $p \in Q, \sigma \in \Sigma$
$$\sum_{q \in Q} \delta(p, \sigma, q) \leq 1$$

- It realizes a function $[\![\mathcal{A}]\!] : \Sigma^* \to ([0,1] \cap \mathbb{Q})$ s.t. $w_1 \dots w_n \mapsto$

$$\sum \left[\iota(q_0) \cdot \prod_{i=0}^{n-1} \delta(q_i, w_{i+1}, q_{i+1}) \;\middle|\; q_0 w_1 \dots w_n q_n \text{ is an acc. run} \right]$$

Probabilistic automata

A PA $\mathcal{A}$ is a tuple $(\Sigma, Q, \delta, \iota, F)$



1. $\sum_{p \in Q} \iota(p) \leq 1$
2. for all $p \in Q, \sigma \in \Sigma$
$$\sum_{q \in Q} \delta(p, \sigma, q) \leq 1$$

- It realizes a function $[\![\mathcal{A}]\!] : \Sigma^* \to ([0,1] \cap \mathbb{Q})$ s.t. $w_1 \dots w_n \mapsto$

$$\sum \left[\iota(q_0) \cdot \prod_{i=0}^{n-1} \delta(q_i, w_{i+1}, q_{i+1}) \;\middle|\; q_0 w_1 \dots w_n q_n \text{ is an acc. run} \right]$$

- Example: for the PA above, if $\sigma_0 = 0, \sigma_1 = 1$,

$$w_1 \dots w_n \mapsto \sum_{i=0}^{n} \frac{w_i}{2^{i+1}}$$

The containment problem

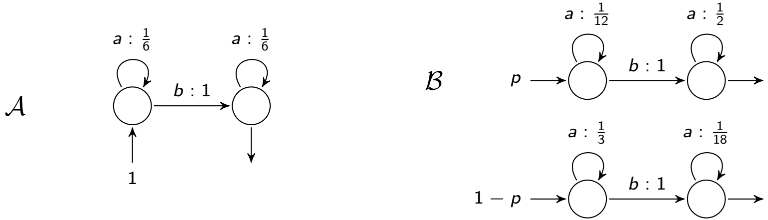
Containment ($[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$)

INPUT: Two PAs $\mathcal{A}, \mathcal{B}$
QUESTION: Is it the case that $[\![\mathcal{A}]\!](w) \leq [\![\mathcal{B}]\!](w)$ for all $w \in \Sigma^*$?

The containment problem

Containment ($[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$)

INPUT: Two PAs $\mathcal{A}, \mathcal{B}$
QUESTION: Is it the case that $[\![\mathcal{A}]\!](w) \leq [\![\mathcal{B}]\!](w)$ for all $w \in \Sigma^*$?

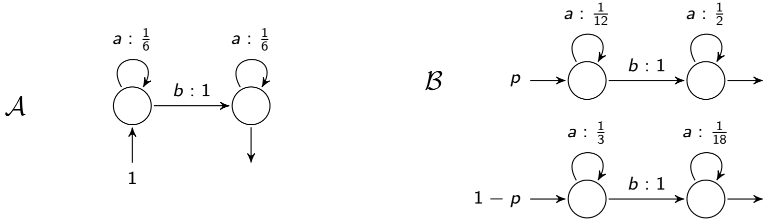


- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?

The containment problem

Containment ($[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$)

INPUT: Two PAs $\mathcal{A}, \mathcal{B}$
QUESTION: Is it the case that $[\![\mathcal{A}]\!](w) \leq [\![\mathcal{B}]\!](w)$ for all $w \in \Sigma^*$?



- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?

Decidability status

The general problem is undecidable [Paz 71].

Motivation

Model

- PAs can be seen as blind POMDPs
  - artificial intelligence
- verification of probabilistic systems
- reasoning about inexact hardware
- quantum complexity theory
- uncertainty in runtime modelling
- text and speech processing

Motivation

Model

- PAs can be seen as blind POMDPs
  - artificial intelligence
- verification of probabilistic systems
- reasoning about inexact hardware
- quantum complexity theory
- uncertainty in runtime modelling
- text and speech processing

Containment for PAs

- quantitative extension of Boolean language inclusion
- automata-based verification of probabilistic systems
  - together with emptiness, universality, etc.

TL;DR: When is containment decidable?

$$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]?$$

Theorem (Undecidable)

Containment is undecidable when either $\mathcal{A}$ or $\mathcal{B}$ are at least linearly ambiguous.

Theorem (Decidable)

Containment is decidable when $\mathcal{A}$ and $\mathcal{B}$ are finitely-ambiguous and at least one of them is unambiguous.

- *if only $\mathcal{A}$ is unambiguous, we assume Schanuel's conjecture is true (so the theory of the reals with $\exp(\cdot)$ is decidable)*
- *if $\mathcal{B}$ is unambiguous, our result does not depend on any conjectures*

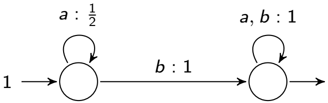
Open problem

Is containment decidable when $\mathcal{A}$ and $\mathcal{B}$ are finitely-ambiguous (and none of them is unambiguous)?

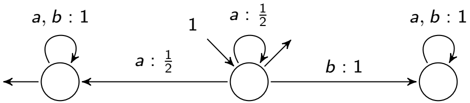
Ambiguity

How many accepting runs does $\mathcal{A}$ have on w?

- Unambiguous: at most 1 for all words



- Bounded or finitely ambiguous: for some k, at most k for all words
- Linearly ambiguous: for some k, at most $k|w|$ for all words w



- Polynomially ambiguous: for some polynomial function p, at most $p(|w|)$ for all words w
- Exponentially ambiguous. . .

Motivation and state of the art

Why should we care about automata with bounded ambiguity?

For quantitative automata we often have that less ambiguity means better complexity (decidability) for decision problems.

- Emptiness for PA: decidable for finitely-ambiguous PA, undecidable in general [Fijalkow et al. 17]
- Universality for Max-Plus automata: decidable for finitely-ambiguous, undecidable in general [Filiot et al. 14]

Motivation and state of the art

Why should we care about automata with bounded ambiguity?

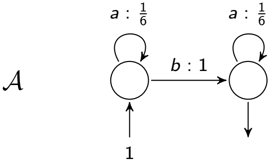
For quantitative automata we often have that less ambiguity means better complexity (decidability) for decision problems.

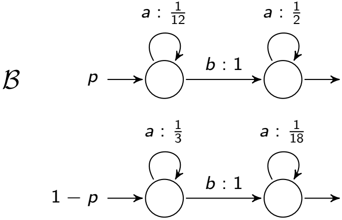
- Emptiness for PA: decidable for finitely-ambiguous PA, undecidable in general [Fijalkow et al. 17]
- Universality for Max-Plus automata: decidable for finitely-ambiguous, undecidable in general [Filiot et al. 14]

Does my automaton have bounded ambiguity?

- structural characterization [Weber, Seidl 91]
- can be decided in polynomial time [WS91; Allauzen et al. 11; Filiot et al. 18]

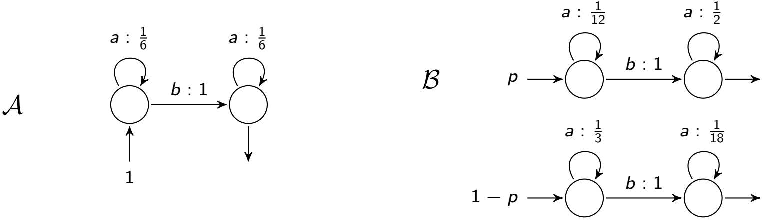
Example: from automata to exponential inequalities (1/2)





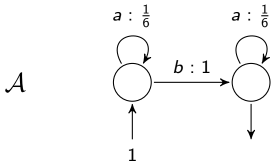
- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?

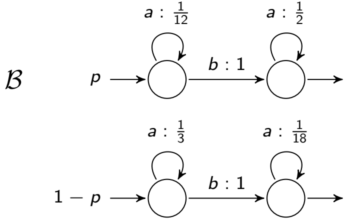
Example: from automata to exponential inequalities (1/2)



- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?
- Only words of the form $a^* b a^*$ have non-zero value

Example: from automata to exponential inequalities (1/2)

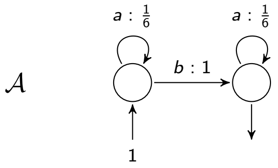


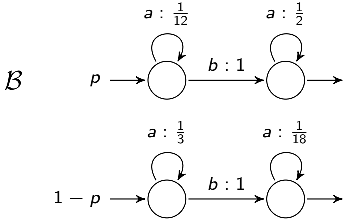


- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?
- Only words of the form $a^* b a^*$ have non-zero value
- Non-containment: are there non-negative integers n_1, n_2 such that

$$\left(\frac{1}{6}\right)^{n_1} \left(\frac{1}{6}\right)^{n_2} > p \left(\frac{1}{12}\right)^{n_1} \left(\frac{1}{2}\right)^{n_2} + (1-p) \left(\frac{1}{3}\right)^{n_1} \left(\frac{1}{18}\right)^{n_2} ?$$

Example: from automata to exponential inequalities (1/2)





- Non-containment: does there exist $w \in \{a, b\}^*$ such that $[\![\mathcal{A}]\!](w) > [\![\mathcal{B}]\!](w)$?
- Only words of the form $a^* b a^*$ have non-zero value
- Non-containment: are there non-negative integers n_1, n_2 such that

$$\left(\frac{1}{6}\right)^{n_1} \left(\frac{1}{6}\right)^{n_2} > p \left(\frac{1}{12}\right)^{n_1} \left(\frac{1}{2}\right)^{n_2} + (1-p) \left(\frac{1}{3}\right)^{n_1} \left(\frac{1}{18}\right)^{n_2} ?$$

- Equivalently, are there non-negative integers n_1, n_2 such that

$$1 > \exp(\ln(p) - n_1 \ln(2) + n_2 \ln(3)) + \exp(\ln(1-p) + n_1 \ln(2) - n_2 \ln(3)) ?$$

Example: from automata to exponential inequalities (2/2)

$$1 > \exp(\ln(p) - n_1 \ln(2) + n_2 \ln(3)) + \exp(\ln(1-p) + n_1 \ln(2) - n_2 \ln(3))$$

- Are there non-negative integers n_1, n_2 such that $e^u + e^v < 1$ where

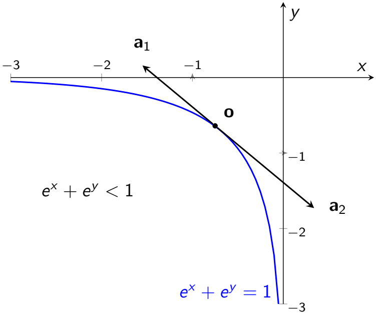
$$\begin{array}{rcccc} u = & \ln(p) & -n_1 \ln(2) & +n_2 \ln(3) \\ v = & \ln(1-p) & +n_1 \ln(2) & -n_2 \ln(3) \\ & \mathbf{o} & n_1 \mathbf{a}_1 & n_2 \mathbf{a}_2 \end{array}$$

Example: from automata to exponential inequalities (2/2)

$$1 > \exp(\ln(p) - n_1 \ln(2) + n_2 \ln(3)) + \exp(\ln(1-p) + n_1 \ln(2) - n_2 \ln(3))$$

- Are there non-negative integers n_1, n_2 such that $e^u + e^v < 1$ where

$$\begin{array}{rcccc} u = & \ln(p) & -n_1 \ln(2) & +n_2 \ln(3) \\ v = & \ln(1-p) & +n_1 \ln(2) & -n_2 \ln(3) \\ & \mathbf{o} & n_1 \mathbf{a}_1 & n_2 \mathbf{a}_2 \end{array}$$

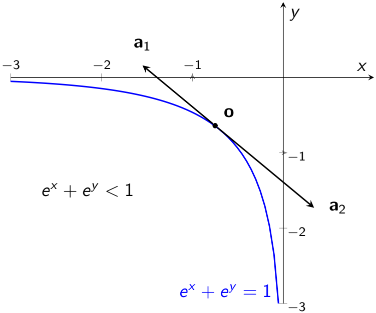


Example: from automata to exponential inequalities (2/2)

$$1 > \exp(\ln(p) - n_1 \ln(2) + n_2 \ln(3)) + \exp(\ln(1-p) + n_1 \ln(2) - n_2 \ln(3))$$

- Are there non-negative integers n_1, n_2 such that $e^u + e^v < 1$ where

$$\begin{array}{rcccc} u = & \ln(p) & -n_1 \ln(2) & +n_2 \ln(3) \\ v = & \ln(1-p) & +n_1 \ln(2) & -n_2 \ln(3) \\ & \mathbf{o} & n_1 \mathbf{a}_1 & n_2 \mathbf{a}_2 \end{array}$$



- if $p \neq \frac{1}{2}$ then the line with $\mathbf{o} + \mathbf{a}_1, \mathbf{o}, \mathbf{o} + \mathbf{a}_2$ is a secant of $e^x + e^y = 1$
- since $\ln(2)$ and $\ln(3)$ are rationally independent, $\exists n_1, n_2 \in \mathbb{N}$ that work!

From automata to exponential inequalities

- Non-containment: $\exists w. \llbracket \mathcal{A} \rrbracket(w) > \llbracket \mathcal{B} \rrbracket(w)$?

Proposition (Focus on Int. Programming with Exponentials)

Given $\mathcal{A}$ (k-ambiguous) and $\mathcal{B}$ (ℓ-ambiguous), one can compute:

1. *a non-negative integer n,*
2. *a finite set of tuples $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s})$ with*
   - $\mathbf{p} \in \mathbb{Q}^{k}_{>0}$, $\mathbf{r} \in \mathbb{Q}^{\ell}_{>0}$, $\mathbf{q} \in \mathbb{Q}^{k \times n}_{>0}$, $\mathbf{s} \in \mathbb{Q}^{\ell \times n}_{>0}$,

such that, for one of those tuples, there exists $\mathbf{x} \in \mathbb{N}^n$ with

$$\sum_{i=1}^{k} p_i q_{i,1}^{x_1} \ldots q_{i,n}^{x_n} > \sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \ldots s_{j,n}^{x_n}$$

if and only if $\exists w. \llbracket \mathcal{A} \rrbracket(w) > \llbracket \mathcal{B} \rrbracket(w)$.

From automata to exponential inequalities

- Non-containment: $\exists w. \llbracket \mathcal{A} \rrbracket(w) > \llbracket \mathcal{B} \rrbracket(w)$?

Proposition (Focus on Int. Programming with Exponentials)

Given $\mathcal{A}$ (k-ambiguous) and $\mathcal{B}$ (ℓ-ambiguous), one can compute:

1. *a non-negative integer n,*
2. *a finite set of tuples $(\mathbf{p}, \mathbf{q}, \mathbf{r}, \mathbf{s})$ with*
   - $\mathbf{p} \in \mathbb{Q}^{k}_{>0}$, $\mathbf{r} \in \mathbb{Q}^{\ell}_{>0}$, $\mathbf{q} \in \mathbb{Q}^{k \times n}_{>0}$, $\mathbf{s} \in \mathbb{Q}^{\ell \times n}_{>0}$,

such that, for one of those tuples, there exists $\mathbf{x} \in \mathbb{N}^n$ with

$$\sum_{i=1}^{k} p_i q_{i,1}^{x_1} \dots q_{i,n}^{x_n} > \sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n}$$

if and only if $\exists w. \llbracket \mathcal{A} \rrbracket(w) > \llbracket \mathcal{B} \rrbracket(w)$.

Proof: use a simple-cycle decomposition for finitely-ambiguous automata

Deciding containment: without Schanuel

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is k-ambiguous and $\mathcal{B}$ is unambiguous.

Deciding containment: without Schanuel

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is k-ambiguous and $\mathcal{B}$ is unambiguous.

The exponential inequalities' version

Does there exist $\mathbf{x} \in \mathbb{N}^n$ such that

$$\sum_{i=1}^{k} p_i q_{i,1}^{x_1} \dots q_{i,n}^{x_n} > r s_1^{x_1} \dots s_n^{x_n}?$$

Deciding containment: without Schanuel

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is k-ambiguous and $\mathcal{B}$ is unambiguous.

The exponential inequalities' version

Does there exist $\mathbf{x} \in \mathbb{N}^n$ such that

$$\sum_{i=1}^{k} p_i q_{i,1}^{x_1} \ldots q_{i,n}^{x_n} > r s_1^{x_1} \ldots s_n^{x_n}?$$

Proposition (Characterization and algorithm)

There exists such an $\mathbf{x} \in \mathbb{N}^n$ if and only if either

1. *There are i, j such that $q_{i,j} > s_j$*
   - *so $\mathbf{x}$ with x_j large enough works;*
2. *or $\mathbf{x} = \mathbf{0}$ works*
   - *if for all i, j we have $q_{i,j} \leq s_j$, then $\mathbf{0}$ works.*

Deciding containment: the hard case (1/3)

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is unambiguous and $\mathcal{B}$ is ℓ-ambiguous.

Deciding containment: the hard case (1/3)

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is unambiguous and $\mathcal{B}$ is ℓ-ambiguous.

The exponential inequalities' version

Does there exist $\mathbf{x} \in \mathbb{N}^n$ such that

$$pq_1^{x_1} \dots q_n^{x_n} > \sum_{j=1}^{\ell} t_j u_{j,1}^{x_1} \dots u_{j,n}^{x_n}$$

or equivalently (after dividing)

$$\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n} < 1?$$

Deciding containment: the hard case (1/3)

$[\![\mathcal{A}]\!] \leq [\![\mathcal{B}]\!]$? When $\mathcal{A}$ is unambiguous and $\mathcal{B}$ is ℓ-ambiguous.

The exponential inequalities' version

Does there exist $\mathbf{x} \in \mathbb{N}^n$ such that

$$p q_1^{x_1} \ldots q_n^{x_n} > \sum_{j=1}^{\ell} t_j u_{j,1}^{x_1} \ldots u_{j,n}^{x_n}$$

or equivalently (after dividing)

$$\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \ldots s_{j,n}^{x_n} < 1?$$

Lemma

The above problem is semi-decidable: just enumerate all possible $\mathbf{x}$ *and verify whether they satisfy the inequality.*

Deciding containment: the hard case (2/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that

$$\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n} < 1?$$

Let $X \subseteq \mathbb{R}^n$ be the set of all real solutions to the above equation.

Deciding containment: the hard case (2/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that

$$\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \ldots s_{j,n}^{x_n} < 1?$$

Let $X \subseteq \mathbb{R}^n$ be the set of all real solutions to the above equation.

Lemma (Key Lemma)

If $X \cap \mathbb{Z}^n = \emptyset$ then there exist non-zero $\mathbf{d} \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$ such that

$$\left\{ \mathbf{d}^\top \mathbf{x} \,\middle|\, \mathbf{x} \in X \right\} \subseteq [a, b]. \tag{1}$$

In words: Since X is nice, if it contains no integer point then there is an integer vector that is almost orthogonal to it.

Deciding containment: the hard case (2/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that

$$\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n} < 1?$$

Let $X \subseteq \mathbb{R}^n$ be the set of all real solutions to the above equation.

Lemma (Key Lemma)

If $X \cap \mathbb{Z}^n = \emptyset$ then there exist non-zero $\mathbf{d} \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$ such that

$$\left\{ \mathbf{d}^\top \mathbf{x} \,\middle|\, \mathbf{x} \in X \right\} \subseteq [a, b]. \tag{1}$$

In words: Since X is nice, if it contains no integer point then there is an integer vector that is almost orthogonal to it.

Tarski with exponentials

Given $\mathbf{d}$, a, and b, Equation (1) is expressible in FO over $(\mathbb{R}, +, \times, \exp)$ and decidable if Schanuel's conjecture holds [Macintyre, Wilkie 96].

Deciding containment: the hard case (3/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that $\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \ldots s_{j,n}^{x_n} < 1$?

Deciding containment: the hard case (3/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that $\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n} < 1$?

The semi-decision procedure

1. Enumerate non-zero $\mathbf{d} \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$
2. Use the encoding into FO $(\mathbb{R}, +, \times, \exp)$ to verify if Equation (1) holds
   - For all $i \in [a, b] \cap \mathbb{Z}$ consider

$$d_1 x_1 + \cdots + d_n x_n = i$$

   - If for some i, the equation has an integer solution $\mathbf{x} \in \mathbb{Z}^n$, recursively start over with dimension reduced by 1 (or check if $\mathbf{x}$ works if $n = 1$)
   - Otherwise, go up in the recursion stack or output `YES`

Deciding containment: the hard case (3/3)

The complementary problem

Is it the case that there is no $\mathbf{x} \in \mathbb{N}^n$ such that $\sum_{j=1}^{\ell} r_j s_{j,1}^{x_1} \dots s_{j,n}^{x_n} < 1$?

The semi-decision procedure

1. Enumerate non-zero $\mathbf{d} \in \mathbb{Z}^n$ and $a, b \in \mathbb{Z}$
2. Use the encoding into FO $(\mathbb{R}, +, \times, \exp)$ to verify if Equation (1) holds
   - For all $i \in [a, b] \cap \mathbb{Z}$ consider

$$d_1 x_1 + \cdots + d_n x_n = i$$

   - If for some i, the equation has an integer solution $\mathbf{x} \in \mathbb{Z}^n$, recursively start over with dimension reduced by 1 (or check if $\mathbf{x}$ works if $n = 1$)
   - Otherwise, go up in the recursion stack or output `YES`

Technical remark: easy to adapt this from $\mathbf{x} \in \mathbb{Z}^n$ to $\mathbf{x} \in \mathbb{N}^n$

Conclusion

Our results

- We can decide it assuming Schanuel's conjecture, both automata are finitely-ambiguous, and one of them is unambiguous.
- It is undecidable as soon as one of the automata is allowed to be linearly-ambiguous.

Conclusion

Our results

- We can decide it assuming Schanuel's conjecture, both automata are finitely-ambiguous, and one of them is unambiguous.
- It is undecidable as soon as one of the automata is allowed to be linearly-ambiguous.

What now?

- Can we remove the dependency on Schanuel's conjecture?
  - maybe by showing some small solution property
  - maybe by finding a "weaker version of $\exp(\cdot)$"
- Can we remove the assumption of unambiguity?
  - X is no longer "nice"
  - we do not know if the key lemma holds