

Costs and Rewards in Priced Timed Automata[☆]

Martin Fränzle^a, Mahsa Shirmohammadi^b, Mani Swaminathan^a,
James Worrell^c

^a*University Of Oldenburg, Germany*

^b*CNRS and IRIF, France*

^c*University of Oxford, UK*

Abstract

We consider Pareto analysis of reachable states in multi-priced timed automata (MPTA). An MPTA is a timed automaton equipped with multiple observers that record costs (to be minimised) and rewards (to be maximised) that are accumulated along a computation. Each observer has a non-negative derivative that is constant in each location of the automaton.

We study the Pareto Domination Problem, which asks whether it is possible to reach a target location via a run in which the accumulated costs and rewards Pareto dominate a given objective vector. We show that this problem is undecidable in general, but decidable for MPTA with at most three observers. For MPTA whose observers are either all costs or all rewards, we show that the Pareto Domination Problem is PSPACE-complete. We also consider an approximate Pareto Domination Problem that is decidable in exponential time without restricting the number and types of observers.

We develop connections between MPTA and Diophantine equations. Undecidability of the Pareto Domination Problem is shown by reduction from Hilbert's 10th Problem, while decidability for three observers is shown by a translation to a decidable fragment of arithmetic involving quadratic forms.

Keywords: Priced Timed Automata, Pareto Domination, Diophantine Equations.

[☆]A preliminary version of this paper [1] appeared in the proceedings of ICALP 2018.

Email addresses: fraenzle@informatik.uni-oldenburg.de (Martin Fränzle),
mahsa.shirmohammadi@irif.fr (Mahsa Shirmohammadi),
swaminathan@informatik.uni-oldenburg.de (Mani Swaminathan),
james.worrell@cs.ox.ac.uk (James Worrell)

1. Introduction

Multi Priced Timed Automata (MPTA) [2, 3, 4, 5, 6] extend priced timed automata [7, 8, 9] with *multiple observers* that capture the accumulation of costs and rewards along a computation. The observers allow to model multi-objective optimisation problems beyond the scope of timed automata [10]. MPTA lie at the frontier between timed automata (for which reachability is decidable [10]) and linear hybrid automata (for which reachability is undecidable [11]). Observers exhibit richer dynamics than clocks in not being confined to having unit slope in locations, but they may neither be queried nor reset on taking edges.

In this paper we distinguish between observers that represent *costs* (to be minimised) and those that represent *rewards* (to be maximised). Formally, we partition the set \mathcal{Y} of observers into cost and reward variables and say that $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ *Pareto dominates* $\gamma' \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ if $\gamma(y) \leq \gamma'(y)$ for each cost variable y and $\gamma(y) \geq \gamma'(y)$ for each reward variable y . Then the *Pareto curve* corresponding to an MPTA consists of all undominated vectors γ that are reachable in an accepting location. While cost and reward variables are syntactically identical in the underlying automaton model, distinguishing between them changes the notion of Pareto domination and the associated decision problems. We introduce in Section 3 a decision version of the problem of computing Pareto curves for MPTA, called the *Pareto Domination Problem*. Here, given a target vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, one asks to reach an accepting location with a vector $\gamma' \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ that Pareto dominates γ .

Our first main result is that the Pareto Domination Problem is undecidable in general. The undecidability proof in Section 4 is by reduction from Hilbert’s 10th problem. Due to the existence of so-called “universal Diophantine equations” (of degree 4 with 58 variables [12]), our proof shows undecidability of the Pareto Domination Problem for some fixed but large number of observers. Undecidability of the Pareto Domination Problem entails that one cannot compute an exact Pareto curve for an arbitrary MPTA.

We consider three different approaches to recover decidability of the Pareto Domination Problem. These approaches have a common foundation, namely given an MPTA we define a regular language whose Parikh image yields a semilinear representation of the set of observer vectors that are reachable along integer-time runs of the MPTA. By analysing convex

combinations of integer runs we reduce the Pareto Domination Problem to the satisfiability of a class of bilinear mixed integer-real constraints. We then consider restrictions on MPTA and variants of the Pareto Domination Problem that allow us to solve this class of constraints.

We first show in Section 6 that restricting to MPTA with only costs or only rewards yields PSPACE-completeness of the Pareto Domination Problem. Here we are able to eliminate integer variables from our bilinear constraints, resulting in a formula of linear real arithmetic.

In Section 7 we allow a mix of cost and reward observers, but restrict to the case that there are at most three observers in total. In this case decidability is achieved by eliminating the real variables from the bilinear constraint system, thus reducing the Pareto Domination Problem to deciding whether a given quadratic form has a zero lying on a given semilinear set, which is known to be decidable from [13].

We consider in Section 8 another method to restore decidability for general MPTA with arbitrarily many costs and rewards, by studying an approximate version of the Pareto Domination Problem, called the *Gap Domination Problem*. Similar to the setting of [14], the Gap Domination Problem represents the decision version of the problem of computing ε -Pareto curves. This problem, whose input includes a tolerance $\varepsilon > 0$ and a vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, permits inconclusive answers if all solutions dominating γ do so with a slack less than ε . We give an exponential-time procedure for the Gap Domination Problem that works by applying relaxation and rounding to find approximate solutions of the above-mentioned bilinear system of constraints.

Drawing together some of the results in the preceding sections, in Section 9 we make some observations about the topological structure of the set of reachable observer vectors in a given MPTA.

Related Work

For MPTA with a single observer, the optimal cost to reach a given location can be computed in polynomial space using extensions of the clock-regions construction [7, 8, 9].

Reachability in MPTA in which all observers are costs was considered in [6], which gives a procedure to minimise the value of a given observer under constraints on the remaining observers. This procedure relies on a well-quasi-order for termination and no complexity bounds are given.

MPTA with both costs and rewards have been studied in [2, 5, 15]. The main result of [2] is a procedure to compute the maximum reward per unit

73 cost over infinite runs of an MPTA with a single cost observer and a single
 74 reward observer. Zhang [15] considers reachability, but restricts attention
 75 to automata with discretely valued observers that are updated on edges.
 76 Meanwhile [5] considers undecidability in more expressive models than in
 77 the present paper.

78 Model checking MPTA against an extension of Computation Tree Logic
 79 in which modalities are annotated with constraints on observers is considered
 80 in [3, 4]. This model checking problem is undecidable over dense time [4] but
 81 is decidable in polynomial space for one-clock MPTA [3].

82 2. Background

83 2.1. Quadratic Diophantine Equations

We recall a decidable class of non-linear Diophantine problems. Consider the quadratic constraint

$$\sum_{i,j=1}^n a_{ij}X_iX_j + \sum_{j=1}^n b_jX_j + c = 0, \quad (1)$$

84 whose coefficients a_{ij} , b_j , and c are rational numbers. Consider also the
 85 family of constraints

$$f_1(X_1, \dots, X_n) \sim c_1 \wedge \dots \wedge f_k(X_1, \dots, X_n) \sim c_k, \quad (2)$$

86 where f_1, \dots, f_k are linear forms with rational coefficients, $c_1, \dots, c_k \in \mathbb{Q}$,
 87 and $\sim \in \{<, \leq\}$.

88 **Theorem 1** ([13]). *There is an algorithm that decides whether a given*
 89 *quadratic equation (1) and family of linear inequalities (2) have a common*
 90 *solution in \mathbb{Z}^n .*

91 Let us emphasise that in Theorem 1 at most one quadratic constraint is
 92 permitted. It is clear (e.g., by introducing a slack variable) that the theorem
 93 remains true if the equality symbol in the quadratic constraint (1) is replaced
 94 by any comparison operator in $\{<, \leq, >, \geq\}$.

95 Write $\mathcal{L}_{\text{quad}}$ for the language of quantifier-free formulas in disjunctive
 96 normal form, in which each clause is a conjunction of a single quadratic
 97 constraint of the form (1) and a set of linear constraints of the form (2). By
 98 Theorem 1 the satisfiability problem for this language is decidable.

2.2. Parikh Images of Regular Languages

Let Σ be a finite alphabet. Denote by $\pi : \Sigma^* \rightarrow \mathbb{N}^\Sigma$ the map such that $\pi(w)(\sigma)$ is the number of occurrences of σ in w for $w \in \Sigma^*$ and $\sigma \in \Sigma$. Given a language $L \subseteq \Sigma^*$, the set $\pi(L) := \{\pi(w) : w \in L\}$ is called the *Parikh image* (or *commutative image*) of L . Given an NFA \mathcal{A} , we write $\pi(\mathcal{A})$ for the Parikh image of the language accepted by \mathcal{A} .

For every vector $\mathbf{v} \in \mathbb{N}^n$ and every finite set $P = \{\mathbf{u}_1, \dots, \mathbf{u}_m\}$ of vectors in \mathbb{N}^n , we define the \mathbb{N} -linear set $S(\mathbf{v}, P) := \{\mathbf{v} + \sum_{i=1}^m a_i \mathbf{u}_i : a_1, \dots, a_m \in \mathbb{N}\}$. We call \mathbf{v} the *base vector* and $\mathbf{u}_1, \dots, \mathbf{u}_m \in P$ the *period vectors* of the set.

The following result gives size bounds on the representation of the Parikh image of the language of an NFA as a union of linear sets. Roughly speaking, the complexity is polynomial in the number of states and exponential in the alphabet size of the NFA.

Theorem 2. [16, Theorem 4.1] *Let \mathcal{A} be an NFA with n states over an alphabet of size k . Then $\pi(\mathcal{A})$ can be written as a union of linear sets $S(\mathbf{v}_1, P_1), \dots, S(\mathbf{v}_m, P_m)$, where the maximum entry of each \mathbf{v}_i is at most $(nk)^{O(k)}$, the maximum entry of each vector in every set P_i is at most n , P_i has cardinality at most k , and m is bounded by $(nk)^{O(k^2)}$. Furthermore, such a decomposition can be computed in time $(nk)^{O(k^2)}$.*

2.3. Geometry

We will need the following elementary geometric facts.

Let $\mathbf{v}_i = (x_i, y_i)$ with $i \in \{1, 2, 3, 4\}$ be four distinct points in \mathbb{R}^2 . Consider the determinant

$$\Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix}$$

involving three points $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{v}_3 . Then $\Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = 0$ if and only if the three points $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{v}_3 are colinear, and $\Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) > 0$ if and only if \mathbf{v}_3 lies on the right of the directed line passing through \mathbf{v}_1 and \mathbf{v}_2 .

We say that two line segments *properly intersect* if they meet at a single point that is not an end point of either line segment. The line segment $\mathbf{v}_1\mathbf{v}_2$ properly intersects the line segment $\mathbf{v}_3\mathbf{v}_4$ if and only if the following two conditions hold:

1. points \mathbf{v}_3 and \mathbf{v}_4 are on the opposite sides of the line passing through \mathbf{v}_1 and \mathbf{v}_2 :

$$(\Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) > 0 \wedge \Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4) < 0) \vee \\ (\Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) < 0 \wedge \Delta(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_4) > 0),$$

2. points \mathbf{v}_1 and \mathbf{v}_2 are on the opposite sides of the line passing through \mathbf{v}_3 and \mathbf{v}_4 :

$$(\Delta(\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_1) > 0 \wedge \Delta(\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_2) < 0) \vee \\ (\Delta(\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_1) < 0 \wedge \Delta(\mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_2) > 0).$$

129 We note that if $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{v}_3 are fixed, then the constraint expressing
 130 that $\mathbf{v}_1\mathbf{v}_2$ and $\mathbf{v}_3\mathbf{v}_4$ properly meet is a formula of linear arithmetic in vari-
 131 ables x_4 and y_4 .

Let us also note that line segment $\mathbf{v}_1\mathbf{v}_2$ properly intersects the half-line parallel to the y -axis with lower endpoint having coordinates (a, c) if and only if the following constraint holds:

$$\left(\begin{vmatrix} x_1 & y_1 & 1 \\ a & c & 1 \\ x_2 & y_2 & 1 \end{vmatrix} < 0 \text{ and } x_1 < a < x_2 \right) \text{ or } \left(\begin{vmatrix} x_1 & y_1 & 1 \\ a & c & 1 \\ x_2 & y_2 & 1 \end{vmatrix} > 0 \text{ and } x_2 < a < x_1 \right) \quad (3)$$

132 Let $\mathbf{v}_i = (x_i, y_i, z_i)$ with $i \in \{1, 2, 3, 4\}$ be four distinct points in \mathbb{R}^3 .
 133 Assume that the list of vertices $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ describes a triangle with anti-
 134 clockwise orientation. Consider the determinant

$$\Delta = \begin{vmatrix} x_2 - x_1 & x_3 - x_1 & x_4 - x_1 \\ y_2 - y_1 & y_3 - y_1 & y_4 - y_1 \\ z_2 - z_1 & z_3 - z_1 & z_4 - z_1 \end{vmatrix}.$$

135 Then $\Delta = 0$ if and only if the point \mathbf{v}_4 lies in the plane affinely spanned
 136 by the three points $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{v}_3 , and $\Delta > 0$ if and only if \mathbf{v}_4 lies above
 137 that plane. Note that if \mathbf{v}_1 and \mathbf{v}_4 are fixed, then the constraint expressing
 138 that \mathbf{v}_4 lies above the plane affinely spanned by $\mathbf{v}_1, \mathbf{v}_2$ and \mathbf{v}_3 is a quadratic
 139 formula in the variables x_2, y_2, x_3 and y_3 .

140 3. Multi-Priced Timed Automata and Pareto Domination

141 Let $\mathbb{R}_{\geq 0}$ denote the set of non-negative real numbers. Given a set $\mathcal{X} =$
 142 $\{x_1, \dots, x_n\}$ of *clocks*, the set $\Phi(\mathcal{X})$ of *clock constraints* is generated by the
 143 grammar

$$\varphi ::= \text{true} \mid x \leq k \mid x \geq k \mid \varphi \wedge \varphi,$$

144 where $k \in \mathbb{N}$ is a natural number and $x \in \mathcal{X}$. A *clock valuation* is a map-
 145 ping $\nu : \mathcal{X} \rightarrow \mathbb{R}_{\geq 0}$ that assigns to each clock a non-negative real number.
 146 We denote by $\mathbf{0}$ the valuation such that $\mathbf{0}(x) = 0$ for all clocks $x \in \mathcal{X}$. We
 147 write $\nu \models \varphi$ to denote that ν satisfies the constraint φ . Given $t \in \mathbb{R}_{\geq 0}$,
 148 we let $\nu + t$ be the clock valuation such that $(\nu + t)(x) = \nu(x) + t$ for all
 149 clocks $x \in \mathcal{X}$. Given $\lambda \subseteq \mathcal{X}$, let $\nu[\lambda \leftarrow 0]$ be the clock valuation such that
 150 $\nu[\lambda \leftarrow 0](x) = 0$ if $x \in \lambda$, and $\nu[\lambda \leftarrow 0](x) = \nu(x)$ otherwise.

151 A *multi-priced timed automaton* (MPTA) $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$, is
 152 specified as a tuple with a finite set L of *locations*, an *initial location* $\ell_0 \in L$,
 153 a set $L_f \subseteq L$ of *accepting locations*, a finite set \mathcal{X} of *clock variables*, a finite
 154 set \mathcal{Y} of *observers*, a set $E \subseteq L \times \Phi(\mathcal{X}) \times 2^{\mathcal{X}} \times L$ of *edges*, and a *rate*
 155 *function* $R : L \rightarrow \mathbb{N}^{\mathcal{Y}}$. Intuitively $R(\ell)$ is a vector that gives the rates of each
 156 observer in location ℓ . We write $\|\mathcal{A}\|$ for the length of the description of \mathcal{A} ,
 157 where all numerical quantities are given in binary.

158 A *state* of \mathcal{A} is a triple (ℓ, ν, t) where ℓ is a location, ν a clock valuation,
 159 and $t \in \mathbb{R}_{\geq 0}$ is a *time stamp*. A *run* of \mathcal{A} is an alternating sequence of states
 160 and edges $\rho = (\ell_0, \nu_0, t_0) \xrightarrow{e_1} (\ell_1, \nu_1, t_1) \xrightarrow{e_2} \dots \xrightarrow{e_m} (\ell_m, \nu_m, t_m)$, where
 161 $t_0 = 0$, $\nu_0 = \mathbf{0}$, $t_{i-1} \leq t_i$ for all $i \in \{1, \dots, m\}$, and $e_i = \langle \ell_{i-1}, \varphi, \lambda, \ell_i \rangle \in E$ is
 162 such that $\nu_{i-1} + (t_i - t_{i-1}) \models \varphi$ and $\nu_i = (\nu_{i-1} + (t_i - t_{i-1}))[\lambda \leftarrow 0]$ for $i =$
 163 $1, \dots, m$. The run is *accepting* if $\ell_m \in L_f$ and is said to have *granularity* $\frac{1}{g}$ for
 164 a fixed $g \in \mathbb{N}$ if all $t_i \in \mathbb{Q}$ are positive integer multiples of $\frac{1}{g}$. The *cost* of such
 165 a run is a vector $\text{cost}(\rho) \in \mathbb{R}^{\mathcal{Y}}$, defined by $\text{cost}(\rho) = \sum_{j=0}^{m-1} (t_{j+1} - t_j) R(\ell_j)$.

166 Henceforth we will assume that the set \mathcal{Y} of observers of a given MPTA
 167 is partitioned into a set \mathcal{Y}_c of *cost variables* and a set \mathcal{Y}_r of *reward variables*.
 168 With respect to this partition we define a *domination ordering* \leq on the set
 169 of vectors $\mathbb{R}^{\mathcal{Y}}$, where $\gamma \leq \gamma'$ if $\gamma(y) \leq \gamma'(y)$ for all $y \in \mathcal{Y}_r$ and $\gamma'(y) \leq \gamma(y)$
 170 for all $y \in \mathcal{Y}_c$. Intuitively $\gamma \leq \gamma'$ (read γ' dominates γ) if γ' is at least as
 171 good as γ in all respects.

172 Given $\varepsilon > 0$ we define an ε -*domination ordering* \leq_{ε} , where $\gamma \leq_{\varepsilon} \gamma'$
 173 (read γ' ε -dominates γ) if $\gamma(y) + \varepsilon \leq \gamma'(y)$ for all $y \in \mathcal{Y}_r$ and $\gamma'(y) + \varepsilon \leq \gamma(y)$
 174 for all $y \in \mathcal{Y}_c$. We can think of $\gamma \leq_{\varepsilon} \gamma'$ as denoting that γ' is better than γ

175 by an additive factor of ε in all dimensions. In particular we clearly have
 176 that $\gamma \leq_{\varepsilon} \gamma'$ implies $\gamma \leq \gamma'$.

177 The *Pareto Domination Problem* is as follows. Given an MPTA \mathcal{A} with
 178 a set \mathcal{Y} of observers and a partition of \mathcal{Y} into sets \mathcal{Y}_c and \mathcal{Y}_r of cost and
 179 reward variables, with a target $\gamma \in \mathbb{R}^{\mathcal{Y}}$, decide whether there is an accepting
 180 run ρ of \mathcal{A} such that $\gamma \leq \text{cost}(\rho)$.

181 The *Gap Domination Problem* is a variant of the above problem in which
 182 the input additionally includes an accuracy parameter $\varepsilon > 0$. If there is some
 183 run ρ such that $\gamma \leq_{\varepsilon} \text{cost}(\rho)$ then the output should be “dominated” and
 184 if there is no run ρ such that $\gamma \leq \text{cost}(\rho)$ then the output should be “not
 185 dominated”. In case neither of these alternatives hold (i.e., γ is dominated
 186 but not ε -dominated) then there is no requirement on the output.

187 In the (Pareto) Domination Problem the objective is to *reach* an accept-
 188 ing location while satisfying a family of upper-bound constraints on cost
 189 variables and lower-bound constraints on reward variables. We say that an
 190 instance of the problem is *pure* if all observers are cost variables or all are
 191 reward variables (and hence all constraints are upper bounds or all are lower
 192 bounds); otherwise we call the instance *mixed*. Our problem formulation
 193 involves only simple constraints on observers, i.e., those of the form $y \leq c$
 194 or $y \geq c$ for $y \in \mathcal{Y}$. However such constraints can be used to encode more gen-
 195 eral linear constraints of the form $a_1y_1 + \dots + a_ky_k \sim c$, where $y_1, \dots, y_k \in \mathcal{Y}$,
 196 $a_1, \dots, a_k, c \in \mathbb{N}$ and $\sim \in \{\leq, \geq, =\}$. To do this one introduces a fresh ob-
 197 server to denote each linear term $a_1y_1 + \dots + a_ky_k$ (two fresh observers are
 198 needed for an equality constraint).

199 Note that we consider timed automata without *difference constraints* on
 200 clocks, i.e., without clock guards of the form $x_i - x_j \sim k$, for $k \in \mathbb{N}$. As
 201 discussed in Appendix A all our decidability and complexity results hold
 202 also in case of such constraints.

203 4. Undecidability of the Pareto Domination Problem

204 In this section we prove undecidability of the Pareto Domination Problem.
 205 To give some insight we first give in Figure 1 an MPTA, in which the Pareto
 206 constraint $c_1 \leq 1, c_2 \geq 1$ is used to enforce that when control enters the
 207 MPTA the value of clock x is $\frac{1}{n}$ for some positive integer n .

208 We prove undecidability of the Pareto Domination Problem by reduc-
 209 tion from the satisfiability problem for a fragment of arithmetic given by a

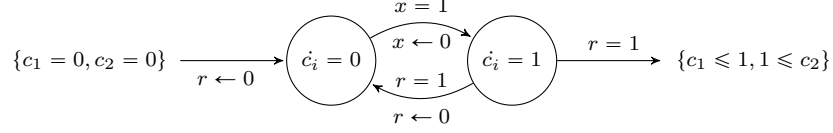


Figure 1: Predicates in curly brackets denote observer values enforced by initialisation, $c_i = 0$ with $i \in \{1, 2\}$, and the Pareto constraint upon exit $\{c_1 \leq 1, 1 \leq c_2\}$. Denoting the initial value of clock x by x^* , the value of both c_1 and c_2 after n full traversals of the central cycle is nx^* . Meeting the final Pareto constraint from initial values thus requires that x^* be $\frac{1}{n}$ for some positive integer n .

210 language \mathcal{L} that is defined as follows. There is an infinite family of vari-
 211 ables X_1, X_2, X_3, \dots and formulas are given by the grammar

$$\varphi ::= X = Y + Z \mid X = YZ \mid \varphi \wedge \varphi,$$

212 where X, Y, Z range over the set of variables. The satisfiability problem for \mathcal{L}
 213 asks, given a formula φ , whether there is an assignment of positive integers
 214 to the variables that satisfies φ . We first show that the satisfiability problem
 215 for \mathcal{L} is undecidable by reduction from Hilbert's Tenth Problem.

216 **Proposition 1.** *The satisfiability problem for \mathcal{L} is undecidable.*

217 *Proof.* The proof is by reduction from Hilbert's Tenth Problem: given a
 218 polynomial $P \in \mathbb{Z}[X_1, \dots, X_k]$, does P have a zero over the set of positive
 219 integers? Given such a polynomial P , we write an \mathcal{L} -formula φ_P whose
 220 variables include X_1, \dots, X_k , such that the satisfying assignments of φ_P are
 221 in one-to-one correspondence with the positive integer roots of P .

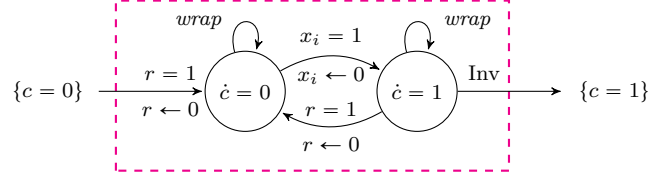
222 The idea is simple: write $P = P_1 - P_2$, where all monomials in P_1 and P_2
 223 appear with positive coefficients. We then introduce an \mathcal{L} -variable for each
 224 subterm of P_1 and P_2 and write constraints to ensure that the variable takes
 225 the same value as the corresponding term. Finally we assert that P_1 is equal
 226 to P_2 through the constraint $P_1 = P_2X \wedge X = XX$. \square

227 Proposition 1 leads to undecidability of the Pareto Domination Problem

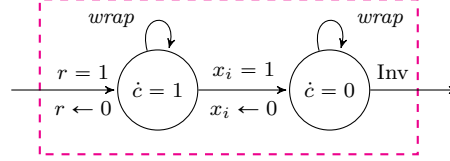
228 **Theorem 3.** *The Pareto Domination Problem is undecidable.*

229 *Proof.* Consider the following problem of reaching a single vector in $\mathbb{R}_{\geq 0}^{\mathcal{Y}}$:
 230 given an MPTA $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$, and target vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$,
 231 decide whether there is an accepting run ρ of \mathcal{A} such that $\text{cost}(\rho) = \gamma$.

Integer test $\frac{1}{x_i^*} \stackrel{?}{\in} \mathbb{N}$:



Decrement $c \leftarrow c + 1 - x_i^*$:



Quotient $c \leftarrow c + \frac{x_i^*}{x_j^*}$:

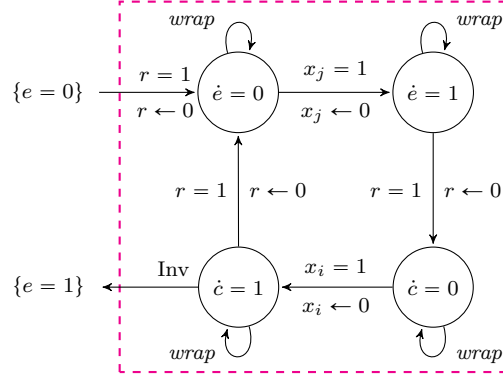


Figure 2: The *wrap* self-loop denotes a family of m wrapping edges, as in [11, Fig. 14], where the j -th edge has guard $x_j = 1$ and resets x_j . In the quotient gadget, e is a fresh observer, as is c in the integer test. The integer test and quotient gadgets are annotated with predicates in curly brackets indicating the initial values of observers on entering and their target values on exiting the gadget. Enforcing these target values through a corresponding Pareto constraint guarantees the desired behaviour of the gadget.

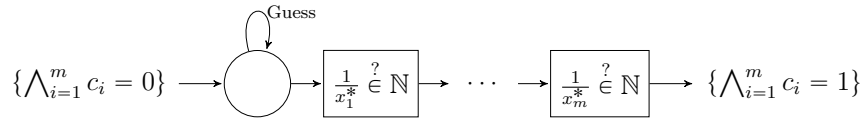
232 One can reduce the problem of reaching a given vector to the Pareto
 233 Domination Problem as follows. Transform the MPTA \mathcal{A} to an MPTA \mathcal{A}'
 234 that has the same locations and edges as \mathcal{A} but with two copies of each
 235 observer $y \in \mathcal{Y}$, with each copy having the same rate as y in each location.
 236 Formally \mathcal{A}' has set of observers $\mathcal{Y}' = \{y_1, y_2 : y \in \mathcal{Y}\}$, where y_1 is a cost
 237 variable and y_2 is a reward variable. Then, defining $\gamma' \in \mathbb{R}_{\geq 0}^{\mathcal{Y}'}$ by $\gamma'(y_1) =$
 238 $\gamma'(y_2) = \gamma(y)$, we have that \mathcal{A}' has an accepting run ρ' such that $\text{cost}(\rho')$
 239 dominates γ' just in case \mathcal{A} has an accepting run ρ such that $\text{cost}(\rho) = \gamma$.

240 Now we give a reduction from the satisfiability problem for \mathcal{L} to the
 241 problem of reaching a single vector. Consider an \mathcal{L} -formula φ over vari-
 242 ables X_1, \dots, X_m . We define an MPTA \mathcal{A} over the set of clocks $\mathcal{X} =$
 243 $\{x_1, \dots, x_m, r\}$. Clock x_i corresponds to the variable X_i , for $i = 1, \dots, m$,
 244 while r is a *reference clock*. The reference clock is reset whenever it reaches 1
 245 and is not otherwise reset—thus it keeps track of global time modulo one.
 246 After an initialisation phase the remaining clocks x_1, \dots, x_m are likewise re-
 247 set in a cyclic fashion, whenever they reach 1 and not otherwise. We denote
 248 by x_i^* the value of clock x_i whenever r is 1. During the initialisation phase
 249 the values x_i^* are established non-deterministically such that $0 < x_i^* \leq 1$.
 250 The idea is that $\frac{1}{x_i^*}$ represents the value of variable X_i in φ ; in particular, x_i^*
 251 is the reciprocal of a positive integer. For each atomic sub-formula in φ
 252 the automaton \mathcal{A} contains a gadget that checks that the guessed valuation
 253 satisfies the sub-formula.

254 To present the reduction we first define three primitive gadgets. The
 255 first “integer test” gadget checks that the initial value x_i^* of clock x_i is a
 256 reciprocal of a positive integer, by adding wrapping edges on all clocks x_j
 257 other than x_i to the MPTA from Figure 1. The construction of each gadget
 258 is such that the precondition $r = 0$ holds when control enters the gadget and
 259 the postcondition $r = 1 \wedge \bigwedge_{j=1}^m x_j \leq 1$ holds on exiting the gadget. This
 260 last postcondition is abbreviated to Inv in the figures. For an observer c
 261 and $1 \leq i, j \leq m$, we define these three gadgets as in Figure 2.

262 In the following we show how to compose the three primitive operations
 263 in an MPTA to enforce the atomic constraints in the language \mathcal{L} . The initial-
 264 isation automaton below is such that for $i = 1, \dots, m$ the value x_i^* of clock x_i
 265 is such that $\frac{1}{x_i^*} \in \mathbb{N}$. Herein the Guess self-loop denotes a family of m edges,
 266 where the j -th edge non-deterministically resets clock x_j . Note that the in-
 267 coming edge of the integer test gadget enforces $r = 1$ such that the initial
 268 guesses for the clocks x_i satisfy $x_i^* \in [0, 1]$. Of these, only reciprocals $\frac{1}{x_i^*} \in \mathbb{N}$
 269 pass the subsequent series of integer tests.

270 **Initialisation** $X_1, \dots, X_n \in \mathbb{N}$:



Let $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$ be an MPTA. For a sequence of edges $e_1, \dots, e_m \in E$, define $Runs(e_1, \dots, e_m) \subseteq \mathbb{R}_{\geq 0}^m$ to be the collection of sequences of timestamps $(t_1, \dots, t_m) \in \mathbb{R}_{\geq 0}^m$ such that \mathcal{A} has a run

$$\rho = (\ell_0, \nu_0, t_0) \xrightarrow{e_1} (\ell_1, \nu_1, t_1) \xrightarrow{e_2} \dots \xrightarrow{e_m} (\ell_m, \nu_m, t_m).$$

Recalling that by convention $t_0 = 0$ and $\nu_0 = \mathbf{0}$, once the edges e_1, \dots, e_m have been fixed then the run ρ is determined solely by the timestamps t_1, \dots, t_m . When the sequence of edges e_1, \dots, e_m is understood, we call such a sequence of timestamps a run.

Proposition 2. *$Runs(e_1, \dots, e_m) \subseteq \mathbb{R}_{\geq 0}^m$ is defined by a conjunction of difference constraints.*

Proof. Given a sequence $(t_1, \dots, t_m) \in \mathbb{R}_{\geq 0}^m$, we define a corresponding sequence of clock valuations $\nu_1, \dots, \nu_m \in \mathbb{R}_{\geq 0}^{\mathcal{X}}$ by $\nu_i(x) = t_i$ if none of the edges e_1, \dots, e_{i-1} reset clock x and otherwise $\nu_i(x) := t_i - t_j$, where $j < i$ is the maximum index such that x is reset by edge e_j . In order for a sequence (t_1, \dots, t_m) to be an element of $Runs(e_1, \dots, e_m)$ we require that the t_i be non-negative and non-decreasing and that for every index $i \in \{1, \dots, m\}$, the guard φ_i of edge e_i be satisfied by the clock valuation ν_i defined above. Clearly the above requirements can be expressed by difference constraints on t_1, \dots, t_m . \square

Proposition 3. *$Runs(e_1, \dots, e_m)$ is equal to the convex hull of the set of its integer points.*

Proof. Fix a positive integer M . From Proposition 2 it immediately follows that the set $Runs(e_1, \dots, e_m) \cap [0, M]^m$ can be written as a conjunction of closed difference constraints $A\mathbf{t} \leq \mathbf{b}$, where A is an integer matrix, \mathbf{t} the vector of time-stamps $t_1 \dots t_m$, and \mathbf{b} an integer vector. Given this, it follows that $Runs(e_1, \dots, e_m) \cap [0, M]^m$, being a closed and bounded polygon, is the convex hull of its vertices. Moreover each vertex is an integer point since the matrix A here, being by Proposition 2 the incidence matrix of a balanced signed graph with half edges, is totally unimodular [17, Proposition 8A.5]. \square

Proposition 4 shows that for Pareto reachability on an MPTA \mathcal{A} with $|\mathcal{Y}| = d$ observers, it suffices to look at $d + 1$ -simplices of integer runs.

326 **Proposition 4.** *For any run ρ of \mathcal{A} there exists a set S of at most $d + 1$*
 327 *integer-time runs, all over the same sequence of edges as ρ , such that $\text{cost}(\rho)$*
 328 *lies in the convex hull of $\text{cost}(S)$.*

329 *Proof.* Let ρ be a run of \mathcal{A} over an edge-sequence e_1, \dots, e_m with time stamps
 330 t_0, \dots, t_m , given by $\rho = (\ell_0, \nu_0, t_0) \xrightarrow{e_1} (\ell_1, \nu_1, t_1) \xrightarrow{e_2} \dots \xrightarrow{e_m} (\ell_m, \nu_m, t_m)$.
 331 By Proposition 3, (t_1, \dots, t_m) lies in the convex hull of the set I of integer
 332 points in $\text{Runs}(e_1, \dots, e_m)$.

333 Since the map $\text{cost} : \text{Runs}(e_1, \dots, e_m) \rightarrow \mathbb{R}^d$ is linear we have that $\text{cost}(\rho)$
 334 lies in the convex hull of $\text{cost}(I)$. Moreover by Carathéodory's Theorem there
 335 exists a subset $S \subseteq I$ of cardinality at most $d + 1$ such that $\text{cost}(\rho)$ lies in
 336 the convex hull of $\text{cost}(S)$. \square

337 We exploit Proposition 4 by introducing an NFA $\mathcal{S}(\mathcal{A})$ which we call the
 338 *simplex automaton*. The definition of $\mathcal{S}(\mathcal{A})$ is such that the set of reachable
 339 observer vectors for \mathcal{A} can be computed from the Parikh image $\pi(\mathcal{S}(\mathcal{A}))$.
 340 Intuitively a run of $\mathcal{S}(\mathcal{A})$ encodes a $(d + 1)$ -tuple of integer runs of \mathcal{A} , such
 341 that all $d + 1$ runs execute the same sequence of edges in \mathcal{A} and differ only
 342 in the times at which the edges are taken.

343 A basic component of the simplex automaton is the *integer-time automa-*
 344 *ton* $\mathcal{Z}(\mathcal{A})$. Intuitively this is an NFA that accepts words that encode integer-
 345 time runs of \mathcal{A} , such that the total number of time units spent by a run in
 346 each location of \mathcal{A} can be read off from the corresponding word.

347 The definition of $\mathcal{Z}(\mathcal{A})$ is as follows. Let $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$ be an
 348 MPTA. Write $M_{\mathcal{X}} \in \mathbb{N}$ for the smallest positive integer that is strictly greater
 349 than every clock constant in \mathcal{A} and define a successor operation $\oplus 1$ on clock
 350 valuations by $(\nu \oplus 1)(x) := \min(\nu(x) + 1, M_{\mathcal{X}})$ for all $x \in \mathcal{X}$. We define
 351 $\mathcal{Z}(\mathcal{A}) := \langle \Sigma, Q, q_0, Q_f, \Delta \rangle$, with alphabet $\Sigma := L \cup E$, set of states $Q :=$
 352 $L \times \{0, 1, \dots, M_{\mathcal{X}}\}^{\mathcal{X}}$, initial state $q_0 := (\ell_0, \mathbf{0})$, set of accepting states $Q_f :=$
 353 $\{(\ell, \nu) \in Q : \ell \in L_f\}$, and transition relation $\Delta \subseteq Q \times \Sigma \times Q$ comprising a triple
 354 $((\ell, \nu), \ell, (\ell, \nu \oplus 1))$ for every state $(\ell, \nu) \in Q$ and a triple $((\ell, \nu), e, (\ell', \nu'))$ for
 355 every edge $e = (\ell, \varphi, \lambda, \ell')$ in \mathcal{A} such that $\nu \models \varphi$ and $\nu'[\lambda \leftarrow 0]$.

356 The set of observer vectors reachable along integer runs of \mathcal{A} can be
 357 reconstructed from the Parikh image of $\mathcal{Z}(\mathcal{A})$. Intuitively if $v \in \pi(\mathcal{Z}(\mathcal{A}))$
 358 then for each location $\ell \in L$, $v(\ell)$ gives the total time spent in location ℓ
 359 along a run. We obtain a cost vector from such a run of $\mathcal{Z}(\mathcal{A})$ by multiplying
 360 the amount $v(\ell)$ of time spent in each location ℓ by the rate vector $R(\ell)$.

361 Formally, we define

$$\text{Reach}(\mathcal{Z}(\mathcal{A})) := \{\sum_{\ell \in L} R(\ell)v(\ell) : v \in \pi(\mathcal{Z}(\mathcal{A}))\}.$$

362 We then have:

363 **Proposition 5.** *Given a vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, there exists an integer-time accept-*
 364 *ing run ρ of \mathcal{A} with $\text{cost}(\rho) = \gamma$ if and only if $\gamma \in \text{Reach}(\mathcal{Z}(\mathcal{A}))$.*

365 The simplex automaton $\mathcal{S}(\mathcal{A})$ is built from $d + 1$ copies of automaton
 366 $\mathcal{Z}(\mathcal{A}) = \langle \Sigma, Q, q_0, Q_f, \Delta \rangle$ that synchronise on transitions labelled from E and
 367 otherwise proceed asynchronously. Formally $\mathcal{S}(\mathcal{A}) := \langle \Sigma', Q^{d+1}, \mathbf{q}_0, Q_f^{d+1}, \Delta \rangle$,
 368 where

- 369 • the alphabet is $\Sigma' := (L \times \{1, \dots, d + 1\}) \cup E$,
- 370 • the initial state is $\mathbf{q}_0 = (q_0, \dots, q_0) \in Q^{d+1}$,
- 371 • the transition relation $\Delta \subseteq Q^{d+1} \times \Sigma' \times Q^{d+1}$ comprises those tuples
 372 $((q_1, \dots, q_{d+1}), \sigma, (q'_1, \dots, q'_{d+1}))$ such that
 - 373 – if $\sigma \in E$ then $(q_i, \sigma, q'_i) \in \Delta$ for all $i = 1, \dots, d + 1$,
 - 374 – if $\sigma = (\ell, i)$ for some i , then $(q_i, \ell, q'_i) \in \Delta$, and $q_j = q'_j$ for all $j \neq i$.

375 Define $\text{Reach}(\mathcal{S}(\mathcal{A})) \subseteq (\mathbb{R}_{\geq 0}^{\mathcal{Y}})^{d+1}$ to be the collection of $(d + 1)$ -tuples of
 376 observer valuations, given by

$$\text{Reach}(\mathcal{S}(\mathcal{A})) := \{\sum_{\ell \in L} (R(\ell)v(\ell, 1), \dots, R(\ell)v(\ell, d + 1)) : v \in \pi(\mathcal{S}(\mathcal{A}))\}.$$

377 By Proposition 5, $(\gamma_1, \dots, \gamma_{d+1}) \in \text{Reach}(\mathcal{S}(\mathcal{A}))$ if and only if there exist $d + 1$
 378 accepting integer-time runs of \mathcal{A} , all over a common sequence of edges, that
 379 respectively reach observer vectors $\gamma_1, \dots, \gamma_{d+1} \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$. By Proposition 4 we
 380 have:

381 **Proposition 6.** *Given $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, there exists an accepting run ρ of \mathcal{A} with*
 382 *$\text{cost}(\rho) = \gamma$ if and only if there exists $(\gamma_1, \dots, \gamma_{d+1}) \in \text{Reach}(\mathcal{S}(\mathcal{A}))$ such*
 383 *that γ lies in the convex hull of $\{\gamma_1, \dots, \gamma_{d+1}\}$.*

384 Since $\text{Reach}(\mathcal{S}(\mathcal{A}))$ is the image of $\pi(\mathcal{S}(\mathcal{A}))$ under a linear map, from
 385 Theorem 2 we obtain:

386 **Proposition 7.** *The set $\text{Reach}(\mathcal{S}(\mathcal{A})) \subseteq \mathbb{N}^{d(d+1)}$ can be written as a union of*
 387 *linear sets, such that each linear set has a description of length polynomial in*
 388 *$\|\mathcal{A}\|$ and the list of all linear sets can be computed in time exponential in $\|\mathcal{A}\|$.*
 389

390 We now introduce the following “master system” of bilinear inequalities
 391 that expresses whether $\gamma \leq \text{cost}(\rho)$ for some accepting run ρ of \mathcal{A} .

$$\begin{aligned}
 \gamma &\leq \lambda_1 \gamma_1 + \dots + \lambda_{d+1} \gamma_{d+1} \\
 1 &= \lambda_1 + \dots + \lambda_{d+1} \\
 0 &\leq \lambda_1, \dots, \lambda_{d+1} \\
 (\gamma_1, \dots, \gamma_{d+1}) &\in \text{Reach}(\mathcal{S}(\mathcal{A}))
 \end{aligned} \tag{4}$$

392 The system has real variables $\lambda_1, \dots, \lambda_{d+1} \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ and integer variables
 393 $\gamma_1, \dots, \gamma_{d+1} \in \mathbb{N}^{\mathcal{Y}}$. The key property of the master system is stated in the
 394 following Proposition 8, which follows immediately from Proposition 6.

395 **Proposition 8.** *Given a vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ there is an accepting run ρ of \mathcal{A} such*
 396 *that $\gamma \leq \text{cost}(\rho)$ if and only if the system of inequalities (4) has a solution.*

397 Given Proposition 8, the results of Section 4 imply that satisfiability
 398 of the master system (4) is not decidable in general. In the rest of the
 399 paper we pursue different approaches to showing decidability of restrictions
 400 and variants of the Pareto Domination Problem by solving appropriately
 401 restricted versions of (4).

402 6. Pareto Domination Problem with Pure Constraints

403 In this section we show that the Pareto Domination Problem is decidable
 404 in polynomial space for the class of MPTA in which the observers are all costs.
 405 We prove this complexity upper bound by exhibiting for such an MPTA \mathcal{A}
 406 and target $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ a positive integer M , whose bit-length is polynomial in
 407 the size of \mathcal{A} and γ , such that there exists a run ρ of \mathcal{A} reaching the target
 408 location with $\gamma \leq \text{cost}(\rho)$ iff there exists such a run of granularity $\frac{1}{M_1}$ for
 409 some $M_1 \leq M$. To show this we rewrite the bilinear system of inequalities
 410 (4) into an equisatisfiable disjunction of linear systems of inequalities. We
 411 thus obtain a bound on the bit-length of any satisfying assignment of (4)
 412 from which we obtain the above granularity bound. A similar bound in case
 413 of all reward variables is obtained in Appendix B.

414 Consider an MPTA $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$ and write $d = |\mathcal{Y}|$ for the
 415 number of cost variables. Recall that the reachability set $\text{Reach}(\mathcal{S}(\mathcal{A}))$ can
 416 be written as a union of linear sets $S(\mathbf{v}_i, P_i)$, $i \in I$. More precisely, let M_Y
 417 be the maximum rate occurring in the rate function R of the given MPTA
 418 \mathcal{A} . We then have the following Proposition.

419 **Proposition 9.** *The set $\text{Reach}(\mathcal{S}(\mathcal{A}))$ can be written as a finite union of lin-*
 420 *ear sets $\bigcup_{i \in I} S(\mathbf{v}_i, P_i)$ such that for each $i \in I$ the base vectors \mathbf{v}_i and period*
 421 *vectors in P_i have entries of magnitude bounded by $\text{poly}(d, |L|, M_Y, M_X)^{d(d+1)|\mathcal{X}|}$.*

422

423 *Proof.* The number of control states of $\mathcal{Z}(\mathcal{A})$ is at most $(M_X)^{|\mathcal{X}|}|L|$ and
 424 the number of states of $\mathcal{S}(\mathcal{A})$ is at most $((M_X)^{|\mathcal{X}|}|L|)^{d+1}$. Moreover the
 425 vectors occurring in the transitions of $\mathcal{S}(\mathcal{A})$ have entries of magnitude at
 426 most $M_Y M_X$. We now apply Proposition 7 to $\mathcal{S}(\mathcal{A})$. We get that the
 427 base vectors \mathbf{v}_i and period vectors in P_i have entries of magnitude at most
 428 $\text{poly}(d, |L|, M_Y, M_X)^{d(d+1)|\mathcal{X}|}$. \square

429 Suppose that the set of observers \mathcal{Y} with $|\mathcal{Y}| = d$ is comprised exclu-
 430 sively of cost variables. We will apply Proposition 9 to analyse the Pareto
 431 Domination Problem. The key observation is that in this case we can equiv-
 432 alently rewrite the bilinear system (4) as a disjunction of linear systems of
 433 inequalities.

434 As a first step we can rewrite the constraint $(\gamma_1, \dots, \gamma_{d+1}) \in \text{Reach}(\mathcal{S}(\mathcal{A}))$
 435 in (4) as a disjunction of constraints $(\gamma_1, \dots, \gamma_{d+1}) \in S(\mathbf{v}_i, P_i)$, for $i \in I$. But
 436 since the period vectors in P_i are non-negative we can further observe that
 437 in order to satisfy the upper bound constraints on cost variables, the optimal
 438 choice of $(\gamma_1, \dots, \gamma_{d+1}) \in S(\mathbf{v}_i, P_i)$ is the base vector \mathbf{v}_i . Thus we can treat
 439 $\gamma_1, \dots, \gamma_{d+1}$ as a constant in (4).

440 Thus we rewrite (4) as a finite disjunction of systems of linear inequalities—
 441 one such system for each $i \in I$. For a given $i \in I$ let $\mathbf{v}_i = (\gamma_1^{(i)}, \dots, \gamma_{d+1}^{(i)})$
 442 be the base vector of the linear set $S(\mathbf{v}_i, P_i)$. The corresponding system of
 443 inequalities specialising (4) is

$$\begin{aligned} \gamma &\leq \lambda_1 \gamma_1^{(i)} + \dots + \lambda_{d+1} \gamma_{d+1}^{(i)} \\ 1 &= \lambda_1 + \dots + \lambda_{d+1} \\ 0 &\leq \lambda_1, \dots, \lambda_{d+1}. \end{aligned} \tag{5}$$

444 Recall that if a set of linear inequalities $A\mathbf{x} \geq \mathbf{a}$, $B\mathbf{x} > \mathbf{b}$ is feasi-
 445 ble then it is satisfied by some $\mathbf{x} \in \mathbb{Q}^n$ of bit-length $\text{poly}(n, b)$, where b

is the total bit-length of the entries of A , B , \mathbf{a} , and \mathbf{b} . Applying this bound and Proposition 9 we see that a solution of (5) can be written in the form $\lambda_1 = \frac{p_1}{g}, \dots, \lambda_{d+1} = \frac{p_{d+1}}{g}$ for integers p_1, \dots, p_{d+1}, g of bit-length at most $\text{poly}(d, |\mathcal{X}|, |L|, \log(M_Y), \log(M_X))$. This entails that the cost vector $\lambda_1 \gamma_1^{(i)} + \dots + \lambda_{d+1} \gamma_{d+1}^{(i)}$ arises from a run of \mathcal{A} with granularity $\frac{1}{g}$, thus indirectly addressing the open problem stated in [6, Section 8] on the granularity of optimal runs in MPTA.

Together with Proposition 9, this yields PSPACE-membership for the Pareto Domination Problem. As reachability in timed automata is already PSPACE-hard [10] we have:

Theorem 4. *The Pareto Domination Problem with pure constraints is PSPACE-complete.*

7. Pareto Domination Problem with Three Mixed Observers

In this section we show decidability of the Pareto Domination Problem for MPTA with three observers. In the case of three cost variables or three reward variables the results of Section 6 apply, so it remains to consider the case in which both cost and reward observers are present. To this end, the main technical proposition is as follows:

Proposition 10. *Let \mathcal{Y} be a set of observers consisting either of two cost and one reward observer or two reward and one cost observer. Then for each fixed vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, the condition on $\gamma_1, \dots, \gamma_4 \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$ that γ be dominated by some vector in the convex hull of $\{\gamma_1, \dots, \gamma_4\}$ can be expressed by a formula of the language $\mathcal{L}_{\text{quad}}$ (as described in Section 2.1), in which the variables of each constraint denote the respective coordinates of $\gamma_1, \dots, \gamma_4$.*

The proof of Proposition 10, relies on detailed but elementary geometric reasoning. The main challenge is to show that the weak form of constraints permitted in $\mathcal{L}_{\text{quad}}$ is sufficiently expressive for the task at hand.

With this result in hand we can prove:

Theorem 5. *The Pareto Domination Problem is decidable for MPTA with three observers.*

Proof. Let \mathcal{A} be an MPTA and γ a target vector to be dominated. By Proposition 6, \mathcal{A} has an accepting run ρ such that $\gamma \preceq \text{cost}(\rho)$ if and only

478 if there exists $(\gamma_1, \dots, \gamma_4) \in \text{Reach}(\mathcal{S}(\mathcal{A}))$ such that γ is dominated by some
 479 vector in the convex hull of $\{\gamma_1, \dots, \gamma_4\}$.

480 But $\text{Reach}(\mathcal{S}(\mathcal{A}))$ can be written as a union of linear sets $S(\mathbf{v}, P)$, where \mathbf{v}
 481 and P are integer vectors in \mathbb{R}^{12} . Moreover by Proposition 10 the condi-
 482 tion that some vector $(\gamma_1, \dots, \gamma_4) \in S(\mathbf{v}, P)$ is such that the convex hull of
 483 $\{\gamma_1, \dots, \gamma_4\}$ dominates γ can be expressed as a disjunction of constraints in
 484 $\mathcal{L}_{\text{quad}}$. To conclude the proof we recall from Section 2.1 that the satisfiability
 485 problem for $\mathcal{L}_{\text{quad}}$ is decidable. \square

486 Theorem 5 was proven by reduction to satisfiability of a system of arith-
 487 metic constraints with a *single* quadratic term. For the case of four observers
 488 this technique does not appear to yield arithmetic constraints in a known de-
 489 cidable class. Note that satisfiability of systems of constraints featuring two
 490 distinct quadratic terms or a single cubic term is not known to be decidable
 491 in general.

492 *Proof of Proposition 10*

493 It remains to prove Proposition 10. In this subsection we give the proof
 494 in the case of two cost variables and one reward variable. The similar case
 495 of two reward variables and one cost variable is handled in Appendix C.

496 Identify $\mathbb{R}_{\geq 0}^{\mathcal{Y}}$ with $\mathbb{R}_{\geq 0}^3$ and denote by $T \subseteq \mathbb{R}_{\geq 0}^3$ the set of vectors that
 497 dominate a given fixed vector $\gamma \in \mathbb{R}_{\geq 0}^3$. Then T has the form $T = \{(x, y, z) \in$
 498 $\mathbb{R}_{\geq 0}^3 : x \leq a \wedge y \leq b \wedge z \geq c\}$, where a, b, c are non-negative integer constants.
 499 Denote by $\pi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ the projection of \mathbb{R}^3 onto the xy -plane, where
 500 $\pi(x, y, z) = (x, y)$ for all $x, y, z \in \mathbb{R}$. Write $\pi(T)$ and $\pi(S)$ for the respective
 501 images of T and S under π (see the left-hand side of Figure 3).

502 We seek a quantifier-free formula of arithmetic expressing that T meets
 503 the 4-simplex S given by the the convex hull of $\{\gamma_1, \dots, \gamma_4\}$. However, since T
 504 is unbounded, it is clear that T meets S just in case it meets a face of S
 505 (which is a 3-simplex). Thus it will suffice to express the condition that a
 506 3-simplex S given by the convex hull of $\{\gamma_1, \gamma_2, \gamma_3\}$ meets T . Henceforth S
 507 always denotes such a 3-simplex.

508 It is geometrically clear that S intersects T iff either S lies inside T , the
 509 boundary of S meets T , or the boundary of T meets S . More specifically we
 510 have the following proposition:

511 **Proposition 11.** *Let $S \subseteq \mathbb{R}_{\geq 0}^3$ be a 3-simplex. Then $T \cap S$ is nonempty if*
 512 *and only if at least one of the following holds: (a) Some vertex of S lies in T ;*

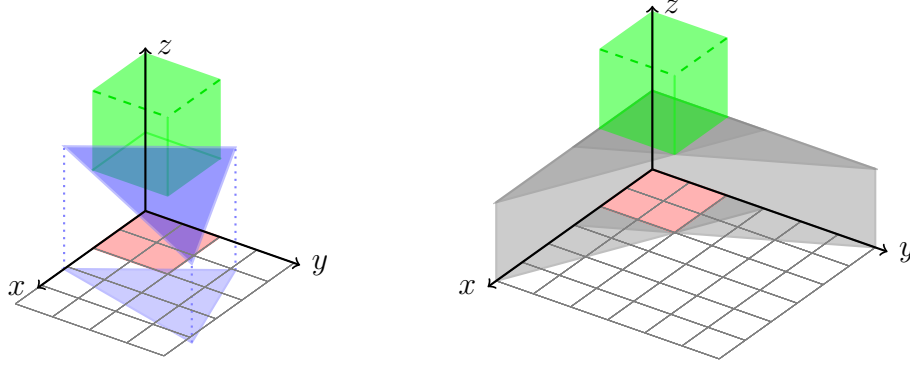


Figure 3: The target T is the green rectangular region and the blue region is S . The pink region is $\pi(T)$ and the light blue region $\pi(S)$. The grey region F is described in equation (6).

- 513 (b) Some bounding edge of S intersects either the face of T supported by the
 514 plane $x = a$ or the face of T supported by the plane $y = b$; (c) The bounding
 515 edge of T supported by the line $x = a \cap y = b$ intersects S .

516 *Proof.* Assume first that T meets some bounding edge of S . We show that
 517 either Condition (a) or Condition (b) holds. Indeed, if T does not contain
 518 a vertex of S then there is a bounding edge E of S such that E meets T
 519 but neither endpoint of E lies in T . Such an edge must cross two faces of T .
 520 Since $S \subseteq \mathbb{R}_{\geq 0}^3$, E cannot cross either of the planes $x = 0$ or $y = 0$, hence it
 521 must cross at least one of the two faces of T respectively supported by the
 522 planes $x = a$ or $y = b$, i.e., Condition (b) holds.

523 On the other hand, suppose that $S \cap T$ is non-empty but T does not
 524 meet any bounding edge of S . Then $S \cap T = P_S \cap T$, where P_S is the
 525 plane affinely spanned by S . We show that Condition (c) holds. Indeed,
 526 since $P_S \cap T$ is bounded, the intersection of P_S and the boundary of T is a
 527 closed curve that is comprised of line segments—each line segment being the
 528 intersection of P_S with a particular face of T . But P_S does not meet either
 529 of the faces $T \cap (x = 0)$ or $T \cap (y = 0)$ since a point of P_S lying on either of
 530 these faces would necessarily lie on some bounding edge of S (and we have
 531 assumed that no bounding edge of S meets T). It follows that P_S meets
 532 all three remaining faces: $T \cap (x = a)$, $T \cap (y = b)$, and $T \cap (z = c)$. We
 533 conclude that P_S (and hence S) meets the bounding edge of T supported by
 534 the line $(x = a) \cap (y = b)$. \square

535 The following definition and proposition are key to expressing intersec-

536 tions of the form identified in Case (c) of Proposition 11 in terms of quadratic
 537 constraints. The idea is to identify a bounded region $F \subseteq \mathbb{R}_{\geq 0}^3$ such that in
 538 Case (c) one of the vertices of S lies in F .

Define a region $F \subseteq \mathbb{R}_{\geq 0}^3$ (depicted as the grey-shaded region on the right of Figure 3) by:

$$F = \{(x, y, z) \in \mathbb{R}_{\geq 0}^3 \mid z < c \wedge (x + ay \leq a(b + 1) \vee y + bx \leq b(a + 1))\}. \quad (6)$$

539 Then we have:

540 **Proposition 12.** *Let $S \subseteq \mathbb{R}_{\geq 0}^3$ be a 3-simplex such that $S \cap T$ is non-empty
 541 but none of the bounding edges of S meets T . Then some vertex of S lies
 542 in F .*

543 *Proof.* Since $S \cap T \neq \emptyset$, we have $\pi(S) \cap \pi(T) \neq \emptyset$. Hence there are
 544 vertices \mathbf{x}, \mathbf{y} of S such that the edge $\pi(\mathbf{x})\pi(\mathbf{y})$ meets $\pi(T)$. By Proposition 15
 545 we have either that one of $\pi(\mathbf{x})$ and $\pi(\mathbf{y})$ lies in $\pi(T)$ or that both $\pi(\mathbf{x})$
 546 and $\pi(\mathbf{y})$ lie in $\pi(F)$.

547 Suppose $\pi(\mathbf{x}) \in \pi(T)$. Since the edge $\mathbf{x}\mathbf{y}$ is assumed not to meet T we
 548 must have that $x_3 < c$ and hence $\mathbf{x} \in F$. Likewise the assumption that
 549 $\pi(\mathbf{y}) \in \pi(T)$ yields $\mathbf{y} \in F$. Finally, if both $\pi(\mathbf{x})$ and $\pi(\mathbf{y})$ lie in $\pi(F)$ then the
 550 assumption that $\mathbf{x}\mathbf{y}$ does not meet T implies that either $x_3 < c$ or $y_3 < c$.
 551 Hence $\mathbf{x} \in F$ or $\mathbf{y} \in F$. \square

552 We write separate $\mathcal{L}_{\text{quad}}$ -formulas $\varphi_T^{(1)}, \varphi_T^{(2)}, \varphi_T^{(3)}$, respectively expressing
 553 the three necessary and sufficient conditions for $T \cap S$ to be nonempty, as
 554 identified in Proposition 11. The free variables of these formulas denote the
 555 coordinates of the three vertices of S .

556 **Some vertex of S lies in T .** Denote the vertices of S by $\mathbf{p}, \mathbf{q}, \mathbf{r}$.
 557 Formula $\varphi_T^{(1)}$ expresses that $\mathbf{p} \in T$ or $\mathbf{q} \in T$ or $\mathbf{r} \in T$. This is clearly a
 558 formula of linear arithmetic.

559 **Some bounding edge of S meets a face of T .** It is straightforward to
 560 obtain $\varphi_T^{(2)}$ given a formula ψ expressing that an arbitrary line segment $\mathbf{x}\mathbf{y}$
 561 in $\mathbb{R}_{\geq 0}^3$ meets a given fixed face of T . We outline such a formula in the rest of
 562 this sub-section. For concreteness we consider the face of T supported by the
 563 plane $x = a$, which maps under π to the line segment $L = \{(a, y) : 0 \leq y \leq b\}$.
 564 Formula ψ has six free variables, respectively denoting the coordinates
 565 of $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$.

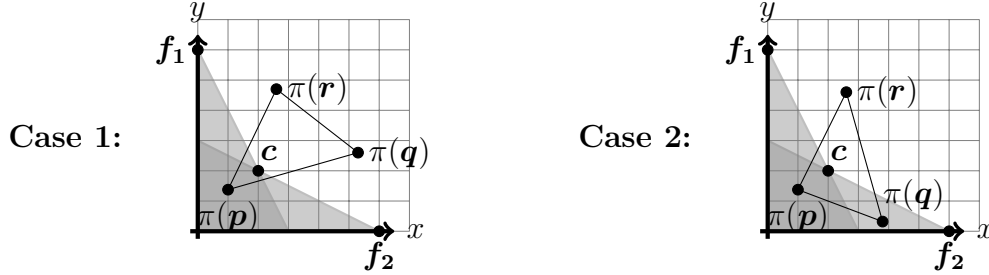


Figure 4: Two cases for expressing that $\mathbf{c} \in \pi(S)$. The grey region is $\pi(F)$.

566 Formula ψ is a conjunction of two parts. The first part expresses that
 567 $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L . Since the complement of $\pi(F)$ is a convex region in $\mathbb{R}_{\geq 0}^2$
 568 that excludes $\pi(T)$ we have that either $\pi(\mathbf{x}) \in \pi(F)$ or $\pi(\mathbf{y}) \in \pi(F)$. More-
 569 over since $\pi(F)$ contains finitely many integer points, we can write sepa-
 570 rate sub-formulas expressing that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L for each fixed value of
 571 $\pi(\mathbf{x}) \in \pi(F)$ and each fixed value of $\pi(\mathbf{y}) \in \pi(F)$. Each of these sub-formulas
 572 can then be written in linear arithmetic, see Section 2.3.

573 Suppose now that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L . Then the line $\mathbf{x}\mathbf{y}$ meets the face of
 574 T supported by the plane $x = a$ iff the line in xz -plane connecting (x_1, x_3) and
 575 (y_1, y_3) passes above (a, c) . This requirement is expressed by the quadratic
 576 constraint 3 in Section 2.3.

577 **A bounding edge of T meets S .** We proceed to describe the for-
 578 mula $\varphi_T^{(3)}$ expressing that the bounding edge E of T , supported by the line
 579 $x = a \cap y = b$, meets S . Note that image of E under the projection π is the
 580 single point $\mathbf{c} = (a, b)$. Thus E meets S just in case $\mathbf{c} \in \pi(S)$ and the point
 581 (a, b, c) lies below the plane affinely spanned by S . We describe two formulas
 582 that respectively express these requirements.

583 Denote the vertices of S by \mathbf{p} , \mathbf{q} , and \mathbf{r} . We first give a formula of linear
 584 arithmetic expressing that $\mathbf{c} \in \pi(S)$. Notice that if $\mathbf{c} \in \pi(S)$ then at least
 585 one vertex of $\pi(S)$ must lie in $\pi(F)$. We now consider two cases. The first
 586 case is that exactly one vertex of $\pi(S)$ (say $\pi(\mathbf{p})$) lies in $\pi(F)$. The second
 587 case is that at least two vertices of $\pi(S)$ (say $\pi(\mathbf{p})$ and $\pi(\mathbf{q})$) lie in $\pi(F)$.
 588 The two cases are respectively denoted in Figure 4, that we refer to in the
 589 following.

590 In the first case we can express that $\mathbf{c} \in \pi(S)$ by requiring that the line
 591 segment $\pi(\mathbf{p})\pi(\mathbf{q})$ crosses the edge $\mathbf{f}_2\mathbf{c}$ and $\pi(\mathbf{p})\pi(\mathbf{r})$ crosses the edge $\mathbf{f}_1\mathbf{c}$.
 592 By writing a separate constraint for each fixed value of $\pi(\mathbf{p}) \in \pi(F)$ the

593 above requirements can be expressed in linear arithmetic.

594 In the second case we can express that $\mathbf{c} \in \pi(S)$ by requiring that \mathbf{c} lies
 595 on the left of each of the directed line segments $\pi(\mathbf{p})\pi(\mathbf{q})$, $\pi(\mathbf{q})\pi(\mathbf{r})$, and
 596 $\pi(\mathbf{r})\pi(\mathbf{p})$. By writing such a constraint for each fixed value of $\pi(\mathbf{p})$ and $\pi(\mathbf{q})$
 597 in $\pi(F)$ we obtain, again, a formula of linear arithmetic, see Section 2.3.

598 It remains to give a formula expressing that (a, b, c) lies below the plane
 599 affinely spanned by \mathbf{p} , \mathbf{q} , and \mathbf{r} under the assumption that $\mathbf{c} \in \pi(S)$. Note
 600 here that the above-described formula expressing that $\pi(\mathbf{c}) \in \pi(S)$ specifies
 601 *inter alia* that $\pi(\mathbf{p})$, $\pi(\mathbf{q})$, and $\pi(\mathbf{r})$ are oriented counter-clockwise. Thus
 602 (a, b, c) lies below the plane affinely spanned by \mathbf{p} , \mathbf{q} , and \mathbf{r} iff

$$\begin{vmatrix} q_1 - p_1 & r_1 - p_1 & a - p_1 \\ q_2 - p_2 & r_2 - p_2 & b - p_2 \\ q_3 - p_3 & r_3 - p_3 & c - p_3 \end{vmatrix} < 0$$

603 The above expression is cubic, but by Proposition 12 we may assume
 604 that \mathbf{p} lies in the set F , which has finitely many integer points. Thus by a
 605 case analysis we may regard \mathbf{p} as being fixed and so write the desired formula
 606 as a disjunction of atoms, each with a single quadratic term.

607 8. Gap Domination Problem

608 In this section we give a decision procedure for the Gap Domination
 609 Problem. Given an MPTA \mathcal{A} , vector $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, and a rational tolerance $\varepsilon > 0$,
 610 our procedure is such that

- 611 • if there is an accepting run ρ of \mathcal{A} such that $\gamma \leq_{\varepsilon} \text{cost}(\rho)$ then we
 612 output “dominated”;
- 613 • if there is no accepting run ρ of \mathcal{A} such that $\gamma \leq \text{cost}(\rho)$ then we output
 614 “not dominated”.

615 **Theorem 6.** *The Gap Domination Problem is decidable in exponential time.*

616 *Proof.* Let \mathcal{A} be an MPTA, $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$, and $\varepsilon > 0$. Recall from Proposition 8
 617 that \mathcal{A} has an accepting run ρ such that $\gamma \leq \text{cost}(\rho)$ if and only if the
 618 bilinear system of inequalities (4) is satisfiable. Our approach to solve the
 619 Gap Domination Problem is to find approximate solutions of (4) by relaxation
 620 and rounding.

621 Compute a decomposition of $\text{Reach}(\mathcal{S}(\mathcal{A}))$ as a union of linear sets and
 622 let $S := S(\mathbf{v}, P)$ be one such linear set, where $P = \{\mathbf{u}_1, \dots, \mathbf{u}_k\}$. Replace
 623 the constraint $(\gamma_1, \dots, \gamma_{d+1}) \in \text{Reach}(\mathcal{S}(\mathcal{A}))$ in (4) with

$$(\gamma_1, \dots, \gamma_{d+1}) = \mathbf{v} + n_1 \mathbf{u}_1 + \dots + n_k \mathbf{u}_k,$$

624 where n_1, \dots, n_k are variables ranging over \mathbb{N} . We thus obtain for each choice
 625 of S a bilinear system of inequalities φ_S of the form (7), where I and J are
 626 finite sets and for each $i \in I$ and $j \in J$, it holds that f_i, g_j are linear forms
 627 (i.e., polynomials of degree one with no constant terms) with non-negative
 628 integer coefficients and c_i and d_j are rational constants.

$$\begin{aligned} f_i(n_1 \lambda_1, n_1 \lambda_2, \dots, n_k \lambda_{d+1}) &\leq c_i & (i \in I) & \lambda_1, \dots, \lambda_{d+1} &\geq 0 \\ g_j(n_1 \lambda_1, n_1 \lambda_2, \dots, n_k \lambda_{d+1}) &\geq d_j & (j \in J) & \lambda_1 + \dots + \lambda_{d+1} &= 1 \\ n_1, \dots, n_k &\in \mathbb{N} \end{aligned} \tag{7}$$

629 Fix a particular system φ_S , as depicted in (7). Let μ be the maximum
 630 coefficient of the f_i , $i \in I$. Given $T \subseteq \{1, \dots, d+1\}$, we define the following
 631 constraint ψ_T on $\lambda_1, \dots, \lambda_{d+1}$:

$$\psi_T := \bigwedge_{i \in T} \lambda_i \leq \frac{\varepsilon}{(d+1)k\mu} \wedge \bigwedge_{i \notin T} \lambda_i \geq \frac{\varepsilon}{(d+1)k\mu}.$$

632 Intuitively, ψ_T expresses that λ_i is “small” for $i \in T$ and “large” for $i \notin T$.
 633 Given any satisfying assignment of φ_S it is clear that $\lambda_1, \dots, \lambda_{d+1}$ must satisfy
 634 φ_T for some $T \subseteq \{1, \dots, d+1\}$.

635 Now fix a set $T \subseteq \{1, \dots, d+1\}$ and consider the satisfiability of $\varphi_S \wedge \psi_T$.
 636 If $i \notin T$ then for any term $\lambda_i n_j$ that appears in a constraint of the form
 637 $f(n_1 \lambda_1, \dots, n_k \lambda_{d+1}) \leq c$ in φ_S , we must have $n_j \leq \lceil \frac{c(d+1)\mu}{\varepsilon} \rceil$ in order for the
 638 constraint to be satisfied. Thus by enumerating all values of n_j up to this
 639 bound we can eliminate this variable. By doing this we may assume that in
 640 $\varphi_S \wedge \psi_T$, for any term $\lambda_i n_j$ that appears on the left-hand side of an upper-
 641 bound constraint we have $i \in T$ and hence that λ_i must be “small” in any
 642 satisfying assignment.

643 The next step is relaxation—try to solve $\varphi_S \wedge \psi_T$ (after the above de-
 644 scribed elimination step), letting the variables n_1, \dots, n_k range over the non-
 645 negative reals. Recall here that the existential theory of real closed fields is
 646 decidable in polynomial space. If there is no real solution of $\varphi_S \wedge \psi_T$ for
 647 any S and T then there is certainly no solution over the naturals. and we

648 can output “not dominated”. On the other hand, if there is a run ρ with
649 $\gamma \preceq_\varepsilon \text{cost}(\rho)$ then for some S and T , the system $\varphi_S \wedge \psi_T$ will have a real
650 solution in which moreover the inequalities $f_i(n_1\lambda_1, \dots, n_k\lambda_{d+1}) \leq c_i$ for $i \in I$
651 all hold with slack at least ε . Given such a solution, replace n_j with $\lceil n_j \rceil$ for
652 $j = 1, \dots, k$. Consider the left-hand side $f_i(n_1\lambda_1, \dots, n_k\lambda_{d+1})$ of an upper
653 bound constraint in φ_S . Since the variables λ_i mentioned in such a linear
654 form are small, the effect of rounding is to increase this term by at most ε .
655 Hence the rounded vector still satisfies φ_S thanks to the slack in the origi-
656 nal solution. This completes the description and proof of correctness of the
657 procedure. It remains to account for the complexity.

658 By Proposition 7 we can compute a decomposition of $\text{Reach}(\mathcal{S}(\mathcal{A}))$ as a
659 union of linear sets in time exponential in $\|\mathcal{A}\|$, with each linear set in this
660 decomposition having a description of size polynomial in $\|\mathcal{A}\|$. It follows that
661 each of the above-defined formulas $\varphi_S \wedge \psi_T$ has size polynomial in $\|\mathcal{A}\|$. Both
662 the number of such formulas and time to decide satisfiability of each formula
663 over the reals is exponential in $\|\mathcal{A}\|$. It follows that our decision procedure
664 runs in time exponential in $\|\mathcal{A}\|$. \square

665 9. Topology of Reachable Observer Vectors

666 The decidability of the Gap Domination Problem has counter-intuitive
667 implications for the topology of the set of reachable observer vectors, namely
668 that for MPTA featuring closed guards (and no invariants) the set of reach-
669 able observer vectors is not necessarily closed. This follows from undecid-
670 ability of the Pareto Domination Problem (Theorem 3) and the following
671 two propositions, the second being a direct consequence of decidability of
672 the Gap Domination Problem (Theorem 6).

673 **Proposition 13.** *The Pareto Domination Problem is semidecidable.*

674 *Proof.* For any given depth bound $k \in \mathbb{N}$, it is decidable whether an MPTA
675 \mathcal{A} can within k transitions reach an observer vectors γ dominating a given
676 Pareto target γ' . A corresponding decision procedure can be obtained by
677 a straightforward reduction to the existential theory of linear arithmetic, as
678 employed in bounded model-checking of linear hybrid automata [18], a proper
679 superset of MPTA.

680 By checking for increasingly larger depth bounds $k \in \mathbb{N}$ until we find a
681 dominating reachable observer vector $\gamma \preceq \gamma'$, we obtain the desired semide-
682 cision procedure for the Pareto Domination Problem. \square

683 **Proposition 14.** *The Pareto Domination Problem is co-semidecidable for*
 684 *MPTA featuring a closed set of reachable observer vector.*

685 *Proof.* Consider a Pareto target vector γ and an MPTA \mathcal{A} . Denote by
 686 $\text{Reach}_{\mathcal{O}(\mathcal{A})}$ the set of observer vectors reachable in \mathcal{A} . Assume that $\text{Reach}_{\mathcal{O}(\mathcal{A})}$
 687 is closed.

688 If no $\gamma' \in \text{Reach}_{\mathcal{O}(\mathcal{A})}$ dominates the target γ , then due to topological
 689 closedness of $\text{Reach}_{\mathcal{O}(\mathcal{A})}$ there exists $\varepsilon > 0$ such that

$$\forall \gamma \in \text{Reach}_{\mathcal{O}(\mathcal{A})} : \left(\begin{array}{l} \exists y \in \mathcal{Y}_r : \gamma(y) - \varepsilon > \gamma'(y) \\ \vee \exists y \in \mathcal{Y}_c : \gamma'(y) - \varepsilon > \gamma(y) \end{array} \right), \quad (8)$$

690 i.e., any reachable observer vector γ' misses the target γ by at least ε in at
 691 least one dimension.

692 Now denote by γ_δ the target observer vector defined as $\gamma_\delta(y) = \gamma(y) - \delta$
 693 for each $y \in \mathcal{Y}_r$ and $\gamma_\delta(y) = \gamma(y) + \delta$ for each $y \in \mathcal{Y}_c$. The target γ_δ
 694 represents a relaxed Pareto target in the sense of adding δ to the cost bounds
 695 and subtracting δ from the reward bounds. Condition (8) is equivalent to
 696 $\neg(\gamma_{2\varepsilon} \leq \gamma')$ and obviously implies $\neg(\gamma_{2\varepsilon} \leq \gamma')$. Accordingly, the procedure
 697 for deciding the Gap Domination Problem from Theorem 6 will terminate
 698 with “not dominated” when applied to MPTA \mathcal{A} and Pareto target $\gamma_{2\varepsilon}$ with
 699 a gap of ε .

700 Consequently, we obtain a co-semidecision procedure for the Pareto Domi-
 701 nation Problem for MPTA featuring a closed set of reachable observer vectors
 702 by repeatedly, for increasing $k \in \mathbb{N}$, applying the decision procedure for the
 703 Gap Domination Problem to instances featuring a Pareto target $\gamma_{\frac{2}{k}}$ and a
 704 gap $\frac{1}{k}$ until the decision procedure reports “not dominated”. \square

705 As Propositions 13 and 14 combine into a decision procedure for the
 706 Pareto Domination Problem for MPTA featuring a closed set of reachable
 707 observer vectors, yet the Pareto Domination Problem is undecidable in gen-
 708 eral due to Theorem 3, we obtain

709 **Corollary 1.** *The Pareto Domination Problem is decidable for MPTA with*
 710 *closed guards featuring a closed set of reachable observer vectors. Further-*
 711 *more, the set of observer vectors reachable in MPTA featuring closed guards*
 712 *is in general not closed.*

713 To this end please note that all MPTA in this paper feature closed guards
 714 only, including those employed for the reduction of Diophantine equations in
 715 the proof of Theorem 3.

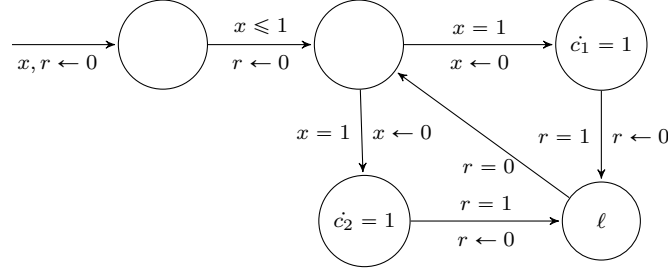


Figure 5: An MPTA with closed guards, where the rate of two observers c_1 and c_2 is zero in all locations except in two indicated locations. This MPTA generates a set of reachable observer vectors that is both dense and co-dense in $\mathbb{R}_{\geq 0}^2$.

A concrete example of an MPTA \mathcal{A} generating a set $\text{Reach}_{\mathcal{O}(\mathcal{A})}$ of reachable observer vectors that is both dense and co-dense in $\mathbb{R}_{\geq 0}^2$ and thus not closed is shown in Fig. 5. The set of observer vectors reachable in location l is $\{(c_1, c_2) \mid c_1, c_2 \in \mathbb{R}_{\geq 0}, \exists q \in \mathbb{Q}_{\geq 0} : c_1 = qc_2\}$.

Acknowledgements. We thank Dan Segal for discussions concerning [13] and the reviewers of [1] for their feedback.

References

References

- [1] M. Fränzle, M. Shirmohammadi, M. Swaminathan, J. Worrell, Costs and rewards in priced timed automata, in: ICALP, LIPICS, 2018, pp. 63:1–63:13.
- [2] P. Bouyer, E. Brinksma, K. G. Larsen, Optimal infinite scheduling for multi-priced timed automata, Formal Methods in System Design 32 (1) (2008) 3–23.
- [3] P. Bouyer, K. G. Larsen, N. Markey, Model checking one-clock priced timed automata, Logical Methods in Computer Science 4 (2008) 1–28.
- [4] T. Brihaye, V. Bruyère, J. Raskin, On model-checking timed automata with stopwatch observers, Inf. Comput. 204 (3) (2006) 408–433.
- [5] M. Fränzle, M. Swaminathan, Revisiting decidability and optimum reachability for multi-priced timed automata, in: FORMATS, Vol. 5813 of LNCS, Springer, 2009, pp. 149–163.

- 737 [6] K. G. Larsen, J. I. Rasmussen, Optimal reachability for multi-priced
738 timed automata, TCS 390 (2-3) (2008) 197–213.
- 739 [7] R. Alur, S. L. Torre, G. J. Pappas, Optimal paths in weighted timed
740 automata, in: HSCC, Vol. 2034 of LNCS, Springer, 2001, pp. 49–62.
- 741 [8] G. Behrmann, A. Fehnker, T. Hune, K. G. Larsen, P. Pettersson,
742 J. Romijn, F. W. Vaandrager, Minimum-cost reachability for priced
743 timed automata, in: HSCC, Vol. 2034 of LNCS, Springer, 2001, pp.
744 147–161.
- 745 [9] K. G. Larsen, G. Behrmann, E. Brinksma, A. Fehnker, T. Hune, P. Pet-
746 tersson, J. Romijn, As cheap as possible: Efficient cost-optimal reacha-
747 bility for priced timed automata, in: CAV, Vol. 2102 of LNCS, Springer,
748 2001, pp. 493–505.
- 749 [10] R. Alur, D. Dill, A theory of timed automata, TCS 126 (2) (1994) 183–
750 235.
- 751 [11] T. A. Henzinger, P. W. Kopke, A. Puri, P. Varaiya, What’s decidable
752 about hybrid automata?, J. Comput. Syst. Sci. 57 (1) (1998) 94–124.
- 753 [12] J. P. Jones, Undecidable diophantine equations, Bull. Amer. Math. Soc.
754 3 (1980) 859–862.
- 755 [13] F. Grunewald, D. Segal, On the integer solutions of quadratic equations,
756 Journal für die reine und angewandte Mathematik 569 (2004) 13–45.
- 757 [14] I. Diakonikolas, M. Yannakakis, Small approximate pareto sets for biob-
758 jective shortest paths and other problems, SIAM J. Comput. 39 (4)
759 (2009) 1340–1371.
- 760 [15] Z. Zhang, B. Nielsen, K. G. Larsen, G. Nies, M. Stenger, H. Hermanns,
761 Pareto optimal reachability analysis for simple priced timed automata,
762 in: ICFEM, Vol. 10610 of LNCS, Springer, 2017, pp. 481–495.
- 763 [16] A. W. To, Parikh images of regular languages: Complexity and appli-
764 cations Report at <http://arxiv.org/abs/1002.1464>.
- 765 [17] T. Zaslavsky, Signed graphs, Discrete Applied Mathematics 4 (1) (1982)
766 47 – 74.

- 767 [18] G. Audemard, M. Bozzano, A. Cimatti, R. Sebastiani, Verifying indus-
768 trial hybrid systems with mathsat, *Electr. Notes Theor. Comput. Sci.*
769 119 (2) (2005) 17–32.
- 770 [19] P. Bouyer, T. Brihaye, V. Bruyère, J.-F. Raskin, On the optimal reacha-
771 bility problem of weighted timed automata, *Formal Methods in System*
772 *Design* 31 (2) (2007) 135–175.

773 Appendix A. Difference Constraints

774 As summarized in [19, Section 5.3] for the setting of a single observer,
 775 given an MPTA \mathcal{A} with difference clock constraints, we can find an MPTA \mathcal{A}'
 776 without difference clock constraints such that \mathcal{A} and \mathcal{A}' are strongly time-
 777 bisimilar. The Domination Problems for \mathcal{A} can thus be reduced to those
 778 for \mathcal{A}' . Although eliminating difference clock constraints from MPTA results
 779 in an exponential blow-up in the number of locations and edges [19, Section
 780 5.3], the PSPACE complexity for the Pareto Domination Problem in the case
 781 of all cost variables and all reward variables (see Section 6 and Appendix B)
 782 remains true. Indeed the granularity bounds that were used to establish
 783 PSPACE complexity, while exponential in the number of observers, are only
 784 polynomial in the number of locations of the MPTA and hence remain singly
 785 exponential in magnitude even after an exponential blow-up in the number
 786 of locations.

787 Appendix B. Pareto Domination with All Reward Variables

788 Now we suppose that the set of observers \mathcal{Y} is comprised exclusively of
 789 reward variables. We will again apply Proposition 9 to rewrite (4) as a finite
 790 disjunction of systems of linear inequalities.

791 Fix an index $i \in I$. Let the base vector of the linear set $S(\mathbf{v}_i, P_i)$ be
 792 $\mathbf{v}_i = (\gamma_1, \dots, \gamma_{d+1})$. We write a linear constraint to express that there exists
 793 a vector $(\gamma'_1, \dots, \gamma'_{d+1}) \in S(\mathbf{v}_i, P_i)$ and a convex combination $\sum_{j=1}^{d+1} \lambda_j \gamma'_j$ that
 794 dominates a given $\gamma \in \mathbb{R}_{\geq 0}^{\mathcal{Y}}$. We write this constraint as a disjunction of
 795 finitely many systems of linear inequalities—one system for each possible
 796 choice of the support $S' \subseteq \{1, \dots, d+1\}$ of the the convex sum. Fix such
 797 a set S' and let $\mathcal{Y}_{S'} \subseteq \mathcal{Y}$ be the set of variables y such that there is some
 798 period vector $(\gamma'_1, \dots, \gamma'_{d+1}) \in P_i$ and $j \in S'$ with $\gamma'_j(y) > 0$. Then the system
 799 of inequalities is as follows:

$$\begin{aligned}
 \gamma(y) &\leq \lambda_1 \gamma_1(y) + \dots + \lambda_{d+1} \gamma_{d+1}(y) & (y \notin \mathcal{Y}_{S'}) \\
 1 &= \lambda_1 + \dots + \lambda_{d+1} \\
 0 &< \lambda_j & (j \in S') \\
 0 &= \lambda_j & (j \notin S')
 \end{aligned} \tag{B.1}$$

800 To see why this works, note that for $y \in \mathcal{Y}_{S'}$ there exists some period vec-
 801 tor $(\gamma'_1, \dots, \gamma'_{d+1}) \in P_i$ and $j \in S'$ with $\gamma'_j(y) > 0$. By adding suitable multi-
 802 ples of to the solution of the above system we can make value of the variable y
 803 arbitrarily large.

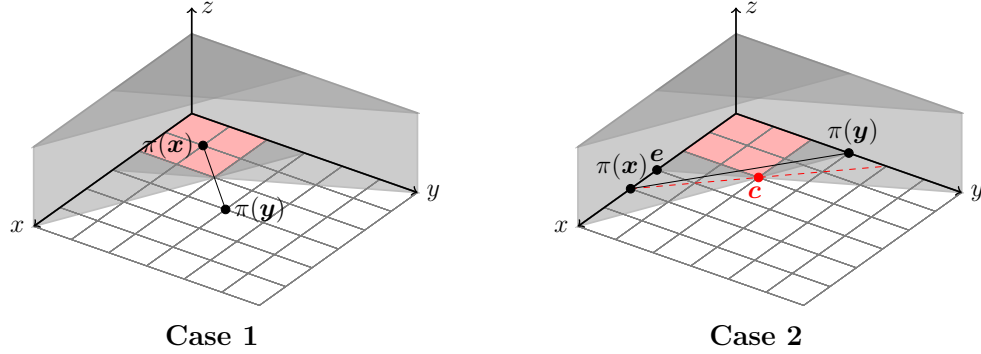


Figure C.6: Two cases in the proof of Proposition 15, where the grey region is F and the pink region is R .

Recall that if a set of linear inequalities $A\mathbf{x} \geq \mathbf{a}$, $B\mathbf{x} > \mathbf{b}$ is feasible then it is satisfied by some $\mathbf{x} \in \mathbb{Q}^n$ of bit-length $\text{poly}(n, b)$, where b is the total bit-length of the entries of A , B , \mathbf{a} , and \mathbf{b} . Applying this bound and Proposition 9 we see that a solution of (B.1) can be written in the form $\lambda_1 = \frac{p_1}{g}, \dots, \lambda_{d+1} = \frac{p_{d+1}}{g}$ for integers p_1, \dots, p_{d+1}, g of bit-length at most $\text{poly}(d, |L|, \log(M_Y), \log(M_X))$. This entails that the cost vector $\lambda_1 \gamma_1 + \dots + \lambda_{d+1} \gamma_{d+1}$ arises from a run of \mathcal{A} with granularity $\frac{1}{g}$.

Appendix C. Pareto Domination with Three Mixed Observers: Two Reward Variables and One Cost Variable

Recall the set F , defined in Equation (6) and consider its projection $\pi(F)$ in the xy -plane. Moreover write $R := \{(x, y) \in \mathbb{R}_{\geq 0}^2 : x \leq a \wedge y \leq b\}$ (see Figure C.6).

Proposition 15. *Let L be an edge in $\mathbb{R}_{\geq 0}^2$ that intersects R . Then L has either one endpoint in R or has both endpoints in $\pi(F)$.*

Proof. Let L have endpoints $\mathbf{x}, \mathbf{y} \in \mathbb{R}_{\geq 0}^2$. Since the complement of $\pi(F)$ is a convex region in $\mathbb{R}_{\geq 0}^2$ that excludes R , at least one of \mathbf{x} or \mathbf{y} lies in $\pi(F)$. Without loss of generality, assume that $\mathbf{x} \in \pi(F)$. To prove the proposition it suffices to show that if $\mathbf{x} \notin R$ then both $\mathbf{x}, \mathbf{y} \in \pi(F)$.

Suppose $\mathbf{x} \notin R$. Now $\pi(F) \setminus R = F_0 \cup F_1$, where

$$F_0 = \{(x, y) \in \mathbb{R}_{\geq 0}^2 \mid y + bx \leq b(a + 1) \text{ and } x \geq a\}$$

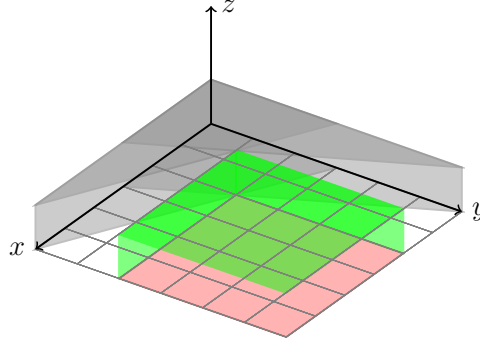


Figure C.7: The target T is the green rectangular region, the grey region is F , and the pink region is $\pi(T)$.

823 and

$$F_1 = \{(x, y) \in \mathbb{R}_{\geq 0}^2 \mid x + ay \leq a(b + 1) \text{ and } y \geq b\}.$$

824 Thus \mathbf{x} lies in either F_0 or F_1 . We show that $\mathbf{x} \in F_i$ only if $\mathbf{y} \in F_{1-i}$ for
825 $i \in \{0, 1\}$ and conclude that both $\mathbf{x}, \mathbf{y} \in F$.

826 Assume that $\mathbf{x} \in F_0$. Since the edge $\mathbf{x}\mathbf{y}$ meets R , clearly $\mathbf{y} \notin F_0$. Draw
827 a line through \mathbf{x} and \mathbf{c} , shown as the dashed red line in the diagram. The
828 point \mathbf{y} is below this line for otherwise edge $\mathbf{x}\mathbf{y}$ fails to meet R . Consider
829 the point $\mathbf{e} = (0, b + 1)$. Then the edges \mathbf{ec} and \mathbf{xc} meet at \mathbf{c} . Since edge
830 \mathbf{xc} intersects the x -axis above \mathbf{e} , it intersects the y -axis below the edge \mathbf{ec} ,
831 i.e. in $\pi(F)$. We conclude that $\mathbf{y} \in F_1$.

832 The argument for the case $\mathbf{x} \in F_1$ is symmetric. Thus we have shown
833 that $\mathbf{x}, \mathbf{y} \in \pi(F)$. \square

834 Consider a reachability objective $T \subseteq \mathbb{R}_{\geq 0}^3$ given by two upper-bound
835 constraints and one lower-bound constraint, see Figure C.7. Write

$$T = \{(x, y, z) \in \mathbb{R}_{\geq 0}^3 : x \geq a \wedge y \geq b \wedge z \leq c\},$$

836 where a, b, c are non-negative integer constants. We write a quantifier-free
837 first-order formula φ_T of arithmetic expressing that a 3-simplex $S \subseteq \mathbb{R}_{\geq 0}^3$
838 meets T . This formula has nine free variables: one for each of the coordinates
839 of the three vertices of S .

840 Write $\pi(T)$ for the projection of T in the xy -plane, see Figure C.7.

841 The following two propositions are syntactically identical to Proposi-
842 tion 11 and Proposition 12, although now referring to a different form of

the target set T . The respective proofs follow the same ideas as those earlier results, but with small adaptations to the new target set.

Proposition 16. *Let $S \subseteq \mathbb{R}_{\geq 0}^3$ be a 3-simplex. Then $T \cap S$ is nonempty if and only if at least one of the following holds:*

1. *Some vertex of S lies in T .*
2. *Some bounding edge of S intersects either the face of T supported by the plane $x = a$ or the face of T supported by the plane $y = b$.*
3. *The bounding edge of T supported by the line $x = a \cap y = b$ intersects S .*

Proof. Assume first that T meets some bounding edge of S . We show that either Condition (a) or Condition (b) holds. Indeed, if T does not contain a vertex of S then there is a bounding edge E of S such that E meets T but neither endpoint of E lies in T . Such an edge must cross two faces of T . Since $S \subseteq \mathbb{R}_{\geq 0}^3$, E cannot be the plane $z = 0$ or $y = 0$, it must cross at least one of the two faces of T respectively supported by the planes $x = a$ or $y = b$, i.e., Condition (b) holds.

On the other hand, suppose that $S \cap T$ is non-empty but T does not meet any bounding edge of S . Then $S \cap T = P_S \cap T$, where P_S is the plane affinely spanned by S . We show that Condition (c) holds. Indeed, since $P_S \cap T$ is bounded, the intersection of P_S and the boundary of T is a closed curve that is comprised of line segments—each line segment being the intersection of P_S with a particular face of T . But P_S does not meet the face $T \cap (z = 0)$ since a point of P_S lying on this face would necessarily lie on some bounding edge of S (and we have assumed that no bounding edge of S meets T). It follows that P_S meets all three remaining faces: $T \cap (x = a)$, $T \cap (y = b)$, and $T \cap (z = c)$. We conclude that P_S (and hence S) meets the bounding edge of T supported by the line $(x = a) \cap (y = b)$. \square

The following Proposition refers to the set F as defined in (6).

Proposition 17. *Let $S \subseteq \mathbb{R}_{\geq 0}^3$ be a 3-simplex such that $S \cap T$ is non-empty, but no bounding edge of S meets T . Then some vertex of S lies in F .*

Proof. Under the assumptions of this proposition, Items 1 and 2 of Proposition 16 do not hold. Hence the bounding edge of T that is supported by the line segment $x = a \cap y = b$ meets S at some point not on a bounding edge of S . In particular, considering the projection in the xy -plane, we have that the point (a, b) lies in the interior of $\pi(S)$.

877 Now consider the plane in $\mathbb{R}_{\geq 0}^3$ affinely spanned by S . Write the equation
878 of this plane in the form $z = f(x, y)$ for some affine function f . From the
879 assumption that no bounding edge of S meets T , we deduce that (a, b) is the
880 only vertex of the convex set $\pi(S) \cap \pi(T)$ at which f is bounded above by
881 c . It follows that f has positive derivative in the direction of the positive
882 x -axis and positive y -axis. Hence f is bounded above by c on the entire
883 region $R := \{(x, y) \in \mathbb{R}_{\geq 0}^2 : x \leq a, y \leq b\}$.

884 Now since (a, b) lies in the interior of $\pi(S)$, there is a bounding edge $\mathbf{x}\mathbf{y}$
885 of S such that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets the region R . By Proposition 15, $\pi(\mathbf{x})\pi(\mathbf{y})$
886 either has some endpoint in R (say $\pi(\mathbf{x})$) or has both endpoints in $\pi(F)$.
887 Since f is bounded above by c on R , in the first case we have that $x_3 \leq c$
888 and hence $\mathbf{x} \in F$. In the second case we have that either $x_3 \leq c$ or $y_3 \leq c$
889 and hence either $\mathbf{x} \in F$ or $\mathbf{y} \in F$. \square

890 We write separate formulas $\varphi_T^{(1)}, \varphi_T^{(2)}, \varphi_T^{(3)}$, respectively expressing the
891 three necessary and sufficient conditions for $T \cap S$ to be nonempty as identi-
892 fied in Proposition 16. These are formulas of arithmetic whose free variables
893 denote the coordinates of the three vertices of S . The definitions of the
894 formulas $\varphi_T^{(1)}$ and $\varphi_T^{(3)}$ are almost identical to those of the corresponding for-
895 mulas in Section 7. The only difference is that for $\varphi_T^{(3)}$ we ask to express that
896 the point (a, b, c) lies above the plane affinely spanned by \mathbf{p}, \mathbf{q} , and \mathbf{r} (rather
897 than below the plane, as in Section 7).

898 There are more substantial differences in the definition of the formula $\varphi_T^{(2)}$.
899 Recall that this formula expresses that some bounding edge of S meets a face
900 of T . As in Section 7, it is straightforward to obtain $\varphi_T^{(2)}$ given a formula ψ
901 expressing that an arbitrary line segment $\mathbf{x}\mathbf{y}$ in $\mathbb{R}_{\geq 0}^3$ meets a given fixed face
902 of T . We outline such a formula below. For concreteness we consider the
903 face of T supported by the plane $x = a$, which maps under π to the line
904 segment L given by $x = a \cap y \geq b$ (see Figure C.8). Formula ψ has six free
905 variables, respectively denoting the coordinates of \mathbf{x} and \mathbf{y} .

906 Formula ψ is a conjunction of two parts. The first part expresses that
907 $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L . The key is to express this requirement via a formula of
908 linear arithmetic. For each fixed value of $\pi(\mathbf{x}) \in F$ we can write a linear
909 constraint expressing that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L , and likewise for each fixed
910 value of $\pi(\mathbf{y}) \in F$. Thus we may assume that both $\pi(\mathbf{x})$ and $\pi(\mathbf{y})$ lie in the
911 complement of $\pi(F)$. But then $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L just in case $\pi(\mathbf{x})$ and $\pi(\mathbf{y})$
912 lie on opposite sides of the line $x = a$, which is also a linear constraint.

913 Suppose now that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets L , say at a point $\pi(\mathbf{z})$ where \mathbf{z} lies on

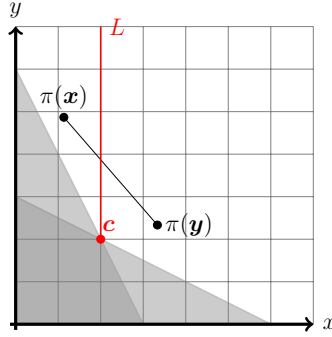


Figure C.8: To express that $\pi(\mathbf{x})\pi(\mathbf{y})$ meets line segment L . The grey region is $\pi(F)$.

914 line segment $\mathbf{x}\mathbf{y}$. The second part of ψ expresses that \mathbf{z} lies below the plane
 915 $z = c$. Such a formula is a disjunction of atoms, each with a single quadratic
 916 term, whose satisfiability is known to be decidable from Theorem 1.