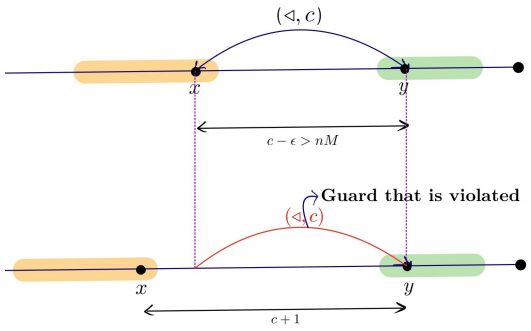

Figure 6 Increasing the difference between x and y using $\simeq$-equivalence.

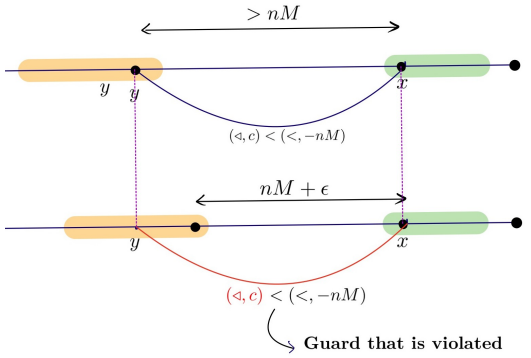

Figure 7 Shrinking the difference between x and y using $\simeq$-equivalence.

Thus, we obtain as a corollary that, for event-predicting automata, we do not even need simulation to obtain finiteness of its zone graph.

▶ **Corollary 46.** *Let $\mathcal{A}$ be an event-predicting automata with diagonal constraints. Then, the zone graph of $\mathcal{A}$ is finite.*

8 Finiteness of the simulation relation

In this section, we will show that the simulation relation $\preceq_{\mathcal{A}}$ defined in Section 5 is finite, which implies that the reachability algorithm terminates. Recall that given a GTA $\mathcal{A}$, we have an associated map $\mathcal{G}$ from states of $\mathcal{A}$ to sets of atomic constraints. Let $M = \max\{|c| \mid c \in \mathbb{Z} \text{ is used in some constraint of } \mathcal{A}\}$, the maximal constant of $\mathcal{A}$. We have $M \in \mathbb{N}$ and constraints in the sets $\mathcal{G}(q)$ use constants in $\{-\infty, \infty\} \cup \{c \in \mathbb{Z} \mid |c| \leq M\}$. We will refer to such constraints as *M-bounded integral constraints*.

Recall that the simulation relation $\preceq_{\mathcal{A}}$ was defined on nodes of the zone graph of $\mathcal{A}$ by $(q, Z) \preceq_{\mathcal{A}} (q', Z')$ if $q = q'$ and $Z \preceq_{\mathcal{G}(q)} Z'$. This simulation relation $\preceq_{\mathcal{A}}$ is *finite* if for any infinite sequence $(q, Z_0), (q, Z_1), (q, Z_2), \ldots$ of *safely reachable* nodes in the zone graph of $\mathcal{A}$ we find $i < j$ with $(q, Z_j) \preceq_{\mathcal{A}} (q, Z_i)$, i.e., $Z_j \preceq_{\mathcal{G}(q)} Z_i$. Notice that we restrict to *safely reachable* zones in the definition above. Our goal now is to prove that the relation $\preceq_{\mathcal{A}}$ is finite. The structure of the proof is as follows.

1. We proved in Lemma 44 of Section 7 that for any *safely reachable* node (q, Z) of the zone graph of $\mathcal{A}$, the canonical distance graph $\mathbb{G}(Z)$ satisfies a set of conditions, that we call (†) conditions, which depend only on the maximal constant M of $\mathcal{A}$ and the number of

future clocks in $\mathcal{A}$.

2. We will now introduce an equivalence relation $\sim_M$ of *finite index* on valuations (depending on M only) and show in Lemma 54 of Section 8 that, if G is a set of atomic constraints using *M-bounded integral constraints* and if Z is a zone such that its canonical distance graph $\mathbb{G}(Z)$ satisfies (†) conditions, then $\downarrow_G Z$ is a union of $\sim_M^n$ equivalence classes.

An equivalence relation of finite index on valuations. We first define an equivalence relation of finite index $\sim_M$ on valuations. First, we define $\sim_M$ on $\alpha, \beta \in \overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$ by $\alpha \sim_M \beta$ if $(\alpha \lhd c \iff \beta \lhd c)$ for all $(\lhd, c)$ with $\lhd \in \{<, \leq\}$ and $c \in \{-\infty, \infty\} \cup \{d \in \mathbb{Z} \mid |d| \leq M\}$. In particular, if $\alpha \sim_M \beta$ then $(\alpha = -\infty \iff \beta = -\infty)$ and $(\alpha = \infty \iff \beta = \infty)$.

Next, for valuations $v_1, v_2 \in \mathbb{V}$, we define $v_1 \sim_M^n v_2$ by two conditions: $v_1(x) \sim_{nM} v_2(x)$ and $v_1(x) - v_1(y) \sim_{(n+1)M} v_2(x) - v_2(y)$ for all clocks $x, y \in X$. Notice that we use $(n+1)M$ for differences of values. Clearly, $\sim_M^n$ is an equivalence relation of finite index on valuations. Using this, we can show that the zones that are reachable in a safe GTA are unions of $\sim_M^n$-equivalence classes.

Distance graph for valuations that simulate a given valuation. For a valuation v, we let $\uparrow_G v = \{v' \in \mathbb{V} \mid v \preceq_G v'\}$, i.e., the set of valuations v' which simulate v. We will define a distance graph, denoted $\mathbb{G}_G(v)$, such that $[\![\mathbb{G}_G(v)]\!] = \uparrow_G v$. We remark that $[\![\mathbb{G}_G(v)]\!]$ is not really a zone since it may use constants that are not integers.

We will now define the distance graph $\mathbb{G}_G(v)$ which denotes the set $\uparrow_G v$. We will define $\mathbb{G}_G(v)$ as the intersection of a distance graphs $\mathbb{G}_v^G$ and a guard g_v^G.

▶ **Definition 47.** *The distance graph $\mathbb{G}_v^G$ is defined as follows.*

- *For each future clock $x \in X_F$, we have the edges $x \xrightarrow{(\leq, -v(x))} 0$ and $0 \xrightarrow{(\leq, v(x))} x$.*
- *For each history clock $y \in X_H$, we have*
  - *the edge $0 \to y$ with weight $(\leq, v(y))$ if there is a constraint $y \lhd c \in G$ with $c < \infty$ and $v \models y \lhd c$.*
  - *the edge $y \to 0$ with weight $(\leq, -v(y))$ if there is a constraint $c \lhd y \in G$ with $c < \infty$ and $v \not\models c \lhd y$.*

▶ **Definition 48.** *The guard g_v^G is given by the set of all constraints of the form $y - x \lhd c$ in G where $x, y \in X \cup \{0\}$ and $v \models y - x \lhd c$.*

With this definition, we can show that if G is a set of atomic constraints containing both $x \leq 0$ and $0 \leq x$ for each clock $x \in X_F$, then $\uparrow_G v = [\![\mathbb{G}_v^G]\!] \cap [\![g_v^G]\!]$.

▶ **Lemma 49.** *Let G be a set of constraints such that for all future clock $x \in X_F$ we have both $x \leq 0$ and $0 \leq x$ in G. We have $\uparrow_G v = [\![\mathbb{G}_v^G]\!] \cap g_v^G$.*

Proof. $\subseteq$: Let v' be such that $v \preceq_G v'$. By definition of the simulation relation, for all $g' = y - x \lhd c$ in G such that $v \models g'$, we have $v' \models g'$. Hence, $v' \models g_v^G$. Next, let $x \in X_F$ be a future clock. If $v(x) = -\infty$ then for all $0 \leq \delta < \infty$ we have $v + \delta \models x \leq 0$. Since $v \preceq_G v'$ we get $v' + \delta \models x \leq 0$, which implies $v'(x) = -\infty = v(x)$. Otherwise, let $0 \leq \delta = -v(x) < \infty$. Since $v + \delta \models x \leq 0 \wedge 0 \leq x$ and $v \preceq_G v'$, we get $v' + \delta \models x \leq 0 \wedge 0 \leq x$. We deduce that $v'(x) = v(x)$. Therefore, v' satisfies the edges $x \xrightarrow{\leq, -v(x)} 0$ and $0 \xrightarrow{\leq, v(x)} x$ of $\mathbb{G}_v^G$.

Now, let $x \in X_H$ be a history clock. Assume that $v \models x \lhd c$ for some $x \lhd c$ in G with $0 \leq c < \infty$. Using $v \preceq_{x \lhd c} v'$, we get $v'(x) \leq v(x)$. Hence, v' satisfies the edge $0 \xrightarrow{\leq, v(x)} x$ of $\mathbb{G}_v^G$. Assume that $v \not\models c \lhd x$ for some $c \lhd x$ in G with $0 \leq c < \infty$. Again, we obtain $v(x) \leq v'(x)$ from $v \preceq_{c \lhd x} v'$. Hence, v' satisfies the edge $x \xrightarrow{\leq, -v(x)} 0$ of $\mathbb{G}_v^G$. Thus, v' satisfies all constraints of $\mathbb{G}_v^G$, i.e., $v' \in [\![\mathbb{G}_v^G]\!]$.

$\supseteq$: Let $v \in [\![\mathbb{G}_v^G]\!]$ with $v \models g_v^G$. Let $g' = y - x \lhd c$ be a diagonal constraint in G with $x, y \in X$. If $v \models g'$ then g' is in g_v^G and $v' \models g'$. Therefore, $v \preceq_{g'} v'$.

Now, let g' be a non-diagonal constraint on a future clock, i.e., $x \lhd c$ or $c \lhd x$ with $x \in X_F$. Since $v \in [\![\mathbb{G}_v^G]\!]$ we get $v'(x) = v(x)$ and we deduce that $v \preceq_{g'} v'$. Let g' be an upper non-diagonal constraint $x \lhd c$ on a history clock $x \in X_H$. If $v \not\models g'$ then $v \preceq_{g'} v'$. If $v \models g'$ and c is finite then we get $v'(x) \leq v(x)$ from the edge $0 \xrightarrow{\leq, v(x)} x$ of $\mathbb{G}_v^G$. Hence, $v \preceq_{g'} v'$. If g' is $x < \infty$ and $v \models g'$ then g' is in g_v^G and we get $v'(x) < \infty$ from $v' \models g_v^G$. We deduce that $v \preceq_{g'} v'$. If g' is $x \leq \infty$ then g' is equivalent to *true* and $v \preceq_{g'} v'$. Let g' be a lower non-diagonal constraint $c \lhd x$ on a history clock $x \in X_H$. If $v \models g'$ then g' is in g_v^G and we get $v' \models g'$. Therefore, $v \preceq_{g'} v'$. Assume now that $v \not\models g'$. If c is finite then we get $v(x) \leq v'(x)$ from the edge $x \xrightarrow{\leq, -v(x)} 0$ of $\mathbb{G}_v^G$. We deduce that $v \preceq_{g'} v'$. If g' is $\infty < x$ then g' is equivalent to *false* and $v \preceq_{g'} v'$. Lastly, when g' is $\infty \leq x$ and $v(x)$ is finite. Then, for all $0 \leq \delta < \infty$ we have $v + \delta \not\models g'$. Therefore, $v \preceq_{g'} v'$. ◀

▶ Remark 50. **1.** $\mathbb{G}_v^G$ is in standard form, but not necessarily in normal form.
2. $[\![\mathbb{G}_v^G]\!]$ is non-empty, since $v \in [\![\mathbb{G}_v^G]\!]$.
3. g_v^G is a conjunction of atomic constraints, each of which is (X_D, M)-safe.

Further, we show that if $\mathbb{G}_v^G \cap Z'$ is empty and $\mathbb{G}'$ is the normalized distance graph of Z', then there is a small witness, i.e., a negative cycle in $\min(\mathbb{G}_v^G, \mathbb{G}')$ containing at most three edges, and belonging to one of three specific forms. This also gives us an efficient simulation check for GTA zone graphs.

▶ **Lemma 51.** *Let v be a valuation, Z' a non-empty* reachable *event zone with canonical distance graph $\mathbb{G}'$ and G a set of atomic constraints. Then, $\mathbb{G}_v^G \cap Z'$ is empty iff there is a negative cycle in one of the following forms:*
1. $0 \to x \to 0$ *with* $0 \to x$ *from* $\mathbb{G}_v^G$ *and* $x \to 0$ *from* $\mathbb{G}'$,
2. $0 \to y \to 0$ *with* $0 \to y$ *from* $\mathbb{G}'$ *and* $y \to 0$ *from* $\mathbb{G}_v^G$, *and*
3. $0 \to x \to y \to 0$, *with weight of* $x \to y$ *from* $\mathbb{G}'$ *and the others from* $\mathbb{G}_v^G$.

Proof. Since the distance graph $\mathbb{G}'$ is in normal form, it has no negative cycle. Similarly, $\mathbb{G}_v^G$ has no negative cycle since $v \in \mathbb{G}_v^G \neq \emptyset$. We know that $\mathbb{G}_v^G \cap Z' = \emptyset$ iff there is a (simple) negative cycle in $\min(\mathbb{G}_v^G, \mathbb{G}')$. Since $\mathbb{G}'$ is in normal form, we may restrict to negative cycles which do not use two consecutive edges from $\mathbb{G}'$. Further, note that all edges of $\mathbb{G}_v^G$ are adjacent to node 0. Hence, if a simple cycle uses an edge from $\mathbb{G}'$ which is adjacent to 0, it consists of only two edges $0 \to x \to 0$, one from $\mathbb{G}'$ and one from $\mathbb{G}_v^G$. Otherwise, the simple cycle is of the form $0 \to x \to y \to 0$ where the edge $x \to y$ is from $\mathbb{G}'$ and the other two edges are from $\mathbb{G}_v^G$. ◀

▶ **Lemma 52.** *Let $v \sim_M^n v'$ and G be a set of M-bounded integral constraints. Then, we have the following*
1. $g_{v'}^G = g_v^G$.
2. *The graph $\mathbb{G}_{v'}^G$ is obtained by replacing the weights $(\leq, v(x))$ (resp. $(\leq, -v(x))$) by $(\leq, v'(x))$ (resp. $(\leq, -v'(x))$) in the graph $\mathbb{G}_v^G$.*

Proof. **1.** $g_{v'}^G = g_v^G$ is easy to see from the definition of $\mathbb{G}_{v'}^G$ and $\mathbb{G}_v^G$, and the fact that $v \sim_{(n+1)M} v'$.
2. For a future clock $x \in X_F$, this is easy to see from the definition for edges $x \to 0$ and $0 \to x$ adjacent to x.
We consider now edges adjacent to history clocks $y \in X_H$.

- Consider the edge $0 \to y$. If its weight is $(\leq, v(y))$ in $\mathbb{G}_v^G$ then there is some $y \lhd c \in G$ with $c < \infty$ and $v(y) \lhd c$. Since $v \sim_{(n+1)M} v'$, we deduce that $v'(y) \lhd c$ and the edge $0 \to y$ has weight $(\leq, v'(y))$ in $\mathbb{G}_{v'}^G$.
- Consider the edge $y \to 0$. If its weight is $(\leq, -v(y))$ in $\mathbb{G}_v^G$, then there is some $c \lhd y \in G$ with $c < \infty$ and $c \not\lhd v(y)$. Since $v \sim_{(n+1)M} v'$, we deduce that $c \not\lhd v'(y)$ and the edge $y \to 0$ has weight $(\leq, -v'(y))$ in $\mathbb{G}_{v'}^G$. ◀

Using all the results above, we can now show that the zones that are reachable in a safe GTA are unions of $\sim_M^n$-equivalence classes.

▶ Remark 53. Before we state the lemma, we list some properties that we will use extensively in the proof of the lemma.

1. $-b \lhd a$ iff $-a \lhd b$ iff $(\leq, 0) \leq (\lhd, a + b)$.
2. $a \lhd b$ iff $\neg(b \tilde{\lhd} a)$ where $\tilde{\leq} = <$ and $\tilde{<} = \leq$.
3. $\alpha \sim_M \beta$ and $c \in \mathbb{R}$ is such that $-M \leq c \leq M$ or $(\lhd, c) \in \{(\leq, -\infty), (<, \infty), (\leq, \infty)\}$, then, $c \lhd \alpha$ iff $c \lhd \beta$. This is because
   - $c \lhd \alpha$ iff $\neg(\alpha \tilde{\lhd} c)$ by (2) above.
   - $\neg(\alpha \tilde{\lhd} c)$ iff $\neg(\beta \tilde{\lhd} c)$ by definition of $\sim_M$ equivalence.
   - $\neg(\beta \tilde{\lhd} c)$ iff $c \lhd \beta$ by (2) above.

▶ **Lemma 54.** *Let G be a set of X_D-safe M-bounded integral constraints which contains both $x \leq 0$ and $0 \leq x$ for each future clock $x \in X_F$. Let Z be a zone with a canonical distance graph $\mathbb{G}(Z)$ satisfying the (†) conditions of Lemma 44. Let $v_1, v_2 \in \mathbb{V}$ be valuations with $v_1 \sim_M^n v_2$. Then, $v_1 \in \downarrow_G Z$ iff $v_2 \in \downarrow_G Z$.*

Proof. Notice that $v \in \downarrow_G Z$ iff $\uparrow_G v \cap Z \neq \emptyset$. We need to show that $\uparrow_G v_1 \cap Z \neq \emptyset$ iff $\uparrow_G v_2 \cap Z \neq \emptyset$. Using the characterization of up-sets given by Lemma 49, this amounts to $Z \cap g_{v_1}^G \cap [\![\mathbb{G}_{v_1}^G]\!] \neq \emptyset$ iff $Z \cap g_{v_2}^G \cap [\![\mathbb{G}_{v_2}^G]\!] \neq \emptyset$.

Further, since $v_1 \sim_M^n v_2$, using Lemma 52, it follows that $g_{v_2}^G = g_{v_1}^G$. Let $Z' = Z \cap g_{v_2}^G = Z \cap g_{v_1}^G$. If Z' is empty then the equivalence holds. Otherwise, let $\mathbb{G}(Z')$ be the normalized distance graph of Z'. Note that since Z was an (X_D, M)-safely reachable zone and $g_{v_1}^G$ is a conjunction of atomic constraints, each of which is (X_D, M)-safe, it follows that Z' is an (X_D, M)-safely reachable zone. As a consequence, the † conditions of Lemma 44 apply to Z'.

In the rest of the proof, we will now work with the zone Z' (using its normalized distance graph representation $\mathbb{G}(Z')$) and the standard distance graphs $\mathbb{G}_{v_1}^G$ and $\mathbb{G}_{v_2}^G$. The proof proceeds by contradiction. We assume that $\uparrow_G v_1 \cap Z \neq \emptyset$ and $\uparrow_G v_2 \cap Z = \emptyset$. This is equivalent to $Z' \cap [\![\mathbb{G}_{v_1}^G]\!] \neq \emptyset$ and $Z' \cap [\![\mathbb{G}_{v_2}^G]\!] = \emptyset$. By Lemma 51, we can find a negative cycle C_2 using one edge from $\mathbb{G}(Z')$ and one or two edges from $\mathbb{G}_{v_2}^G$. By Lemma 52, we have a corresponding cycle C_1 using the same edge from $\mathbb{G}(Z')$ and the same one or two edges from $\mathbb{G}_{v_1}^G$ (with weights using v_1 instead of v_2). The cycle C_1 is not negative since $Z' \cap [\![\mathbb{G}_{v_1}^G]\!] \neq \emptyset$

The rest of the proof involves a case analysis of the various forms that the cycle C_2 can take, which we provide below. We consider the different cases.

1. Cycle $C_2 = 0 \xrightarrow{(\leq, v_2(y))} y \xrightarrow{Z'_{y0}} 0$ for some history clock $y \in X_H$.
   We have $C_1 = 0 \xrightarrow{(\leq, v_1(y))} y \xrightarrow{Z'_{y0}} 0$.
   Since we have the edge $0 \xrightarrow{(\leq, v_1(y))} y$ in $\mathbb{G}_{v_1}^G$, there is a constraint $y \lhd' c'$ in G with $c' < \infty$ and $v_1(y) \lhd' c'$. We deduce that $0 \leq v_1(y) \leq M$.
   Let $Z'_{y0} = (\lhd, c)$. Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c + v_1(y))$, which is equivalent to $-c \lhd v_1(y)$. Using $0 \leq v_1(y) \leq M$ and $v_1 \sim_M^n v_2$ we deduce that $-c \lhd v_2(y)$. This is equivalent to $(\leq, 0) \leq (\lhd, c + v_2(y))$, a contradiction with C_2 being a negative cycle.

2. Cycle $C_2 = 0 \xrightarrow{Z'_{0y}} y \xrightarrow{(\leq,-v_2(y))} 0$ for some history clock $y \in X_H$.
We have $C_1 = 0 \xrightarrow{Z'_{0y}} y \xrightarrow{(\leq,-v_1(y))} 0$.
Since we have the edge $y \xrightarrow{(\leq,-v_1(y))} 0$ in $\mathbb{G}^G_{v_1}$, there is a constraint $c' \lhd' y$ in G with $c' < \infty$ and $c' \not\lhd' v_1(y)$. We deduce that $0 \leq v_1(y) \leq M$.
Let $Z'_{0y} = (\lhd, c)$. Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c - v_1(y))$, which is equivalent to $v_1(y) \lhd c$. Using $v_1 \sim^n_M v_2$ and $0 \leq v_1(y) \leq M$, we deduce that $v_2(y) \lhd c$. This is equivalent to $(\leq, 0) \leq (\lhd, c - v_2(y))$, a contradiction with C_2 being a negative cycle.

3. Cycle $C_2 = 0 \xrightarrow{(\leq,v_2(x))} x \xrightarrow{Z'_{x0}} 0$ for some future clock $x \in X_F$.
We have $C_1 = 0 \xrightarrow{(\leq,v_1(x))} x \xrightarrow{Z'_{x0}} 0$.
Since C_2 is negative, we have $Z'_{x0} \neq (\leq, \infty)$. Also, if $Z'_{x0} = (<, \infty)$ then we must have $v_2(x) = -\infty$, which implies $v_1(x) = -\infty$ since $v_1 \sim^n_M v_2$, a contradiction with C_1 being non-negative. Hence, $Z'_{x0} = (\lhd, c)$ is finite and by $(\dagger_1)$, we infer $0 \leq c \leq nM$.
Since C_1 is not negative, we get $(\leq, 0) \leq (\lhd, c + v_1(x))$, which is equivalent to $-c \lhd v_1(x)$. Using $v_1 \sim^n_M v_2$ and $0 \leq c \leq nM$ we deduce that $-c \lhd v_2(x)$. This is equivalent to $(\leq, 0) \leq (\lhd, c + v_2(x))$, a contradiction with C_2 being a negative cycle.

4. Cycle $C_2 = 0 \xrightarrow{Z'_{0x}} x \xrightarrow{(\leq,-v_2(x))} 0$ for some future clock $x \in X_F$.
We have $C_1 = 0 \xrightarrow{Z'_{0x}} x \xrightarrow{(\leq,-v_1(x))} 0$.
Let $Z'_{0x} = (\lhd, c)$. Since C_2 is negative, we deduce that $v_2(x) \neq -\infty$. Using $v_1 \sim^n_M v_2$, we infer $v_1(x) \neq -\infty$. Since C_1 is not negative, we get $Z'_{0x} \neq (\leq, -\infty)$. From $(\dagger_2)$, we infer $(<, -nM) \leq Z'_{0x} \leq (\leq, 0)$ and $-nM \leq c \leq 0$.
Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c - v_1(x))$, which is equivalent to $v_1(x) \lhd c$. Using $v_1 \sim^n_M v_2$ and $-nM \leq c \leq 0$, we deduce that $v_2(x) \lhd c$. This is equivalent to $(\leq, 0) \leq (\lhd, c - v_2(x))$, a contradiction with C_2 being a negative cycle.

5. Cycle $C_2 = 0 \xrightarrow{(\leq,v_2(y))} y \xrightarrow{Z'_{yx}} x \xrightarrow{(\leq,-v_2(x))} 0$ for some history clock $y \in X_H$ and future clock $x \in X_F$.
We have $C_1 = 0 \xrightarrow{(\leq,v_1(y))} y \xrightarrow{Z'_{yx}} x \xrightarrow{(\leq,-v_1(x))} 0$.
Let $Z'_{yx} = (\lhd, c)$. As in case 1 above, we get $0 \leq v_1(y) \leq M$. From the fact that the cycle $0 \xrightarrow{(\leq,v_1(y))} y \xrightarrow{Z'_{y0}} 0$ is not negative, we get $(\leq, -M) \leq Z'_{y0}$. Since C_2 is negative, we get $v_2(x) \neq -\infty$. Using $v_1 \sim^n_M v_2$, we infer $v_1(x) \neq -\infty$. From the fact that the cycle $0 \xrightarrow{Z'_{0x}} x \xrightarrow{(\leq,-v_1(x))} 0$ is not negative, we deduce $Z'_{0x} \neq (\leq, -\infty)$. Using $(\dagger_3)$ we obtain

$$(\leq, -M) + (<, -nM) \leq Z'_{y0} + (<, -nM) \leq Z'_{yx} = (\lhd, c)$$

and we deduce that $-(n+1)M \leq c \leq 0$.
Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c + v_1(y) - v_1(x))$, which is equivalent to $-c \lhd v_1(y) - v_1(x)$. Using $v_1 \sim^n_M v_2$ and $-(n+1)M \leq c \leq 0$ we deduce that $-c \lhd v_2(y) - v_2(x)$. We conclude as in the previous cases.

6. Cycle $C_2 = 0 \xrightarrow{(\leq,v_2(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq,-v_2(y))} 0$ for some history clock $y \in X_H$ and future clock $x \in X_F$.
We have $C_1 = 0 \xrightarrow{(\leq,v_1(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq,-v_1(y))} 0$.
Since C_2 is negative but not C_1, we get first $Z'_{xy} \neq (\leq, \infty)$ and then $v_1(x) \neq -\infty$. As in case 2 above, we get $0 \leq v_1(y) \leq M$. We deduce that $Z'_{xy} = (\lhd, c) < (<, \infty)$ and $c \neq \infty$.
From $(\dagger_1)$ we obtain $Z'_{x0} \leq (\leq, nM)$. Since $0 \xrightarrow{(\leq,v_1(x))} x \xrightarrow{Z'_{x0}} 0$ is not a negative cycle, we get $-nM \leq v_1(x) \leq 0$. Finally, we obtain $0 \leq v_1(y) - v_1(x) \leq (n+1)M$.

Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c + v_1(x) - v_1(y))$, which is equivalent to $v_1(y) - v_1(x) \lhd c$. Using $v_1 \sim_M^n v_2$ and $0 \leq v_1(y) - v_1(x) \leq (n+1)M$, we deduce that $v_2(y) - v_2(x) \lhd c$. We conclude as in the previous cases.

7. Cycle $C_2 = 0 \xrightarrow{(\leq, v_2(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq, -v_2(y))} 0$ with $x \neq y$ for future clocks $x, y \in X_F$.
We have $C_1 = 0 \xrightarrow{(\leq, v_1(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq, -v_1(y))} 0$.
Since C_2 is negative but not C_1, using $v_1 \sim_M^n v_2$ we get successively $Z'_{xy} \neq (\leq, \infty)$, $v_2(y) \neq -\infty \neq v_1(y)$, $v_1(x) \neq -\infty \neq v_2(x)$, and finally $(\leq, -\infty) < Z'_{xy} < (<, \infty)$.
Let $Z'_{xy} = (\lhd, c)$. From $(\dagger_4)$, we deduce that $-nM \leq c \leq nM$.
Since C_1 is not a negative cycle, we get $(\leq, 0) \leq (\lhd, c + v_1(x) - v_1(y))$, which is equivalent to $v_1(y) - v_1(x) \lhd c$. Using $v_1 \sim_M^n v_2$ and $-nM \leq c \leq nM$, we deduce that $v_2(y) - v_2(x) \lhd c$.
We conclude as in the previous cases.
8. Cycle $C_2 = 0 \xrightarrow{(\leq, v_2(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq, -v_2(y))} 0$ with $x \neq y$ for history clocks $x, y \in X_H$.
We have $C_1 = 0 \xrightarrow{(\leq, v_1(x))} x \xrightarrow{Z'_{xy}} y \xrightarrow{(\leq, -v_1(y))} 0$.
As in case 1 above, we get $0 \leq v_1(x) \leq M$. As in case 2 above, we get $0 \leq v_1(y) \leq M$. We obtain $-M \leq v_1(y) - v_1(x) \leq M$.
Let $Z'_{xy} = (\lhd, c)$. Since C_1 is not negative, we get $(\leq, 0) \leq (\lhd, c + v_1(x) - v_1(y))$, which is equivalent to $v_1(y) - v_1(x) \lhd c$. Using $v_1 \sim_M^n v_2$ and $-M \leq v_1(y) - v_1(x) \leq M$, we deduce that $v_2(y) - v_2(x) \lhd c$. We conclude as in the previous cases.

Notice that we have crucially used the "$(n+1)M$" occurring in the definition of $v_1 \sim_M^n v_2$ (as $v_1(x) - v_1(y) \sim_{(n+1)M} v_2(x) - v_2(y)$) in the cases where we deal with cycles containing one future clock and one history clock (Cases 5 and 6). ◀

Finally, from Lemmas 44 and 54, we obtain our main theorem of the section.

▶ **Theorem 55.** *The simulation relation $\preceq_{\mathcal{A}}$ is finite if $\mathcal{A}$ is safe.*

Proof. Let $(q, Z_0), (q, Z_1), (q, Z_2), \ldots$ be an infinite sequence of *reachable* nodes in the zone graph of $\mathcal{A}$. By Lemma 44, for all i, the distance graph $\mathbb{G}(Z_i)$ in canonical form satisfies conditions $(\dagger)$.

The set $\mathcal{G}(q)$ contains only X_D-safe and M-bounded integral constraints. Let G be $\mathcal{G}(q)$ together with the constraints $x \leq 0$ and $0 \leq x$ for each future clock $x \in X_F$. From Lemma 54 we deduce that for all i, $\downarrow_G Z_i$ is a union of $\sim_M^n$-classes. Since $\sim_M^n$ is of finite index, there are only finitely many unions of $\sim_M^n$-classes. Therefore, we find $i < j$ with $\downarrow_G Z_i = \downarrow_G Z_j$, which implies $Z_j \preceq_G Z_i$. Since $\mathcal{G}(q) \subseteq G$, this also implies $Z_j \preceq_{\mathcal{G}(q)} Z_i$. ◀

9 Experimental evaluation

We have implemented a prototype that takes as input a GTA, as given in Definition 6, and applies our reachability algorithm, in the open source tool TCHECKER [29]. To do so, we extend TCHECKER to allow clocks to be declared as one of *normal*, *history*, *prophecy*, or *timer*, and extend the syntax of edges to allow arbitrary interleaving of guards and clock changes (reset/release). Our tool, along with the benchmarks used in this paper, is publicly available and can be downloaded from https://github.com/anirjoshi/GTA-Model. We present selected results in Table 1, with further details in Appendix A.

First, we consider timed automata models from standard benchmarks[41, 19, 36]. Despite the overhead induced by our framework (e.g., maintaining general programs on transitions), we are only slightly worse off w.r.t. running time than the standard algorithm, while visiting and storing the same number of nodes. We illustrate this in rows 1-3 of Table 1 by providing a