Appendix to *SpaceEx: Scalable Verification of Hybrid Systems*

Goran Frehse[1], Colas Le Guernic[2], Alexandre Donzé[1], Rajarshi Ray[1], Olivier Lebeltel[1], Rodolfo Ripado[1], Antoine Girard[3], Thao Dang[1], Oded Maler[1]

[1] Université Grenoble 1 Joseph Fourier - Verimag, 38610 Gières, France
[2] New York University CIMS, New York, NY 10012
[3] Laboratoire Jean Kuntzmann, 38041 Grenoble Cedex 9, France

Abstract. In *SpaceEx: Scalable Verification of Hybrid Systems*, we present a scalable reachability algorithm for hybrid systems with piecewise affine, non-deterministic dynamics. It combines polyhedra and support function representations of continuous sets to compute an overapproximation of the reachable set of states in the form of template polyhedra. The algorithm improves over previous work by using variable time steps, adapted separately for each template direction to guarantee a given error bound. In addition, we propose coordinate transformations to reduce the approximation error and a clustering technique to avoid an explosion in the number of continuous sets. The algorithm is implemented as part of SpaceEx, a new verification platform for hybrid systems, available at `spaceex.imag.fr`. Experimental results of full fixed-point computations with hybrid systems with more than 100 variables illustrrate the scalability of the approach.

A Proof of Proposition 1

Before showing that the sequence Ω_k indeed covers the reachable set, we first show that the Ψ_k overapproximates the input accumulation S_{t_k}.

Lemma 5. $\mathrm{Reach}_{t_k,t_k}(\{0\}) \subseteq \Psi_k$

Proof. Since $t_0 = 0$, it is clear that $\mathrm{Reach}_{t_0,t_0}(\{0\}) = \{0\} \subseteq \Psi_0$

With $t_{k+1} = t_k + \delta_k$,

$$\begin{aligned}\mathrm{Reach}_{t_{k+1},t_{k+1}}(\{0\}) &= \left\{ \int_0^{t_{k+1}} e^{(t_{k+1}-s)A} u(s) ds \mid \forall s \in [0, t_{k+1}],\, u(s) \in \mathcal{U} \right\} \\ &= \left\{ \int_0^{t_k} e^{(t_k-s')A} u(s'+\delta_k) ds \mid \forall s \in [\delta_k, t_{k+1}],\, u(s) \in \mathcal{U} \right\} \\ &\quad \oplus \left\{ e^{t_k A} \int_0^{\delta_k} e^{(\delta_k-s)A} u(s) ds \mid \forall s \in [0, \delta_k],\, u(s) \in \mathcal{U} \right\}\end{aligned}$$

Thus, $\mathrm{Reach}_{t_{k+1},t_{k+1}}(\{0\}) = \mathrm{Reach}_{t_k,t_k}(\{0\}) \oplus e^{At_k}\mathrm{Reach}_{\delta_k,\delta_k}(\{0\})$. The conclusion follows by induction.

Now we establish the main result.

Proposition 1. *Given a sequence of time steps* $\delta_0, \dots, \delta_{N-1}$ *with* $\sum_{i=0}^{N-1} \delta_i = T$, *the sequence* Ω_k *defined by (7) satisfies*

$$\mathrm{Reach}_{0,T}(\mathcal{X}_0) \subseteq \bigcup_{k=0}^{N-1} \Omega_k. \tag{21}$$

Proof. With lemma 1, we have

$$\mathrm{Reach}_{t_k,t_{k+1}}(\mathcal{X}_0) = e^{At_k}\mathrm{Reach}_{0,\delta_k}(\mathcal{X}_0) \oplus \mathrm{Reach}_{t_k,t_k}(\{0\}),$$

and with lemma 5 and equation (6),

$$\mathrm{Reach}_{t_k,t_{k+1}}(\mathcal{X}_0) \subseteq e^{At_k}\Omega_{[0,\delta_k]}(\mathcal{X}_0,\mathcal{U}) \oplus \Psi_{t_k}.$$

Then by induction with (6) as base case, $\mathrm{Reach}_{t_k,t_{k+1}}(\mathcal{X}_0) \subseteq \Omega_k$. The conclusion follows directly.

B Proof of Lemma 2

Lemma 2. *Let* $\Psi_\delta(\mathcal{U})$ *be the set defined by*

$$\Psi_\delta(\mathcal{U}) = \delta\mathcal{U} \oplus \mathcal{E}_\Psi(\mathcal{U},\delta), \tag{22}$$

$$\mathcal{E}_\Psi(\mathcal{U},\delta) = \boxdot\big(\Phi_2(|A|,\delta) \boxdot (A\mathcal{U})\big). \tag{23}$$

Then, $\mathrm{Reach}_{\delta,\delta}(\{0\}) \subseteq \Psi_\delta(\mathcal{U})$.

Proof.

$$\mathrm{Reach}_{\delta,\delta}(\{0\}) = \left\{ \int_0^\delta e^{(\delta-s)A}u(s)ds \mid \forall s \in [0;\delta]\, u(s) \in \mathcal{U} \right\}$$

We want to over-approximate this set by a *simpler* one. In order to do so, we over-approximate the support function of $\mathrm{Reach}_{\delta,\delta}(\{0\})$ by the support function of another set. For any $v \in \mathrm{Reach}_{\delta,\delta}(\{0\})$ there exist $u(.)$ such that for any ℓ:

$$\begin{aligned}
v \cdot \ell &= \int_0^\delta e^{(\delta-s)A}u(s)ds \cdot \ell \\
&= \sum_{i=0}^{\infty} \int_0^\delta \frac{(\delta-s)^i}{i!} A^i u(s) \cdot \ell ds \\
&\leq \sum_{i=0}^{k-1} \int_0^\delta \frac{(\delta-s)^i}{i!} \sup_{u \in \mathcal{U}} \left(A^i u \cdot \ell\right) ds + \sum_{i=k}^{\infty} \int_0^\delta \frac{(\delta-s)^i}{i!} A^i u(s) \cdot \ell ds \\
v \cdot \ell &\leq \sum_{i=0}^{k-1} \frac{\delta^{i+1}}{(i+1)!} \rho(\ell, A^i\mathcal{U}) + \sum_{i=k}^{\infty} \left| \int_0^\delta \frac{(\delta-s)^i}{i!} A^k u(s) ds \cdot (A^{i-k})^\top \ell \right|
\end{aligned}$$

By taking $\rho(\ell, A^i\mathcal{U})$ we lose the correlation between all the u, but it allows us to apply a coarse over-approximation on a smaller set. For sake of simplicity we will limit ourselves to $k = 1$.

$$v \cdot \ell \leq \delta\rho(\ell,\mathcal{U}) + \sum_{i=1}^{\infty} \left| \int_0^\delta \frac{(\delta - s)^i}{i!} Au(s) ds \cdot (A^{i-1})^\top \ell \right|$$

Before going further, let us remark a few properties of $|.|$. For any two vectors x and y, it is easy to show that: $|x \cdot y| \leq |x| \cdot |y|$. It is also clear that for any two matrices A and B, $|ABx| \leq |A||B||x|$ component wise.

We now focus on: $\left| \int_0^\delta \frac{(\delta-s)^i}{i!} Au(s)ds \cdot (A^{i-1})^\top \ell \right|$

$$\left| \int_0^\delta \frac{(\delta - s)^i}{i!} Au(s) ds \cdot (A^{i-1})^\top \ell \right| \leq \int_0^\delta \frac{(\delta - s)^i}{i!} \left| Au(s) \right| ds \cdot |A^\top|^{i-1} |\ell|$$

We now take $u_1^{\max} \in \boxdot(A\mathcal{U})$ such that for all $u \in \mathcal{U}$: $|Au| \leq u_1^{\max}$ component wise.

$$\begin{aligned} \left| \int_0^\delta \frac{(\delta - s)^i}{i!} Au(s) ds \cdot (A^{i-1})^\top \ell \right| &\leq \int_0^\delta \frac{(\delta - s)^i}{i!} u_1^{\max} ds \cdot |A^\top|^{i-1} |\ell| \\ &\leq \frac{\delta^{i+1}}{(i+1)!} u_1^{\max} \cdot |A^\top|^{i-1} |\ell| \\ &\leq \frac{\delta^{i+1}}{(i+1)!} |A|^{i-1} u_1^{\max} \cdot |\ell| \end{aligned}$$

Going back to $v \cdot \ell$ we get:

$$v \cdot \ell \leq \delta\rho(\ell,\mathcal{U}) + \sum_{i=1}^{\infty} \frac{\delta^{i+1}}{(i+1)!} |A|^{i-1} u_1^{\max} \cdot |\ell|$$

If we call e_1 the point:

$$e_1 = \sum_{i=1}^{\infty} \frac{\delta^{i+1}}{(i+1)!} |A|^{i-1} u_1^{\max}$$

we have:

$$\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\})) \leq \delta\rho(\ell,\mathcal{U}) + |e_1| \cdot |\ell|$$

Let $\mathcal{E}_{\varPsi}(\mathcal{U}, \delta) = \boxdot(\{e_1\})$, it is easy to show that $\rho(\ell, \mathcal{E}_{\varPsi}(\mathcal{U}, \delta)) = |e_1| \cdot |\ell|$, and that $\mathcal{E}_{\varPsi}(\mathcal{U}, \delta)$ is also equal to $\boxdot\left(\sum_{i=1}^{\infty} \frac{\delta^{i+1}}{(i+1)!} |A|^{i-1} \boxdot(A\mathcal{U})\right)$

For all ℓ, we have:

$$\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\})) \leq \delta\rho(\ell,\mathcal{U}) + \rho(\ell, \mathcal{E}_{\varPsi}(\mathcal{U}, \delta))$$

Thus, $\mathrm{Reach}_{\delta,\delta}(\{0\}) \subseteq \delta\mathcal{U} \oplus \mathcal{E}_{\varPsi}(\mathcal{U}, \delta) = \varPsi_\delta(\mathcal{U})$ which ends the proof of the lemma.

C Proof of Lemma 3

Lemma 3. *Let $\lambda \in [0,1]$, and $\Omega_\lambda(\mathcal{X}_0,\mathcal{U},\delta)$ be the convex set defined by :*

$$\begin{aligned}\Omega_\lambda(\mathcal{X}_0,\mathcal{U},\delta) = (1-\lambda)\mathcal{X}_0 \oplus \lambda e^{\delta A}\mathcal{X}_0 \oplus \lambda\delta\mathcal{U} \\ \oplus \left(\lambda\mathcal{E}^+_\Omega(\mathcal{X}_0,\delta) \cap (1-\lambda)\mathcal{E}^-_\Omega(\mathcal{X}_0,\delta)\right) \oplus \lambda^2\mathcal{E}_\Psi(\mathcal{U},\delta)\end{aligned}$$

$$\begin{aligned}\textit{where } \mathcal{E}^+_\Omega(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta) \boxdot \left(A^2\mathcal{X}_0\right)\right) \\ \textit{and } \mathcal{E}^-_\Omega(\mathcal{X}_0,\delta) &= \boxdot\left(\Phi_2(|A|,\delta) \boxdot \left(A^2e^{\delta A}\mathcal{X}_0\right)\right) \\ \textit{and } \mathcal{E}_\Psi(\mathcal{U},\delta) &= \boxdot\left(\Phi_2(|A|,\delta) \boxdot (A\mathcal{U})\right).\end{aligned}$$

Then $\mathrm{Reach}_{\lambda\delta,\lambda\delta}(\mathcal{X}_0,\mathcal{U}) \subseteq \Omega_\lambda(\mathcal{X}_0,\mathcal{U},\delta)$*. If we define* $\Omega_{[0,\delta]}(\mathcal{X}_0,\mathcal{U})$ *as:*

$$\Omega_{[0,\delta]}(\mathcal{X}_0,\mathcal{U}) = \mathrm{CH}\big(\bigcup_{\lambda\in[0,1]}\Omega_\lambda(\mathcal{X}_0,\mathcal{U},\delta)\big), \tag{24}$$

then $\mathrm{Reach}_{0,\delta}(\mathcal{X}_0) \subseteq \Omega_{[0,\delta]}(\mathcal{X}_0,\mathcal{U})$*.*

Proof. We already now that for any t:

$$\mathrm{Reach}_{0,t}(\mathcal{X}_0) = e^{tA}\mathcal{X}_0 \oplus \mathrm{Reach}_{t,t}(\{0\})$$

We want to over-approximate $\mathrm{Reach}_{0,t}(\mathcal{X}_0)$ by a *simpler* set. A set that can be expressed as a sum of sets constructed from $\mathcal{X}_0$, $e^{\delta A}\mathcal{X}_0$ and $\mathcal{U}$.

Let us first focus on $e^{tA}\mathcal{X}_0$. For a given x_0, we approximate $e^{tA}x_0$ by a linear interpolation. The interpolation error is:

$$e^{tA}x_0 - \left(\left(1-\frac{t}{\delta}\right)x_0 + \frac{t}{\delta}e^{\delta A}x_0\right) \tag{25}$$

We will approximate this error by an expression independent of t by two different methods. We will first privilege the forward direction, leading to an expression in t/δ and x_0, then the backward direction, leading to an expression in $(1-t/\delta)$ and $e^{\delta A}x_0$.

Let's start going forward:

$$\begin{aligned}e^{tA}x_0 - \left(\left(1-\frac{t}{\delta}\right)x_0 + \frac{t}{\delta}e^{\delta A}x_0\right) &= (e^{tA}-I)x_0 - \frac{t}{\delta}(e^{\delta A}-I)x_0 \\ &= \sum_{k=2}^{\infty}\left(\frac{t^k}{k!} - \frac{t}{\delta}\frac{\delta^k}{k!}\right)A^kx_0 \\ &= \frac{t}{\delta}\sum_{k=2}^{\infty}\frac{\delta^k}{k!}\left(\left(\frac{t}{\delta}\right)^{k-1} - 1\right)A^kx_0\end{aligned}$$

Similarly to the proof of lemma 2, we can deduce that:

$$e^{tA}x_0 - \left(\left(1-\frac{t}{\delta}\right)x_0 + \frac{t}{\delta}e^{\delta A}x_0\right) \in \frac{t}{\delta}\mathcal{E}^+_\Omega(\mathcal{X}_0,\delta) \tag{26}$$

with $\mathcal{E}^{+}_{\Omega}(\mathcal{X}_0,\delta) = \boxdot\left(|A|^{-2}\left(e^{\delta|A|} - I - \delta|A|\right) \boxdot \left(A^2 X_0\right)\right)$.

Again, starting from eq. (25), but this time going backward:

$$\begin{aligned}
&e^{tA}x_0 - \left(\left(1-\frac{t}{\delta}\right)x_0 + \frac{t}{\delta}e^{\delta A}x_0\right)\\
&= (e^{(t-\delta)A} - I)e^{\delta A}x_0 - \left(1-\frac{t}{\delta}\right)(e^{-\delta A}-I)e^{\delta A}x_0\\
&= \sum_{k=2}^{\infty}\left(\frac{(t-\delta)^k}{k!} - \left(1-\frac{t}{\delta}\right)\frac{(-\delta)^k}{k!}\right)A^k e^{\delta A}x_0\\
&= \left(1-\frac{t}{\delta}\right)\sum_{k=2}^{\infty}\frac{(-\delta)^k}{k!}\left(\left(1-\frac{t}{\delta}\right)^{k-1} - 1\right)A^k e^{\delta A}x_0
\end{aligned}$$

Then:

$$e^{tA}x_0 - \left(\left(1-\frac{t}{\delta}\right)x_0 + \frac{t}{\delta}e^{\delta A}x_0\right) \in \left(1-\frac{t}{\delta}\right)\mathcal{E}^{-}_{\Omega}(\mathcal{X}_0,\delta) \qquad (27)$$

with $\mathcal{E}^{-}_{\Omega}(\mathcal{X}_0,\delta) = \boxdot\left(|A|^{-2}\left(e^{\delta|A|} - I - \delta|A|\right) \boxdot \left(A^2 e^{\delta A} X_0\right)\right)$.

Using equations (26) and (27) we can deduce that for all λ in $[0,1]$ we have:

$$e^{\lambda\delta A}X_0 \subseteq (1-\lambda)X_0 \oplus \lambda e^{\delta A}X_0 \oplus \left(\lambda\mathcal{E}^{+}_{\Omega}(\mathcal{X}_0,\delta) \cap (1-\lambda)\mathcal{E}^{-}_{\Omega}(\mathcal{X}_0,\delta)\right) \qquad (28)$$

Please remark that we lost the correlation between the points x_0 and $e^{\delta A}x_0$.

Similarly we can prove that for all λ in $[0,1]$:

$$\mathrm{Reach}_{\lambda\delta,\lambda\delta}(\{0\}) \subseteq \lambda\delta\mathcal{U} \oplus \lambda^2\mathcal{E}_{\Psi}(\mathcal{U},\delta) \qquad (29)$$

which ends the proof of the lemma since:

$$\mathrm{Reach}_{0,\delta}(\mathcal{X}_0) = \bigcup_{\lambda\in[0,1]}\mathrm{Reach}_{\lambda\delta,\lambda\delta}(\mathcal{X}_0) \subseteq \bigcup_{\lambda\in[0,1]}\Omega_{\lambda}(\mathcal{X}_0,\mathcal{U},\delta) \qquad (30)$$

D Proof of Lemma 4

Lemma 4. *For any ℓ in $\mathbb{R}^n$:*

$$\begin{aligned}
\varepsilon_{\Psi_\delta(\mathcal{U})}(\ell) &\leq \rho(\ell,\mathcal{E}_{\Psi}(\mathcal{U},\delta)) + \rho\left(\ell,-A\Phi_2(A,\delta)\mathcal{U}\right) && (31)\\
\varepsilon_{\Omega_{[0,\delta]}(\mathcal{X}_0,\mathcal{U})}(\ell) &\leq \max_{\lambda\in[0,1]}\Big\{\rho\Big(\ell,\left(\lambda\mathcal{E}^{+}_{\Omega}(\mathcal{X}_0,\delta)\cap(1-\lambda)\mathcal{E}^{-}_{\Omega}(\mathcal{X}_0,\delta)\right)\Big)\\
&\qquad +\lambda^2\rho(\ell,\mathcal{E}_{\Psi}(\mathcal{U},\delta)) + \lambda\rho\left(\ell,-A\Phi_2(A,\delta)\mathcal{U}\right)\Big\}. && (32)
\end{aligned}$$

Proof. First, we have to bound, for all ℓ, $\varepsilon_{\Psi_\delta(\mathcal{U})}(\ell)$, the difference between $\rho(\ell, \Psi_\delta(\mathcal{U}))$ and $\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\}))$.

$$\begin{aligned}
&\rho(\ell, \Psi_\delta(\mathcal{U})) - \rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\})) \\
&= \delta\rho(\ell, \mathcal{U}) + \rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) - \rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\})) \\
&= \rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) + \max\{\delta u \cdot \ell \mid u \in \mathcal{U}\} \\
&\quad - \max\Big\{ \int_0^\delta e^{(\delta - s)A} u(s) ds \cdot \ell \mid \forall s \in [0; \delta]\, u(s) \in \mathcal{U} \Big\} \\
&\leq \rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) + \max\Big\{ \left(\delta u - \int_0^\delta e^{(\delta - s)A} u ds \right) \cdot \ell \mid u \in \mathcal{U} \Big\} \\
&\leq \rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) + \rho\left(\ell, A^{-1}(I + \delta A - e^{\delta A})U\right)
\end{aligned}$$

which ends the proof of the first part of the lemma.

We now have to bound, for all ℓ, $\varepsilon_{\Omega_{[0,\delta]}(\mathcal{X}_0, \mathcal{U})}(\ell)$, the difference between $\rho(\ell, \Omega_{[0,\delta]}(\mathcal{X}_0, \mathcal{U}))$ and $\rho(\ell, \mathrm{Reach}_{0,\delta}(\mathcal{X}_0))$. Let us first remark that:

$$\begin{aligned}
\rho(\ell, \mathrm{Reach}_{0,\delta}(\mathcal{X}_0)) &\geq \rho(\ell, \mathrm{Reach}_{0,0}(\mathcal{X}_0)) \\
\text{and } \rho(\ell, \mathrm{Reach}_{0,\delta}(\mathcal{X}_0)) &\geq \rho(\ell, \mathrm{Reach}_{\delta,\delta}(\mathcal{X}_0))
\end{aligned}$$

We can deduce that for all λ in $[0, 1]$:

$$\rho(\ell, \mathrm{Reach}_{0,\delta}(\mathcal{X}_0)) \geq (1 - \lambda)\rho(\ell, \mathrm{Reach}_{0,0}(\mathcal{X}_0)) + \lambda\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\mathcal{X}_0))$$

Then,

$$\begin{aligned}
&\rho(\ell, \Omega_{[0,\delta]}(\mathcal{X}_0, \mathcal{U})) - \rho(\ell, \mathrm{Reach}_{0,\delta}(\mathcal{X}_0)) \\
&\leq \max_{\lambda \in [0,1]} \{\rho(\ell, \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)) - (1 - \lambda)\rho(\ell, \mathrm{Reach}_{0,0}(\mathcal{X}_0)) - \lambda\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\mathcal{X}_0))\}
\end{aligned}$$

For a given λ in $[0, 1]$ we have:

$$\begin{aligned}
&\rho(\ell, \Omega_\lambda(\mathcal{X}_0, \mathcal{U}, \delta)) - (1 - \lambda)\rho(\ell, \mathcal{X}_0) - \lambda\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\mathcal{X}_0)) \\
&\quad \leq (1 - \lambda)\rho(\ell, X_0) + \lambda\rho(\ell, e^{\delta A}X_0) + \rho(\ell, \left(\lambda\mathcal{E}^+_\Omega(\mathcal{X}_0, \delta) \cap (1 - \lambda)\mathcal{E}^-_\Omega(\mathcal{X}_0, \delta)\right)) \\
&\qquad + \lambda\rho(\ell, \delta\mathcal{U}) + \lambda^2\rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) - (1 - \lambda)\rho(\ell, \mathcal{X}_0) - \lambda\rho(\ell, \mathrm{Reach}_{\delta,\delta}(\mathcal{X}_0)) \\
&\qquad\quad \leq \rho(\ell, \left(\lambda\mathcal{E}^+_\Omega(\mathcal{X}_0, \delta) \cap (1 - \lambda)\mathcal{E}^-_\Omega(\mathcal{X}_0, \delta)\right)) + \lambda^2\rho(\ell, \mathcal{E}_\Psi(\mathcal{U}, \delta)) \\
&\qquad\qquad + \lambda\left(\rho(\ell, \delta\mathcal{U}) - \rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\}))\right)
\end{aligned}$$

As we have already showed previously:

$$\rho(\ell, \delta\mathcal{U}) - \rho(\ell, \mathrm{Reach}_{\delta,\delta}(\{0\})) \leq \rho\left(\ell, A^{-1}(I + \delta A - e^{\delta A})U\right)$$

which ends the proof of lemma 3.