Safety Verification for Impulsive Systems ⋆

Petro Feketa * **Sergiy Bogomolov** ** **Thomas Meurer** *

* *Chair of Automatic Control, Faculty of Engineering, Kiel University, 24143 Kiel, Germany (e-mail: {pf,tm}@tf.uni-kiel.de)*
** *Newcastle University, UK; Australian National University, Australia (e-mail: sergiy.bogomolov@newcastle.ac.uk)*

Abstract: The problem of safety verification for a subclass of hybrid systems, namely for impulsive systems with fixed moments of jumps is considered. Sufficient conditions are derived for the safety of impulsive systems whose continuous dynamics may steer the state outside the safe region. For this purpose auxiliary barrier certificates with nonlinear rates are introduced and equipped with appropriate dwell-time conditions which restrict the upper bound for the inter-jump interval in order to ensure the desired safety property. The proposed approach is demonstrated by performing safety verification of linear and nonlinear impulsive systems.

Keywords: Safety analysis, Hybrid systems, Impulsive systems, Barrier certificates, Nonlinear rate functions

1. INTRODUCTION

The study of safety property in the context of dynamical systems dates back to the work of Nagumo (1942) who provides necessary and sufficient conditions for the set invariance under the continuous flow. We refer the reader to the papers (Blanchini, 1999; Ames et al., 2019; Henzinger, 1996) and references therein for a detailed literature overview and historical origins of the safety verification problem. A number of approaches to solve this problem for hybrid dynamical systems have been proposed. These include methods based on flow-pipe construction (Frehse et al., 2011; Chen et al., 2012; Bogomolov et al., 2019, 2018; Gurung et al., 2018), SMT techniques (Gao et al., 2013) and theorem proving (Platzer and Quesel, 2008). In this paper, we present a method to analyze safety of dynamical systems using *barrier certificates* (Prajna and Jadbabaie, 2004; Prajna, 2006; Prajna and Rantzer, 2005; Prajna et al., 2007; Kong et al., 2013; Dai et al., 2017). These are auxiliary functions that characterize the dynamics of the system with respect to the safe and unsafe sets. The conditions ensuring safety of hybrid system derived in these works may be described as follows: flow and jump maps that govern the dynamics of the hybrid system should be such that (a) the state of the system can not leave the safe region while it evolves along the trajectories of differential equations (flow); (b) discrete transitions transfer the state from the safe region to the safe region. This situation can be described as a 'good–good' process where the flows and jumps do not violate the safety property.

⋆ This work was partially supported by the Deutsche Forschungsgemeinschaft (DFG) in the project 412842380 "Stability analysis and safety verification of nonlinear hybrid dynamical systems and their interconnections" and by the Air Force Office of Scientific Research under award number FA2386-17-1-4065. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force.

The main idea of this paper is to transfer techniques used in the stability analysis of hybrid systems to solve the safety verification problem for a narrower class of hybrid systems, namely, for impulsive differential equations with fixed moments of jumps. Stability analysis of impulsive systems can be performed under the assumptions that the flows and jumps have a different impact on stability. For example, continuous flows may contribute towards stability and vice versa, discrete transitions play against the stability property of the system. Then, the goal is to design a system in such a way that the jumps occur not too frequently. This would balance continuous dynamics and discontinuous dynamics and does not allow for the impulsive jumps to destroy stability (see, e.g., Hespanha et al. (2008); Dashkovskiy and Mironchenko (2013); Dashkovskiy and Feketa (2017); Feketa and Bajcinca (2019b)).

The main goal of this note is to find analytic relations between the set of initial states and the frequency of discrete transitions ensuring safety property for a given impulsive system with a 'bad' continuous dynamics and a 'good' discrete dynamics. The attributes 'bad' and 'good' correspond to the flows that may steer the state outside the safe set and to the jumps that transfer the state to the safe set, respectively. The paper proposes new sufficient conditions for the safety of nonlinear impulsive systems in terms of auxiliary scalar functions whose evolution along the piece-wise continuous trajectories of the system can be estimated with nonlinear rate functions.

The rest of the paper is organized as follows. In Section 2, the problem of safety verification for impulsive systems is formulated and motivating examples are provided. New sufficient conditions for the safety and examples demonstrating the usage of the main results are provided in Section 3. In Section 4, a corollary of the main theorem is derived that is based on the barrier certificates of the exponential type, i.e., for the case of linear rate functions.

Finally, an example with nonlinear rates and a short discussion conclude the paper.

2. PROBLEM STATEMENT AND EXAMPLES

Consider impulsive system (Samoilenko and Perestyuk, 1987) with fixed moments of jumps

$$\begin{aligned} \dot{x}(t) &= f(x(t)), \quad t \neq t_i \\ x(t) &= g(x^-(t)), \, t = t_i, \quad i \in \mathbb{N} \end{aligned} \tag{1}$$

where $t \in \mathbb{R}$, $x(t) \in X \subseteq \mathbb{R}^N$, $N \in \mathbb{N}$, $f : X \to \mathbb{R}^N$, $g : X \to X$, $0 := t_0 < t_1 < \ldots < t_i < \ldots$ with

$$\theta_1 \leq t_i - t_{i-1} \leq \theta_2 \tag{2}$$

for all $i \in \mathbb{N}$ and some positive $\theta_2 > \theta_1 > 0$. Assume that the flow map f is such that the solutions to the first equation in (1) are forward complete in X. The state x of the impulsive system is assumed to be right-continuous and to have left limits at all times. Denote by $(\cdot)^-$ the left-limit operator, i.e., $x^-(t) = \lim_{s \nearrow t} x(s)$.

Assume that

$$X = X_{\text{SAFE}} \cup X_{\text{UNSAFE}}, \quad X_{\text{SAFE}} \cap X_{\text{UNSAFE}} = \varnothing$$

and the initial state

$$x_0 \in X_0 \subseteq X_{\text{SAFE}} \subseteq X.$$

The problem of safety verification of the system (1) is to prove that its solution cannot reach the unsafe set X_{UNSAFE} from the initial set X_0.

Proposition 1. (adapted from Kong et al. (2013)). If there exists a continuously differentiable function $V : X \to \mathbb{R}$ such that

$$\begin{array}{lll} V(x) & \leq 0 & \forall x \in X_0 \\ \dot{V}(x) & \leq \lambda V(x) & \forall x \in X \\ V(g(x)) & \leq \gamma V(x) & \forall x \in X_{\text{SAFE}} \\ V(x) & > 0 & \forall x \in X_{\text{UNSAFE}} \end{array}$$

for some $\lambda \in \mathbb{R}$ and some $\gamma \in (0, \infty)$, then the safety property is satisfied by system (1).

Example 1 (Example of a safe system). Consider the system

$$\dot{x} = -x, \, t \neq n\theta, \quad x = \frac{x^-}{2}, \, t = n\theta, \tag{3}$$

where $t \in \mathbb{R}$, $x(t) \in \mathbb{R}$, $n \in \mathbb{N}$, $\theta > 0$. Let

$$X_0 = [0, \infty), \, X_{\text{SAFE}} = [0, \infty), \, X_{\text{UNSAFE}} = (-\infty, 0).$$

It is easy to see that system (3) satisfies the conditions of the Proposition 1 with $V(x) = -x$ and $\lambda = -1$, $\gamma = \frac{1}{2}$. System (3) is safe for any $\theta > 0$.

Next, an example of an impulsive system is considered that does not satisfy Proposition 1.

Example 2 (Motivating example). Consider the system

$$\dot{x} = -1, \, t \neq n\theta, \quad x = 3x^-, \, t = n\theta, \tag{4}$$

where $t \in \mathbb{R}$, $x(t) \in \mathbb{R}$, $n \in \mathbb{N}$, $\theta > 0$. Let

$$X_{\text{SAFE}} = [0, \infty), \, X_{\text{UNSAFE}} = (-\infty, 0).$$

Task: Find a tuple (X_0, θ) such that system (4) is safe.

Empirical solution: in system (4), the flow map is 'bad' since it steers the state of the system into the unsafe region, and the jump map is 'good' since it transfers the safe states further from the unsafe region. Additional constraint on the frequency of jumps should be imposed in order to balance continuous dynamics and discontinuous dynamics of the system.

3. SUFFICIENT CONDITIONS FOR SAFETY

In this section new sufficient conditions for the safety of impulsive systems are provided.

Theorem 2. Let there exist a continuously differentiable function $V : X \to \mathbb{R}$ for system (1) such that

$$\begin{array}{lll} V(x) & \leq 0 & \forall x \in X_{\text{SAFE}} \\ \dot{V}(x) & \leq \varphi(V(x)) & \forall x \in X_{\text{SAFE}} \\ V(g(x)) & \leq \psi(V(x)) & \forall x \in X_{\text{SAFE}} \\ V(x) & > 0 & \forall x \in X_{\text{UNSAFE}} \end{array} \tag{5}$$

for some continuous non-increasing function $\varphi : (-\infty, 0] \to [0, \infty)$, $\varphi(s) = 0 \Rightarrow s = 0$ [1], and continuous increasing function $\psi : (-\infty, 0] \to (-\infty, 0]$. If for some $a < 0$ and $b \leq 0$ the conditions

$$\theta_2 \leq \int_a^0 \frac{ds}{\varphi(s)} \tag{6}$$

and

$$\theta_2 \leq \int_{\psi(b)}^b \frac{ds}{\varphi(s)} \tag{7}$$

hold true, then solutions to (1) cannot reach the unsafe set X_{UNSAFE} from the initial set

$$X_0 = \{x \in X_{\text{SAFE}} : V(x) \leq \min\{a, c\}\}, \tag{8}$$

where constant c satisfies $\int_c^b \frac{ds}{\varphi(s)} \geq \theta_2$.

Remark 1. Constants a and b in Theorem 2 should be chosen as large as possible in order to enlarge the set X_0.

Proof. Consider any solution $x = x(t)$ to (1) starting at $x_0 \in X_{\text{SAFE}}$ such that $V(x_0) = a$. If such $x_0 \in X_{\text{SAFE}}$ with $V(x_0) = a$ does not exist then, following (8), the set $X_0 \equiv \varnothing$. Now, consider the case when there exists an $x_0 \in X_{\text{SAFE}}$ with $V(x_0) = a$ and prove that X_0 is non-empty under the conditions of Theorem 2. Denote by $v(t) := V(x(t))$. Then, from (5) it follows that $\dot{v}(t) \leq \varphi(v(t))$ and

$$\frac{dv(t)}{\varphi(v(t))} \leq dt$$

unless the point remains in the safe region and $v(t) \neq 0$. Since the rate function φ may be positive in $(-\infty, 0]$, the continuous flow may steer the point out of the safe region X_{SAFE} if the impulsive jump occurs too late. Integrate the last inequality from 0 to some t^*:

$$\int_0^{t^*} \frac{dv(t)}{\varphi(v(t))} \leq t^*.$$

Denoting $v(t) = s$ on the left-hand side of the last inequality one obtains

$$\int_{v(0)}^{v(t^*)} \frac{ds}{\varphi(s)} \leq t^* \quad \Rightarrow \quad \int_a^{v(t^*)} \frac{ds}{\varphi(s)} \leq t^*$$

$$\Rightarrow \quad \int_a^0 \frac{ds}{\varphi(s)} + \int_0^{v(t^*)} \frac{ds}{\varphi(s)} \leq t^*$$

[1] Implication $\varphi(s) = 0 \Rightarrow s = 0$ means that there exists no $s < 0$ such that $\varphi(s) = 0$. It is admissible that φ takes only positive values.

$$\Rightarrow \quad \int_0^{v(t^*)} \frac{ds}{\varphi(s)} \le t^* - \int_a^0 \frac{ds}{\varphi(s)}.$$

A combination of the last inequality with (6) leads to the following estimate

$$\int_0^{v(t^*)} \frac{ds}{\varphi(s)} \le t^* - \theta_2 \le 0 \quad \text{for} \quad t^* \in [0, \theta_2]. \tag{9}$$

This means that $v(t) \le 0$ for any $t \in [0, \theta_2]$ assuming that the point moves along the continuous flow of the systems (1). This implies that the point remains in the safe region X_{SAFE} for all times $t \in [0, t_1]$.

Now, pick any solution to (1) starting at $x_0 \in X_{\text{SAFE}}$ such that $V(x_0) = c \le a < 0$. If such $x_0 \in X_{\text{SAFE}}$ with $V(x_0) = c$ does not exist then, following (8), the set $X_0 \equiv \varnothing$. Next, consider the case when there exists an $x_0 \in X_{\text{SAFE}}$ with $V(x_0) = c$ and prove that under dwell-time condition (7), the state remains within the safe region after each impulsive jump and does not leave X_{SAFE} during flows. For this purpose it is sufficient to show that $\psi(v(\theta_2)) \le a$.

From (5), one obtains

$$\int_{v(0)}^{v(\theta_2)} \frac{ds}{\varphi(s)} \le \theta_2 \quad \Rightarrow \quad \int_c^{v(\theta_2)} \frac{ds}{\varphi(s)} \le \theta_2$$

$$\Rightarrow \quad \int_c^a \frac{ds}{\varphi(s)} + \int_a^{\psi(v(\theta_2))} \frac{ds}{\varphi(s)} + \int_{\psi(v(\theta_2))}^{v(\theta_2)} \frac{ds}{\varphi(s)} \le \theta_2.$$

Then,

$$\int_a^{\psi(v(\theta_2))} \frac{ds}{\varphi(s)} \le \theta_2 - \int_c^a \frac{ds}{\varphi(s)} - \int_{\psi(v(\theta_2))}^{v(\theta_2)} \frac{ds}{\varphi(s)}.$$

From the last inequality, $\psi(v(\theta_2)) \le a$ holds only if

$$\theta_2 \le \int_{\psi(v(\theta_2))}^{v(\theta_2)} \frac{ds}{\varphi(s)} + \int_c^a \frac{ds}{\varphi(s)}. \tag{10}$$

If $v(\theta_2) \le b$, due to the monotonicity properties of the rate functions φ and ψ, the dwell-time condition (7) implies (10). Hence, $\psi(v(\theta_2)) \le a$ for such initial values that $\int_c^b \frac{ds}{\varphi(s)} \ge \theta_2$.

Combining two parts of the proof, any trajectory starting at the initial value $x_0 \in X_{\text{SAFE}}$ such that $V(x_0) \le \min\{a, c\}$ remains within the safe region for all times $t \in [0, \infty)$. This completes the proof. □

Remark 3. From the proof it is clear that the theorem remains true if the rate functions φ and ψ are defined on the interval $(-\infty, b]$. The choice of X_0 in (8) prevents the state to reach the region where $V(x) > b$.

Example 2 (revisited). Impulsive jumps in system (4) are equidistant, i.e. $\theta_1 = \theta_2 = \theta$. System (4) satisfies conditions (5) with $V(x) = -x$, $\varphi(s) = 1$, and $\psi(s) = 3s$. Next, conditions (6) and (7) are to be verified. From (6), one obtains:

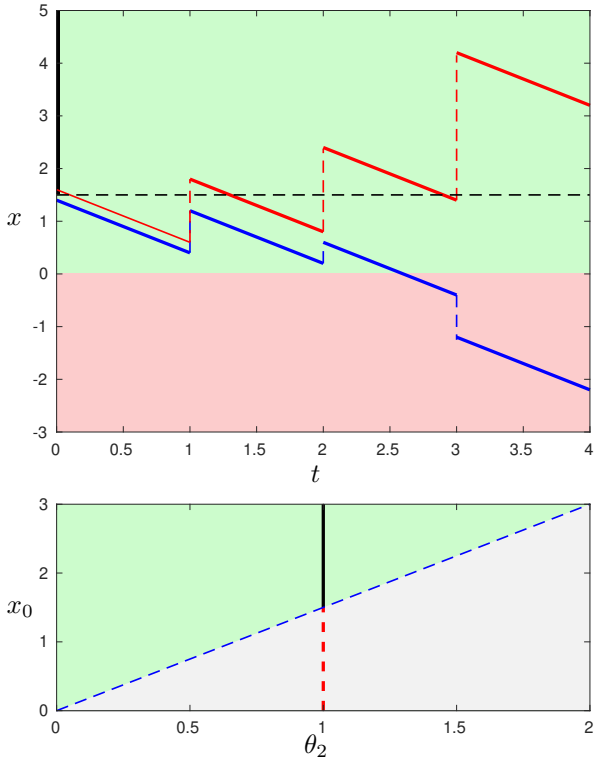

Fig. 1. *Top figure*: plots of the solutions to (4) with $\theta = 1$ for two different initial values $x_0 = 1.4$ and $x_0 = 1.6$; X_{SAFE} – green, X_{UNSAFE} – red, X_0 – solid black. Safety property is satisfied for initial values $x_0 \ge \frac{3}{2}$. *Bottom figure*: the set X_0 is in solid black for a given $\theta_2 = 1$. The domain of admissible pairs (θ_2, x_0) is filled with green.

$$\int_a^0 \frac{ds}{\varphi(s)} = \int_a^0 ds = -a \ge \theta_2 \quad \Rightarrow \quad a \le -\theta_2.$$

Finally, from (7):

$$\int_{\psi(b)}^b \frac{ds}{\varphi(s)} = \int_{3b}^b ds = -2b \ge \theta_2 \quad \Rightarrow \quad b \le -\frac{1}{2}\theta_2.$$

Constant c can be found from the relation

$$\int_c^{-\frac{1}{2}\theta_2} ds = -\frac{\theta_2}{2} - c \ge \theta_2 \quad \Rightarrow \quad c \le -\frac{3}{2}\theta_2.$$

Them, from (8),

$$V(x) = -x \le \min\left\{-\theta_2, -\frac{3}{2}\theta_2\right\} \quad \Rightarrow \quad x \ge \frac{3}{2}\theta_2.$$

Hence, for a given $\theta_2 > 0$, the initial set $X_0 = \left\{x \ge 0 : x \ge \frac{3}{2}\theta_2\right\}$ ensures the safety property of (4) (see Figure 1).

The following theorem proposes sufficient conditions for the safety in the case when the condition (6) holds true for any $a < 0$.

Theorem 4. Let there exist a continuously differentiable function $V : X \to \mathbb{R}$ for system (1) such that

$$\begin{array}{lll} V(x) & \leq 0 & \forall x \in X_{\text{SAFE}} \\ \dot{V}(x) & \leq \varphi(V(x)) & \forall x \in X_{\text{SAFE}} \\ V(g(x)) & \leq \psi(V(x)) & \forall x \in X_{\text{SAFE}} \\ V(x) & > 0 & \forall x \in X_{\text{UNSAFE}} \end{array} \tag{11}$$

for some continuous functions $\varphi : (-\infty, 0] \to [0, \infty)$ and $\psi : (-\infty, 0] \to (-\infty, 0]$. If for any $a < 0$

$$\theta_2 \leq \int_a^0 \frac{ds}{\varphi(s)} \tag{12}$$

then, solutions to (1) cannot reach the unsafe set X_{UNSAFE} from the initial set $X_0 = X_{\text{SAFE}}$.

Proof. Similarly to the proof of Theorem 2, condition (12) implies that any trajectory of (1) starting in $x_0 \in X_{\text{SAFE}}$ with $V(x_0) < 0$ remains in the safe region.

Additionally, (12) implies $\varphi(0) = 0$ since (12) holds true for any $a < 0$. Hence, trajectories of (1) corresponding to the initial value x_0 with $V(x_0) = 0$ also remain inside X_{SAFE} under the continuous dynamics of the system. The discontinuous jumps cannot transfer the state to the unsafe region due to the properties of the rate function ψ. Hence, X_0 coincides with the X_{SAFE}. The distance θ_2 between the jumps does not influence the safety property of the system. □

Theorem 4 is applicable for the safety verification of the system from Example 1.

Example 1 (revisited). System (3) satisfies safety property according to the Proposition 1. Let us verify safety using Theorem 4. Pick the same barrier function $V(x) = -x$. Then, conditions (5) are satisfied with $\varphi(s) = -s$ and $\psi(s) = \frac{s}{2}$. Let us verify (12):

$$\int_a^0 \frac{ds}{\varphi(s)} = -\int_a^0 \frac{ds}{s} = \{\ln|s|\}_0^a = \infty \geq \theta_2.$$

From Theorem 4, $X_0 = [0, \infty)$ for any $\theta_2 > 0$, i.e., the frequency of jumps does not influence the safety property of the system. Exactly the same conclusion follows from Proposition 1.

Finally, the usage of Theorem 2 is demonstrated for non-scalar impulsive system.

Example 3. Let $x(t), y(t) \in \mathbb{R}$, $n \in \mathbb{N}$,

$$X_{\text{SAFE}} = \left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \geq 1\right\},$$
$$X_{\text{UNSAFE}} = \left\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\right\}.$$

Find X_0 satisfying safety property for the system

$$\begin{array}{lll} \dot{x} = -x + y, \ t \neq n\theta, & x = \sqrt{2}x^-, \ t = n\theta, \\ \dot{y} = -x - y, \ t \neq n\theta, & y = \sqrt{2}y^-, \ t = n\theta \end{array}$$

depending on parameter $\theta > 0$.

Pick $V(x, y) = 1 - x^2 - y^2$ as a candidate for barrier certificate. Then,

$$\begin{aligned} \dot{V}(x, y) &= -2x(-x + y) - 2y(-x - y) = 2x^2 + 2y^2 \\ &= -2(1 - x^2 - y^2) + 2 \quad \Rightarrow \quad \varphi(s) = -2s + 2 \end{aligned}$$

and

$$\begin{aligned} V(g(x, y)) &= V(\sqrt{2}x, \sqrt{2}y) = 1 - 2x^2 - 2y^2 \\ &= 2V(x, y) - 1 \quad \Rightarrow \quad \psi(s) = 2s - 1. \end{aligned}$$

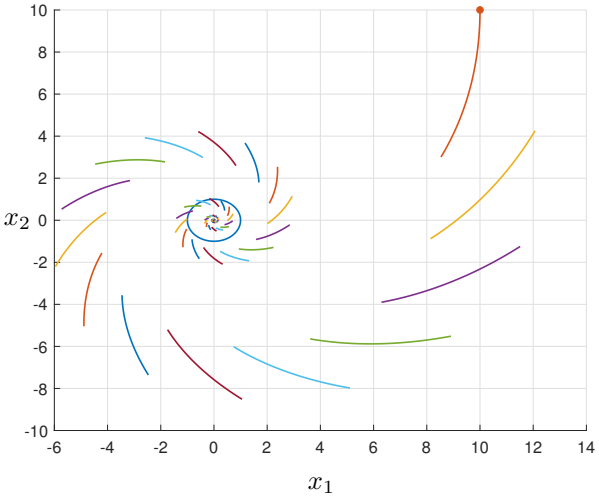

Fig. 2. For $\theta > \frac{\ln 2}{2}$, trajectories arrive inside a unit circle (unsafe region) for any initial value, e.g., $x_0 = (10, 10)$.

Condition (6) leads to

$$\theta \leq \int_a^0 \frac{ds}{2(1-s)} = \frac{\ln(1-a)}{2} \quad \Rightarrow \quad a \leq 1 - e^{2\theta}. \tag{13}$$

From (7), it follows that

$$\theta \leq \int_{2b-1}^b \frac{ds}{2(1-s)} = \frac{\ln 2}{2} \quad \forall b \leq 0. \tag{14}$$

Since (14) holds true for $b = 0$, constant c coincides with the constant a from the relation (13). Then, from Theorem 2, $X_0 = \left\{(x, y) \in X_{\text{SAFE}} : 1 - x^2 - y^2 \leq a\right\}$. Finally, combining with (13), (14), the desired set of initial values X_0 is given by

$$X_0 = \left\{(x, y) \in X_{\text{SAFE}} : x^2 + y^2 \geq e^{2\theta}, \theta \leq \frac{\ln 2}{2}\right\}.$$

Theorem 2 suggests that if the time-distance between jumps is larger than $\frac{\ln 2}{2}$, the safety property cannot by guaranteed even for very large initial values (see Figure 2). If the distance between jumps $\theta \leq \frac{\ln 2}{2}$, there is a dependence between θ and a region of the 'safe' initial values (see Figure 3).

4. EXPONENTIAL VERSION OF THEOREM 2

In this section, a particular case of Theorem 2 with linear functions φ and ψ is considered. Sufficient conditions that are based on linear rates do not require computationally difficult integral conditions (6), (7). However, they provide more conservative estimates for the distance between jumps compared to the ones with nonlinear rates.

Theorem 5. Let for system (1) there exist a continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ such that

$$\begin{array}{lll} V(x) & \leq 0 & \forall x \in X_{\text{SAFE}} \\ \dot{V}(x) & \leq -\varphi_1 V(x) + \varphi_2 & \forall x \in X_{\text{SAFE}} \\ V(g(x)) & \leq \psi_1 V(x) - \psi_2 & \forall x \in X_{\text{SAFE}} \\ V(x) & > 0 & \forall x \in X_{\text{UNSAFE}} \end{array} \tag{15}$$

for some positive constants $\varphi_1, \varphi_2, \psi_1, \psi_2 > 0$. If for some $a < 0$, $b \leq 0$ the following conditions

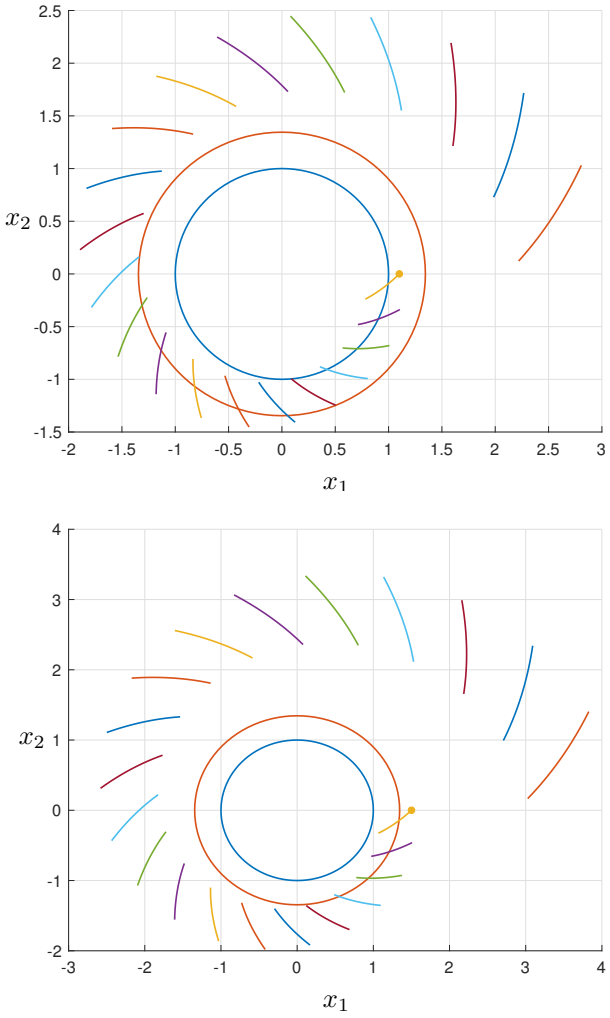

Fig. 3. For $\theta \leq \frac{\ln 2}{2}$, trajectories arrive inside a unit circle (unsafe region) only for the initial values lying inside the red circle $x^2+y^2 < e^{2\theta}$. Safety property is satisfied for the initial values outside the red circle.

$$a \leq \frac{\varphi_2}{\varphi_1}\left(1 - e^{\varphi_1\theta_2}\right), \tag{16}$$

$$e^{\varphi_1\theta_2} \leq \frac{\varphi_2 - \varphi_1(\psi_1 b - \psi_2)}{\varphi_2 - \varphi_1 b} \tag{17}$$

hold true, then the solutions to (1) cannot reach the unsafe set X_{UNSAFE} from the initial set

$$X_0 = \left\{x \in X_{\text{SAFE}} : V(x) \leq a + e^{\varphi_1\theta_2} b\right\}. \tag{18}$$

Proof. Proof follows directly from Theorem 2 by plugging linear functions into the equations (5)-(8). □

Example 3 (revisited). Conditions (15) of Theorem 5 are satisfied with $(\varphi_1, \varphi_2, \psi_1, \psi_2) = (2, 2, 2, 1)$. From (16),(17), and (18) it follows that

$$X_0 = \left\{(x, y) \in X_{\text{SAFE}} : V(x, y) \leq 1 - e^{2\theta}, \theta \leq \frac{\ln 2}{2}\right\}.$$

5. EXAMPLE WITH NONLINEAR RATE FUNCTIONS φ AND ψ

In this section, the application of Theorem 2 to impulsive system with nonlinear flow and jump maps is demonstrated. For this case it is essentially important to employ barrier certificates with nonlinear rates φ, ψ in order to derive less conservative sufficient conditions compared to the ones employing linear rates. Further examples and comparison between linear and nonlinear rates of the corresponding auxiliary functions in the context of stability analysis of impulsive systems can be found in (Feketa and Bajcinca, 2019a) and (Mancilla-Aguilar et al., 2019).

Example 4. Let $x(t) \in \mathbb{R}$, $n \in \mathbb{N}$,

$$X_{\text{SAFE}} = \{x \in \mathbb{R} : |x| \geq 1\},$$
$$X_{\text{UNSAFE}} = \{x \in \mathbb{R} : |x| < 1\}.$$

Find X_0 satisfying safety property for the system

$$\dot{x} = -x^3,\ t \neq n\theta, \quad x = (x^-)^2,\ t = n\theta,$$

depending on parameter $\theta > 0$.

Pick $V(x) = 1 - x^2$ as a candidate for the barrier certificate. Then,

$$\dot{V}(x) = -2x(-x^3) = 2x^4$$
$$= 2(1 - V(x))^2 \quad \Rightarrow \quad \varphi(s) = 2(1-s)^2$$

and

$$V(g(x)) = V(x^2) = 1 - x^4$$
$$= 1 - (V(x) - 1)^2 \quad \Rightarrow \quad \psi(s) = 2s - s^2.$$

Condition (6) leads to

$$\theta \leq \int_a^0 \frac{ds}{2(1-s)^2} = \frac{1}{2(1-s)}\Big|_a^0$$
$$\Rightarrow \quad a \leq -\frac{2\theta}{1-2\theta} \quad \text{if only} \quad \theta \leq \frac{1}{2}.$$

From (7), one gets

$$\theta \leq \int_{2b-b^2}^{b} \frac{ds}{2(1-s)^2} = \frac{1}{2}\left(\frac{1}{1-b} - \frac{1}{1-2b+b^2}\right).$$

From the last inequality the relation between θ and b is given by

$$\theta \leq -\frac{b}{2(1-b)^2}. \tag{19}$$

Values of b satisfying (19) lie in the interval $[b_-, b_+]$ with

$$b_\pm = \frac{-(1-4\theta) \pm \sqrt{1-8\theta}}{4\theta} \quad \text{if only} \quad \theta \leq \frac{1}{8}.$$

According to Remark 1, the maximal value of b should be chosen. Hence,

$$b = \frac{-(1-4\theta) + \sqrt{1-8\theta}}{4\theta}.$$

Since $\theta \in (0, \frac{1}{8}]$, the corresponding values of b lie in the interval $[-1, 0)$. Finally,

$$\theta \leq \int_c^{\frac{-(1-4\theta)+\sqrt{1-8\theta}}{4\theta}} \frac{ds}{2(1-s)^2}$$
$$\Rightarrow \quad c \leq -\frac{1 - 2\theta - (1+2\theta)\sqrt{1-8\theta}}{2\theta(1+\sqrt{1-8\theta})}.$$

Summarizing, the desired set of initial values is given by

$$X_0 = \Big\{x \in X_{\text{SAFE}} : V(x) \leq \min\Big\{-\frac{2\theta}{1-2\theta}, -\frac{1-2\theta-(1+2\theta)\sqrt{1-8\theta}}{2\theta(1+\sqrt{1-8\theta})}\Big\}, \theta \leq \frac{1}{8}\Big\}. \tag{20}$$

For the distances between impulsive jumps $\theta \leq \frac{1}{8}$ one can always find such initial values (from (20)) that do not

violate safety property. Starting positions should not be too close to the unsafe region.

Case study: Let $\theta = \frac{3}{32} < \frac{1}{8}$. Then, $a \leq -\frac{3}{13}$, $c \leq -\frac{7}{9}$, and

$$1 - x^2 \leq -\frac{7}{9} \quad \Rightarrow \quad |x| \geq \frac{4}{3}.$$

The set of initial values is then defined as $X_0 = \left\{x \in X_{\text{SAFE}} : |x| \geq \frac{4}{3}\right\}$.

6. CONCLUSION

New sufficient conditions for the safety verification of impulsive systems with fixed moments of jumps have been derived. Important feature of the these conditions is usage of nonlinear rates φ, ψ for the corresponding barrier certificates V. This makes possible to apply the results of the paper to nonlinear impulsive systems with different types of nonlinearity in flow and jump maps.

As for the next steps, finding analytical methods for the barrier certificates construction and computational algorithms for the numerical verification of the conditions (6), (7) are of a high interest. Another interesting direction is an extension of the proposed approach to switched systems and impulsive systems with state-dependent moments of jumps.

ACKNOWLEDGEMENTS

Petro Feketa is grateful to Sergiy Bogomolov and his group for their hospitality during his research stay at the Australian National University, Canberra in March, 2019. This research was supported in part by the Deutsche Forschungsgemeinschaft (DFG) in the project 412842380 "Stability analysis and safety verification of nonlinear hybrid dynamical systems and their interconnections" and by the Air Force Office of Scientific Research under award number FA2386-17-1-4065. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Air Force.

REFERENCES

Ames, A.D., Coogan, S., Egerstedt, M., Notomista, G., Sreenath, K., and Tabuada, P. (2019). Control barrier functions: Theory and applications. *arXiv preprint arXiv:1903.11199*.

Blanchini, F. (1999). Set invariance in control. *Automatica*, 35(11), 1747–1767.

Bogomolov, S., Forets, M., Frehse, G., Podelski, A., Schilling, C., and Viry, F. (2018). Reach set approximation through decomposition with low-dimensional sets and high-dimensional matrices. In *21th International Conference on Hybrid Systems: Computation and Control (HSCC 2018)*, 41–50. ACM.

Bogomolov, S., Forets, M., Frehse, G., Potomkin, K., and Schilling, C. (2019). JuliaReach: a toolbox for set-based reachability. In *22nd ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2019)*, 39–44. ACM.

Chen, X., Abraham, E., and Sankaranarayanan, S. (2012). Taylor model flowpipe construction for non-linear hybrid systems. In *2012 IEEE 33rd Real-Time Systems Symposium*, 183–192. IEEE.

Dai, L., Gan, T., Xia, B., and Zhan, N. (2017). Barrier certificates revisited. *J. Symb. Comput.*, 80, 62–86.

Dashkovskiy, S. and Feketa, P. (2017). Input-to-state stability of impulsive systems and their networks. *Nonlinear Analysis: Hybrid Systems*, 26, 190 – 200.

Dashkovskiy, S. and Mironchenko, A. (2013). Input-to-state stability of nonlinear impulsive systems. *SIAM Journal on Control and Optimization*, 51(3), 1962–1987.

Feketa, P. and Bajcinca, N. (2019a). Average dwell-time for impulsive control systems possessing ISS-Lyapunov function with nonlinear rates. In *2019 18th European Control Conference (ECC)*, 3686–3691. IEEE.

Feketa, P. and Bajcinca, N. (2019b). On robustness of impulsive stabilization. *Automatica*, 104, 48–56.

Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., and Maler, O. (2011). Spaceex: Scalable verification of hybrid systems. In S.Q. Ganesh Gopalakrishnan (ed.), *Proc. 23rd International Conference on Computer Aided Verification (CAV)*, LNCS. Springer.

Gao, S., Kong, S., and Clarke, E. (2013). Satisfiability modulo ODEs. In *International Conference on Formal Methods in Computer-Aided Design (FMCAD)*.

Gurung, A., Ray, R., Bartocci, E., Bogomolov, S., and Grosu, R. (2018). Parallel reachability analysis of hybrid systems in XSpeed. *International Journal on Software Tools for Technology Transfer (STTT)*, 1–23.

Henzinger, T.A. (1996). The theory of hybrid automata. In *IEEE Symp. Logic in Computer Science*, 278.

Hespanha, J.P., Liberzon, D., and Teel, A.R. (2008). Lyapunov conditions for input-to-state stability of impulsive systems. *Automatica*, 44(11), 2735–2744.

Kong, H., He, F., Song, X., Hung, W.N., and Gu, M. (2013). Exponential-condition-based barrier certificate generation for safety verification of hybrid systems. In *International Conference on Computer Aided Verification*, 242–257. Springer.

Mancilla-Aguilar, J.L., Haimovich, H., and Feketa, P. (2019). Uniform stability of nonlinear time-varying impulsive systems with eventually uniformly bounded impulse frequency. *arXiv preprint arXiv:1912.04343*.

Nagumo, M. (1942). Über die Lage der Integralkurven gewöhnlicher Differentialgleichungen. *Proc. of the Physico-Mathematical Society of Japan*, 24, 551–559.

Platzer, A. and Quesel, J.D. (2008). KeYmaera: A hybrid theorem prover for hybrid systems (system description). In A. Armando, P. Baumgartner, and G. Dowek (eds.), *Automated Reasoning*, volume 5195 of *LNCS*, 171–178. Springer.

Prajna, S. (2006). Barrier certificates for nonlinear model validation. *Automatica*, 42(1), 117–126.

Prajna, S. and Jadbabaie, A. (2004). Safety verification of hybrid systems using barrier certificates. In *International Workshop on Hybrid Systems: Computation and Control*, 477–492. Springer.

Prajna, S., Jadbabaie, A., and Pappas, G.J. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8), 1415–1428.

Prajna, S. and Rantzer, A. (2005). On the necessity of barrier certificates. *IFAC Proc. Vol.*, 38(1), 526–531.

Samoilenko, A. and Perestyuk, N. (1987). *Differential equations with impulse effect*. Visca Skola, Kiev.