Tight Continuous-Time Reachtubes for Lagrangian Reachability

Jacek Cyranka[1], Md. Ariful Islam[2], Scott A. Smolka[3], Sicun Gao[1], Radu Grosu[4]

***Abstract*— We introduce continuous Lagrangian reachability (CLRT), a new algorithm for the computation of a tight, conservative and continuous-time reachtube for the solution flows of a nonlinear, time-variant dynamical system. CLRT employs finite strain theory to determine the deformation of the solution set from time t_i to time t_{i+1}. We have developed simple explicit analytic formulas for the optimal metric for this deformation; this is superior to prior work, which used semi-definite programming. CLRT also uses infinitesimal strain theory to derive an optimal time increment h_i between t_i and t_{i+1}, nonlinear optimization to minimally bloat (i.e., using a minimal radius) the state set at time t_i such that it includes all the states of the solution flow in the interval $[t_i, t_{i+1}]$. We use δ-satisfiability to ensure the correctness of the bloating. Our results on a series of benchmarks show that CLRT performs favorably compared to state-of-the-art tools such as CAPD in terms of the continuous reachtube volumes they compute.**

I. Introduction

Recent work introduced *Lagrangian ReachTube algorithm* (LRT), a new approach for the reachability analysis of continuous, nonlinear, dynamical systems [4]. LRT constructs a discrete reachtube (or flowpipe) that tightly overestimates at each discrete time point the set of states reached at that time point by a dynamical system.

The main idea of LRT was to construct a ball-overestimate in a metric space that minimizes the *Cauchy-Green stretching factor* at every discrete time instant. LRT was shown to compare favorably to other reachability analysis tools, such as CAPD [1], [17], [18] and Flow* [2], [3] in terms of the discrete reachtube volumes they compute on a set of well-known benchmarks.

This paper proposes a continuous-time-reachtube extension of LRT, the motivation for which is two-fold. First, LRT, while being optimal in the discrete setting, is not sound in the continuous setting: it is not obvious how to find a ball tightly overestimating the dynamics between two discrete points. Second, LRT is not directly applicable to the analysis of hybrid systems, as the dynamics of a hybrid system may change dramatically between two discrete time points due to a mode switch.

The main goal of our algorithm, which we call *continuous Lagrangian ReachTube algorithm* (CLRT), is to efficiently construct an ellipsoidal continuous-reachtube overestimate that is tighter than those constructed by available state-of-the-art tools such as CAPD. CLRT combines a number of techniques to achieve its goal, including *infinitesimal strain theory, analytic formulas for the tightest deformation metric, nonconvex optimization, and δ-satisfiability*. Computing an as tight-as-possible continuous-reachtube overestimate helps avoid false positives when checking if a set of unsafe states can be reached from a set of initial states.

The class of continuous dynamical systems in which we are interested is described by nonlinear, time-variant, ordinary differential equations (ODEs):

$$x'(t) = f(t, x(t)), \tag{1a}$$

$$x(t_0) = x_0, \tag{1b}$$

where $x\colon \mathbb{R} \to \mathbb{R}^n$. We assume f is a smooth function, which guarantees short-term existence of solutions. The class of time-variant systems includes the class of time-invariant systems. Time-variant equations may contain additional terms, e.g., excitation variables and periodic forcing terms.

Given an initial time t_0, set of initial states $\mathcal{X} \subset \mathbb{R}^n$, and time bound $T > t_0$, CLRT computes a conservative *reachtube* of (1), that is, a sequence of time-stamped sets of states $(R_1, t_1), \ldots, (R_k, t_k = T)$ satisfying:

$$\text{Reach}\left((t_0, \mathcal{X}), [t_{i-1}, t_i]\right) \subset R_i \text{ for } i = 1, \ldots, k,$$

where $\text{Reach}\left((t_0, \mathcal{X}), [t_{i-1}, t_i]\right)$ denotes the set of all reachable states of ODE system (1) in the time interval $[t_{i-1}, t_i]$. The time steps are not necessarily uniformly spaced, and are chosen using infinitesimal strain theory (IST).

In contrast to LRT [4], which only computes the set of states reachable at discrete and uniformly spaced time steps t_i, for $i \in \{1, \ldots, k\}$, CLRT computes a conservative overestimate for the set of states reachable in non-uniformly spaced continuous time intervals $[t_{i-1}, t_i]$. Hence, CLRT computes space-time cylinders overestimating the continuous-time reachtube.

We also note that the LRT approach, as in prior work on reachability [8], [13], employed *semi-definite programming* to compute a tight deformation metric minimizing the *Cauchy-Green stretching factor*. We show that this approach is inferior and should be avoided, as it increases the total running time of the algorithm significantly, and can result in numerical instabilities (refer to the discussion in [4]). We instead derive a very simple analytic formula for the tightest deformation metric. Thus, there is no need to invoke an optimization procedure to find a tight deformation metric, as the formula for the tightest one is now available. Also, we provide a very concise proof of this fact.

Let $\text{Reach}\left((t_0, \mathcal{X}), t_{i-1}\right) \subset B_{M_{i-1}}(x_{i-1}, \delta_{i-1})$, where $B_{M_{i-1}}(x_{i-1}, \delta_{i-1})$ is the ball computed by LRT for time t_{i-1}. To construct a conservative continuous reachtube overestimate for the interval $[t_{i-1}, t_i]$, we bloat the

Jacek Cyranka and Md. Ariful Islam contributted equally to this work. [1]University of California, San Diego, 9500 Gilman Dr, La Jolla, CA 92093, [2]Carnegie Mellon University, [3]Stony Brook University, [4]Vienna University of Technology

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

radius of this ball to $\Delta_{i-1} > \delta_{i-1}$, until it becomes a conservative over-estimate for the entire interval; i.e., Reach $((t_0, \mathcal{X}), [t_{i-1}, t_i]) \subset B_{M_{i-1}}(x_{i-1}, \Delta_{i-1})$.

To ensure that the bloating is as tight as possible, we proceed as follows. First, we find the largest time t_i such that the displacement gradient tensor of the solutions originating in $B_{M_{i-1}}(x_{i-1}, \delta_{i-1})$ becomes sufficiently close to linear. Second, we assume that f in (1) is linear in the interval $[t_{i-1}, t_i]$, and solve a convex optimization problem to obtain an estimate $\hat{\Delta}_{i-1}$. Third, we compute a sound estimate of Δ_{i-1} by checking the δ-satisfiability over the reals of a logical formula with initial estimate $\hat{\Delta}_{i-1}$.

We implemented prototype CLRT in C++, and thoroughly investigated its performance on a set of benchmarks, including those used in [4]. Our results show that compared to CAPD, CLRT performs favorably in terms of the continuous-reachtube volume they compute. Also note that contrary to LRT, CLRT is fully implemented in C++, which greatly improves the scalability of our algorithm. At present CLRT uses externally CAPD to compute gradients of the flow, but we know how to achieve this independently, and we currently work on implementing/distributing CLRT as a software library written in C++.

The rest of the paper is organized as follows. Section II provides background on infinitesimal strain theory, LRT, and convex optimization. Sections IV and V describe the bloating factor and optimization steps that we use. Section VI presents the CLRT algorithm. Section VII contains our experimental results. Section VIII offers our concluding remarks and directions for future work.

II. Background

This section gives the necessary background, such that paper is self contained. We present techniques that are used by the CLRT algorithms presented in Section VI to construct overestimating tight continuous reachtubes.

A. Finite and Infinitesimal Strain Theory

A central assumption in continuum mechanics is that a body can be modeled as a continuum, and that the physical quantities distributed over the body can be therefore represented by continuous fields [16].

A body $\mathbb{B}$ is composed of an infinite number of *material points* P and the assignment of each of these material points to a *unique position* in space defines a *configuration* of $\mathbb{B}$. A *reference (or initial)* configuration of $\mathbb{B}$ occupying region $\mathcal{R}$ is used for comparison with the *current* configurations of $\mathbb{B}$ occupying region $\mathcal{R}_t$ at subsequent moments of time t.

Given a material point $P \in \mathbb{B}$, the position vector $\mathbf{X}(P)$ of P relative to a prescribed origin O in $\mathcal{R}$ is called P's *reference position*. The position vector $\mathbf{x}(P,t)$ of P relative to O in $\mathcal{R}_t$ is called the *current position* of P. For simplicity, Figure 1(Left) uses the same coordinate systems for $\mathcal{R}$ and $\mathcal{R}_t$. However, as we show later, it is convenient to use different coordinate systems or vector bases, which minimize the associated norms of $\mathcal{R}$ and $\mathcal{R}_t$. The coordinates of the

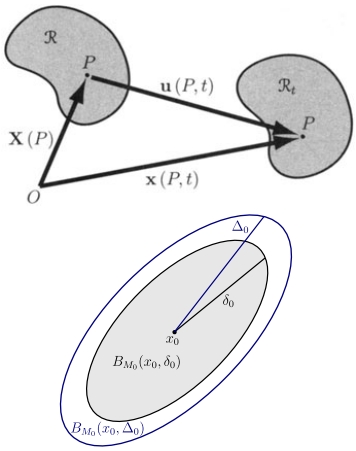

Fig. 1: (Top) The reference (or initial) configuration $\mathcal{R}$ and the current configuration $\mathcal{R}_t$ of a body $\mathbb{B}$ subjected to deformation [16]. A material point P has reference coordinates $\mathbf{X}(P)$ in $\mathcal{R}$, and current coordinates $\mathbf{x}(P,t)$ in $\mathcal{R}_t$, if one uses the same system of coordinates. The displacement vector u shows how the position of a material point P changes from $\mathcal{R}$ to $\mathcal{R}_t$. (Bottom) The larger ball $B_{M_0}(x_0, \Delta_0)$ depicted in blue, is a conservative over-estimate for the reachtube continuous segment Reach $([t_0, t_0 + h], \mathcal{X})$, that is, it is such that $\chi_{t_0}^{[t_0, t_0+h]}(B_{M_0}(x_0, \delta_0)) \subset B_{M_0}(x_0, \Delta_0)$.

reference (undeformed) $\mathcal{R}$ are called *Lagrangian*, whereas the ones of the current (deformed) $\mathcal{R}_t$ are called *Eulerian*.

The *displacement* $\mathbf{u}$ of a material point P from its position in $\mathcal{R}$ to its position in $\mathcal{R}_t$ is defined by the following vector equation:

$$\mathbf{u}(P,t) = \mathbf{x}(P,t) - \mathbf{X}(P) \tag{2}$$

Assuming that each material point P in $\mathbb{B}$ occupies a single position in space at time t, there is a (nonlinear) vector operator χ, mapping $\mathbf{X}(P)$ to $\mathbf{x}(P,t)$, that is, $\mathbf{x} = \chi(\mathbf{X}, t)$. Using χ, the Lagrangian description of the *displacement field* is given by the following equation:

$$\mathbf{u} = \chi(\mathbf{X}, t) - \mathbf{X} \tag{3}$$

A tensor $\mathbf{T}(P,t)$ is a physical quantity associated with the material point P of a body $\mathbb{B}$ at the time t. This representation can be given in either Lagrangian coordinates as $\mathbf{T} = \mathbf{\Psi}(\mathbf{X}, t)$ or Eulerian coordinates as $\mathbf{T} = \psi(\mathbf{x}, t)$. Since the tensor is the same no matter in which coordinates it is expressed, the Lagrangian description is related to the Eulerian description by:

$$\mathbf{\Psi}(\mathbf{X}, t) = \psi(\chi(\mathbf{x}, t), t) \tag{4}$$

A particularly important (nonsingular) tensor is the *deformation gradient tensor* $\mathbf{F}$ defined by the following equation:

$$\mathbf{F} = \nabla_X \mathbf{x} = \nabla_X \chi(\mathbf{X}, t) \tag{5}$$

By Equations (2,3), the *displacement gradient tensor* is related to the deformation gradient tensor as follows:

$$\nabla_X \mathbf{u} = \mathbf{F} - \mathbf{I} \tag{6}$$

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

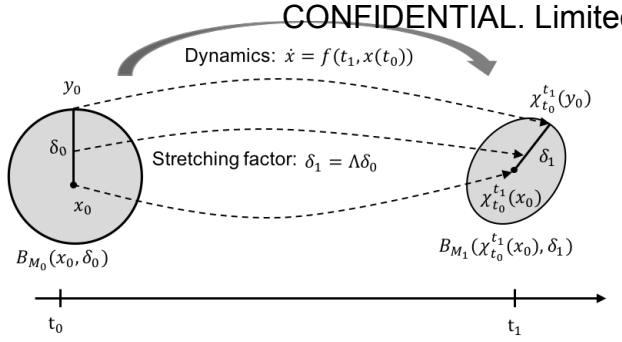

Fig. 2: An overview of LRT from [4]. The dashed arrows reflect the solution flow χ and the evolution of state discrepancy.

A description of the deformation independent of both translation and rotation is given by a *strain tensor*, of which the *right Cauchy-Green* deformation tensor $\mathbf{C}$ and the *Green-St. Venant* strain tensor $\mathbf{E}$, are two examples:

$$\mathbf{C} = \mathbf{F}^T \cdot \mathbf{F} \qquad \mathbf{E} = (\mathbf{C} - \mathbf{I})/2 \tag{7}$$

Now by using the definition of $\mathbf{F}$ from Equation 6, the Green-St. Venant strain tensor $\mathbf{E}$ can be rewritten as follows:

$$\mathbf{E} = [(\nabla_X \mathbf{u}) + (\nabla_X \mathbf{u})^T + (\nabla_X \mathbf{u})^T \cdot (\nabla_X \mathbf{u})]/2 \tag{8}$$

If the norm $\|\nabla_X \mathbf{u}\| \ll 1$, that is, each component of $\nabla_X \mathbf{u}$ is of order $O(\varphi)$, for small φ, then one speaks about *infinitesimal deformation* and the associated theory is called the *infinitesimal strain theory (IST)*.

In this case, the product $(\nabla_X \mathbf{u})^T \cdot (\nabla_X \mathbf{u})$ is of order $O(\varphi^2)$, and it can be therefore neglected. This, leads to the linearized version ε of $\mathbf{E}$:

$$\varepsilon = [(\nabla_X \mathbf{u}) + (\nabla_X \mathbf{u})^T]/2 \tag{9}$$

which is called the *infinitesimal strain tensor* ε. Similarly, the *infinitesimal rotation tensor* ω is defined as follows:

$$\omega = [(\nabla_X \mathbf{u}) - (\nabla_X \mathbf{u})^T]/2 \tag{10}$$

For infinitesimal deformations, $d\mathbf{X} = d\mathbf{x}$, and for any tensor $\mathbf{T}$, the gradients of $\mathbf{T}$ with respect to the Lagrangian and Eulerian coordinates are the same, as $\delta\mathbf{T}/\delta X = \delta\mathbf{T}/\delta x$. Hence, in IST it is not necessary to distinguish anymore between Lagrangian and Eulerian coordinates.

B. Review of the LRT Algorithm

The LRT algorithm computes of a conservative, discrete-time reachtube for nonlinear, time-variant dynamical systems, based on finite strain theory [4].

The main idea of LRT is to use the right Cauchy-Green strain tensor $\mathbf{C}$ to determine, in a tightest metric, the *stretching factor (SF)* of a ball propagated by the system dynamics in the next time step. According to Eqs. (6,7), $\mathbf{C} = \mathbf{F}^T \cdot \mathbf{F}$, $\mathbf{F} = \nabla_X \mathbf{x}$, and $\mathbf{x} = \chi(\mathbf{X}, t)$, where $\chi(\mathbf{X}, t)$ is the *solution-flow* of the system. $\mathbf{F}$ is the *sensitivity matrix* [5].

Let matrices $M_0, M_1 \succ 0$ define two metric spaces (we use the standard notation $\succ 0$ of positive definiteness, and $\succeq 0$ of positive semi-definiteness), and let $B_{M_0}(x_0, \delta_0)$ be an initial region, given as a ball in metric space M_0, centered at x_0 and of radius δ_0. Let y_0 be a point on the surface of $B_{M_0}(x_0, \delta_0)$, and $x_0' = \chi_{t_0}^{t_1}(x_0)$ and $y_0' = \chi_{t_0}^{t_1}(y_0)$, where $\chi_{t_0}^{t_1}(x)$ abbreviates the solution flow $\chi(x, t_0, t_1)$ of x when time passes from t_0 to t_1. Let δ_1 be the distance between y_0' and x_0' in the metric space defined by matrix M_1 (see Figure 2 for a geometric representation).

The SF Λ measures the deformation of the ball $B_{M_0}(x_0, \delta_0)$ into the ball $B_{M_1}(x_0', \delta_1)$, that is, $\Lambda = \delta_1/\delta_0$. One can thus use the SF to bound the infinite set of reachable states at time t_1 with the ball-overestimate $B_{M_1}(\chi_{t_0}^{t_1}(x_0), \delta_1)$ in an appropriate metric $M_1 \succ 0$, which may differ from $M_0 \succ 0$. If we put $M_1 = M_0$, we refer to the computed SF as M_0 SF , if we put $M_0 = M_1$ we refer to the computed SF as M_1 SF , if $M_0 \neq M_1$ we refer to the computed SF as $M_{0,1}$ SF.

LRT's performance depends on an appropriate choice of matrix M_1. LRT computes $M_1 \succ 0$ by solving a semi-definite optimization problem. Note that the output provided by LRT can be used to compute a validated bound for the *finite-time Lyapunov exponent* $\mathrm{FTLE} = \ln(\mathrm{SF})/T$, where T is the time horizon, for a whole set of solutions. FTLE is used for example in climate research, in order to detect Lagrangian coherent structures. The main theorem underlying the correctness of the LRT algorithm is as follows [4].

Theorem 1 (Thm. 1 in [4]): Let $t_0 \leq t_1$ be time points, and $\chi_{t_0}^{t_1}(x)$ the solution at t_1 of the Cauchy problem (1), with initial condition (t_0, x). Let $\nabla_x \chi_{t_0}^{t_1}(x)$ be the deformation gradient tensor, $M_0, M_1 \in \mathbb{R}^{n \times n}$ with $M_0, M_1 \succ 0$, and $A_0^T A_0 = M_0$, $A_1^T A_1 = M_1$ their respective decompositions. Let the ball in the M_0-norm with center x_0 and radius δ_0, $\mathcal{X} = B_{M_0}(x_0, \delta_0) \subseteq \mathbb{R}^n$ be a set of initial states for (1). Assume that there exists a compact, conservative enclosure $\mathcal{F} \subseteq \mathbb{R}^{n \times n}$ for the gradients such that:

$$\nabla_x \chi_{t_0}^{t_1}(x) \in \mathcal{F}, \quad \forall x \in \mathcal{X}. \tag{11}$$

Suppose $\Lambda > 0$ is an upper bound of the whole set of $M_{0,1}$ SFs, that is:

$$\Lambda \geq \sqrt{\lambda_{max}\left((A_0^T)^{-1} F^T M_1 F A_0^{-1}\right)}, \quad \forall F \in \mathcal{F}. \tag{12}$$

Then, every solution at time t_1 belongs to the ball:

$$\chi_{t_0}^{t_1}(x) \in B_{M_1}(\chi_{t_0}^{t_1}(x_0), \Lambda \cdot \delta_0). \tag{13}$$

Observe that

$$\sqrt{\lambda_{max}\left((A_0^T)^{-1} F^T M_1 F A_0^{-1}\right)} = \left\|A_1 F A_0^{-1}\right\|_2,$$

where $\|\cdot\|_2$ is spectral (Euclidean) matrix norm.

III. Explicit Analytic Computation of the Tightest Deformation Metric

Observe that Thm. 1 provides freedom in switching metric spaces used from step to step (by convention, $M_0 \succ 0$ denotes the initial metric, and $M_1 \succ 0$ denotes the metric of the solution-set bound after one time-step). To decide if a change of norm should be performed, we compute the $\hat{M}_1$ that minimizes the M_1-stretching factor $\left(\sqrt{\lambda_{max}\left((A_1^T)^{-1} F^T M_1 F A_1^{-1}\right)}\right)$, and decide based on that; i.e., if the resulting $\hat{M}_1$-stretching factor (SF) is

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

by some measure significantly smaller than the M_0-SF $\left(\sqrt{\lambda_{max}\left((A_0^T)^{-1}F^T M_0 F A_0^{-1}\right)}\right)$, then switching to $\hat{M}_1$ may result in a tighter over-estimate.

We provide here a surprising argument that the optimal choice of $\hat{M}_1$ minimizing the M_1-SF, as well as its decomposition $\hat{M}_1 = \hat{A}_1^T \hat{A}_1$ can be obtained using a straightforward computation that we present here.

Motivated by related work [8], [13], the LRT approach [4] identified a tight metric by solving a Semi-Definite Programming (SDP) problem. We show that we do not need to invoke any (convex) optimization technique to find a tight deformation metric, because there actually exist explicit simple and neat analytical formulas for the tightest deformation metric. In particular, this improves upon existing results two-fold: the computation is much faster, and the computed bounds are tighter than the ones computed using SDP. We provide an illustrative example to support our claim in Fig. 3. We are convinced that our technique can be applied in the related settings considered in [8], [13].

Our goal is to minimize the value of Λ, the upper bound for the M_1-SF given in Theorem 1. As finding the best enclosure for a set of SF is a hard problem, we use the following heuristics. The set of gradients $\mathcal{F} \subset \mathbb{R}^{n\times n}$ in our algorithm is given by an interval matrix. Our choice of M_1 is determined by the value of the gradient F being the middle of $\mathcal{F}$, i.e. $F = \mathrm{mid}\,(\mathcal{F})$. We derive an analytical formula for $\hat{M}_1$ minimizing the M_1-SF for F. We devote the remainder of this section to answer the following crucial question.

For a given gradient matrix F, what is the $\hat{M}_1$ minimizing the M_1 SF?

Definition 1 (Analytic $\hat{M}_1 \succ 0$): Let $F \in \mathbb{R}^{n\times n}$ be a full-rank matrix (in our application a gradient of the flow). Let $V(F) \in \mathbb{C}^{n\times n}$ denote an invertible matrix of eigenvectors of F (column-wise). To make this matrix invertible in the case of higher-dimensional eigenspaces (where some eigenvectors are equal), we need to include generalized eigenvectors. For gradients of nonlinear flow this almost never happens; hence we do not treat the case of equal eigenvalues in detail.

We define $\hat{M}_1$ as follows:

$$\hat{A}_1(F) = V(F)^{-1} \quad \text{and} \quad \hat{M}_1(F) = \hat{A}_1(F)^T \hat{A}_1(F) \quad (14)$$

When F is known from context, we simply write $\hat{A}_1 = \hat{A}_1(F)$, and $\hat{M} = \hat{M}_1(F)$.

We now prove that the choice made in Def. 1 is optimal, i.e. it minimizes the M_1 SF.

Theorem 2 ($\hat{M}_1$ is optimal): Let $F \in \mathbb{R}^{n\times n}$ be a full-rank matrix. Let $\hat{A}_1$ and $\hat{M}_1$ be defined by (14). Let the M_1-SF be given by

$$\Lambda(A_1, F) = \sqrt{\lambda_{max}\left((A_1^T)^{-1}F^T M_1 F A_1^{-1}\right)} = \left\|A_1 F A_1^{-1}\right\|_2$$

It holds that

$$\min_{\substack{A_1\in\mathbb{R}^{n\times n}\\ A_1 \text{ is invertible}}} \Lambda(A_1, F) = \Lambda(\hat{A}_1, F),$$

i.e., $\hat{M}_1 = \hat{A}_1^T \hat{A}_1$ minimizes the M_1-SF.

Proof: First, for arbitrary A_1, it holds that

$$\sigma_1(A_1 F A_1^{-1}) = \|A_1 F A_1^{-1}\|_2 = \max_{\|x\|=1,\|y\|=1} \left|y^T A_1 F A_1^{-1} x\right|,$$

where σ_1 denotes the largest singular value of $A_1 F A_1^{-1}$.

Let us pick $y^T = w^T$, and $x = w$, where w is the normalized eigenvector corresponding to the largest eigenvalue of $A_1 F A_1^{-1}$. We have

$$\|A_1 F A_1^{-1}\|_2 = \max_{\|x\|_2=1,\|y\|_2=1} \left|y^T A_1 F A_1^{-1} x\right| \geq$$
$$\left|w^T A_1 F A_1^{-1} w\right| = |\lambda_{max}(A_1 F A_1^{-1})| = |\lambda_{max}(F)|.$$

Hence, the M_1 SF cannot be smaller than $|\lambda_{max}(F)|$.

Second, we show that this lower bound is in fact attained for $\hat{A}_1 = \hat{A}_1(F)$ defined by (14). We have

$$\|\hat{A}_1 F \hat{A}_1^{-1}\|_2 = \sqrt{\lambda_{max}\left((\hat{A}_1^T)^{-1}F^T \hat{A}_1^T \hat{A}_1 F \hat{A}_1^{-1}\right)}$$
$$= \sqrt{\lambda_{max}\left(\mathrm{diag}(|\lambda_1|^2, \ldots, |\lambda_n|^2)\right)} = |\lambda_{max}(F)|,$$

where $\lambda_1, \ldots, \lambda_n$ denote the eigenvalues of F. ∎

Remark 1: Let us remark on how we compute matrix $\hat{A}_1$ in practice. Generally, this matrix is complex, as the gradient of the flow is expected to involve some rotation. We do not work within the field $\mathbb{C}$ as we apply algorithms for bounding eigenvalues of real matrices. Instead, we compute the equivalent real matrix $\hat{A}_1$, such that the resulting product $\hat{A}_1 F \hat{A}_1^{-1}$ is block-diagonal (having two dimensional blocsk corresponding to complex eigenvalues). For example, for $F = \begin{bmatrix} 1 & 1 \\ -4 & 1 \end{bmatrix}$, we have $\hat{A}_1(F) = \begin{bmatrix} 0 & 0.4472 \\ 0.8944 & 0 \end{bmatrix}$, and $\hat{A}_1 F \hat{A}_1^{-1} = \begin{bmatrix} 1 & -2 \\ 2 & 1 \end{bmatrix}$.

We illustrate the Thm. 2 optimality condition in Figure 3.

IV. Conservative Continuous-Time Reachtubes

We present a simple ellipsoidal construction for conservatively over-estimating the continuous-time segments of a reachtube. For a given ellipsoidal bound for the set of initial states of radius δ_0, if the radius of this bound is bloated as in Figure 1(Right), up to a computable bound Δ_0, such that:

$$\delta_0 + \max_{\substack{x\in B_{M_0}(x_0,\Delta_0)\\ t\in[0,h]}} \|h \cdot f(t_0+t, x)\|_{M_0} \leq \Delta_0,$$

where h is a time increment and f is the dynamics of the Cauchy problem (1), then the resulting ellipsoid becomes a conservative over-estimate of the whole continuous segment $\chi_{t_0}^{[t_0,t_0+h]}(x) \subset \mathbb{R}^n$, representing the set of all values $\chi_{t_0}^t(x)$ of the solution flow of (1), for all times $t \in [t_0, t_0+h]$.

Lemma 1: Given the Cauchy problem (1) with $x_0 \in \mathbb{R}^n$ the initial state, t_0 the current time, h the current time-step, and $\chi_{t_0}^t(x)$ the solution flow, let $\Delta > 0$ and $M \succ 0$ be a matrix defining the metric space being used. Then:

$$\max_{\substack{x\in B_M(x_0,\Delta)\\ t\in[0,h]}} \|h \cdot f(t_0+t, x)\|_M \leq \Delta$$
$$\Rightarrow \chi_{t_0}^{[t_0,t_0+h]}(x_0) \subseteq B_M(x_0, \Delta)$$

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

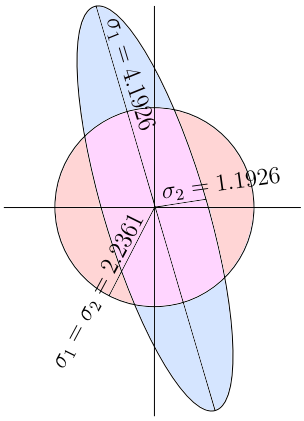

Fig. 3: Illustration of optimality condition of Thm. 2 for $F = [1\ 1]; [-4\ 1]$, F has conjugate pair of complex eigenvalues $1 \pm i\sqrt{2}$. SVD decomposition of F reveals it rotates and transforms unit disc into blue ellipse, where the radii are equal to the singular values ($\sigma_1 = 4.1926$, $\sigma_2 = 1.1926$), resp. SVD of $\hat{A}_1 F \hat{A}_1^{-1}$ reveals, however, that two singular values are equal $\sigma_1 = \sigma_2 = 2.2361$. Recall SF is equal to σ_1; although the two "balls" have the same volume, the circular one results in a significantly smaller SF (2.2361 versus 4.1926).

Proof: Let $\mathcal{C}([t_0, t_0 + h], \mathbb{R}^n)$ denote the space of continuous and differentiable functions defined over the interval $[t_0, t_0 + h]$ and domain $\mathbb{R}^n$. Define the operator $T_{x_0} \colon \mathcal{C}([t_0, t_0 + h], \mathbb{R}^n) \to \mathcal{C}([t_0, t_0 + h], \mathbb{R}^n)$ as follows:

$$T_{x_0}(\chi)(h) = x_0 + \int_0^h f(t_0 + t, \chi_{t_0}^{t_0+t}(x_0))\, dt.$$

Let $\mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta)) \subset \mathcal{C}([t_0, t_0 + h], \mathbb{R}^n)$ be the subspace of continuous, differentiable, and bounded functions having their range contained within $B_M(x_0, \Delta)$. We show that T_{x_0} maps $\mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta))$ into itself. Let $\hat{h} \in [0, h]$, and $\chi \in \mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta))$. Then $\|T_{x_0}(\chi)(\hat{h}) - x_0\|_M$ is bounded as follows:

$$\begin{aligned}\left\| \int_0^{\hat{h}} f(t_0 + t, \chi_{t_0}^{t_0+t}(x_0))\, dt \right\|_M \leq \\ \int_0^{\hat{h}} \left\| f(t_0 + t, \chi_{t_0}^{t_0+t}(x_0)) \right\|_M dt \leq \\ \max_{\substack{x \in B_M(x_0,\Delta) \\ t \in [0,h]}} \left\| \hat{h} \cdot f(t_0 + t, x) \right\|_M \leq \\ \max_{\substack{x \in B_M(x_0,\Delta) \\ t \in [0,h]}} \|h \cdot f(t_0 + t, x)\|_M.\end{aligned}$$

The inequalities are due to the fact that $\chi \in \mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta))$. The second and the third ones allow us to compute the integral explicitly. Now using the assumption $\max_{\substack{x \in B_M(x_0,\Delta) \\ t \in [0,h]}} \|h \cdot f(t_0 + t, x)\|_M \leq \Delta$, we can infer that:

$$T(\chi)(\hat{h}) \in B_M(x_0, \Delta) \text{ for all } \hat{h} \in [0, h].$$

As χ was arbitrary, $T\left(\mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta))\right)$ is a subset of the class of continuous functions $\mathcal{C}([t_0, t_0 + h], B_M(x_0, \Delta))$. For instance, the standard Schauder's fixed-point theorem argument shows that the solution of (1) with the initial condition (t_0, x_0) is a fixed point of T, that is, $\chi_{t_0}^{t_0+s}(x_0) \in B_M(x_0, \Delta), \forall s \in [0, h]$. ■

Theorem 3 (Optimization for a conservative over-estimate): Consider the Cauchy problem (1), and let $\chi_{t_0}^t(x)$ denote the flow generated by (1). Let $x_0 \in \mathbb{R}^n$ be an initial state, t_0 be the current time, h be the current time-step, and $M_0 \succ 0$ be a matrix defining a metric. Let $B_{M_0}(x_0, \delta_0)$ be given (output from the *LRT algorithm*). Then for all $x \in B_{M_0}(x_0, \delta_0)$:

$$\delta_0 + \max_{\substack{x \in B_{M_0}(x_0,\Delta_0) \\ s \in [0,h]}} \|h \cdot f(t_0 + s, x)\|_{M_0} \leq \Delta_0 \Rightarrow \chi_{t_0}^{[t_0, t_0+h]}(x) \subset B_{M_0}(x_0, \Delta_0) \quad (15)$$

Proof: Pick any $\bar{x} \in B_{M_0}(x_0, \delta_0)$. Rewriting the current assumption as

$$\begin{aligned}\max_{\substack{x \in B_{M_0}(\bar{x},\Delta_0-\delta_0) \\ s \in [0,h]}} \|h \cdot f(t_0 + s, x)\|_{M_0} \leq \\ \max_{\substack{x \in B_{M_0}(x_0,\Delta_0) \\ s \in [0,h]}} \|h \cdot f(t_0 + s, x)\|_{M_0} \leq \Delta_0 - \delta_0,\end{aligned}$$

the first inequality holds from $B_{M_0}(\bar{x}, \Delta_0 - \delta_0) \subset B_{M_0}(x_0, \Delta_0)$. From Lemma 1 it immediately follows that

$$\chi_{t_0}^{[t_0, t_0+h]}(\bar{x}) \subset B_{M_0}(\bar{x}, \Delta_0 - \delta_0) \subset B_{M_0}(x_0, \Delta_0).$$

■

The following Corollary is obtained by performing minor changes to the proof of Theorem 3.

Corollary 1 (Applying Thm. 3 backwards in time): Given the ODE system (1), with $x_0 \in \mathbb{R}^n$ the initial state, t_0 the current time, h the current time-step, and $\chi_{t_0}^t(x)$ the solution flow, let $\Delta_0 > 0$ and $M_0 \succ 0$ define the metric space used. Then:

$$\delta_0 + \max_{\substack{x \in B_{M_0}(x_0,\Delta_0) \\ s \in [0,h]}} \|h \cdot f(t_0 - s, x)\|_{M_0} \leq \Delta_0 \Rightarrow \chi_{t_0}^{[t_0-h, t_0]}(x) \subseteq B_{M_0}(x_0, \Delta_0). \quad (16)$$

Remark 2: An important consequence of Theorem 3 and Corollary 1 is that for *time invariant systems*, conditions (15),(16) imply

$$\delta_0 + \max_{x \in B_{M_0}(x_0,\Delta_0)} \|h \cdot f(x)\|_{M_0} \leq \Delta_0 \Rightarrow \chi_{t_0}^{[t_0-h, t_0]}(x) \text{ and } \chi_{t_0}^{[t_0, t_0+h]}(x) \subset B_{M_0}(x_0, \Delta_0). \quad (17)$$

Hence, ball $B_{M_0}(x_0, \Delta_0)$ covers both the forward and backward orbits that initiate within $B_{M_0}(x_0, \delta_0)$.

V. Nonconvex Optimization in CLRT

A. Bounding the Maximal Vector Field in Metric $\mathbf{M}_0$

In Theorem 3 of Section VI, we give a computable condition for determining a conservative over-estimate of a continuous reachtube segment, based on the set of initial states in a ball $B_{M_0}(x_0, \delta_0)$, in some metric $M_0 \succ 0$.

More precisely, a conservative radius (denoted by Δ_0) of the continuous reachtube segment over-estimate needs to satisfy:

$$\max_{\substack{x\in B_{M_0}(x_0,\Delta_0)\\ s\in[0,h]}} \|h\cdot f(t_0+s,x)\|_{M_0} \leq \Delta_0-\delta_0. \tag{18}$$

Verifying conservativeness of Δ_0 requires bounding the maximal vector field value in a metric given by M_0, as in the left-hand side of (18). We emphasize that any convex optimization program (COP) for verifying this condition will not be sound, as we neither assume convexity of f in (1), nor does it follow from our approach.

An interesting problem in this case is to see if the time-step adaptation scheme based on IST leads to the convexity of f. If f is still nonconvex, one may need to further decrease the time-step such that f becomes convex in this small range, and a COP can be used to find Δ_0 satisfying (18).

Due to a possible lack of convexity, we restate the global optimization problem of bounding the left-hand side of (18) as one of ε-satisfiability over the reals [9], [10]. (Normally referred to as δ-satisfiability, we use the name ε-satisfiability to avoid confusion with δ_0, denoting a ball radius in our context.) For an initial guess for $\Delta_0-\delta_0$, given for example by COP, we define the following quantified formula:

$$\exists_{x\in B_{M_0}(x_0,\Delta_0)}\exists_{s\in[0,h]}\|h\cdot f(t_0+s,x)\|_{M_0} > \Delta_0-\delta_0. \tag{19}$$

We provide below an interpretation of the ε-satisfiability answers for (19), where the first answer tells us that $\Delta_0-\delta_0$ is a good bound: UNSAT means that $\forall x\in B_{M_0}(x_0,\Delta_0)$, $\forall s\in[0,h]$, the inequality $\|h\cdot f(t_0+s,x)\|_{M_0}\leq\Delta_0-\delta_0$ holds, and hence (18) is satisfied. ε-SAT means that an ε-weakening is satisfiable, i.e., $\exists x\in B_{M_0}(x_0,\Delta_0)$, $\exists s\in[0,h]$, $|h\cdot f(t_0+s,x)\|_{M_0}-\varepsilon|>\Delta_0-\delta_0$.

VI. The CLRT Reachability Algorithm

Notation. By $[x]$ we denote a product of intervals (a box), i.e., a compact and connected set $[x]\subset\mathbb{R}^n$. We will use the same notation for interval matrices. By $\|\cdot\|_2$ we denote the *Euclidean norm*, by $\|\cdot\|_\infty$ we denote the max norm; we use the same notation for the induced operator norms. Let $B(x,\delta)$ be the closed ball centered at x with radius δ. $B_M(x,\delta)$ is the closed ball in the metric space defined by matrix $M\succ 0$. By $\chi_{t_0}^{t_1}$ we denote the flow induced by (1). $\nabla_x\chi_{t_0}^{t_1}$ denotes the partial derivative in x of the flow WRT the initial condition at time t_1, which we call the *gradient of the flow*, also referred to as the *sensitivity matrix* [5], [6].

Definition 2: Given an initial set $\mathcal{X}$, initial time t_0, and target time $t_1\geq t_0$, we call the following compact sets:

- $\mathcal{W}\subset\mathbb{R}^n$ a *conservative* reach-set enclosure if $\forall x\in\mathcal{X}.\ \chi_{t_0}^{t_1}(x)\in\mathcal{W}$.
- $\mathcal{F}\subset\mathbb{R}^{n\times n}$ a *conservative* gradient enclosure if $\forall x\in\mathcal{X}.\ \nabla_x\chi_{t_0}^{t_1}(x)\in\mathcal{F}$.

Given a set $\mathcal{X}\subset\mathbb{R}^n$ and a time t_0, we call a state $x\in\mathbb{R}^n$ *reachable* within time interval $[t_1,t_2]$ if there is an initial state $x_0\in\mathcal{X}$ at time t_0 and a time $t\in[t_1,t_2]$, such that $x=\chi_{t_0}^t(x_0)$. The set of all reachable states in interval $[t_1,t_2]$ is called the *reach set* and is denoted by $\text{Reach}((t_0,\mathcal{X}),[t_1,t_2])$.

Definition 3 ([7] Def. 2.4): Given an initial set $\mathcal{X}$, initial time t_0, and time bound T, a $((t_0,X),T)$-*reachtube* of (1) is a sequence of time-stamped sets $(R_1,t_1),\ldots,(R_k,t_k)$ satisfying the following properties: (1) $t_0\leq t_1\leq\cdots\leq t_k=T$, (2) $\text{Reach}((t_0,\mathcal{X}),[t_{i-1},t_i])\subset R_i,\forall i=1,\ldots,k$.

We shall henceforth simply use the name *reachtube over-estimate* of the flow defined by ODE system (1). We now present the CLRT algorithm for computing conservative over-estimations for segments (R_i,t_i), with $\text{Reach}((t_0,\mathcal{X}),[t_{i-1},t_i])\subset R_i$, whose union makes up the complete $((t_0,X),T)$-*reachtube* of (1). CLRT therefore computes the *whole conservative reachtube over-estimate* of the flow defined by (1). LRT computes discrete-time slices of the CLRT reachtube.

Input:*ODE system* (1); *Parameters:*Time horizon T, initial time t_0, number of discrete-time steps k, and initial time increment $h=T/k$ (observe that h may change during execution of the algorithm due to the IST condition); *Metric*: Positive-definite symmetric matrix $M_0\succ 0$ for initial norm. *Initial region*: Bounds $[x_0]\subset\mathbb{R}^n$ for the center, and the radius $\delta_0>0$, for the ball $B_{M_0}(x_0,\delta_0)$ with norm M_0 at initial time t_0. *IST threshold*: $\varepsilon_{IST}>0$ – threshold used to check for smallness of the IST displacement gradient tensor. *Increment for ε-satisfiability*: $C_\delta>1$ – increment used for iterative validation of upper bound for maximal speed within bounds using ε-satisfiability. *Norm switch threshold* $C_M>0$ – threshold value used to decide if the metric space used should be updated to a new $\hat{M}_1$.

Output: $\{[x_j]\}_{j=1}^k\subset\mathbb{R}^{n\times k}$: Interval enclosures for ball centers x_j at time t_0+jh. $\{M_j\}_{j=1}^k$: Norms defining metric spaces for the ball enclosures. $\{\Delta_j\}_{j=1}^k\in\mathbb{R}_+^k$: Radii of the ball enclosures at x_j, for $j=1,\ldots,k$.[1]

Begin CLRT

1) *Begin IST*
   a) Set $h=h_{prev}$, where h_{prev} is the time increment used in the previous step of the algorithm or some fixed initial value.
   b) Compute over-estimate for $B_{M_0}([x_0],\delta_0)$, representable in the rigorous tool employed by the LRT, and used to propagate forward in time all solutions initiating in $B_{M_0}([x_0],\delta_0)$. This is a product of intervals in canonical coordinates $[X]\subset\mathbb{R}^n$, such that:
   $$B_{M_0}([x_0],\delta_0)\subset[X].$$
   c) Use the rigorous tool employed by LRT to compute conservative over-estimates for the flow (deformation) gradient tensor, and for the displace-

[1]Observe that the radius is valid for the M_j norm, $B_{M_j}([x_j],\Delta_j)\subset\mathbb{R}^n$ for $j=1,\ldots,k$ is a conservative output, that is, $B_{M_j}([x_j],\Delta_j)$ is an over-approximation for the set of states reachable at times $[t_0,t_1]$ starting from any state (t_0,x), such that $\forall x\in\mathcal{X}$:

$$\text{Reach}((t_0,\mathcal{X}),[t_j,t_{j+1}])\subset B_{M_j}([x_j],\Delta_j),\text{ for } j=1,\ldots,k.$$

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

ment gradient tensor, at time $t_0 + h$:

$$[\nabla_x \chi_{t_0}^{t_1}([X])] \text{ and } [\nabla_X u(X,t)] = [\nabla_x \chi_{t_0}^{t_1}([X])I].$$

d) Use infinitesimal strain theory (IST) to adjust the time increment h by halving or doubling it until the IST condition is satisfied:

$$\|[\nabla_X u(X,t)]\| < \varepsilon_{IST}.$$

After the IST condition holds, set the next time to $t_1 = t_0 + h$.

2) *End IST*
3) *Begin improved LRT*
   a) Compute the interval over-estimate for the center of the ball at time t_1, that is, $[x_1]$.
   b) Using the rigorous tool compute a conservative enclosure for the gradients $[D_x \chi_{t_0}^{t_1}([x_0])]$.
   c) Let F be gradient in the middle of the computed bounds $F = \text{mid}\,[D_x \chi_{t_0}^{t_1}([x_0])]$. Compute the optimal deformation metric $\hat{M}_1(F)$, and its decomposition $\hat{A}_1(F)^T \hat{A}_1(F)$, as presented in Def. 1.
   d) If it holds that M_0-SF $> C_M \cdot \hat{M}_1$-SF, switch to new metric by setting $M_1 = \hat{M}_1$, use the analytical formulas for $\hat{A}_1(F)$, and $\hat{M}_1(F)$ defined in Def. 1. Otherwise just keep M_0, i.e. $M_1 = M_0$.
   e) Bound $M_{0,1}$-SF (12), and compute the discrete reachtube overestimate at t_1:

$$B_1 = B_{M_1}([x_1], \delta_1), \quad \text{Reach}((t_0, \mathcal{X}), t_1) \subset B_1.$$

4) *End improved LRT*
5) *Begin continuous part*
   a) Initialize $\Delta_0 = \delta_0 \cdot C_\delta$.
   b) By solving a nonlinear convex optimization problem, set $\tilde{\delta}$ to an approximate maximum of the left-hand side in (18), and consider $\hat{\Delta}_0 = \delta_0 + \tilde{\delta}$. Next, validate $\tilde{\delta}$ to become an upper bound for the global maximum of the left-hand side in (18) as follows:
      i) check the following SMT logic formula using dReal:

$$\exists_{x \in B_{M_0}(x_0, \hat{\Delta}_0)} \exists_{s \in [0,h]} \|h \cdot f(t_0 + s, x)\|_{M_0} > \hat{\Delta}_0 - \delta_0 = \tilde{\delta}.$$

      ii) If dReal returns UNSAT, $\tilde{\delta}$ is an upper bound for the global maximum. Otherwise, update $\tilde{\delta} = \tilde{\delta} \cdot C_\delta$ and $\hat{\Delta}_0 = \delta_0 + \tilde{\delta}$ and go to step i.
   c) Using the computed upper bound for maximum $\tilde{\delta}$ if Δ_0 satisfies $\Delta_0 \geq \hat{\Delta}_0 = \delta_0 + \tilde{\delta}_0$, the condition (18) holds, thus Δ_0 is the radius for the conservative continuous tube, i.e.,

$$\text{Reach}((t_0, B_{M_0}([x_0], \delta_0)), [t_0, t_1]) \subset B_{M_0}([x_0], \Delta_0).$$

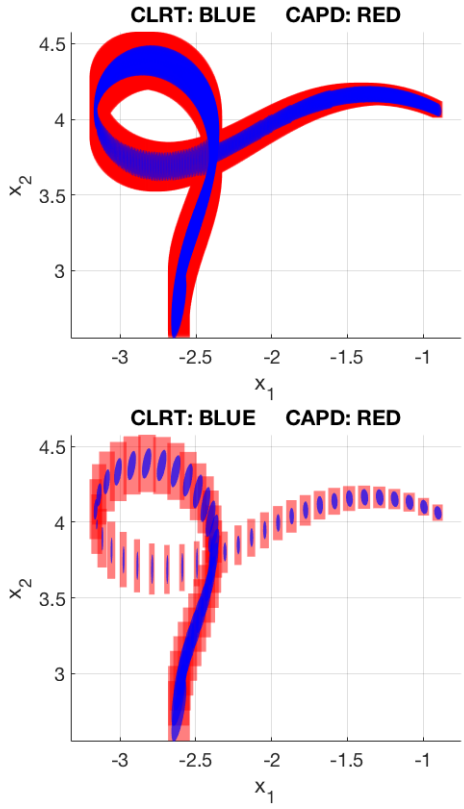

Fig. 4: Comparison of continuous-time reachtubes for Dubins car example with nonlinear steering function $x' = \cos\theta, y' = \sin\theta, \theta' = x \sin t$. See also Table I, row D3. Projection of computed bounds onto x, y is shown. Top figure presents all tube segments for times within $[5, 10]$, whereas figure on bottom shows one segment per 20 sequential segments computed by the algorithms. Set of initial states has center at $(0, 0, 0.7854)$ and radius 0.01.

Otherwise, update $\Delta_0 = \Delta_0 \cdot C_\delta$, and go to step (b).

6) *End continuous part*
7) Set the initial time to t_1, the bounds for the initial center of the ball to $[x_1]$, the current norm to M_1, the radius in M_1-norm to $\delta_1 = \Lambda \cdot \delta_0$, and the ball enclosure for the set of initial states to $B_{M_1}([x_1], \delta_1)$. Save $B_{M_0}([x_0], \Delta_0)$ as conservative over-estimate for $\text{Reach}((t_0, \mathcal{X}), [t_0, t_1])$.
8) If $t_1 \geq T$ terminate. Otherwise go back to 1.

End CLRT

Proposition 1: Assume that the rigorous tool used by LRT produces conservative gradient enclosures for (1), and that LRT terminates on the provided inputs. Let $[t_0, T]$ be the whole time interval, which is traversed by CLRT in k steps. Then, the output of the CLRT is a *conservative reachtube over-approximation of* (1) for all times in $[t_0, T]$; i.e., for $t_{k+1} = T$: $\text{Reach}((t_0, \mathcal{X}), [t_j, t_{j+1}]) \subset B_{M_j}([x_j], \Delta_j)$, for $j = 1, \ldots, k$

Proof: The proof follows from [4, Theorem LRT-Conservativity], Theorems 2 and 3, and the soundness of

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.

the ε-satisfiability algorithm. ■

CLRT is also an efficient algorithm. This follows from the use of IST to derive the proper time increments h, and the use of nonlinear COP to finding initial estimates $\hat{\Delta}_0$, which are passed to the ε-satisfiability algorithm.

VII. Implementation and Experimental Results

We implemented a prototype of CLRT in C++. Our implementation is based on interval arithmetic; i.e., all variables used in the algorithm are over intervals, and all computations performed are executed using interval arithmetic. The prototype runs the CLRT algorithm in two passes. In the first pass, conservative over-estimates for discrete segments of reachtube are generated using the LRT algorithm. In the second pass, we run the procedure for constructing continuous conservative over-estimates, in each time interval from the discrete ones. In the first pass, we also compute optimal norms by using the analytical formulas from Def. 1.

To compute an upper bound Λ for the square-root of the maximal eigenvalue of all symmetric matrices in some interval bounds, we implemented in C++ several algorithms [11], [15], [14] and used the tightest result available. Source code, numerical data, and readme file describing compilation procedure for LRT are available online [12].

Table I summarizes CLRT's performance on a set of benchmarks (see [4] for details). Fig. 4 presents a visual comparison of computed bounds for benchmark D(3).

TABLE I: Performance comparison CAPD. We use following labels: B(2)- Brusselator, I(2)- Inverse Van der Pol oscillator, D(3)- Dubins Car, F(2)- Forced Van der Pol oscillator, M(2)- Mitchell Schaeffer cardiac-cell model, R(4)- Robot arm, O(7)- Biology model, A(12)-Polynomial system (number in parenthese denotes dimension). T: time horizon, dt: time step, ID: initial diameter in each dimension, TV: total volume in time horizon, AV: average volume in each time step.

BM	T	ID	CLRT		CAPD	
			TV	AV	TV	AV
B(2)	10	0.02	**0.21**	**2.1e-4**	0.59	5.9e-4
I(2)	10	0.02	**0.13**	**6.6e-5**	0.15	7.4e-5
D(3)	10	0.02	**0.237**	**1.18e-4**	2.81	1.4e-3
M(2)	10	0.002	0.005	2.42e-5	**0.003**	**1.58e-6**
R(4)	10	0.02	**1.23**	**1.4e-12**	6.16	1.29e-10
O(7)	5	1e-4	6.59e-16	6.594e-19	**6.28e-20**	**6.28e-23**
P(12)	0.5	1e-4	**1.18e-34**	**1.18e-36**	6.47e-26	6.47e-26

VIII. Conclusions and Future Work

We presented CLRT, a new algorithm for computing tight conservative reachtubes for solution flows of nonlinear systems. CLRT synergistically combines a number of techniques, e.g. finite and infinitesimal strain theory, computation of tightest deformation metric using explicit analytical formulas, δ-satisfiability, and nonconvex optimization.

Future work includes distributing a C++ implementation of CLRT, and extending our approach to Hybrid dynamical systems and PDEs. Consider hybrid systems. A continuous reachtube over-estimate bounds the solutions set within each dynamical mode. To check for possible intersection with a guard region that could result in a jump to another mode, we will wrap ellipsoidal bounds provided by CLRT into polytopes. The tight overestimates that we construct are likely to avoid false-positive intersections of the solution flow with the guard, resulting in a well-performing procedure for bounding the solution set of hybrid dynamical systems.

References

[1] M. Capiński, J. Cyranka, Z. Galias, T. Kapela, M. Mrozek, P. Pilarczyk, D. Wilczak, P. Zgliczyński, and M. Żelawski. CAPD - computer assisted proofs in dynamics, a package for rigorous numerics, http://capd.ii.edu.pl/. Technical report, Jagiellonian University, Kraków, 2016.

[2] X. Chen, E. Abraham, and S. Sankaranarayanan. Taylor model flowpipe construction for non-linear hybrid systems. In *Proceedings of the 2012 IEEE 33rd Real-Time Systems Symposium*, RTSS '12, pages 183–192, Washington, DC, USA, 2012. IEEE Computer Society.

[3] X. Chen, E. Ábrahám, and S. Sankaranarayanan. *Flow*: An Analyzer for Non-linear Hybrid Systems*, pages 258–263. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[4] J. Cyranka, M. A. Islam, G. Byrne, P. Jones, S. A. Smolka, and R. Grosu. *Lagrangian Reachabililty*, pages 379–400. Springer International Publishing, Cham, 2017.

[5] A. Donzé. *Breach, A Toolbox for Verification and Parameter Synthesis of Hybrid Systems*, pages 167–170. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[6] A. Donzé and O. Maler. *Systematic Simulation Using Sensitivity Analysis*, pages 174–189. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[7] C. Fan, J. Kapinski, X. Jin, and S. Mitra. Locally optimal reach set over-approximation for nonlinear systems. In *Proceedings of the 13th International Conference on Embedded Software*, EMSOFT '16, pages 6:1–6:10, New York, NY, USA, 2016. ACM.

[8] C. Fan and S. Mitra. *Bounded Verification with On-the-Fly Discrepancy Computation*, pages 446–463. Springer International Publishing, Cham, 2015.

[9] S. Gao, J. Avigad, and E. M. Clarke. δ-complete decision procedures for satisfiability over the reals. In B. Gramlich, D. Miller, and U. Sattler, editors, *Automated Reasoning*, pages 286–300, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[10] S. Gao, S. Kong, and E. M. Clarke. dreal: An smt solver for nonlinear theories over the reals. In M. P. Bonacina, editor, *Automated Deduction – CADE-24*, pages 208–214, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[11] M. Hladík, D. Daney, and E. Tsigaridas. Bounds on real eigenvalues and singular values of interval matrices. *SIAM Journal on Matrix Analysis and Applications*, 31(4):2116–2129, 2010.

[12] M. A. Islam and J. Cyranka. CLRT implementation. `http://www.cs.cmu.edu/~mdarifui/clrt_source.zip`, 2018.

[13] J. Maidens and M. Arcak. Reachability analysis of nonlinear systems using matrix measures. *IEEE Transactions on Automatic Control*, 60(1):265–270, Jan 2015.

[14] J. Rohn. Bounds on eigenvalues of interval matrices. *ZAMMZ.Angew.Math.Mech.*, 78:1049–1050, 1998.

[15] S. M. Rump. Computational error bounds for multiple or nearly multiple eigenvalues. *Linear Algebra and its Applications*, 324(1):209 – 226, 2001. Linear Algebra in Self-Validating Methods.

[16] W. S. Slaughter. *The Linearized Theory of Elasticity*. Springer Science+Business Media, LLC, 2012.

[17] D. Wilczak and P. Zgliczyński. C^r-Lohner algorithm. *Schedae Informaticae*, 2011(Volume 20), 2012.

[18] P. Zgliczynski. C^1 Lohner Algorithm. *Foundations of Computational Mathematics*, 2(4):429–465, 2002.

Preprint submitted to 57th IEEE Conference on Decision and Control.
Received March 20, 2018.