15. Reach Set Computation Using Optimal Control

Pravin Varaiya*

Abstract

Reach set computation is a basic component of many verification and control synthesis procedures. Effective computation schemes are available for discrete systems described by finite state machines and continuous-variable systems described by linear differential inequalities. This paper suggests an approach based on the Pontryagin maximum principle of optimal control theory. The approach is elaborated for linear systems, and it may prove useful for more general continuous-variable systems.

1. Introduction

Consider a state machine $S = (X, U, T)$ where X is the finite set of states, U is the finite set of control values, and $T : X \times U \to X$ is the transition function: for $x \in X$ and $u \in U$, $x' = T(x, u)$ is the next state. A trajectory of S is a pair of sequences $x_0, \dots, x_t$ and $u_0, \dots, u_{t-1}$ such that $x_{i+1} = T(x_i, u_i)$. When it is unimportant to recall the control sequence, the sequence $x_0, \dots, x_t$ by itself is called a trajectory. For a set of initial states $X_0 \subset X$ and $t \geq 0$, the set of all states x for which there is a trajectory $x_0, \dots, x_t$ with $x_0 \in X_0$ and $x = x_t$ is called the *reach set* from X_0 at time t. This set is denoted $R(X_0, t)$. ($R(X_0, 0) = X_0$.)

Important properties of S can be cast in terms of properties of the reach set. Some controller synthesis problems can also be cast in this way. For example, one may want to synthesize a trajectory starting in X_0 and ending at time t in a specified target set X_t. For these reasons much work has been devoted to effective means of computing the reach set function $R(\cdot, \cdot)$. The reach set is a semi-group,

$$R(X_0, s + t) = R(R(X_0, s), t), \tag{1.1}$$

and so it can be computed recursively from the one-step function $R(\cdot, 1)$. The *reachable set* at time t,

$$\bar{R}(X_0, t) = \cup_{s \leq t} R(X_0, s),$$

* Research supported by the National Science Foundation Grant ECS9725148

M. K. Inan et al. (eds.), *Verification of Digital and Hybrid Systems*

is the set of states that can be reached within t and the reachable set

$$\bar{R}(X_0) = \cup_{t\geq 0}\bar{R}(X_0,t) = \cup_{t\geq 0}R(X_0,t),$$

is the set of states that can be reached at some time. $\bar{R}(X_0)$ is the smallest fixpoint ξ containing X_0 of the equation

$$f(\xi) = \xi \cup R(\xi, 1) = \xi,$$

and it too can be computed as the limit of the recursion

$$\xi_{i+1} = f(\xi_i),$$

starting at X_0. This recursion terminates in at most $|X|$ steps.

Consider now a system $S = (R^n, U, f)$, where R^n is the set of states, $U \subset R^n$ is the set of control values, and $f : R^n \times R^n \to R^n$ is the flow function. An initial state x_0 and a control function $u(s)$, $0 \leq s \leq t$, together yield the trajectory $x(\cdot)$ given by the solution of the differential equation

$$\dot{x}(s) = f(x(s), u(s)),\ 0 \leq s \leq t,\ x(0) = x_0. \tag{1.2}$$

For (1.2) to be well-defined, we require f to be Lipschitz, have linear growth (i.e. there exist constants k_1, k_2 such that $|f(x,u)| < k_1 + k_2|x|$ for all x, u), and the control function $u(\cdot)$ to be piecewise continuous (or measurable). We assume these conditions hold.

Define, as before, $R(X_0, t)$ to be the set of states reached at time t by trajectories starting in X_0. This reach set function also has the semigroup property (1.1). Similarly define the functions $\bar{R}(X_0, t)$ and $\bar{R}(X_0)$. Because time is dense and there are infinitely many states, there is no recursive way of computing the reach set function. In the case of finite state machines, the reach set is represented by enumeration. (Logical formulas like binary decision diagrams are used to obtain a more compact, symbolic representation.) For continuous-variable systems we need a symbolic representation for the reach set.

2. Convex Reach Set Function

A convex polyhedron has two convenient symbolic representations. One way is to represent it as the convex hull of its vertices: if $x^1, \ldots, x^k$ are the k vertices of a polyhedon X,

$$X = \{\sum_0^k \lambda_i x^i \mid \lambda_i \geq 0,\ \sum \lambda_i = 1\}.$$

Alternatively, a convex polyhedron can be represented as the intersection of (say) m half-spaces,

$$X = \bigcap_1^m \{x \mid \langle a_i, x\rangle \le \alpha_i\}.$$

(Above, $\langle x, y\rangle = \sum_i x_i y_i$ is the inner product of vectors x and y.)

Constant derivatives

In the special case of (1.2) where the right hand side does not depend on x,

$$\dot{x}(s) = u(s) \in U, \tag{2.1}$$

and U is convex, one has

$$R(X_0, t) = X_0 + tU. \tag{2.2}$$

(Here, if $\tau \in R$, and A, B are subsets of R^n, then $A+B = \{a+b \mid a \in A, b \in B\}$ and $\tau A = \{\tau a \mid a \in A\}$.)

In particular, if X_0 and U are convex polyhedra, so is $R(X_0, t)$. Moreover, if X_0 and U are represented by finitely many vertices (x^i and u^j) then the vertices of $R(X_0, t)$ are contained in the set $\{x^i + tu^j\}$ from which one can extract the subset of points that are indeed vertices. Similarly, if X_0 and U are represented as intersections of half-spaces $\{\langle a_i, x\rangle \le \alpha_i\}$ and $\{\langle b_j, u\rangle \le \beta_j\}$ then $R(X_0, t)$ can be represented as the intersection of a subset of half-spaces of the form $\langle c_k, x\rangle \le \gamma_k$, where $c_k = a_i$ or b_j.

These representations are used in [2] to compute reach sets of hybrid systems with flows of type (2.1). Note that although these flows are very simple, hybrid systems constructed out of them can approximate arbitrary systems of type (1.2), see [4].

Linear systems

Consider now the special case of (1.2) where the right hand side depends linearly on x,

$$\dot{x}(s) = Ax(s) + u(s), \tag{2.3}$$

where A is a $n \times n$ matrix and $u(s) \in U$. Suppose U is a convex, compact subset of R^n, and X_0 is also a convex, compact subset of R^n. Then $R(X_0, t)$ is also convex and compact. Convexity is immediate: if x_1, x_2 are trajectories corresponding to u_1 and u_2, $\lambda_1 x_1 + \lambda_2 x_2$ is the trajectory corresponding to $\lambda_1 u_1 + \lambda_2 u_2$. Compactness of $R(X_0, t)$ requires a limiting argument to show that it is a closed set. (It is a deep result that $R(X_0, t)$ is convex even if U is not convex.)[1]

The integral of a point-to-set function $F(s)$, $0 \le s \le t$, is defined as

[1] $\bar{R}(X_0, t)$ is convex in the case of constant derivatives (2.1), but not in the case of linear systems (2.3).

$$\int_0^t F(s)ds = \lim_{\Delta \to 0} \sum_{i=0}^{\lfloor t/\Delta \rfloor} \Delta F(i\Delta).$$

With this definition, $R(X_0, t)$ can be expressed in 'closed form' as

$$\begin{aligned} R(X_0, t) &= e^{tA}X_0 + \int_0^t e^{(t-s)A}Uds = e^{tA}X_0 + \int_0^t e^{sA}Uds \\ &= e^{tA}X_0 + \lim_{\Delta \to 0} \sum_0^{\lfloor t/\Delta \rfloor} \Delta e^{i\Delta A}U. \end{aligned} \quad (2.4)$$

Unlike (2.2), the system (2.3) creates a special difficulty in obtaining a symbolic representation of $R(X_0, t)$. Even if U is a convex polyhedron, the sum on the right in (2.4) need not be a polyhedron because it is of the form

$$\sum_i \Delta e^{i\Delta A}U.$$

The matrices $e^{i\Delta A}$ are different for each i, and so each $e^{i\Delta A}U$ can be a differently shaped polyhedron with the same number of vertices as U. Hence the sum can have as many as $\lfloor t/\Delta \rfloor \times |V(U)|$ vertices (where $V(U)$ is the set of vertices of U). In the limit (2.4) can be a smooth convex set, even if X_0 and U are polyhedra. Since arbitrary convex sets do not have a finite symbolic representation, we must use approximations in order to obtain a finite symbolic representation of the reach set (2.4). The following result indicates such an approximation.

Approximation of a convex set

Let F be a convex, compact set. We say that (c, γ) is a supporting hyperplane of F if

$$\gamma = \max\{\langle c, x\rangle \mid x \in F\},$$

and if $x^* \in \arg\max\{\langle c, x\rangle \mid x \in F\}$ we say that the hyperplane (c, γ) supports F at x^*. The definition is illustrated in Figure 2.1.

Let ∂F be the boundary of F. Then there is a hyperplane supporting F at a point iff that point is in ∂F. Hence if $x^1, \ldots, x^K$ are points in ∂F with supporting hyperplanes $(c_1, \gamma_1), \ldots, (c_K, \gamma_K)$, we have the inner and outer approximation,

$$co\{x^1, \ldots, x^K\} \subset F \subset \bigcap_i \{\langle c_i, x\rangle \leq \gamma_i\}. \quad (2.5)$$

(Here, $co\{x^1, \ldots, x^K\}$ denotes the convex hull of $\{x^1, \ldots, x^K\}$.) See Figure 2.2.

If F is a convex set in R^n then we need $K = O(\frac{1}{\delta^{n-1}})$ points in order to obtain approximations that are within δ of F, i.e.,

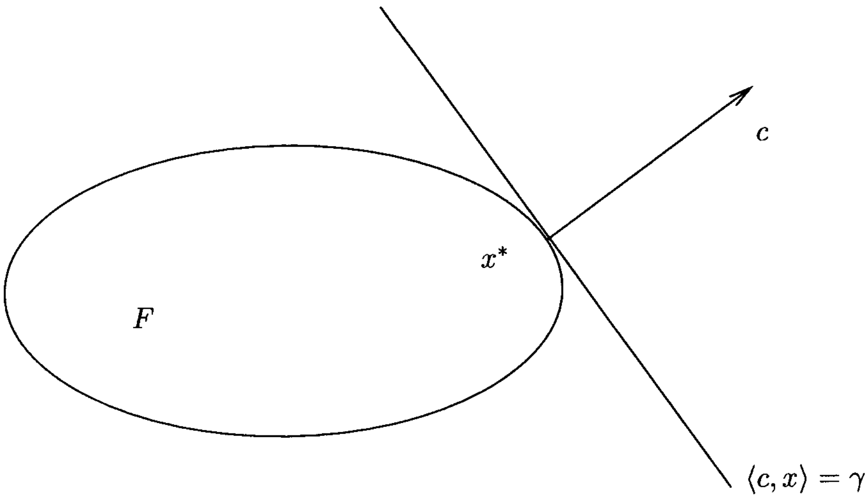

Fig. 2.1. The supporting hyperplane at x^*

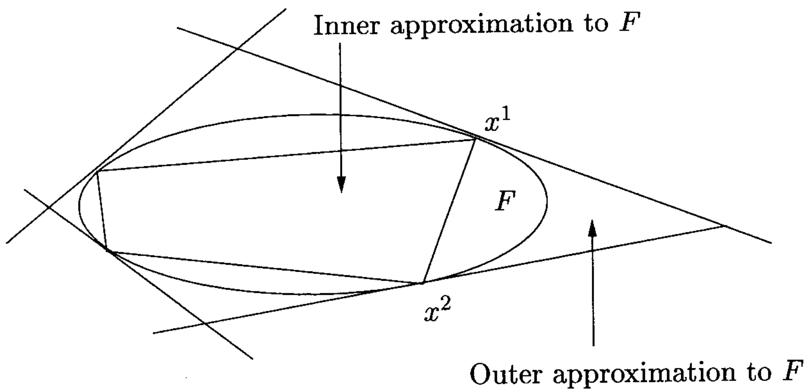

Fig. 2.2. Approximations to F

$$F \subset co\{x^1, \ldots, x^K\} + S_\delta, \ \bigcap_i \{\langle c_i, x\rangle \le \gamma_i\} \subset F + S_\delta.$$

(Here, S_δ is the sphere of radius δ.) We now introduce some results from optimal control.

3. Maximum principle

Consider again the linear system

$$\dot{x}(t) = Ax(s) + u(s), \ 0 \le s \le t, \tag{3.1}$$

with initial state in X_0 and $u(s) \in U$, both compact and convex. $R(X_0, s)$ is its reach set. Let (c_0, γ_0^*) be a supporting hyperplane to X_0 at x_0^*,

$$\langle c_0, x\rangle \le \gamma_0^* = \langle c_0, x_0^*\rangle, \ x \in X_0.$$

Let $x^*(s), \lambda^*(s), u^*(s), \ 0 \le s \le t$, be solutions to the following three equations,

$$\begin{aligned} \dot{x}^*(s) &= Ax^*(s) + u^*(s), \ x^*(0) = x_0^*, & (3.2)\\ \dot{\lambda}^*(s) &= -A^T\lambda^*(s), \ \lambda^*(0) = c_0, & (3.3)\\ u^*(s) &\in \arg\max\{\langle \lambda^*(s), Ax^*(s) + u\rangle \mid u \in U\}. & (3.4) \end{aligned}$$

Let $\gamma^*(s) = \langle \lambda^*(s), x^*(s)\rangle$.

Proposition 3.1 (Maximum principle). *$(\lambda^*(s), \gamma^*(s))$ is a supporting hyperplane to $R(X_0, s)$ at $x^*(s)$ for every s, $0 \le s \le t$.*

Proof. Let $x(\cdot), u(\cdot)$ be any solution of (3.1) with $x(0) \in X_0$ and $u(s) \in U$. Then

$$\begin{aligned} \frac{d}{ds}\langle \lambda^*(s), x(s)\rangle &= \langle \dot{\lambda}^*(s), x(s)\rangle + \langle \lambda^*(s), \dot{x}(s)\rangle \\ &= -\langle \lambda^*(s), Ax(s)\rangle + \langle \lambda^*(s), Ax(s) + u(s)\rangle, \text{ by (3.3, 3.1)} \\ &= \langle \lambda^*(s), u(s)\rangle \\ &\le \langle \lambda^*(s), u^*(s)\rangle, \text{ by (3.4)} \\ &= -\langle \lambda^*(s), Ax^*(s)\rangle + \langle \lambda^*(s), Ax^*(s) + u^*(s)\rangle \\ &= \frac{d}{ds}\langle \lambda^*(s), x^*(s)\rangle = \frac{d}{ds}\gamma^*(s). \end{aligned}$$

Combining this inequality with

$$\langle \lambda^*(0), x(0)\rangle \le \langle \lambda^*(0), x^*(0)\rangle = \gamma^*(0),$$

gives the following relation which yields the result,

$$\langle \lambda^*(s), x(s)\rangle \le \langle \lambda^*(s), x^*(s)\rangle = \gamma^*(s).$$

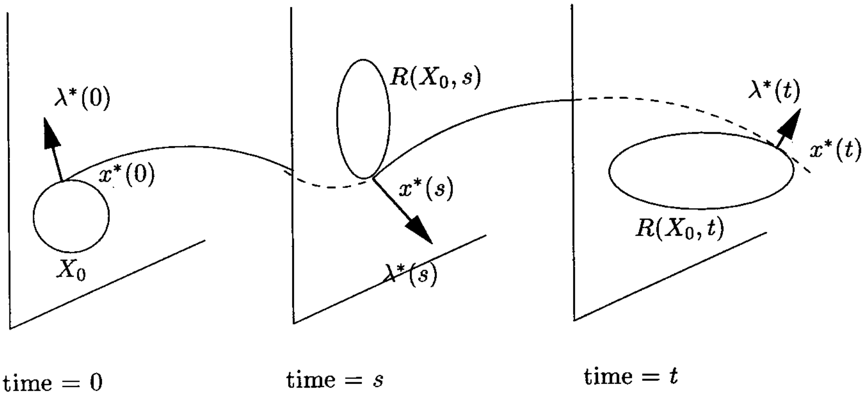

Fig. 3.1. Illustration of Maximum principle

The Maximum principle is illustrated in Figure 3.1. Combining the Maximum principle with the approximation (2.5) yields the following result:

Proposition 3.2. (Symbolic representation of reach set for linear systems). *Let (c_i, γ_i^*) be hyperplanes supporting X_0 at x_i^*, $i = 1, \ldots, K$. Let $x_i^*(s), \lambda_i^*(s), u_i^*(s)$, $0 \le s \le t$, be solutions to the following three equations,*

$$\begin{aligned} \dot{x}_i^*(s) &= Ax_i^*(s) + u_i^*(s), \;\; x^*(0) = x_i^*, && (3.5)\\ \dot{\lambda}_i^*(s) &= -A^T\lambda_i^*(s), \;\; \lambda_i^*(0) = c_i, && (3.6)\\ u_i^*(s) &\in \arg\max\{\langle \lambda_i^*(s), Ax_i^*(s) + u\rangle \mid u \in U\}. && (3.7) \end{aligned}$$

Let $\gamma_i^*(s) = \langle \lambda_i^*, x^*(s)\rangle$. Then

$$co\{x_1^*(s), \ldots, x_K^*(s)\} \subset R(X_0, s) \subset \bigcap_i \{\langle \lambda_i^*, x\rangle \le \gamma_i^*(s)\}. \qquad (3.8)$$

We briefly discuss the effort involved in computing this symbolic approximation. First, $K = O(\frac{1}{\delta^{n-1}})$ to achieve an approximation of order δ. Equation (3.6) has the 'closed form' solution

$$\lambda_i^*(s) = e^{-sA^T} c_i, \qquad (3.9)$$

so one needs to compute the matrix e^{-sA^T} for every s.

Next, the control functions u_i^* are obtained by solving

$$u_i^*(s) \in \arg\max\{\langle \lambda_i^*(s), u\rangle \mid u \in U\}.$$

If U is a polyhedron with finitely many vertices $V(U)$, then $u_i^*(s)$ is obtained by solving the finite problem

$$u_i^*(s) \in \arg\max\{\langle \lambda_i^*(s), u\rangle \mid u \in V(U)\}. \qquad (3.10)$$

Finally x_i^* is given by

$$x_i^*(s) = e^{sA}x_i^* + \int_0^s e^{(s-\tau)A}u_i^*(\tau)d\tau. \tag{3.11}$$

One way of solving (3.9) is by taking the Laplace transform of e^{-tA^T}. Inversion of the Laplace transform requires solving for the complex roots of the characteristic equation which are the eigenvalues of $-A^T$.

The u_i^* in (3.10) can be obtained via a dual representation. For each vertex v of U, there is a convex polyhedral cone $\Lambda(v)$ such that

$$v \in \arg\max\{\langle\lambda, u\rangle \mid u \in U\} \text{ iff } \lambda \in \Lambda(v).$$

The cones $\Lambda(v)$ are expressed in terms of linear inequalities which can be computed from $V(U)$. Combining this with (3.9) allows one to rewrite (3.10) as

$$u_i^*(s) = v \text{ if } e^{-sA^T}c_i \in \Lambda(v),$$

the solution (in s) of which requires solving linear inequalities in $e^{\xi s}$ where the ξ are eigenvalues of $-A^T$.

4. Concluding remarks

The inclusion (3.8) is tight in that we cannot find a polyhedron with K vertices that can be squeezed between the first and the second set or an intersection of K half spaces that can be squeezed between the second and third set.

The symbolic representation offered here is in a certain sense minimal. Let $\lambda^*(0)$ range over the unit sphere in R^n. Suppose X_0 has a smooth boundary, then $R(X_0, t)$ also has smooth boundary. These boundaries are $(n-1)$-dimensional manifolds, as is the unit sphere in R^n.

Let $x^*(\lambda^*(0))$ be the unique maximizer of $\langle\lambda^*(0), x\rangle$ over X_0 and let $\gamma^*(\lambda^*(0))$ be the maximum value. Let $x^*(s, \lambda^*(0))$, $u^*(s, \lambda^*(0))$, $\lambda^*(s, \lambda^*(0))$ and $\gamma^*(s, \lambda^*(0))$ be the corresponding solutions of (3.5)-(3.7).

Then $\lambda^*(0) \mapsto x^*(s, \lambda^*(0))$ is a parametrization of the boundary of $R(X_0, s)$; and $\lambda^*(0) \mapsto (\lambda^*(s, \lambda^*(0)), \gamma^*(s, \lambda^*(0))$ is a parametrization of the hyperplanes that support $R(X_0, s)$.

Second, instead of approximating via polyhedra, there is a recent theory that carries out approximations via ellipsoids, see [3]. That theory (as well as the polyhedral approximations) extends to much more difficult 'game' problems.

Lastly, the Maximum principle extends to nonlinear systems,

$$\dot{x}s = f(x(s), u(s)),$$

and it could be used to 'compute' the reach set along the lines suggested here [1].

References

1. L.S. Pontryagin et al. *The mathematical theory of optimal processes.* Macmillan, 1964.
2. T.A. Henzinger and P.-H. Ho. Hytech: The cornell hybrid technology tool. In *Hybrid Systems II*, pages 265–294. LNCS 999, Springer, 1995.
3. A.B. Kurzhanski and I. Valyi. *Ellipsoidal calculus for estimation and control.* Birkhauser, 1996.
4. A. Puri, V. Borkar, and P. Varaiya. ϵ-approximation of differential inclusions. In *Proceedings of the 34th Conference on Decision and Control*, 1995.