dReach: δ-Reachability Analysis for Hybrid Systems

Soonho Kong, Sicun Gao, Wei Chen, and Edmund Clarke

Computer Science Department, Carnegie Mellon University, USA

Abstract. dReach is a bounded reachability analysis tool for nonlinear hybrid systems. It encodes reachability problems of hybrid systems to first-order formulas over real numbers, which are solved by delta-decision procedures in the SMT solver dReal. In this way, dReach is able to handle a wide range of highly nonlinear hybrid systems. It has scaled well on various realistic models from biomedical and robotics applications.

1 Introduction

dReach is a bounded reachability analysis tool for hybrid systems. It encodes bounded reachability problems of hybrid systems as first-order formulas over the real numbers, and solves them using δ-decision procedures in the SMT solver dReal [12]. dReach is able to handle a wide range of highly nonlinear hybrid systems [16,13,15,3]. Figure 1 highlights some of its features: on the left is an example of some nonlinear dynamics that dReach can handle, and on the right a visualized counterexample generated by dReach on this model.

It is well-known that the standard bounded reachability problems for simple hybrid systems are already highly undecidable [2]. Instead, we work in the framework of δ-reachability of hybrid systems [10]. Here δ is an arbitrary positive rational number, provided by the user to specify the bound on numerical errors that can be tolerated in the analysis. For a hybrid system H and an unsafe region unsafe (both encoded as logic formulas), the δ-reachability problem asks for one of the following answers:

- safe: H cannot reach unsafe.
- δ-unsafe: H^δ can reach unsafe$^\delta$.

Here, H^δ and unsafe$^\delta$ encode (δ-bounded) overapproximations of H and unsafe, defined explicitly as their syntactic variants.It is important to note that the definition makes the answers no weaker than standard reachability: When safe is the answer, we know for certain that H does not reach the unsafe region (no δ is involved); when δ-unsafe is the answer, we know that there exists some δ-bounded perturbation of the system that can render it unsafe. Since δ can be chosen to be very small, δ-unsafe answers in fact discover robustness problem in the system, which should be regarded as unsafe indeed. We have proved that bounded δ-reachabilty is decidable for a wide range of nonlinear hybrid systems, even

C. Baier and C. Tinelli (Eds.): TACAS 2015, LNCS 9035, pp. 200–205, 2015.
DOI: 10.1007/978-3-662-46681-0_15

$$\frac{dx}{dt} = \left(\alpha_x\left(k_1 + \frac{(1-k_1)z}{z+k_2}\right) - \beta_x\left(k_3 + \frac{(1-k_3)z}{z+k_4}\right) - m_1\left(1 - \frac{z}{z_0}\right)\right)x$$

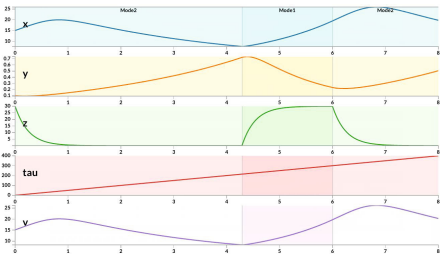
$$\frac{dy}{dt} = m_1\left(1 - \frac{z}{z_0}\right)x + \left(\alpha_y\left(1 - d\,\frac{z}{z_0}\right) - \beta_y\right)y$$

$$\frac{dz}{dt} = \frac{z_0 - z}{\tau}$$

$$\frac{dv}{dt} = \left(\alpha_x\left(k_1 + \frac{(1-k_1)z}{z+k_2}\right) - \beta_x\left(k_3 + \frac{(1-k_3)z}{z+k_4}\right) - m_1\left(1 - \frac{z}{z_0}\right)\right)x$$

$$+ m_1\left(1 - \frac{z}{z_0}\right)x + \left(\alpha_y\left(1 - d\,\frac{z}{z_0}\right) - \beta_y\right)y$$

(a) An example of nonlinear hybrid system model: off-treatment mode of the prostate cancer treatment model [16]



(b) Visualization of a generated counterexample. Change in the shade of colors represents discrete mode changes.

Fig. 1. An example of nonlinear dynamics and counterexample-generation

with reasonable complexity bounds [10]. This framework provides the formal correctness guarantees of dReach.

Apart from solving δ-reachability, the following key features of dReach distinguish it from other existing tools in this domain [7,9,1,8,14,5,6].

1. Expressiveness. dReach allows the user to describe hybrid systems using first-order logic formulas over real numbers with a wide range of nonlinear functions. This allows the user to specify the continuous flows using highly nonlinear differential equations, and the jump and reset conditions with complex Boolean combinations of nonlinear constraints. dReach also faithfully translates mode invariants into $\exists\forall$ logic formulas, which can be directly solved under certain restrictions on the invariants.
2. Property-guided search. dReach maintains logical encodings (the same approach as [6]), whose size is linear in the size of the inputs, of the reachable states of a hybrid system [10]. The tool searches for concrete counterexamples to falsify the reachability properties, instead of overapproximating the full reachable states. This avoids the usual state explosion problem in reachable set computation, because the full set of states does not need to be explicitly stored. This change is analogous to the difference between SAT-based model checking and BDD-based symbolic model checking.
3. Tight integration of symbolic reasoning and numerical solving. dReach delegates the reasoning on discrete mode changes to SAT solvers, and uses numerical constraint solving to handle nonlinear dynamics. As a result, it can combine the full power of both symbolic reasoning and numerical analysis algorithms. In particular, all existing tools for reachable set computation can be easily plugged-in as engines for solving the continuous part of the dynamics, while logic reasoning tools can overcome the difficulty in handling complex mode transitions.

The paper is structured as follows. We describe the system architecture in Section 2, and give some details about the logical encoding in the tool in Section 3. We then explain the input format and usage in Section 4.

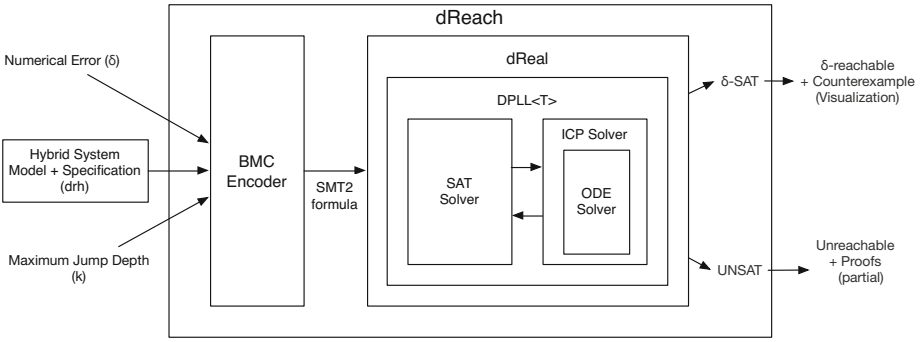


Fig. 2. Architecture of dReach: It consists of an bounded model-checking module and an SMT solver, dReal. In the first phase, the Encoder module translates an input hybrid system into a logic formula. In the second phase, an SMT solver, dReal, solves the encoded δ-reachability problem using a solving framework that combines DPLL(T), Interval Constraint Propagation, and reliable (interval-based) numerical integration.

2 System Description

The system architecture of dReach is given in Figure 2. We ask the user to provide the following input file and two parameters:

- The input file specifies the hybrid system, the reachability properties in question, and some time bounds on the continuous flow in each mode. The grammar is described in Section 4.1.
- A bound on the number of mode changes.
- A numerical error bound δ.

From these inputs, dReach generates a logical encoding that involves existential quantification and universal quantification on the time variables. The logical encoding is compact, always linear in the size of the inputs. The tool then makes iterative calls to the underlying solver dReal [12] to decide the reachability properties. When the answer is δ-reachable, dReach generates a counterexample and its visualization. When the answer is unreachable, no numerical error is involved and a (partial, for now) logical proof of unsatisfiability can be provided [11].

3 Logical Encoding of Reachability

The details of our encoding scheme is given in [10]. Here we focus on explaining how differential equations and the universal quantifications generated by mode invariants are encoded, as an extension of the SMT-LIB [4] standard. Although such formulas are automatically generated by dReach from the hybrid system descrpition, the explanation below can be helpful for understanding the inner mechanism of our solver.

Encoding Integrations. In each mode of a hybrid system, we need to specify continuous flows defined by systems of ordinary differential equations. We extend SMT-LIB with a command `define-ode` to define such systems. For instance, we use `define-ode` as follows to assign a name flow_1 to a group of ODE, $\frac{\mathrm{d}x}{\mathrm{d}t} = v$ and $\frac{\mathrm{d}v}{\mathrm{d}t} = -x^2$.

```
(define-ode flow1 ((= d/dt[x] v) (= d/dt[v] (- 0 (^ x 2)))))
```

We then allow integration terms in the formula. We view the solution of system of differential equations as a constraint between the initial-state variables, time duration, and the end-state variables. We can then write

```
(= [x_t_1 ... x_t_n] (integral 0 t [x_0_1 ... x_0_n] flow_i)),
```

to represent $\boldsymbol{x} = \boldsymbol{x}_0 + \int_0^t \mathit{flow}_i(\boldsymbol{x}(s))\mathrm{d}s$. Note that we do not need to explicitly mention $\boldsymbol{x}(s)$ as a function in the encoding, which can be inferred by the solver.

Universal Quantification for Mode Invariant Constriants. To encode mode invariants in hybrid systems, we need $\exists\forall^t$-formulas [13] which is a restricted form of $\exists\forall$ formula where the universal quantifications are limited to the time variables. In dReach, we introduce a new keyword `forall_t` to encode $\exists\forall^t$ formulas. Given a time bound $[0, time_i]$, mode invariant f at mode n is encoded into `(forall_t n [0 time_i] f)`.

4 Using dReach

4.1 Input Format

The input format for describing hybrid systems and reachability properties consists of five sections: macro definitions, variable declarations, mode definitions, and initial condition, and goals. We focus on intuitive explanations here. Figure 3 shows how to describe a small example hybrid system, an inelastic bouncing ball with air resistance.

- In macro definitions, we allows users to define macros in C preprocessor style which can be used in the following sections. Macro expansions occur before the other parts are processed.
- A variable declaration specifies a real variable and its domain in a real interval. dReach requires special declaration for *time* variable, to specify the upperbound of time duration.
- A mode definition consists of mode id, mode invariant, flow, and jump. *id* is a unique positive interger assigned to a mode. An invariant is a conjuction of logic formulae which must always hold in a mode. A flow describes the continuous dynamics of a mode by providing a set of ODEs. The first formula of *jump* is interpreted as a guard, a logic formula specifying a condition to make a transition. Note that this allows a transition but does not force it. The second argument of *jump*, n denotes the target mode-id. The last one is *reset*, a logic formula connecting the old and new values for the transition.

```
1   #define D 0.45
2   #define K 0.9
3   [0, 15] x; [9.8] g; [-18, 18] v; [0, 3] time;
4   {   mode 1;
5       invt: (v <= 0);  (x >= 0);
6       flow: d/dt[x] = v; d/dt[v] = -g - (D * v ^ 2);
7       jump: (x = 0) ==> @2 (and (x' = x) (v' = - K * v)); }
8   {   mode 2;
9       invt: (v >= 0); (x >= 0);
10      flow: d/dt[x] = v; d/dt[v] = -g + (D * v ^ 2);
11      jump: (v = 0) ==> @1 (and (x' = x) (v' = v)); }
12  init: @1 (and (x >= 5) (v = 0));
13  goal: @1 (and (x >= 0.45));
```

Fig. 3. An example of drh format: Inelastic bouncing ball with air resistance. Lines 1 and 2 define a drag coefficient $D = 0.45$ and an elastic coefficient $K = 0.9$. Line 3 declares variables x, g, v, and *time*. At lines 4 - 7 and 8 - 11, we define two modes – the falling and the bouncing-back modes respectively. At line 12, we specify the hybrid system to start at mode 1 (`@1`) with initial condition satisfying $x \geq 5 \wedge v = 0$. At line 13, it asks whether we can have a trajectory ending at mode 1 (`@1`) while the height of the ball is higher than 0.45.

– *initial-condition* specifies the initial mode of a hybrid system and its initial configuration. *goal* shares the same syntactic structure of *initial-condition*.

4.2 Command Line Options

dReach follows the standard unix command-line usage:

```
dReach <options> <drh file>
```

It has the following options:

– If `-k <N>` is used, set the unrolling bound k as N (Default: 3). It also provides `-u <N>` and `-l <N>` options to specify upper- and lower-bounds of unrolling bound.
– If `--precision <p>` is used, use precision p (Default: 0.001).
– If `--visualize` is set, dReach generates extra visualization data.

We have a web-based visualization toolkit[1] which processes the generated visualization data and shows the counterexample trajectory. It provides a way to navigate and zoom-in/out trajectories which helps understand and debug the target hybrid system better.

[1] The detailed instructions are available at `https://github.com/dreal/dreal/blob/master/doc/ode-visualization.md`

References

1. Althoff, M., Krogh, B.H.: Reachability analysis of nonlinear differential-algebraic systems. IEEE Trans. Automat. Contr. 59(2), 371–383 (2014)
2. Alur, R., Courcoubetis, C., Henzinger, T.A., Ho, P.-H.: Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In: Grossman, R.L., Ravn, A.P., Rischel, H., Nerode, A. (eds.) HS 1991 and HS 1992. LNCS, vol. 736, pp. 209–229. Springer, Heidelberg (1993)
3. Asad, H.U., Jones, K.D., Surre, F.: Verifying robust frequency domain properties of non linear oscillators using SMT. In: 17th International Symposium on Design and Diagnostics of Electronic Circuits Systems, pp. 306–309 (April 2014)
4. Barrett, C., Stump, A., Tinelli, C.: The SMT-LIB Standard: Version 2.0. In: Gupta, A., Kroening, D. (eds.) Proceedings of the 8th International Workshop on Satisfiability Modulo Theories, Edinburgh, UK (2010)
5. Chen, X., Ábrahám, E., Sankaranarayanan, S.: Taylor model flowpipe construction for non-linear hybrid systems. In: RTSS, pp. 183–192 (2012)
6. Cimatti, A., Mover, S., Tonetta, S.: Smt-based verification of hybrid systems. In: Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, Toronto, Ontario, Canada, July 22-26 (2012)
7. Fränzle, M., Teige, T., Eggers, A.: Engineering constraint solvers for automatic analysis of probabilistic hybrid automata. J. Log. Algebr. Program. 79(7), 436–466 (2010)
8. Frehse, G.: PHAVer: Algorithmic verification of hybrid systems past hyTech. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 258–273. Springer, Heidelberg (2005)
9. Frehse, G., Le Guernic, C., Donzé, A., Cotton, S., Ray, R., Lebeltel, O., Ripado, R., Girard, A., Dang, T., Maler, O.: SpaceEx: Scalable verification of hybrid systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) CAV 2011. LNCS, vol. 6806, pp. 379–395. Springer, Heidelberg (2011)
10. Gao, S., Kong, S., Chen, W., Clarke, E.M.: Delta-complete analysis for bounded reachability of hybrid systems. CoRR, abs/1404.7171 (2014)
11. Gao, S., Kong, S., Clarke, E.: Proof generation from delta-decisions. In: SYNASC (2014)
12. Gao, S., Kong, S., Clarke, E.M.: dReal: An SMT solver for nonlinear theories over the reals. In: CADE, pp. 208–214 (2013)
13. Gao, S., Kong, S., Clarke, E.M.: Satisfiability modulo ODEs. In: FMCAD, pp. 105–112 (2013)
14. Herde, C., Eggers, A., Fränzle, M., Teige, T.: Analysis of hybrid systems using hysat. In: ICONS, pp. 196–201 (2008)
15. Kapinski, J., Deshmukh, J.V., Sankaranarayanan, S., Arechiga, N.: Simulation-guided lyapunov analysis for hybrid dynamical systems. In: HSCC 2014, Berlin, Germany, April 15-17, pp. 133–142 (2014)
16. Liu, B., Kong, S., Gao, S., Zuliani, P., Clarke, E.: Parameter identification using delta-decisions for biological hybrid systems. In: CMSB (2014)