Towards Formal Verification Methods for Robotic Lower-Limb Prostheses and Orthoses

Robert D. Gregg[*]
Departments of Mechanical Engineering and Bioengineering
University of Texas at Dallas
rgregg@utdallas.edu

Ufuk Topcu
Department of Electrical and Systems Engineering
University of Pennsylvania
utopcu@seas.upenn.edu

ABSTRACT

Populations including lower-limb amputees, stroke survivors, and the elderly have an increased risk for falls, which significantly limits mobility and quality of life. Recently developed robotic prostheses and orthoses are capable of actively assisting mobility in these populations. New risk management and design control tools are needed to meet the evolving regulatory demands for these increasingly complex systems, which can impart large torques and forces that could potentially harm the user. This paper attempts to introduce formal verification methods to this rapidly developing field by discussing some topical problems, the motivating example of a prosthetic leg, and potential verification metrics that could be used to certify the safety of these robotic medical devices in a pragmatic and cost-effective manner.

1. INTRODUCTION

There are nearly a million lower-limb amputees and even more stroke survivors in the US today, and the incidences of amputation and stroke are expected to increase two-fold by 2050 [2, 13]. Both populations experience frequent falls, which significantly limits mobility and social activity [20]. Falls and the fear of falling also affect the elderly, as falls account for 70 percent of accidental deaths in persons aged 75 years and older [6].

Assistive devices could prevent falls, increase mobility, and consequently improve quality of life in these populations, so the safety of these devices is of the utmost importance. Most prosthetic and orthotic (i.e., exoskeletal) devices are purely passive and limited in their ability to assist. For this reason these devices are considered low risk by the U.S. Food and Drug Administration (FDA), being classified as Class I or II Exempt and therefore not subject to pre-market approval [22]. However, the recent advent of mechanically powered prosthetic legs [33] (e.g., Fig. 1, left) and orthoses [28] presents new assistive capabilities as well as new dangers in how they are controlled. The risk management tools used for decades by manufacturers of conventional passive devices may not be feasible or sufficient for complex robotic devices, which can impart large torques or forces that could destabilize and harm the user.

A key difficulty in establishing assurance for this new generation of medical robots is mainly due to their high degrees of freedom, the large number of modes in which they may operate, and their interactions with patients in unanticipated ways. These relatively unconventional features will likely render the conventional means for building trust—essentially exhaustive physical testing—unaffordable and perhaps impractical. Therefore, there is a need for new mechanisms to limit the cost and time spent for developing new medical devices and for their assurance. In this paper, as a step toward a model-based verification methodology for medical robots, we discuss the use of nonlinear robustness and safety metrics for establishing insights about a robot's behavior under perturbations from nominal operating conditions and external disturbances in the presence of certain types of modeling uncertainties.

The medical community has been slow to adopt model-based simulation and development methods over the past 50 years for a variety of reasons including skepticism [27]. Concerns regarding realism and validity are the primary source of this skepticism in the context of medical education [3]. Given this skepticism, we believe that a pragmatic objective for model-based development and verification methods is to become a design aid and a guide for potentially lowering testing costs related to risk management. For example, a design effort, which maintains mathematically-based models and specifications from the early stages of design, may be able to explore a larger set of options (e.g., to identify the hazardous situations) before the costly testing of the physical system/device takes place. Furthermore, the results from verification may help identify the "corner" cases for further testing (or high-fidelity simulations) that are likely to generate informative insights compared to arbitrary testing.

The rest of the paper is organized as follows. Section 2 discusses a number of applications related to medical robots that provide topical problems in which the use of model-based verification may be effective. Section 3 provides further details using an example prosthetic leg model. Section 4 introduces several verification metrics and Section 5 dis-

[*] Robert De Moss Gregg, IV, Ph.D., holds a Career Award at the Scientific Interface from the Burroughs Wellcome Fund.

cusses a procedure for approximately computing these metrics for a family of system models. Section 6 gives a simple example of the application of the metrics and tools to a problem motivated by the applications discussed in the earlier sections. We conclude with remarks on limitations, open issues and possible future directions. The technical content in this paper partly draws from our earlier publications as cited whenever necessary.

2. TOPICAL PROBLEMS

Robotic prostheses and orthoses have the potential to significantly improve the quality of life for lower-limb amputees and stroke survivors, who frequently experience falls during everyday tasks such as standing, sit-to-stand, and walking. Therefore, balance assistance—specifically the prevention of falls—is a topical application of formal verification methods.

In the case of stationary standing, the goal of an assistive device is to keep the subject upright, i.e., stabilize the equilibrium point associated with a vertical posture. The subject may add unactuated degree(s) of freedom to this control problem, e.g., an ankle-foot orthosis [29] cannot apply control torques at the hip or knee. The control behavior of the subject can be considered a disturbance in the dynamical model of the assistive device, and the mass/inertia properties of the subject can be considered parametric uncertainty in this model. This class of dynamical systems will be defined with safety metrics in Section 4, and a toy example of balance assistance during standing will be presented in Section 6.

Sit-to-stand tasks, such as standing up from the toilet, are difficult without the power-generating capability of an intact biological leg, especially for geriatric patients. A robotic device assists this task by driving the system state from a sitting equilibrium point to a standing equilibrium point. A control strategy could be certified as safe if an invariant subset of the region of attraction (formally defined in Section 4) about the sit-to-stand trajectory was found. Alternatively one could certify safety by finding an invariant subset including the two equilibrium points that is disjoint from the fall region.

Locomotion is a rhythmic task corresponding to a periodic limit cycle [43] that must be stabilized by an assistive device. A wide variety of control strategies have been proposed for this purpose; most discretize the gait cycle into multiple distinct control models, each tracking reference joint torques [4], kinematics (angles/velocities [11, 23]), or impedances (stiffness/viscosity [32, 33]) that resemble human behavior. The only strategy that has been formally analyzed for stability is a recently developed controller [8–10] for the Vanderbilt leg (Fig. 1, left), and even that was done in a numerical fashion without any consideration for safety regions. Equally diverse strategies for powered orthoses [1,28] also lack formal safety analysis, although performance was simulated in [14] and stability was numerically verified in [7].

Assistive wearable robots could be made safer in these tasks if formal verification methods were employed in the control design and certification. We now present a motivating example model of a prosthetic leg to provide context for possible verification metrics.

3. EXAMPLE: PROSTHETIC LEG MODEL

The prosthetic leg of Fig. 1 (left) is modeled as a kinematic chain attached to the human body (Fig. 1, right) as in [8]. The configuration of the leg is given by $q = (q_x, q_z, \phi, \theta_{\mathrm{a}}, \theta_{\mathrm{k}})^T$, where q_x, q_z are the Cartesian coordinates of the heel, ϕ is the foot orientation defined with respect to vertical, θ_{a} is the ankle angle, and θ_{k} is the knee angle. The dynamical system's state is given by vector $x = (q^T, \dot{q}^T)^T$, where $\dot{q}$ contains the joint velocities. The state trajectory evolves according to a differential equation of the form

$$M(q)\ddot{q} + C(q,\dot{q})\dot{q} + G(q) + A^T(q)\lambda \quad = \quad \tau \qquad (1)$$

where M is the inertia/mass matrix, C is the matrix of Coriolis/centrifugal terms, G is the vector of gravitational torques, A is the constraint vector for the rocker foot (modeling inherent foot compliance), and λ is the Lagrange multiplier consisting of forces from the physical foot constraint. The vector of external forces $\tau = Bu + J^T(q)F$ is composed of actuator torques and interaction forces with the body, respectively. The Jacobian matrix J maps interaction forces to torques at the joints of the prosthesis. Ankle and knee actuation is provided by torque input u and mapped into the leg's coordinate system by $B = (0_{2\times 3}, I_{2\times 2})^T$.

Depending on the task at hand, the goal of the control torques may be to stabilize an equilibrium point corresponding to an upright posture, a trajectory corresponding to a sit-to-stand motion, or a limit cycle corresponding to rhythmic locomotion. For example, this prosthesis model was used in [9] to derive an input-output linearizing controller for walking. We now show how this model fits into the class of dynamical systems that can be analyzed using a number of verification metrics (introduced in Section 4) and associated computational tools (discussed in Section 5).

4. SOME VERIFICATION METRICS

Consider the dynamical system whose evolution is governed by the ordinary differential equation

$$\dot{x}(t) = f(x(t), w(t); \delta), \qquad (2)$$

where $x(t) \in \mathbb{R}^n$ and $w(t) \in \mathbb{R}^m$ are the state vector and the disturbance input (e.g., from interaction forces), respectively, at time t, and δ characterizes the parametric uncertainties in the model (e.g., from the human body) and takes values in the bounded set $\Delta \subseteq \mathbb{R}^p$. The map f is assumed to satisfy certain smoothness conditions, e.g., smooth enough that solutions to (2) exist and are unique. For simplicity we consider the model in (2); the concepts and results stated in the following have natural and straightforward extensions to, for example, hybrid systems [25] and more general uncertainty models [40], which may be more suitable for some of the applications discussed in Section 2.

The model in (2) does not include any control inputs. It should be considered as the closed-loop dynamics with a feedback controller already designed by other means. The verification metrics we discuss here characterize the robustness and safety of these closed-loop dynamics in the presence of perturbations from the nominal operating conditions and external disturbances along with modeling uncertainties.

Let us first consider the behavior of (2) due to initial condition perturbations around its nominal operating condition,

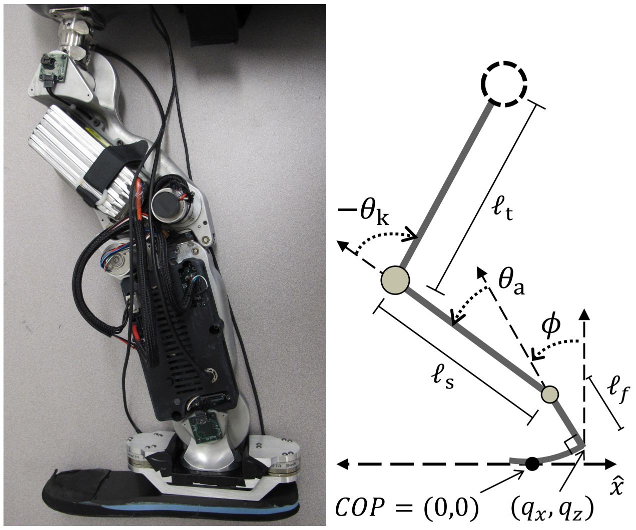

Figure 1: Left: The Vanderbilt leg, a powered knee-ankle prosthesis designed at Vanderbilt University [33] and used in the control validation experiments of [8]. Right: kinematic model of transfemoral prosthetic leg attached to human subject's hip (shown as a dashed circle) from [8]. The origin of the global reference frame is modeled at the center of pressure (COP)—the point on the foot where the resultant reaction force is imparted against the ground. This model was used to design and simulate a prosthetic control strategy in [9].

characterized as one of its equilibria, with no external disturbances (i.e., $w \equiv 0$). With no loss of generality, assume that the equilibrium of interest is at $x = 0$. For simplicity assume that $f(0, 0; \delta) = 0$ for all $\delta \in \Delta$, i.e., $x = 0$ is an equilibrium for all admissible parametric uncertainties.[1] Let $\varphi(\xi, t; \delta)$ denote the solution to (2) with the initial condition $x(0) = \xi$. Then, the region of attraction (ROA)

$$\left\{ \xi \in \mathbb{R}^n \ : \ \varphi(\xi, t; \delta) \xrightarrow{t \to \infty} 0 \text{ for all } \delta \in \Delta \right\}$$

of the origin is the set of all states from which the system converges to the origin. The ROA can be considered as the set of perturbations from which the systems is capable of recovering to its nominal operation conditions.

The ROA characterizes the system's capability to recover from perturbations in the state space without any connection to the source of those perturbations. To this end, we now look at the behavior of the dynamics in (2) under external disturbances, which may drive the system from its nominal operating condition. Let the disturbance input signal $w(\cdot)$ take values over the set $\mathcal{W}$, which is the set of all admissible disturbances and may be established based on prior knowledge on the type and extent of the disturbances the system may be subject to. For example, depending on the particular application of interest, the designer may know that the magnitude of the disturbance cannot exceed a certain level at any time or it can only a have bounded energy content. Alternatively, the designer may ask "what-if" questions, e.g., "what would be the largest perturbations that can occur if the disturbances were bounded in a certain manner," and based on the evidence established from such analysis, design the rest of the system to guarantee that the disturbances respect the hypothesis.

Let $\varphi(\xi, t, w; \delta)$ denote the solution to (2) at time t with the initial condition ξ driven by the disturbance w. Assume that $f(0, 0; \delta) = 0$ for all $\delta \in \Delta$. The set of points reachable from the origin under the dynamics in (2), provided that the disturbance signal w comes from a prespecified set $\mathcal{W}$ of signals, is defined as

$$\{\varphi(0, T, w; \delta) \in \mathbb{R}^n \ : \ T \geq 0, w \in \mathcal{W}, \delta \in \Delta\}. \qquad (3)$$

Take the following scenario as an example of the potential uses of estimates of the ROA and the set of reachable points. Consider that the system initially operates at its nominal operating condition (characterized as the equilibrium at the origin) and a disturbance signal (say, from a set $\mathcal{W}$), which acts for a bounded time period (beginning at time $t = 0$), drives the system from this nominal operating condition and then vanishes. Denote an upper bound on the reachable set defined in (3) by $\Omega_{reach,\mathcal{W}}$. If we can establish an invariant subset of the ROA (for the unforced dynamics) that contains the set $\Omega_{reach,\mathcal{W}}$, then we can guarantee that the system will recover from the effects of such disturbances without the (perhaps impractical) need for simulating the system for all admissible disturbances and modeling uncertainties.

The verification metrics considered so far are concerned with the behavior around an equilibrium point. We now introduce two additional concepts that capture the transient behavior of the system. The first one is a slight generalization of reachability, adapted from [25]. Namely, given a state set $\mathcal{X} \subseteq \mathbb{R}^n$, a set $\mathcal{X}_0 \subseteq \mathcal{X}$ of possible initial states, a target set $\mathcal{X}_r \subseteq \mathcal{X}$, we say that the reachability property holds for the system in (2), if there exist a finite time $T \geq 0$, admissible disturbance signal w, $\delta \in \Delta$, and a solution $\varphi(x(0), t, w; \delta)$ such that $x(0) \in \mathcal{X}_0$, $\varphi(x(0), T, w; \delta) \in \mathcal{X}_r$, and $\varphi(x(0), t, w; \delta) \in \mathcal{X}$ for all $t \in [0, T]$. The main difference in the modified version of this reachability property is that the initial set $\mathcal{X}_0$ may contain multiple points (in fact, may be a continuum) and they do not need to be stationary, whereas, before, we considered $\mathcal{X}_0$ to be a singleton which was an equilibrium point for (2).

The reachability property is concerned with whether a set of target points may be reached by system trajectories. The dual property, namely the safety property, is concerned with whether the set of points that can be reached by the system is safe or, equivalently, whether the system ever enters an unsafe region in the state space. Here, an unsafe set may, for example, be a set of configurations that are associated with falling when the goal is balance assistance. Specifically, let $\mathcal{X} \subseteq \mathbb{R}^n$ and $\mathcal{X}_0 \subseteq \mathcal{X}$ be the state set and the initial set, respectively, as before. Let $\mathcal{X}_u \subseteq \mathcal{X}$ correspond to the set of unsafe configurations (i.e., unsafe set). We say that the safety property holds if there exists no time $T \geq 0$, $\delta \in \Delta$, or admissible disturbance signal w such that t $x(0) \in \mathcal{X}_0$, $\varphi(x(0), T, w; \delta) \in \mathcal{X}_u$, and $\varphi(x(0), t, w; \delta) \in \mathcal{X}$ for all $t \in$

[1] The assumption that the modeling uncertainties do not alter the equilibrium at $x = 0$ may be restrictive. The so-called contraction metrics [16] may be used to alleviate this limitation.

$[0, T]$.

In this section, we discussed definitions of a number of robustness and safety metrics for nonlinear dynamical systems. However, these definitions are not constructive. In fact, computing the ROA and verifying the reachability or safety properties are challenging (even impractical) in general. In the next section, we will present a procedure that "approximates" the ROA or "approximately" verifies the safety and reachability properties. We will refer to the questions of verifying whether a given subset of the state space is contained in the ROA and verifying safety and reachability properties over transient subsets of the state space as *system analysis questions.*

5. COMPUTATIONAL CONSIDERATIONS

For a given system analysis question, the first step of the procedure, which translates the question into a numerical optimization problem, is based on establishing sufficient conditions whose satisfaction witnesses the property of interest. We will use the computation of invariant subsets of the ROA to illustrate the main ideas in this section (rather than an exposition in full detail or formality). It is well-known in nonlinear system theory [41] (refer to [38, 39] for a development similar to that in this section) that if there exists a continuously differentiable function $V : \mathbb{R}^n \to \mathbb{R}$ that satisfies the conditions,

$$V(0) = 0, \ V(x) > 0 \text{ for all nonzero } x \in \mathbb{R}^n, \qquad (4)$$

$$\Omega_V := \{x \in \mathbb{R}^n \ : \ V(x) \leq 1\} \text{ is bounded}, \qquad (5)$$

$$\Omega_V \backslash \{0\} \subseteq \{x \in \mathbb{R}^n \ : \ \nabla V(x) \cdot f(x, 0; \delta) < 0, \ \delta \in \Delta\}, \qquad (6)$$

then the set Ω_V is an invariant set of the ROA around the origin.

Consider now, given a set S of possible initial condition perturbations, the designer is interested in whether S is contained in the ROA, i.e., whether the system can recover from every perturbation in S regardless of the value of $\delta \in \Delta$. One way to establish this fact is to simulate the dynamics in (2) from every point in S and for every value of $\delta \in \Delta$ and to check whether all such trajectories do approach the origin. Such exhaustive verification is obviously impractical. On the other hand, if the designer can find a function V that satisfies the conditions in (4)-(6) and the set containment $S \subseteq \Omega_V$, then she can conclude that S is indeed contained in the ROA without any simulations. Consequently, one pragmatic way to answer the question of containment of S in the ROA is searching for such a function V.

The conditions in (4)-(6) provide sufficient conditions for reformulating the system analysis question as a search for an algebraic function but they do not provide means for executing the search. The main difficulty is checking whether the condition in (6) holds (even for a given function V).

The second step of the procedure discussed here establishes a sufficient condition, which is more suitable for mathematical optimization, for (6). Specifically, fix a positive definite function $l : \mathbb{R}^n \to \mathbb{R}$ and consider that there exists a function $s : \mathbb{R}^n \to \mathbb{R}$ such that

$$-\left(l(x) + \nabla V(x) \cdot f(x, 0; \delta)\right) + s(x)\left(V(x) - 1\right) \geq 0 \qquad (7)$$

for all $x \in \mathbb{R}^n$ and $\delta \in \Delta$ and

$$s(x) \geq 0 \text{ for all } x \in \mathbb{R}^n. \qquad (8)$$

Then, the set containment in (6) holds, i.e., existence of s satisfying (7)-(8) witnesses the satisfaction of this set containment condition.

By putting this series of sufficient conditions end-to-end, for a given the set $S \subseteq \mathbb{R}^n$ and the function l as above, if there exist functions $V : \mathbb{R} \to \mathbb{R}$ and $s : \mathbb{R} \to \mathbb{R}$ that satisfy (4)-(5) and (7)-(8), we can conclude that S is contained in the ROA.

The search for V and s satisfying the conditions (4)-(5) and (7)-(8) can be formulated as a mathematical optimization (or feasibility) question. However, such a question is infinite dimensional and intractable in general. On the other hand, it can still be answered for certain, relatively expressive families of systems. The cases where the map f is linear or polynomial in x (and the set Δ is polytopic) are examples for which there are relatively effective numerical optimization tools to perform the search. For instance, if the map f is polynomial in x, then the search for polynomials V and s of fixed, finite degree that satisfy the conditions in (4)-(5) and (7)-(8) can be performed as a finite-dimensional polynomial optimization problem. Furthermore, the recently developed sum-of-squares relaxations for polynomial optimization [24] and the corresponding numerical optimization packages [15, 26, 31] enable automated search for functions V and s that witness the containment of the set S in the ROA (through the series of sufficient conditions as discussed above).

Note that the choice of the families of functions with finite parametrizations (e.g., finite-degree polynomials in the state variables) within which the search for the certificates V and s is performed affects whether it can be verified that the set S is in the ROA. More specifically, for certain choices of these families, there may not exist V or s that satisfy the conditions in (4)-(5) and (7)-(8), while such V and s may be found if the search is carried out over larger families (e.g., polynomials of greater degree).

In this section so far, we have outlined a procedure that formulates the system analysis question whether a given set S is in the ROA as a finite-dimensional mathematical optimization problem. This procedure applies to the other system analysis questions introduced in Section 4 with modifications mainly in the first step. The so-called storage functions [34, 45] and barrier certificates [25, 42] serve—instead of the simple Lyapunov-type certificate in (4)-(5)—as certificates to bound the set of reachable points from the origin under bounded energy disturbances and to verify reachability or safety over transient subsets of the state space. After the first step, one can similarly apply the sufficient conditions for set containment as in the second step and restrictions in order to obtain finite-dimensional optimization problems as in the last step.

6. A SIMPLE CASE STUDY

Let us return to the topical application of balance assistance during stationary standing. In the case of a knee-ankle prosthetic leg, the device can provide control torques at the prosthetic ankle and knee joints but not at the human hip, i.e., this joint is an unactuated degree-of-freedom from the perspective of the prosthesis. For the sake of simplicity we assume that the prosthetic knee is locked, so our goal is to certify that an ankle control strategy prevents falls given free motion of the human's hip joint.

We use the so-called pendubot dynamics to demonstrate typical results from the analysis methods discussed in Sections 4 and 5. A pendubot is an underactuated two-link pendulum with torque action only on the first link as shown in Figure 2, where q_1 is the position of the first link and q_2 is the position of the second link with respect to the first one. The dynamics of a pendubot are easily derived from the Euler-Lagrange equations [30] and take a form similar to (1):

$$M(q)\ddot{q} + C(q,\dot{q})\dot{q} + G(q) = [\tau,\ 0]^T, \qquad (9)$$

where $q = (q_1, q_2)^T$, τ is the control torque at the base, and the other model terms are defined as in (1). See [30] for details. In general, the expression in (9) leads to a nonlinear dynamical model.

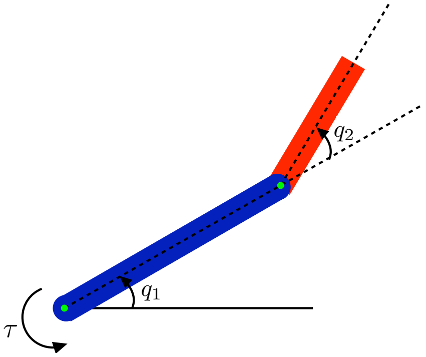

Figure 2: An under actuated, two-link mechanism with positions q_1 and q_2 of the links and torque τ applied only at the first link.

We study the region-of-attraction properties of pendubot dynamics with a controller designed to stabilize its upright configuration (i.e., $q_1 = \pi/2$ and $q_2 = 0$). The controller is a linear quadratic regulator (taken from [36, 37]). It is designed for the linearized dynamics around $q = (\pi/2, 0)$ with the cost function

$$\int_0^\infty \left[10\left((q_1-\pi/2)^2 + q_2^2\right) + 0.1(\dot{q}_1 + \dot{q}_2) + 1000\tau^2\right] dt.$$

The resulting controller, for a particular choice of parameter values, is approximately

$$\tau(t) = 15.89(q_1(t) - \pi/2) + 3.01\dot{q}_1(t) + 15.88q_2(t) + 2.01\dot{q}_2(t).$$

The closed-loop dynamics are not directly amenable to nonlinear robustness analysis methods discussed in Section 5. Therefore, we study a cubic polynomial approximation of the closed-loop dynamics, written as

$$\begin{aligned}
\dot{x}_1 &= x_3,\\
\dot{x}_2 &= x_4\\
\dot{x}_3 &= 782(x_1 - \pi/2) + 689x_2 + 135x_3 + 90x_4,\\
\dot{x}_4 &= 279(x_1 - \pi/2)x_2^2 - 1425(x_1 - \pi/2)\\
&\qquad - 257x_3 + 273x_2^3 - 1249x_2 - 171x_4,
\end{aligned}$$

where $x = (q^T, \dot{q}^T)^T$. The solid curve in Figure 3 shows a slice (for $x_3 = 0$ and $x_4 = 0$) of the verified invariant subset of the ROA around the equilibrium point at

$$x_{eq} = (x_{eq,1}, x_{eq,2}, x_{eq,3}, x_{eq,4})^T = (\pi/2, 0, 0, 0)^T.$$

That is, from all perturbations that are in this estimated set, the system state stays in the set and converges to x_{eq}. In particular, for the initial condition perturbations that are in the region bounded by the solid curve in Figure 3 and have zero initial velocity, the system state approaches the equilibrium configuration x_{eq}. The dots in Figure 3 are a collection of initial condition perturbations (with $x_w = 0$ and $x_4 = 0$) from which the closed-loop system does not converge back to the equilibrium condition.

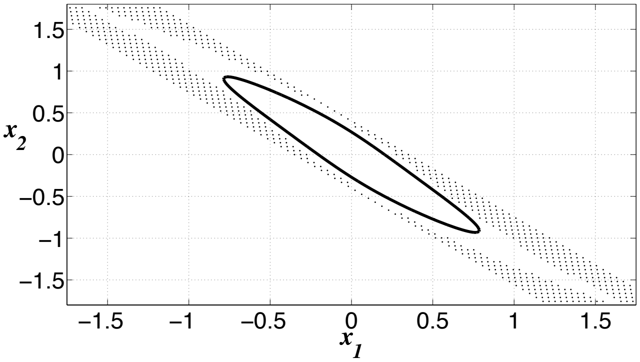

Figure 3: The solid curve is an invariant subset of the ROA computed using the procedure outlines in Section 5 and the dots are initial conditions from which the system does not converge.

7. EXTENSIONS AND IMPLICATIONS

We discussed the role that may be played by model-based verification in establishing assurance of wearable medical robots. Given a differential equation based model, the verification metrics we discussed include the region of attraction and the set of reachable states (under external disturbances) from nominal operating conditions, and the safety and reachability properties over transient regions of the state space. We also summarized a procedure for computing approximations of these metrics. A number of extensions to these models, verification metrics, and computational tools are needed along with solutions to technical, technological, and regulatory limitations in order to bring model-based verification into practice for medical robotics.

The procedure outlined in Section 5 is only one of many possibilities, including the work in [5,21]. Furthermore, properties of systems around limit cycles or other non-stationary solutions (rather than equilibrium points) may be of interest as discussed in Section 2. Recent work in [17–19,35] provides interesting extensions of the notions we discussed here for the analysis of properties around non-stationary trajectories. Moreover, systems evolving over multiple modes, i.e., hybrid system models, naturally arise in medical robotics and extensions to such models are of interest [25].

Computational complexity (both in terms of memory and time) is the main technical bottleneck in developing assurance tools for the development of medical robots. Specifically, the size of the optimization problems resulting from, for example, the procedure in Section 5 grows rapidly with the number of state variables, the number of uncertain parameters (i.e., the dimension of δ), and the dimension of the disturbance vector. Complexity also arises from the "richness" of the families of functions over which the search for certificates is performed. Therefore, the ability to create abstractions of system behavior and specifications of interest at multiple levels of fidelity is a critical need.

As these computational problems are addressed, the variety of verification tools discussed in this paper could be harnessed to improve the safety of powered prosthetic and orthotic control systems. In particular, formal verification tools could fit naturally into the risk management procedures (ISO 14971) mandated by the international quality management standards (ISO 13485) for medical device manufacturers [12, 44]. These standards require manufacturers to establish documented procedures for providing feedback and early warnings regarding product quality and safety, allowing corrective and preventive actions to be taken before a medical device goes into production.

The ISO 14971 standard specifically establishes requirements for risk management to determine the safety of a medical device during its development and product life cycle [12]. The risk management plan must establish risk acceptability criteria and describe verification activities, which could employ many of the technical metrics and tools discussed in this paper. This international standard also requires manufacturers to identify all foreseeable hazards and estimate the risk associated with each hazardous situation, i.e., every sequence or combination of events that could potentially result in a safety hazard. The extreme complexity of robotic devices (e.g., the number of control decisions they can enact) makes this a daunting task using conventional exhaustive testing methods. Formal verification tools could provide conservative estimates of safety regions to prevent the need for exhaustive testing in normal operating conditions. These tools could also be employed in the control design process to actively reduce risks to acceptable levels.

Formal verification tools could be used to meet the evolving regulatory demands in the rapidly developing market of medical robots with minimal cost and delay to device manufacturers. However, due to the pre-market exemptions currently granted by the FDA to many of these new devices, the burden-of-proof rests with the research community to convince regulatory agencies and device manufacturers of the merit and capabilities of these formal methods.

8. REFERENCES

[1] A. Boehler, K. Hollander, T. Sugar, and D. Shin. Design, implementation and test results of a robust control method for a powered ankle foot orthosis (afo). In *IEEE Int. Conf. Robotics & Automation*, pages 2025–2030. IEEE, 2008.

[2] D. Brown et al. Projected costs of ischemic stroke in the United States. *Neurology*, 67(8):1390, 2006.

[3] R. Day. Challenges of biological realism and validation in simulation-based medical education. *Artificial Intelligence in Medicine*, 38(1):47–66, 2006.

[4] M. Eilenberg, H. Geyer, and H. Herr. Control of a powered ankle–foot prosthesis based on a neuromuscular model. *IEEE Trans. Neural Systems & Rehab. Engineering*, 18(2):164–173, 2010.

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

[6] G. F. Fuller. Falls in the elderly. *Am Fam Physician*, 61(7):2159–2168, 2000.

[7] R. D. Gregg, T. W. Bretl, and M. W. Spong. A control theoretic approach to robot-assisted locomotor therapy. In *IEEE Conf. Decision and Control*, pages 1679–1686, Atlanta, GA, 2010.

[8] R. D. Gregg, N. Fey, T. Lenzi, J. W. Sensinger, and L. J. Hargrove. Experimental effective shape control of a powered transfemoral prosthesis. In *IEEE Int. Conf. Rehab. Robotics*, 2013. submitted.

[9] R. D. Gregg and J. W. Sensinger. Biomimetic virtual constraint control of a transfemoral powered prosthetic leg. In *Amer. Control Conf.*, Washington, DC, 2013.

[10] R. D. Gregg and J. W. Sensinger. Towards biomimetic virtual constraint control of a powered prosthetic leg. *IEEE Trans. Control Sys. Tech.*, 2013. in press.

[11] M. A. Holgate, T. G. Sugar, and A. W. Bohler. A novel control algorithm for wearable robotics using phase plane invariants. In *IEEE Int. Conf. Robotics & Automation*, pages 3845–3850, 2009.

[12] International Organization for Standardization. *ISO 14971:2007. Medical devices–Application of risk management to medical devices*, 2007. [Online]. Available: `http://www.iso.org`.

[13] K. Ziegler-Graham et al. Estimating the prevalence of limb loss in the United States: 2005 to 2050. *Arch. Phys. Med. & Rehab.*, 89(3):422–429, 2008.

[14] Y. Li, K. Shorter, E. Hsiao-Wecksler, and T. Bretl. Simulation and experimental analysis of a portable powered ankle-foot orthosis control. In *Dynamic Systems and Control Conference*, pages 77–84. ASME, 2011.

[15] J. Lofberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[16] W. Lohmiller and J.-J. E. Slotine. On contraction analysis for non-linear systems. *Automatica*, 34(6):683–696, 1998.

[17] I. R. Manchester. Tranverse dynamics and regions of stability for nonlinear hybrid limit cycles. In *IFAC World Congress*, volume 18, pages 6285–6290, Milano, Italy, 2011.

[18] I. R. Manchester and J.-J. E. Slotine. Contraction criteria for existence, stability, and robustness of a limit cycle. *CoRR*, abs/1209.4433, 2012.

[19] I. R. Manchester, M. Tobenkin, M. Levashov, and R. Tedrake. Regions of attraction for hybrid limit cycles of walking robots. In *IFAC World Congress*, volume 18, pages 5801–5806, Milano, Italy, 2011.

[20] W. C. Miller, A. B. Deathe, M. Speechley, and J. Koval. The influence of falling, fear of falling, and

balance confidence on prosthetic mobility and social activity among individuals with a lower extremity amputation. *Arch. Phys. Med. Rehab.*, 82(9):1238–1244, 2001.

[21] I. M. Mitchell. A toolbox of level set methods version 1.0, 2004.

[22] B. Morrison. *Robotic Prosthetic Availability Analysis.* PhD thesis, Worcester Polytechnic Institute, 2012.

[23] Össur. POWER KNEE, 2012. [Online]. Available: `http://www.ossur.com/powerknee/`.

[24] P. Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization.* Ph.D. dissertation, California Institute of Technology, May 2000.

[25] S. Prajna. *Optimization-based methods for nonlinear and hybrid systems verification.* PhD thesis, Pasadena, CA, USA, 2005.

[26] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo. *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*, 2004.

[27] K. R. Rosen. The history of medical simulation. *Journal of Critical Care*, 23(2):157–166, 2008.

[28] K. Shorter, J. Xia, E. Hsiao-Wecksler, W. Durfee, and G. Kogler. Technologies for powered ankle-foot orthotic systems: Possibilities and challenges. *IEEE/ASME Transactions on Mechatronics*, 18(1):337–347, 2013.

[29] K. A. Shorter, E. T. Hsiao-Wecksler, G. F. Kogler, E. Loth, and W. K. Durfee. A portable powered ankle-foot-orthosis for rehabilitation. *J. NeuroEng. & Rehab.*, 48(4):459–472, 2011.

[30] M. W. Spong and M. Vidyasagar. *Robot Dynamics and Control.* Wiley, 1989.

[31] J. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1999. Available at `http://sedumi.mcmaster.ca/`.

[32] F. Sup, A. Bohara, and M. Goldfarb. Design and control of a powered transfemoral prosthesis. *Int. J. Robotics. Res.*, 27(2):263–273, 2008.

[33] F. Sup, H. Varol, and M. Goldfarb. Upslope walking with a powered knee and ankle prosthesis: Initial results with an amputee subject. *IEEE Trans. Neural Systems & Rehab. Engineering*, 19(1):71–78, 2011.

[34] W. Tan, U. Topcu, P. Seiler, G. Balas, and A. Packard. Simulation-aided reachability and local gain analysis for nonlinear dynamical systems. In *Proc Conf on Decision and Control*, 2008.

[35] R. Tedrake, I. R. Manchester, M. Tobenkin, and J. W. Roberts. LQR-trees: Feedback motion planning via sums-of-squares verification. *Int. J. Rob. Res.*, 29(8):1038–1052, 2010.

[36] U. Topcu. *Quantitative local analysis of nonlinear systems.* Ph.D. dissertation, UC, Berkeley, 2008.

[37] U. Topcu, A. Packard, and P. Seiler. Local stability analysis using simulations and sum-of-squares programming. *Automatica*, 44:2669 – 2675, 2008.

[38] U. Topcu, A. Packard, P. Seiler, and G. Balas. Help on SOS. *IEEE Control Systems Magazine*, 30:18 – 23, 2010.

[39] U. Topcu, A. Packard, P. Seiler, and T. Wheeler. Stability region analysis using simulations and sum-of-squares programming. In *Proc. American Control Conf.*, pages 6009–6014, New York, NY, 2007.

[40] U. Topcu and A. K. Packard. Local stability analysis for uncertain nonlinear systems. *IEEE Trans. Automat. Contr.*, 54(5):1042–1047, 2009.

[41] M. Vidyasagar. *Nonlinear Systems Analysis.* Prentice Hall, 2^{nd} edition, 1993.

[42] R. Vinter. A characterization of the reachable set for nonlinear control systems. *SIAM Journal on Control and Optimization*, 18(6):599–610, 1980.

[43] E. R. Westervelt, J. W. Grizzle, C. Chevallereau, J. H. Choi, and B. Morris. *Feedback Control of Dynamic Bipedal Robot Locomotion.* CRC Press, New York, NY, 2007.

[44] Wikipedia. ISO 13485, 2013. [Online]. Available: `http://en.wikipedia.org/wiki/ISO_13485`.

[45] J. C. Willems. Dissipative dynamical systems I: General theory. *Arch. Rational Mech. Analysis*, 45:321–343, 1972.