Certifying the Safe Design of a Virtual Fixture Control Algorithm for a Surgical Robot

Yanni Kouskoulas[1] David Renshaw[2] André Platzer[3]
Peter Kazanzides[4]

April 26, 2013

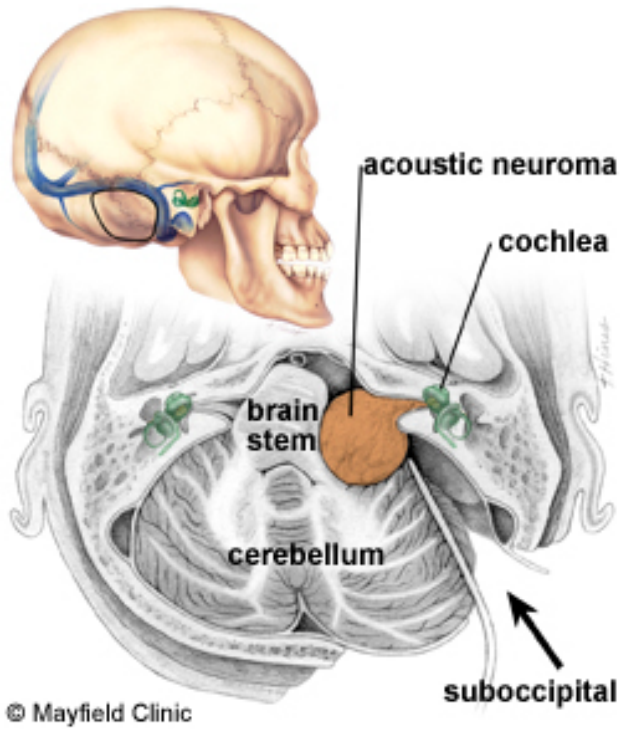
[1]Johns Hopkins University, Applied Physics Laboratory
[2]Carnegie Mellon University
[3]Carnegie Mellon University
[4]Johns Hopkins University, Dept. of Computer Science

Outline

- Objective
- Verification Target
- Formal Methods Approach
- Results
- Conclusions

Medical Background

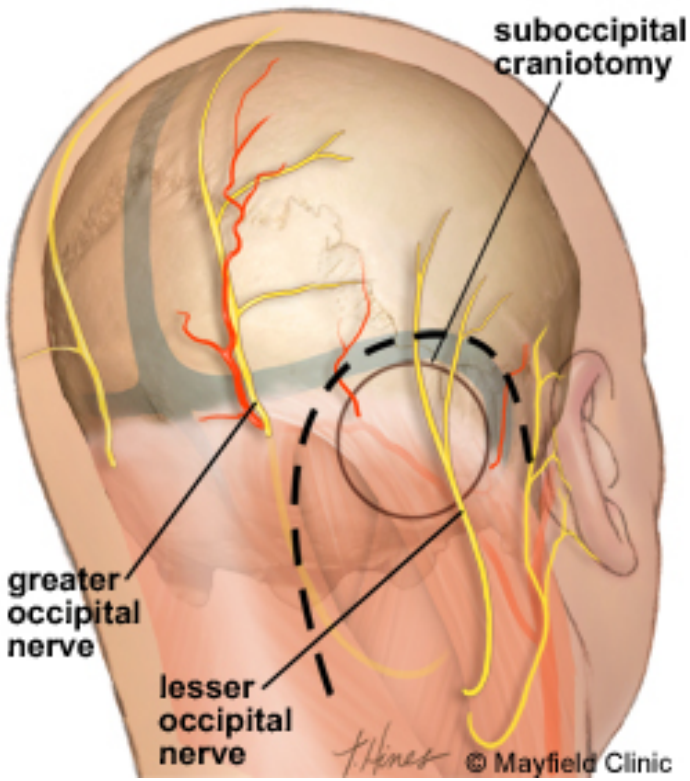
An acoustic neuroma is a tumor that grows from the sheath of nerves responsible for hearing and balance. . . . It can cause serious damage by exerting increasing pressure on surrounding nerves and the brain.



Quote and figures courtesy of the Mayfield Clinic web site.

Medical Background

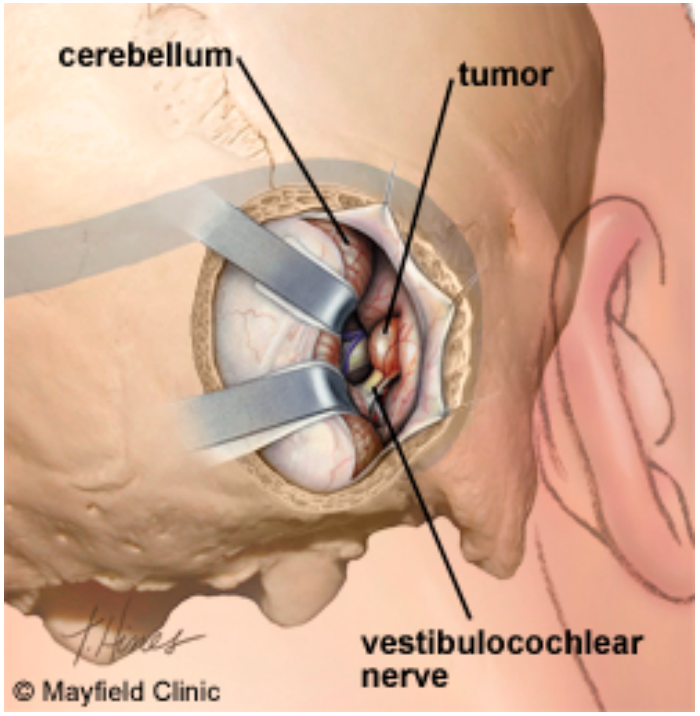
If necessary, surgery can remove such tumors. A suboccipital approach is illustrated. *A high-arching skin incision is made behind the ear (dashed line) that crosses the occipital nerves at the end branches.*



Quote and figures courtesy of the Mayfield Clinic web site.

Medical Background

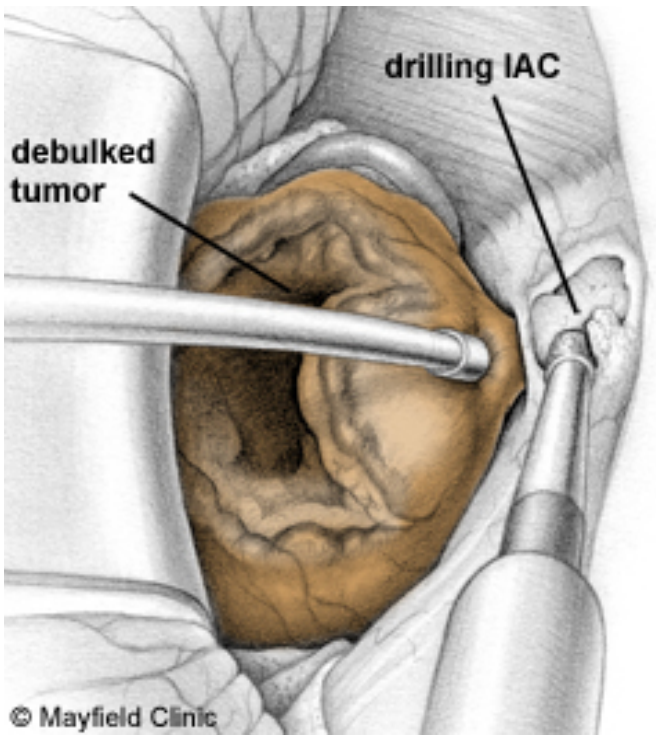
A 1.5 inch-wide craniotomy is made in the occipital bone and the bone flap is removed. The cerebellum is gently held back to expose a small tumor and its attachments to the nerve.



Quote and figures courtesy of the Mayfield Clinic web site.

Motivation

The surgeon must work in an extremely small space, near some very critical organs and nerves. An errant movement could cause the patient great harm. This work aims to help the surgeon and make this procedure safer for the patient.



Quote and figures courtesy of the Mayfield Clinic web site.

Background: Prior Work

- A Skull-Base Surgery (SBS) robot was developed by Computer Integrated Surgical Systems and Technology (CISST) Group at Johns Hopkins University's Homewood Campus
  - Designed to aid in fine, precise control of a tool by damping small movements
  - Designed to confine tool tip to a pre-defined volume with *virtual fixtures*

Background: Prior Work

- T. Xia, et. al, describe the development in *An integrated system for planning, navigation, and robotic assistance for skull base surgery*

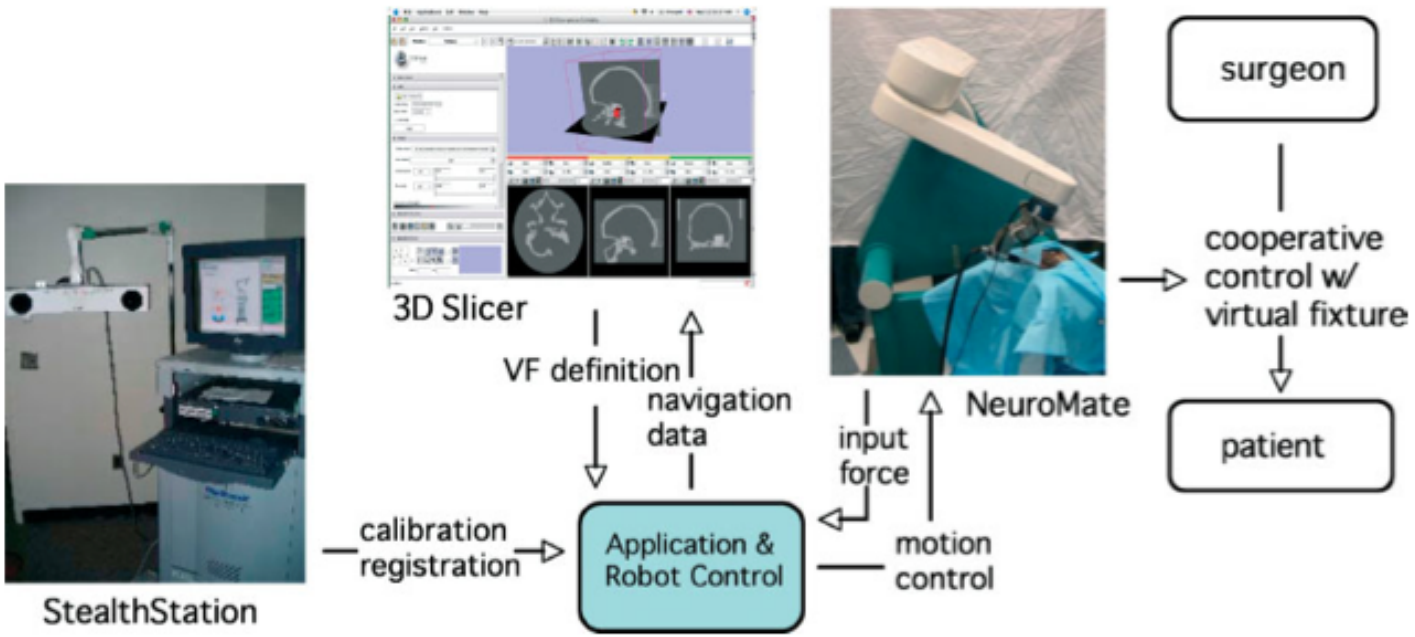
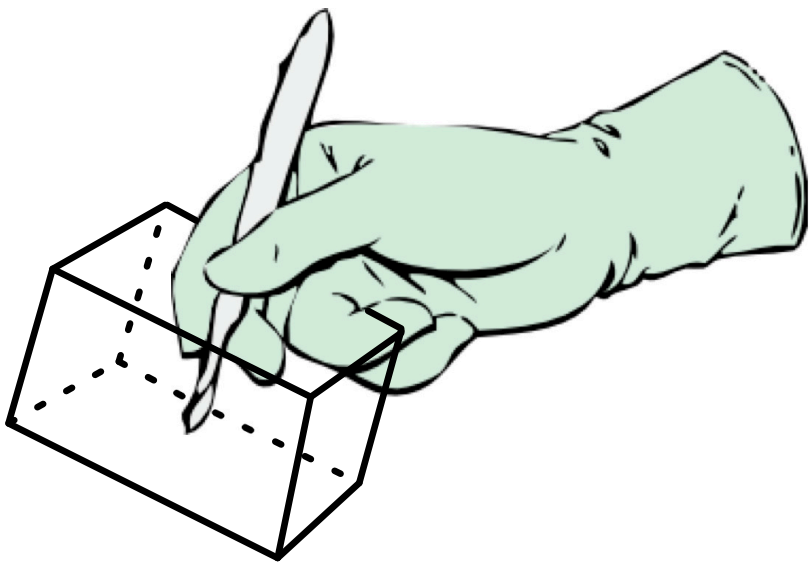


Figure 1. System overview of the image-guided robot for skull base surgery. System components include: modified NeuroMate® robot in cooperative control mode; StealthStation® navigation system; 3D Slicer software for intraoperative visualization; and workstation for application logic and robot control

Current Research Objective

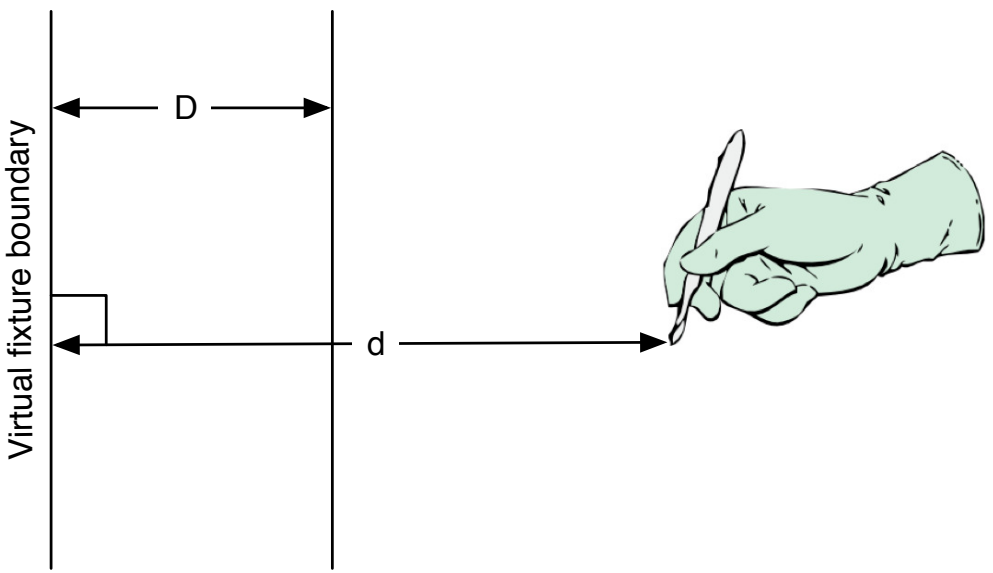
- Help ensure the system's safe operation by proving that the control algorithm that limits the tool's movement correctly enforces safety for all possible input conditions
  - Apply formal methods to this analysis
  - Far stronger safety guarantees than from testing
    - Testing the system can only guarantee that it enforces safety for the specific conditions in the test suite

Verification Target: Design



Verification Target

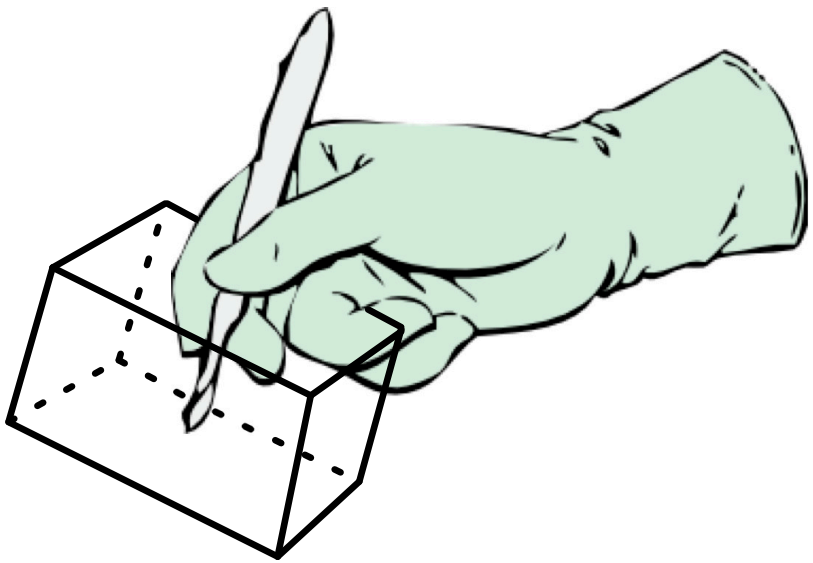
- The behavior of the robot changes abruptly depending on the normal distance from tool tip to virtual fixture boundary
- Three modes of operation



Verification Target: Design

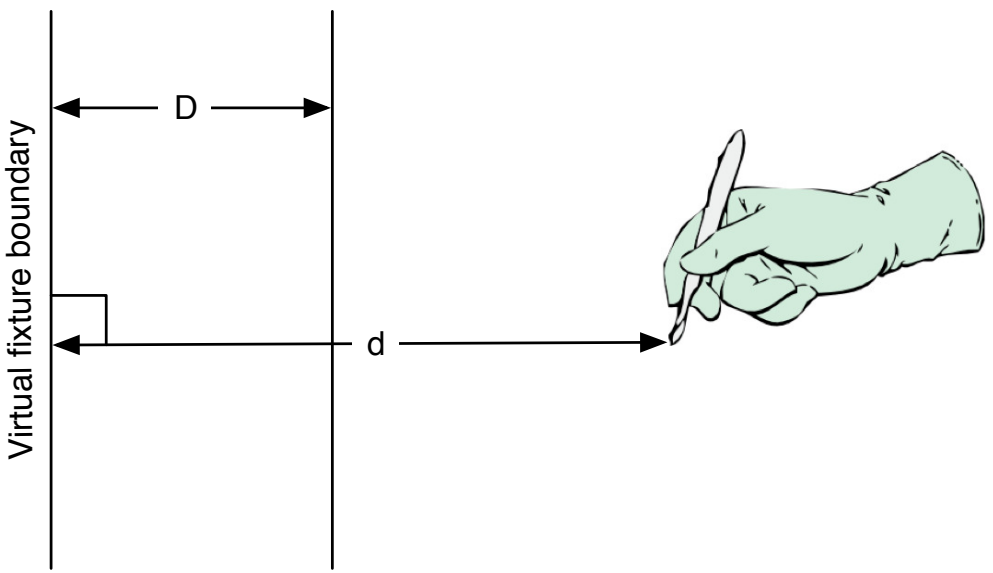
- JHU Admittance control design

$$q' = \overbrace{J^{-1}(q)}^{\text{Jacobian inverse}} \times \overbrace{K(d)}^{\text{scale factor}} \times \overbrace{G(f)}^{\text{admittance gain}} \times \begin{bmatrix} F_w \\ T_w \end{bmatrix}$$



Verification Target: Design

- The form of K changes abruptly depending on the normal distance from tool tip to virtual fixture boundary
- Three modes of operation



FM Approach

- Formal methods are a class of mathematical approaches to reasoning about systems that enable precise description of functionality and rigorous mathematical proof of system properties and behavior
- Each formal method has three components:
  - An language for modeling the system
  - An language for describing the systems behavior
  - An strategy for proving (or disproving) that the system we described has that behavior we specified

FM Approach: Differential Dynamic Logic

- Differential dynamic logic is a hybrid logic applicable to continuous systems with discrete mode switches
- Developed by Andre Platzer in his Ph.D. thesis, applied to automatic vehicle control test case

FM Approach: Modeling Hybrid Systems

- Language used to model hybrid systems in dL:
  - $\alpha; \beta$ Executes α and *beta* in sequence
  - $\alpha*$ Repeats hybrid program α some number of times
  - $\alpha \cup \beta$ Executes either α or β
  - $?\chi$ Represents an assertion about program state
  - $(x := \theta)$ Is a discrete assignment to a state variable
  - $(x' = \theta \& \chi)$ Represents a continuous evolution of the state variables according to the specified differential equations, with the system satisfying χ
- Language used to describe system behavior in dL, and write logical formulae (e.g. χ above):
  - First order logic (i.e. $\forall, \exists, \vee, \wedge, \neg, \rightarrow$)
  - Modal operators (i.e. $[\alpha]\chi$ and $\langle\alpha\rangle\chi$)

Simple Model

- Surgical robot controller with simplifying assumptions: 2D, one boundary

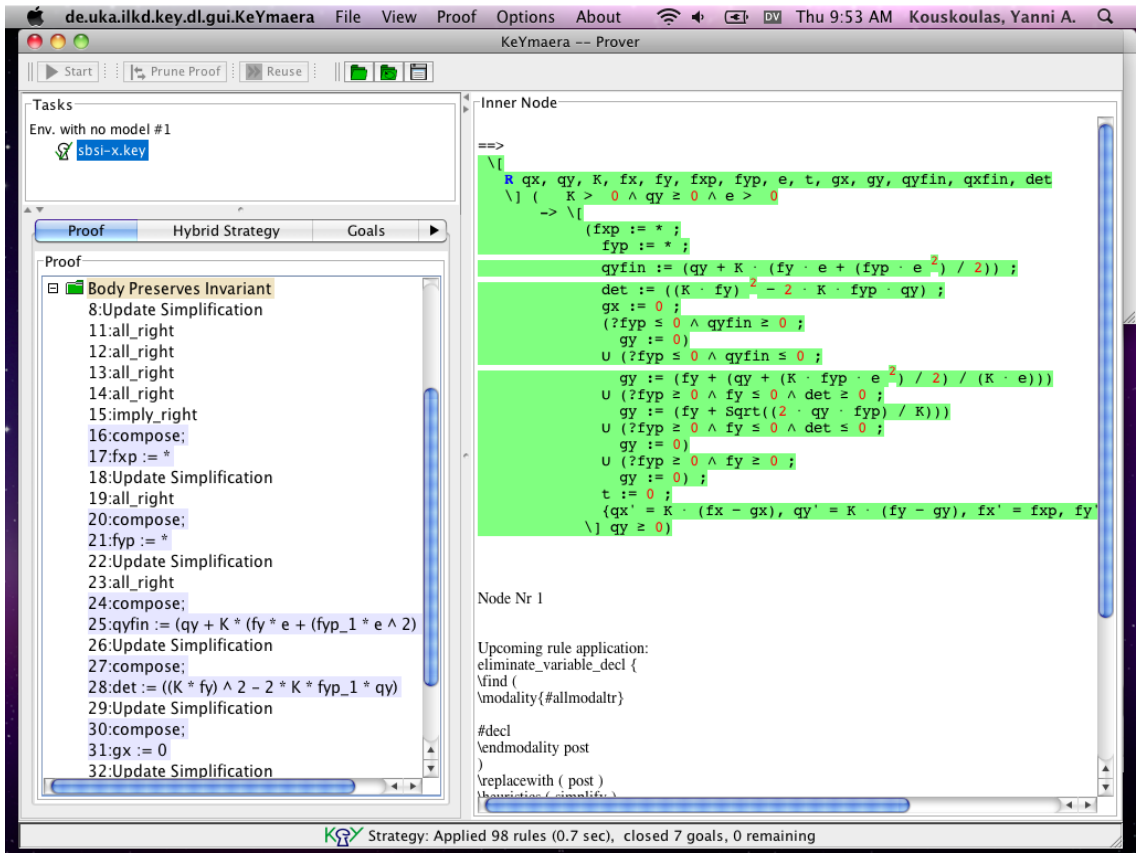
$$
\begin{aligned}
&\text{ctrl} = \\
&(f_{xp} := *; f_{yp} := *; \\
&(q_x' = Kf_x, q_y' = Kf_y, f_x' = f_{xp}, f_y' = f_{yp} \& (q_y > D)) \cup \\
&(q_x' = Kf_x, q_y' = K\tfrac{q_y}{D} f_y, f_x' = f_{xp}, f_y' = f_{yp} \& \\
&(0 \leq q_y \leq D) \wedge (f_y \leq 0)) \cup \\
&(q_x' = Kf_x, q_y' = Kf_y, f_x' = f_{xp}, f_y' = f_{yp} \& \\
&(0 \leq q_y \leq D) \wedge (f_y \geq 0)) \cup \\
&(q_x' = 0, q_y' = 0, f_x' = f_{xp}, f_y' = f_{yp} \& (q_y \leq 0) \wedge (f_y \leq 0)) \cup \\
&(q_x' = 0, q_y' = Kf_y, f_x' = f_{xp}, f_y' = f_{yp} \& (q_y \leq 0) \wedge (f_y \geq 0)) \;) *
\end{aligned}
$$

FM Approach: Property to be proven

$$\forall K, D, q_y, q_x, f_y, f_x, f_{xp}, f_{yp},$$
$$(K > 0) \wedge (D > 0) \wedge (q_y > 0) \rightarrow [\text{ctrl}]\,(q_y \geq 0)$$

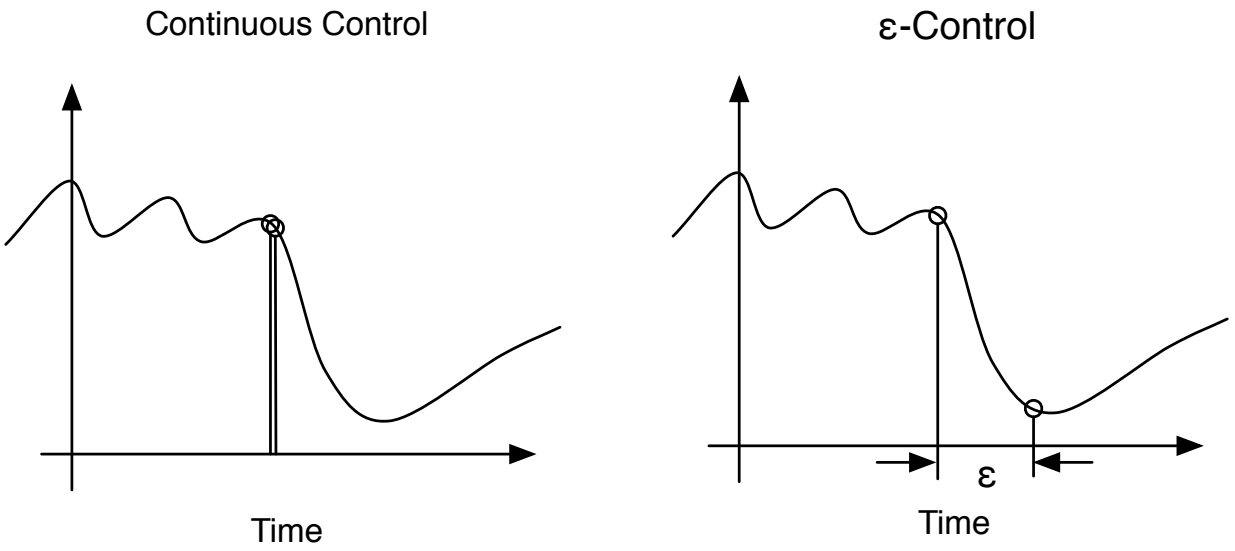
Single-Boundary Safety Proof Using Simplified Model

- We modeled a single virtual fixture boundary in 2D and 3D, and proved that the algorithm safely restricts the tool



Problem 1

- The model (and the description in the original paper) assumes negligable lag in response
- FM technique indicates the problem by preventing us from modeling modeling multiple boundaries
  - This would require an infinitely fast computer running at each moment in time
  - The process of formal verification has indicated to us a problem with our modeling



General Modeling Observation

- Sometimes negligable lag is a reasonable assumption, to use on one part of the controller, but not on another
  - It is reasonable for the underlying admittance controller used to convert force to velocity in the system (continuous control circuit)
  - It is not reasonable for the virtual fixture control algorithm (hybrid system)

More Accurate Model

- Create an improved the model so that it realistically represents delay associated with program computations
- Refactor the logic for each mode, removing it from the continuous dynamics statements, and collecting it into a discrete program

Continuous Control

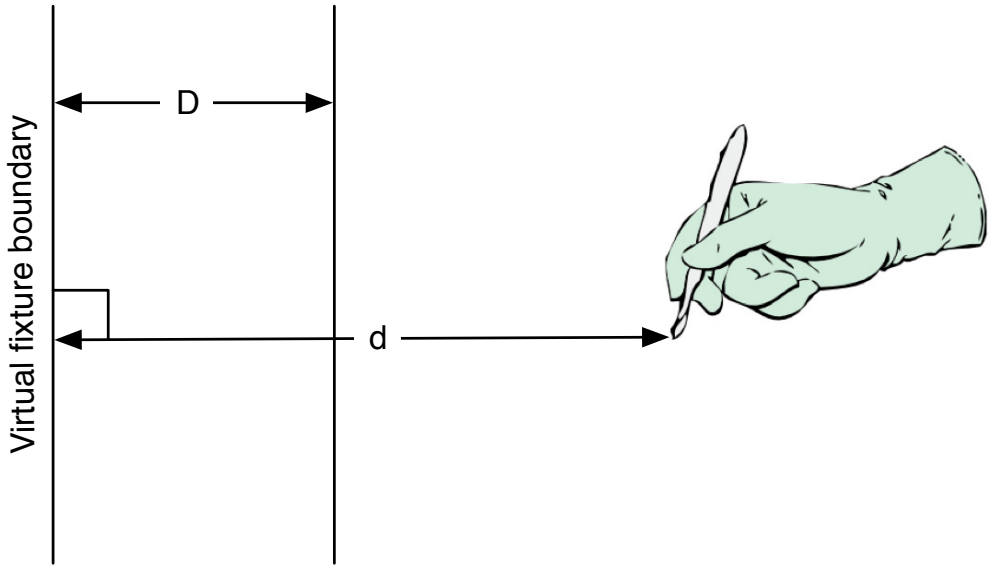
ctrl =
(*disc*;
(mode1dyn)∪
(mode2dyn)∪
(mode3dyn))∗

ϵ Control

ctrl =
(*disc*;
*mode*1*disc*;
*mode*2*disc*;
*mode*3*disc*;
(dyn))∗

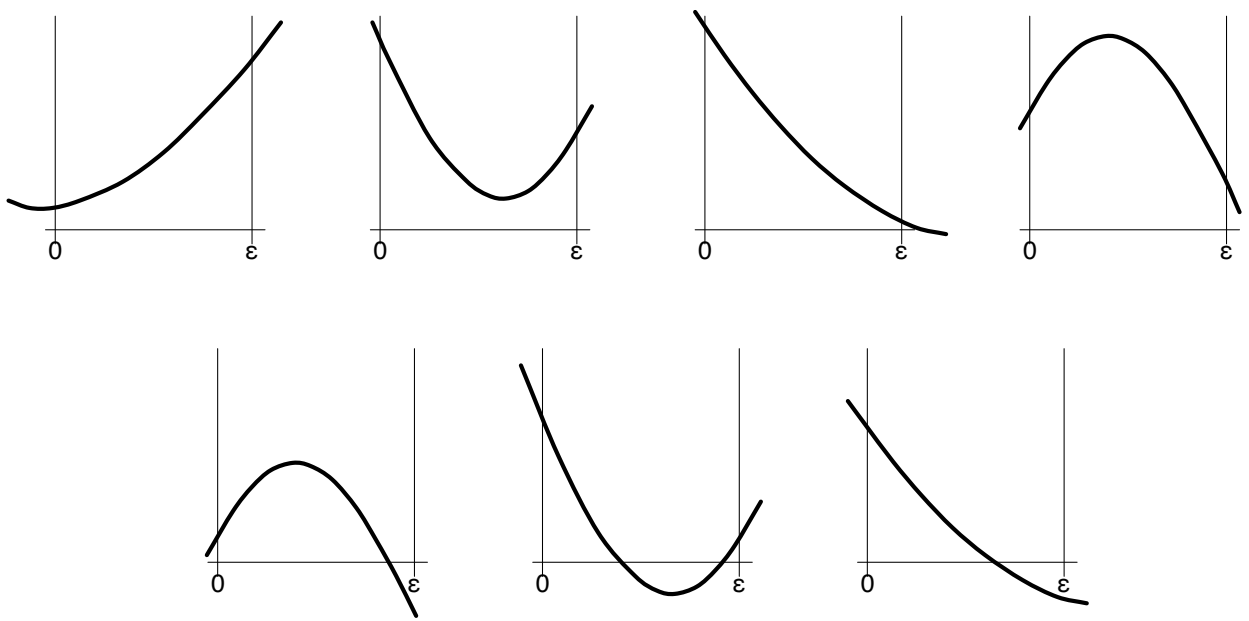
Single Boundary Unsafety proof

- When we consider realistic delay, we discover the buffer zone defined by D is no longer adequate to effectively slow the tool
- For even a single boundary we cannot enforce safety at high tool speeds



Redesign Control Algorithm

- Redesign control algorithm to be predictive
- The process of formal verification forced a redesign, and guides us to ensure that we don't miss any cases



Redesigned SBS Control Algorithm

$$
\begin{aligned}
&\text{ctrl} = ((f_{xp} := *; f_{yp} := *; f_{np} := (f_{xp} n_x + f_{yp} n_y); f_n := (f_x n_x + f_y n_y);\\
&d_0 := (q_x - p_x) n_x + (q_y - p_y) n_y; dist := (d_0 + K(f_n e + \tfrac{f_{np} e^2}{2}));\\
&disc := ((K f_n)^2 - 2 K f_{np} d_0); ((?((f_{np} \leq 0) \wedge (dist \geq 0)); g := 0) \cup\\
&(?((f_{np} \leq 0) \wedge (dist \leq 0)); g := (f_n + ((d_0 + K f_{np}(e^2)/2)/(Ke)))) \cup\\
&(?((f_{np} \geq 0) \wedge (f_n \leq 0) \wedge (disc \leq 0)); g := 0) \cup\\
&\left(?((f_{np} \geq 0) \wedge (f_n \leq 0) \wedge (disc \geq 0) \wedge ((f_n + f_{np} e) \geq 0)); g := f_n + \sqrt{\tfrac{2 d_0 f_{np}}{K}}\right) \cup\\
&\left(?((f_{np} \geq 0) \wedge (f_n \leq 0) \wedge (disc \geq 0) \wedge ((f_n + f_{np} e) \leq 0) \wedge (dist \leq 0)); g := f_n + \sqrt{\tfrac{2 d_0 f_{np}}{K}}\right) \cup\\
&(?((f_{np} \geq 0) \wedge (f_n \leq 0) \wedge (disc \geq 0) \wedge ((f_n + f_{np} e) \leq 0) \wedge (dist \geq 0)); g := 0) \cup\\
&(?((f_{np} \geq 0) \wedge (f_n \geq 0)); g := 0)); t := 0;\\
&(q_x' = K(f_x - g n_x), q_y' = K(f_y - g n_y), f_x' = f_{xp}, f_y' = f_{yp}, t' = 1 \& (t \leq e))) *
\end{aligned}
$$

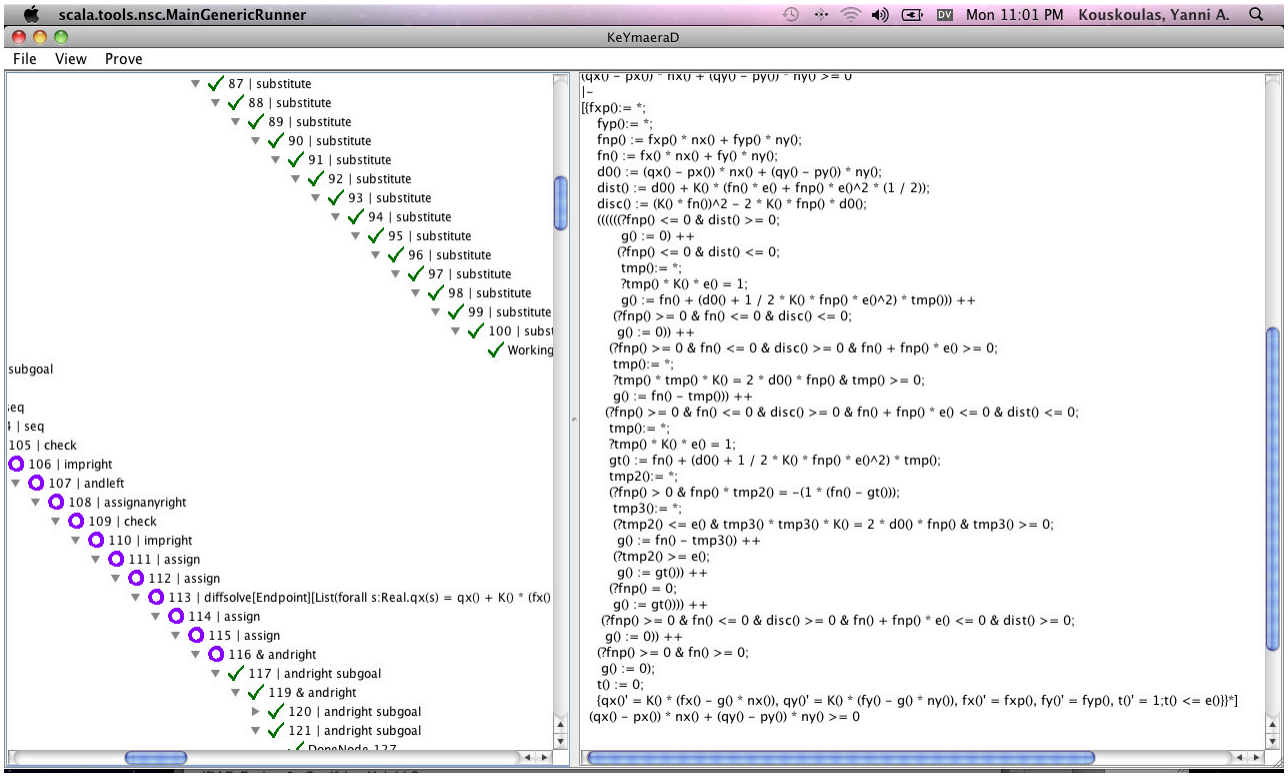
Realistic Model Behavior

- Using KeYmaera and dL, we analyzed the redesigned control strategy, with a realistic model of lag in 3D
  - It safely enforces a single virtual fixture boundary.
  - In certain geometric configurations, the tool can slip through the edge formed by two planar boundaries!
- The process of formal verification highlighted a problem with multiple boundaries

FM approach: Apply QdL using KeYmaeraD

- Using KeYmaeraD, we proved that our new control strategy, with a realistic model 3D safely enforces a single virtual fixture boundary
- The proof is structured much like the model, with the two loops in the model (representing iteration over the boundaries, and over time steps) giving rise to the application of mathematical induction twice.
- Proof has 140 branches (10 damping cases, 7 safety cases, and 2 possible decisions for each boundary, for whether to add damping or not)
- Proof has more than 150,000 steps, and it takes 70 minutes of machine time to machine check it on a laptop

Applying QdL using KeYmaeraD



Conclusion

- This work provides an additional measure of safety for the virtual fixture control algorithm, and any subsequent algorithms derived from it
  - Virtual fixtures can be used to enhance the safety of surgical procedures in many other parts of the body
- This work provides very general lessons on modeling and proving properties about control algorithms in hybrid systems