Semantics of Optimization for Real Time Intelligent Embedded Systems (SORTIES)

Pr. Behçet Açikmese, *University of Texas, Austin*
Pr. Eric Feron, *Georgia Institute of Technology*
Pr. John Hauser, *University of Colorado, Boulder*
Dr. Pierre-Loïc Garoche, Guillaume Davy, *ONERA, France*

Situation:

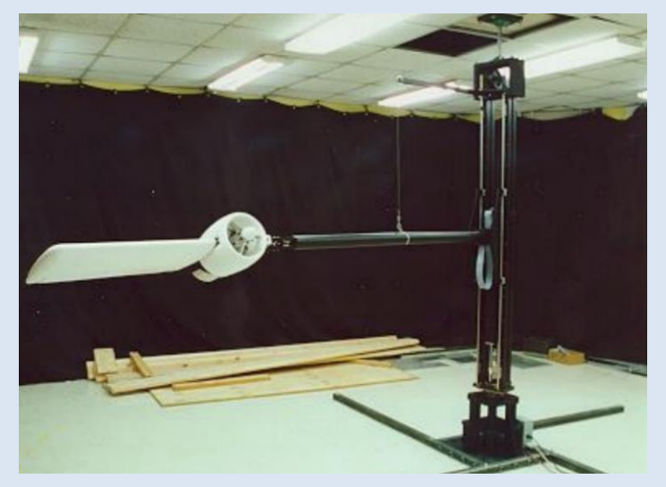
Optimization algorithms used in a real-time and safety-critical context offer the potential for considerably advancing robotic and autonomous systems by improving their ability to execute complex missions. However, this promise cannot happen without proper attention to the considerably stronger operational constraints that real time, safety-critical applications must meet, unlike their non-real-time, desktop counterparts. Advanced real-time algorithms are growing in complexity and length, related to the growth in autonomy, which allows aircraft, automobile, and medical devices to plan paths of their own.

On the other hand, the productivity of safety-critical software developers remains fairly constant at 0.6 to 1 line of code per hour. Knowing that software verification and validation represent fifty percent of their entire engineering development budget, it is then obvious that unless something is done soon, advanced real-time and safety-critical cost development using today's technologies will be unsustainable, if not impossible in the years to come.

Goals:

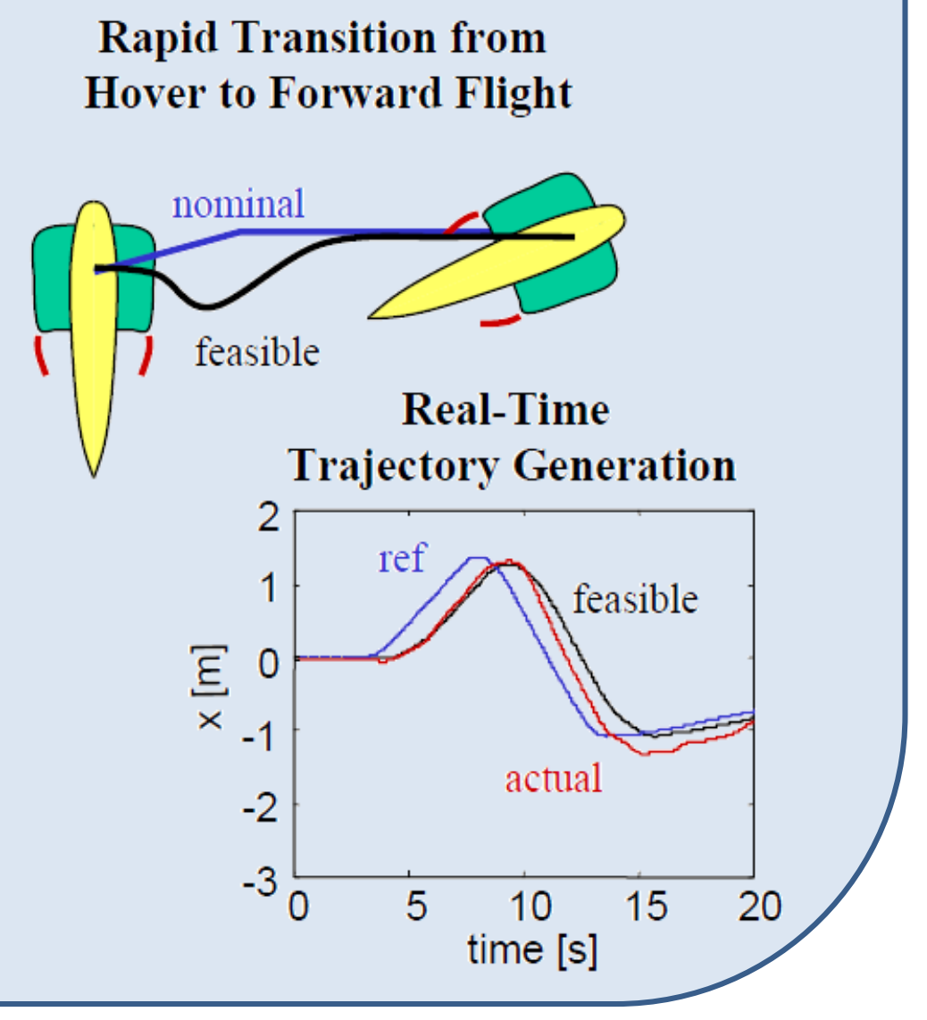
- Demonstrate the relevance and feasibility of embedding modern optimization (and control) algorithms in real-time applications, with strong theoretical guarantees.
- Support the expression of proof elements (including on-line optimization modules) to compile those enriched models down to code, carrying along proof elements.
- Develop the capability to re-check this information of proof elements for other purposes, such as verification and documentation.

High Confidence Reconfigurable Distributed Control

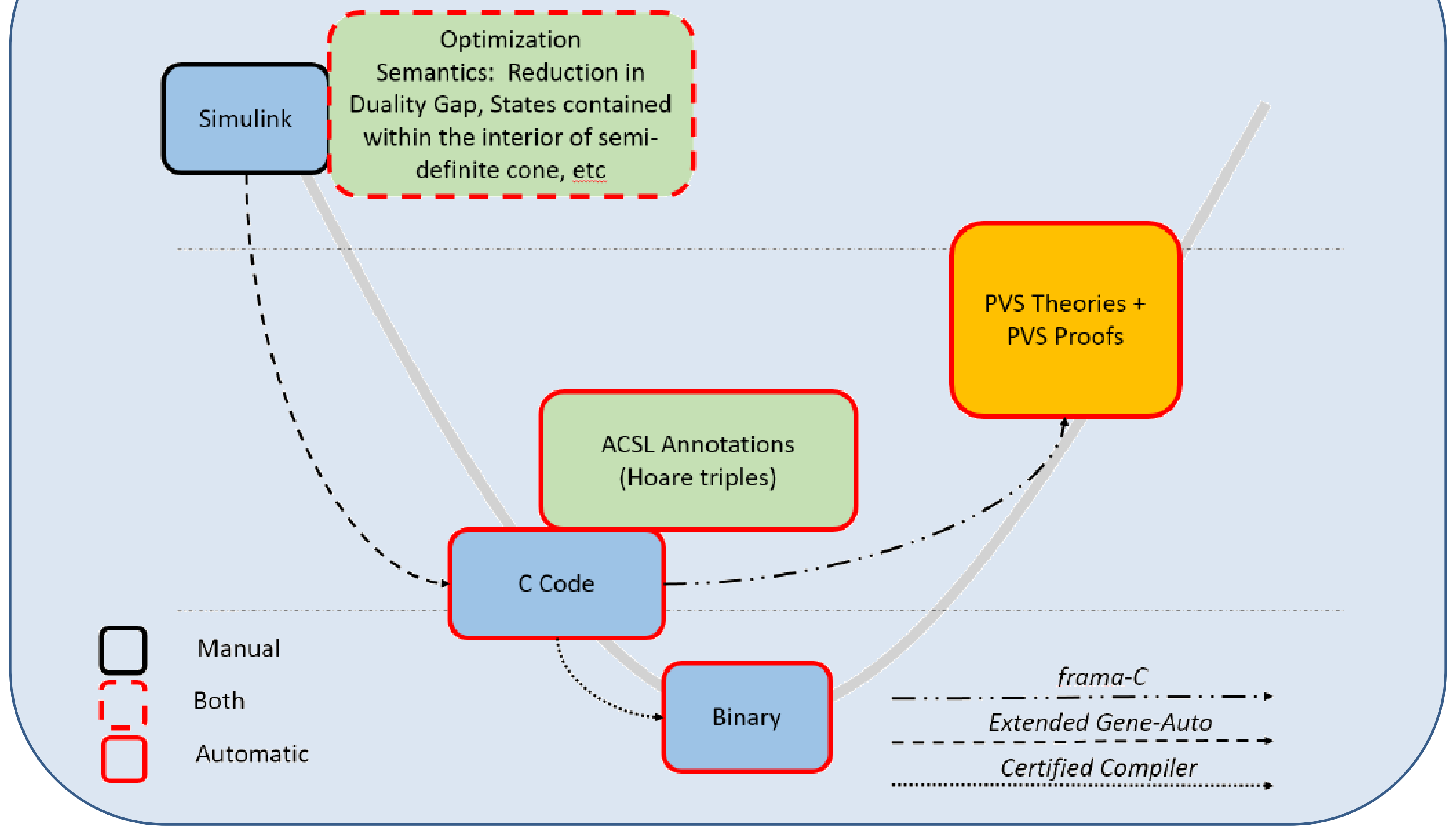


Caltech Ducted Fan

- Develop and validate an optimization-based, hierarchical control architecture for motion control systems.
- Exploit new theoretical results in the development of receding horizon optimization objectives to provide guaranteed stability for aggressive flight vehicles.
- Employ geometric methods to drastically reduce online computational requirements.



Towards a Formally Verified Process



Simulink

Optimization Semantics: Reduction in Duality Gap, States contained within the interior of semi-definite cone, etc

PVS Theories + PVS Proofs

ACSL Annotations (Hoare triples)

C Code

Binary

□ Manual

Both

Automatic

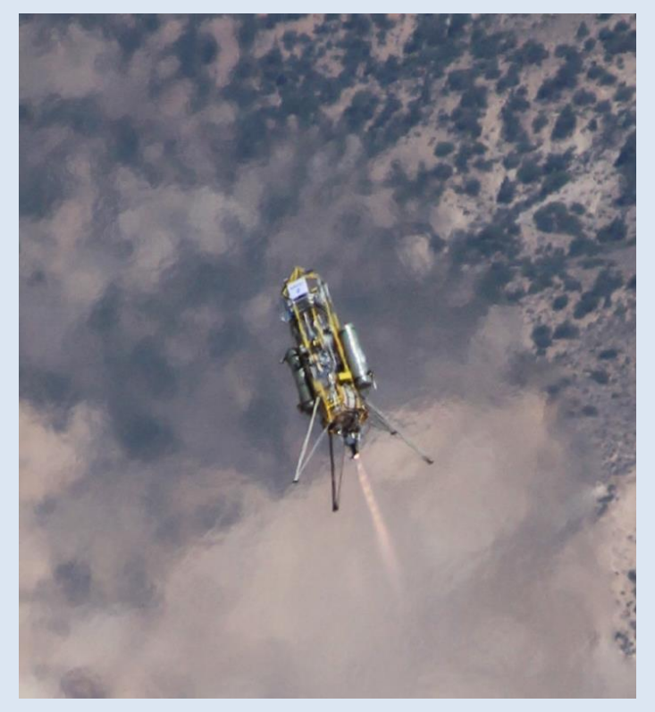
frama-C

Extended Gene-Auto

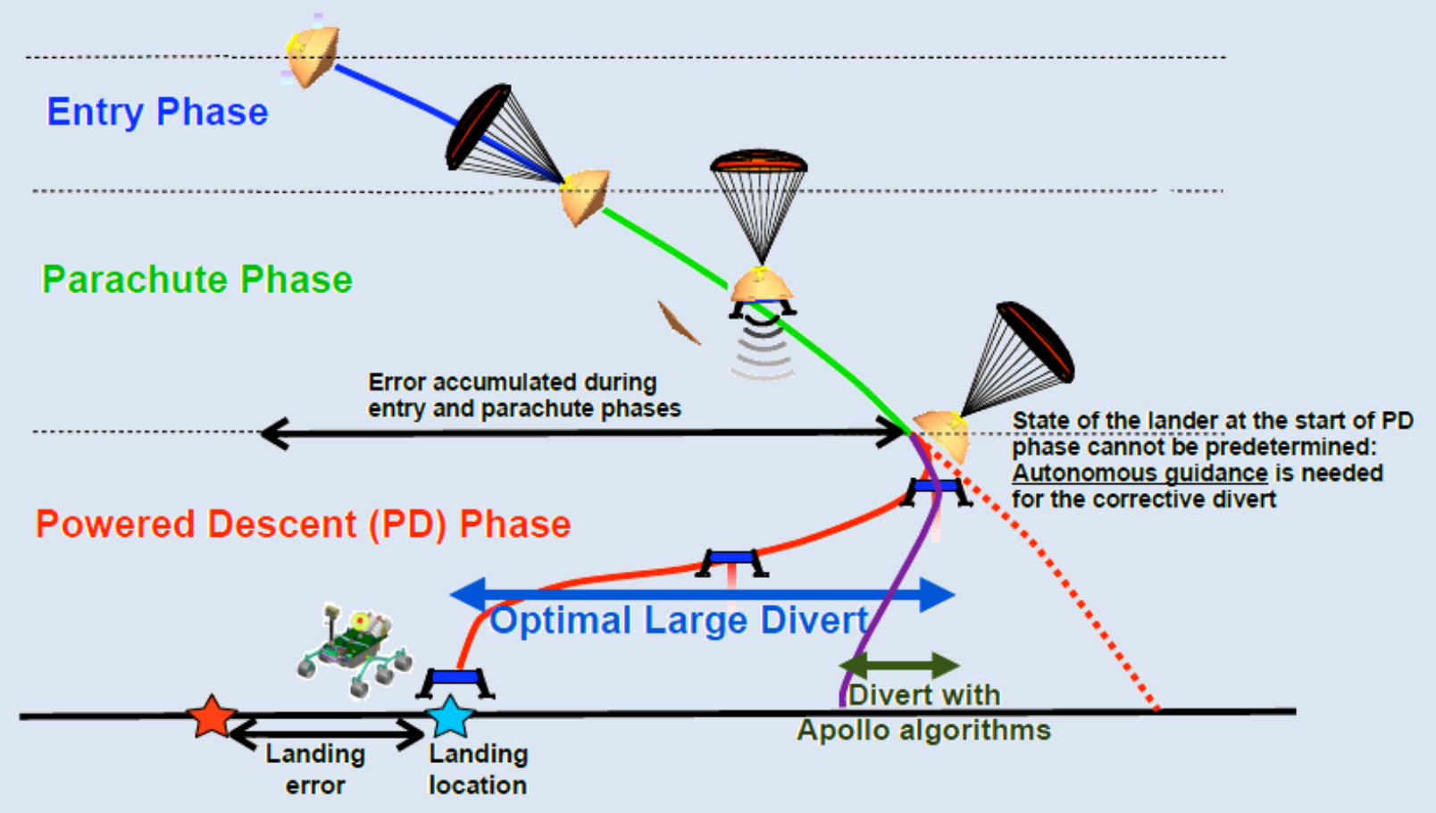
Certified Compiler

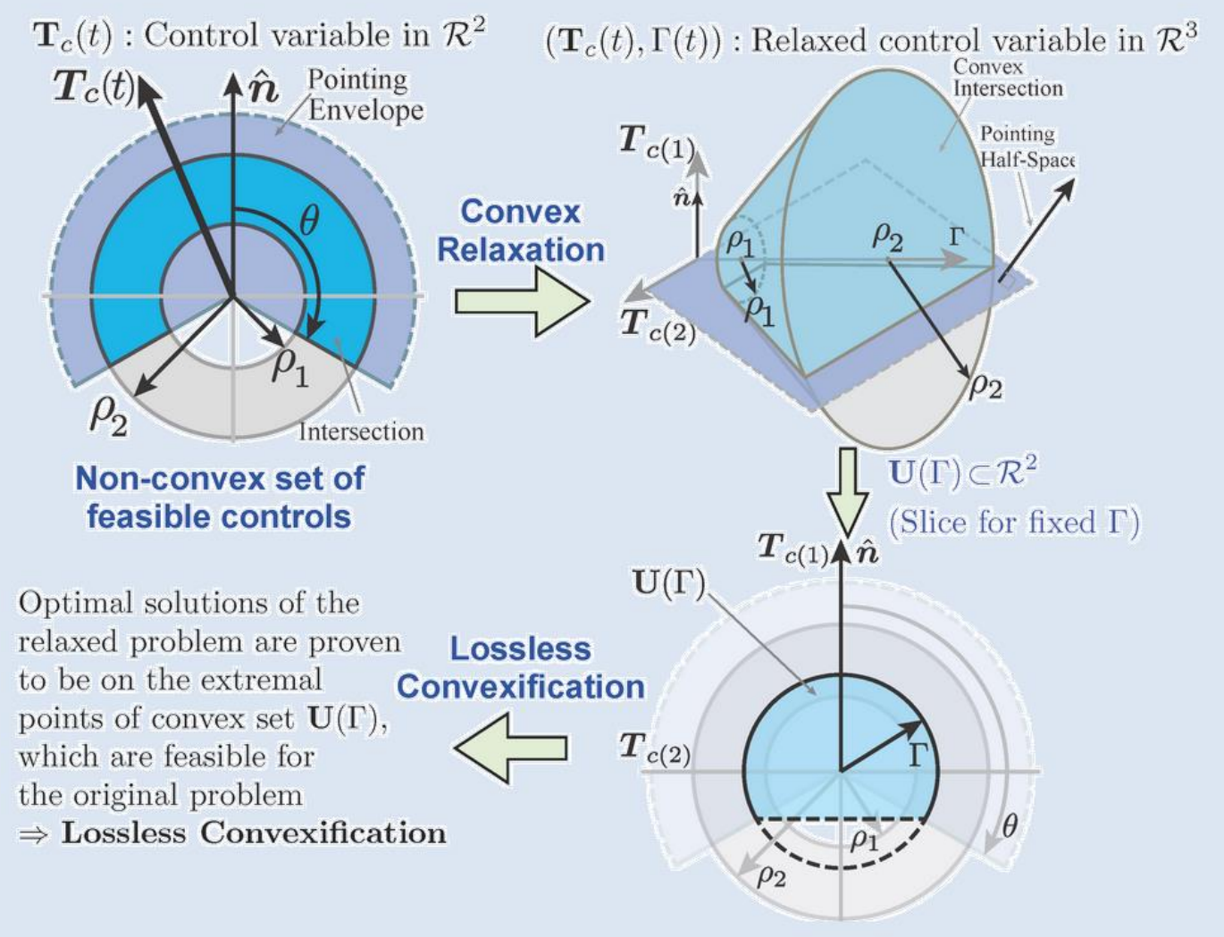
Real Time Convex Optimization: Mars Lander guidance

- NASA test rocket guided by the first real-time convex optimization based control algorithm.
- The rocket has bees guided for an aggressive maneuver that was not possible with traditional methods, proving an order of magnitude improvement on the rocket's flight envelope.



- A fuel optimal guidance planetary powered descent algorithm is developed to autonomously compute the fuel optimal path that takes the lander vehicle to a given surface target on a planet without violating any mission constraints.
- The algorithm is based on a fundamental result, known as lossless convexification that provides the solution of a general class of nonconvex optimal control problems.


Entry Phase
Parachute Phase
Error accumulated during entry and parachute phases
State of the lander at the start of PD phase cannot be predetermined: Autonomous guidance is needed for the corrective divert
Powered Descent (PD) Phase
Optimal Large Divert
Divert with Apollo algorithms
Landing error
Landing location

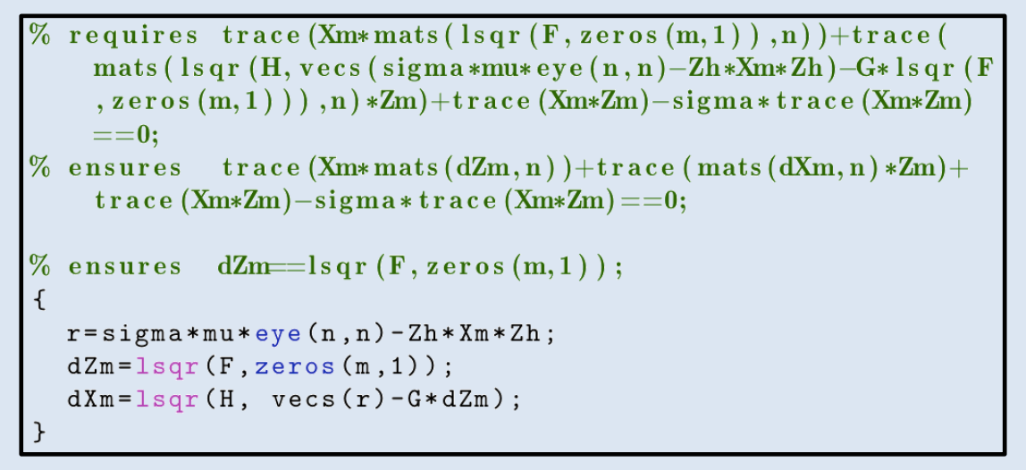

$\mathbf{T}_c(t)$: Control variable in $\mathcal{R}^2$
$(\mathbf{T}_c(t), \Gamma(t))$: Relaxed control variable in $\mathcal{R}^3$
$T_c(t)$
$\hat{n}$
Pointing Envelope
θ
ρ_1
ρ_2
Intersection
Non-convex set of feasible controls
Convex Relaxation
Convex Intersection
Pointing Half-Space
$T_{c(1)}$
$T_{c(2)}$
Γ
$\mathbf{U}(\Gamma) \subset \mathcal{R}^2$
(Slice for fixed Γ)
$\mathbf{U}(\Gamma)$
Lossless Convexification

Optimal solutions of the relaxed problem are proven to be on the extremal points of convex set $\mathbf{U}(\Gamma)$, which are feasible for the original problem
⇒ **Lossless Convexification**

Initial Effort: Manually Carrying down Proof of Convergence to Code Level

- We have manually annotated an Interior Point algorithm written in Matlab with comments describing its semantics
- In particular, high-level properties of interest such as linear duality gap decrease were expressed formally on the implementation.

$$\begin{array}{ll} \inf\limits_{p,X} & \langle b,p\rangle \\ \text{subject to} & F_0 + \sum_{i=1}^{m} p_i F_i + X = 0 \\ & X \succeq 0. \end{array}$$

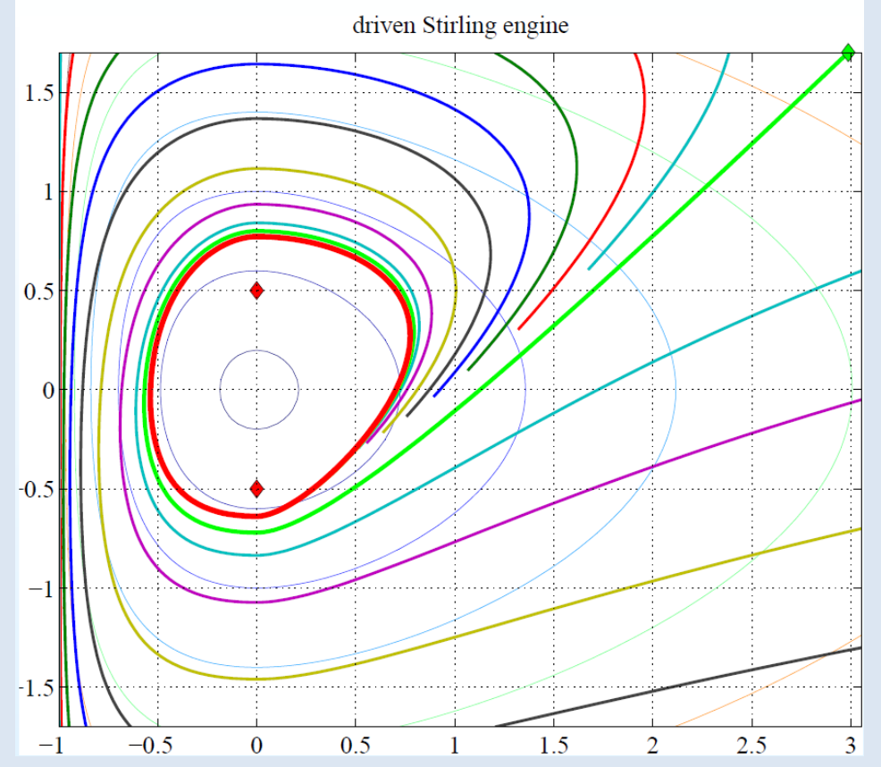


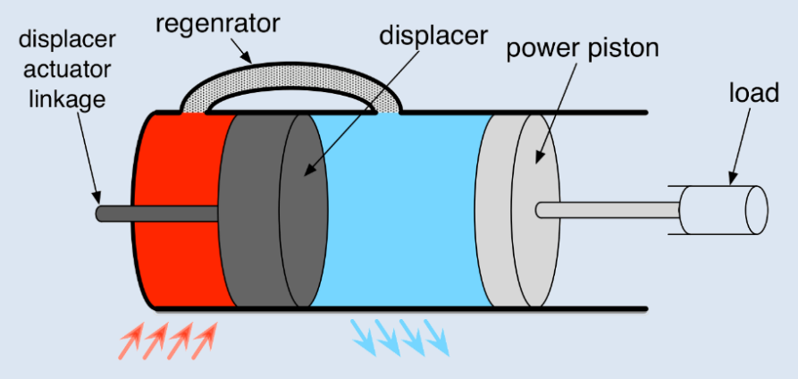
```
% requires  trace(Xm*mats(lsqr(F,zeros(m,1)),n))+trace(
    mats(lsqr(H,vecs(sigma*mu*eye(n,n)-Zh*Xm*Zh)-G*lsqr(F
    ,zeros(m,1))),n)*Zm)+trace(Xm*Zm)-sigma*trace(Xm*Zm)
    ==0;
% ensures   trace(Xm*mats(dZm,n))+trace(mats(dXm,n)*Zm)+
    trace(Xm*Zm)-sigma*trace(Xm*Zm)==0;

% ensures  dZm==lsqr(F,zeros(m,1));
{
  r=sigma*mu*eye(n,n)-Zh*Xm*Zh;
  dZm=lsqr(F,zeros(m,1));
  dXm=lsqr(H, vecs(r)-G*dZm);
}
```

Dynamics of the Stirling Engine

- Hartman-Grobman Theorem gave well defined first return map.
- bounded monotone sequences used to get separatrix (undriven) and bounding periodic orbit (bang-bang).
- Brouwer Fixed Point Theorem showed existence of (at least one) periodic solution of the periodically driven Stirling engine model (and other bounded response systems!)





Equation of the driven stirling engine

$$\dot{z} = w - cz - cu$$
$$\dot{w} = \frac{-z}{1+z}$$
$$u = y + \frac{\dot{y}}{c}$$

Project's Tasks and Output:

- **Proof-Carrying automatic code generation:**
  - Semantics: Identify semantics associated with embedded, real-time optimization algorithms
  - Front-end: proof-carrying autocoder that implements convex optimization algorithms and their semantics
  - Back-end: Analyzer allowing us to demonstrate that the output of the autocoder is indeed analyzable, and provably correct.
- **Floating point arithmetic management**
- **Nonconvex optimization routines**

Output : - *"Credible Autocoding of Convex Optimization Algorithms"* accepted article in *Optimization Engineering.*
- *Building an Autocoder that generates Formally Verified Real Time Optimization Algorithms*