BAHRIA UNIVERSITY (KARACHI CAMPUS)

Assignment 1

Formal methods in software engineering

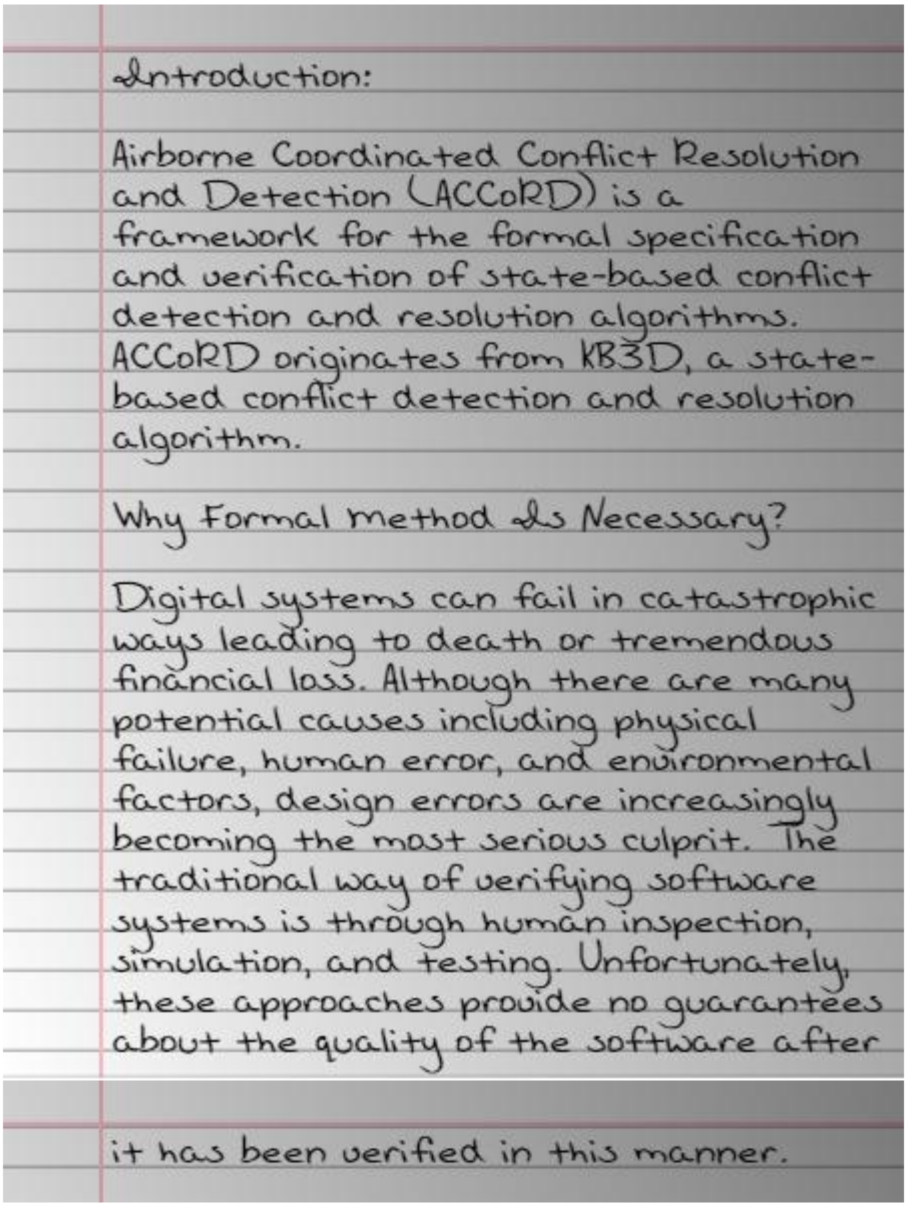
Class: **(BSE 5A/5B)**

Course Instructor: **(FAIZ UL HAQUE ZEYA)** Max Marks:5

Student's Name: M Muaz Shahzad Reg. No:02-131202-081

CLO 1

Summarize **A**irborne **C**oordinated **Co**nflict **R**esolution and **D**etection (**ACCoRD**) of NASA.

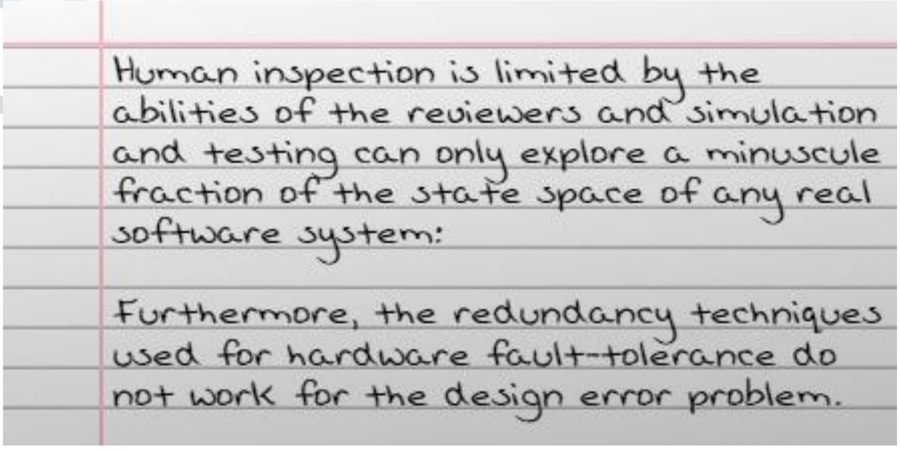


Introduction:

Airborne Coordinated Conflict Resolution and Detection (ACCoRD) is a framework for the formal specification and verification of state-based conflict detection and resolution algorithms. ACCoRD originates from KB3D, a state-based conflict detection and resolution algorithm.

Why Formal method Is Necessary?

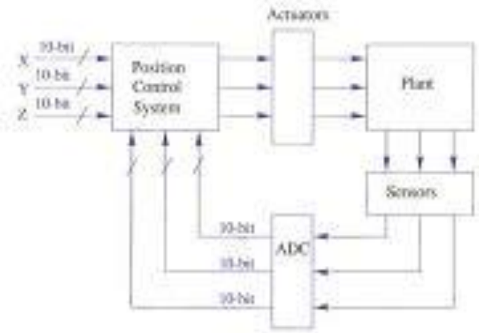
Digital systems can fail in catastrophic ways leading to death or tremendous financial loss. Although there are many potential causes including physical failure, human error, and environmental factors, design errors are increasingly becoming the most serious culprit. The traditional way of verifying software systems is through human inspection, simulation, and testing. Unfortunately, these approaches provide no guarantees about the quality of the software after it has been verified in this manner.

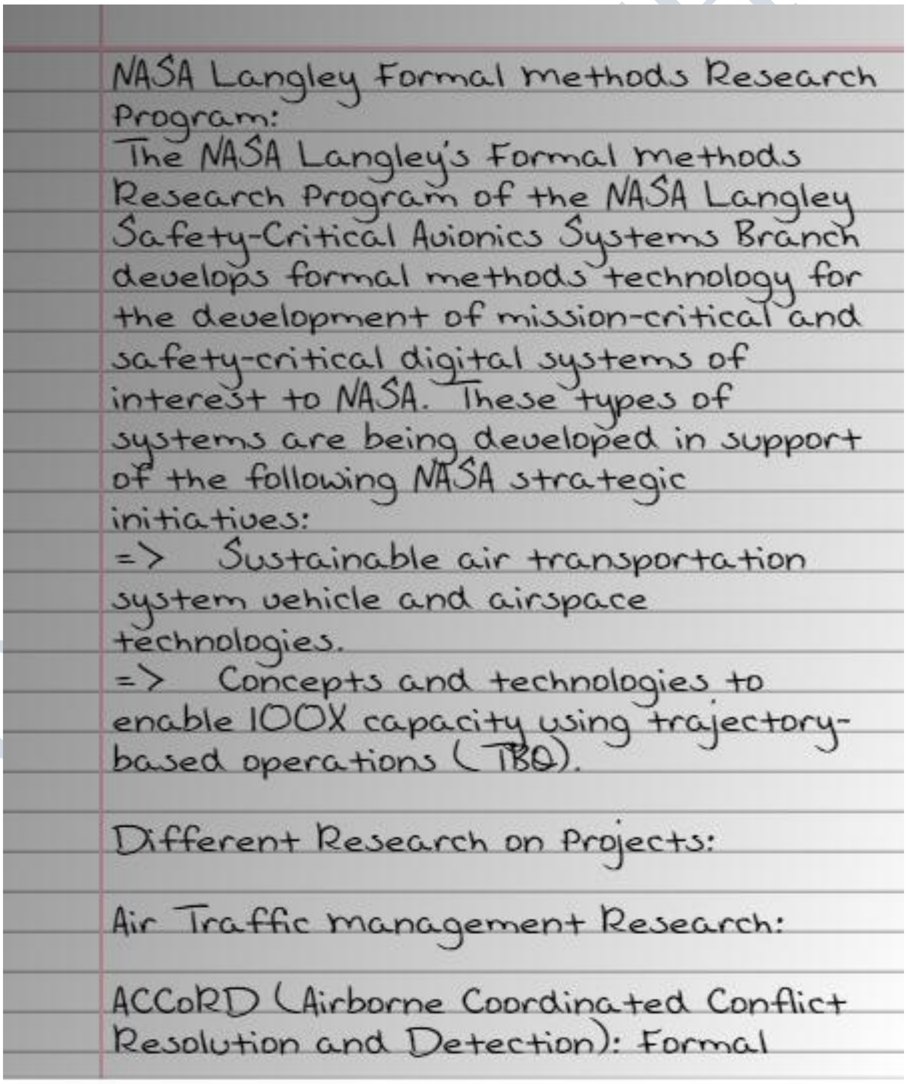


Human inspection is limited by the abilities of the reviewers and simulation and testing can only explore a minuscule fraction of the state space of any real software system:

Furthermore, the redundancy techniques used for hardware fault-tolerance do not work for the design error problem.

Size of State Space for Simple System





NASA Langley Formal methods Research Program:

The NASA Langley's Formal methods Research Program of the NASA Langley Safety-Critical Avionics Systems Branch develops formal methods technology for the development of mission-critical and safety-critical digital systems of interest to NASA. These types of systems are being developed in support of the following NASA strategic initiatives:

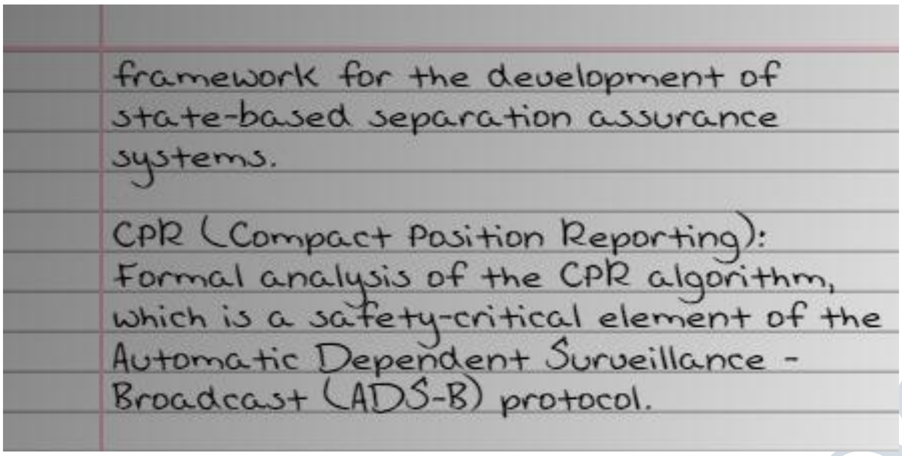
=> Sustainable air transportation system vehicle and airspace technologies.

=> Concepts and technologies to enable 100X capacity using trajectory-based operations (TBO).

Different Research on Projects:

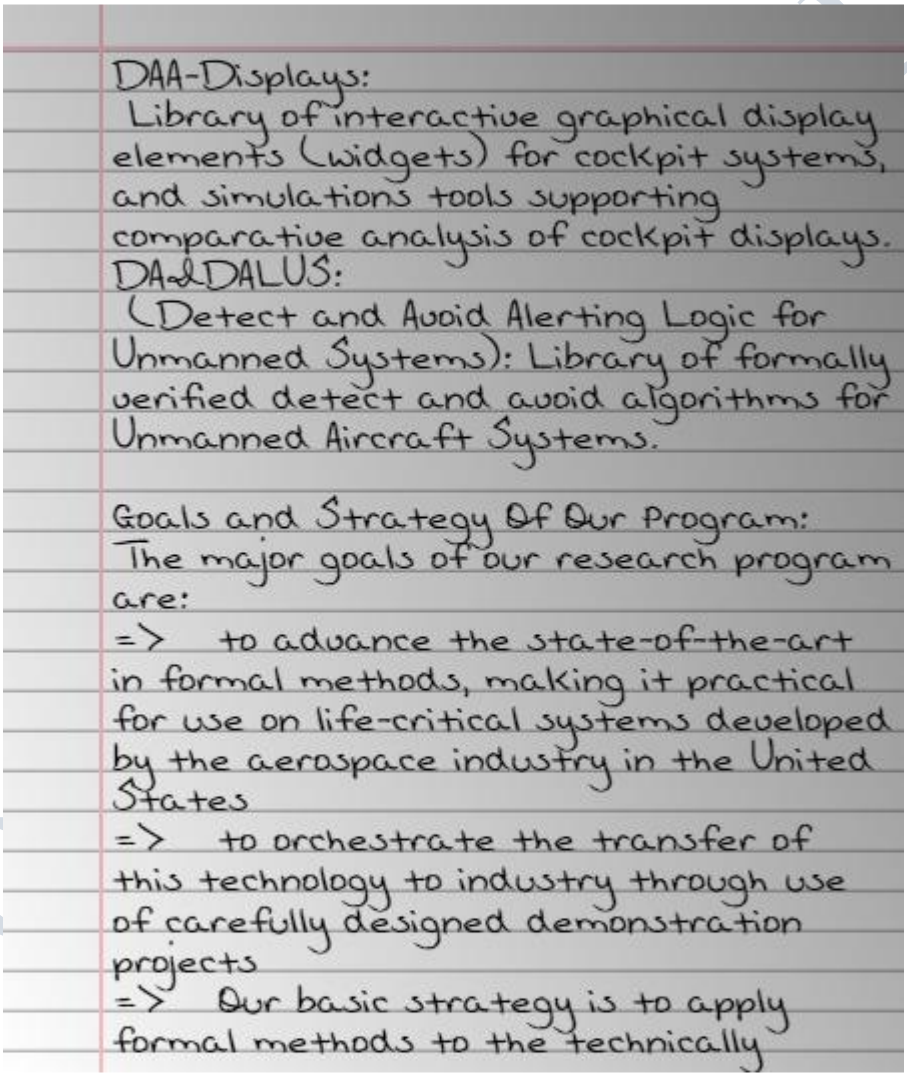
Air Traffic management Research:

ACCoRD (Airborne Coordinated Conflict Resolution and Detection): Formal



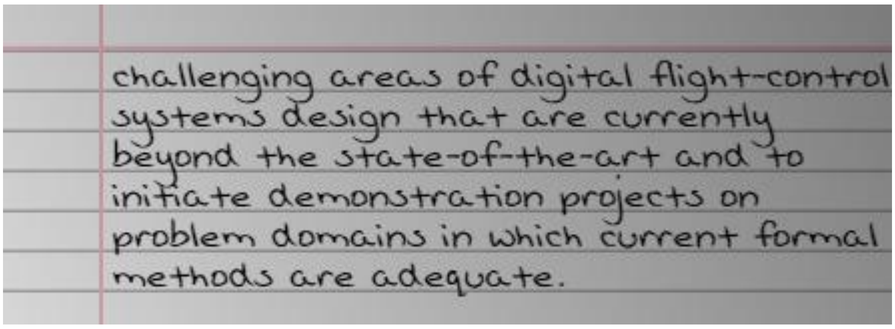
framework for the development of state-based separation assurance systems.

CPR (Compact Position Reporting): Formal analysis of the CPR algorithm, which is a safety-critical element of the Automatic Dependent Surveillance - Broadcast (ADS-B) protocol.

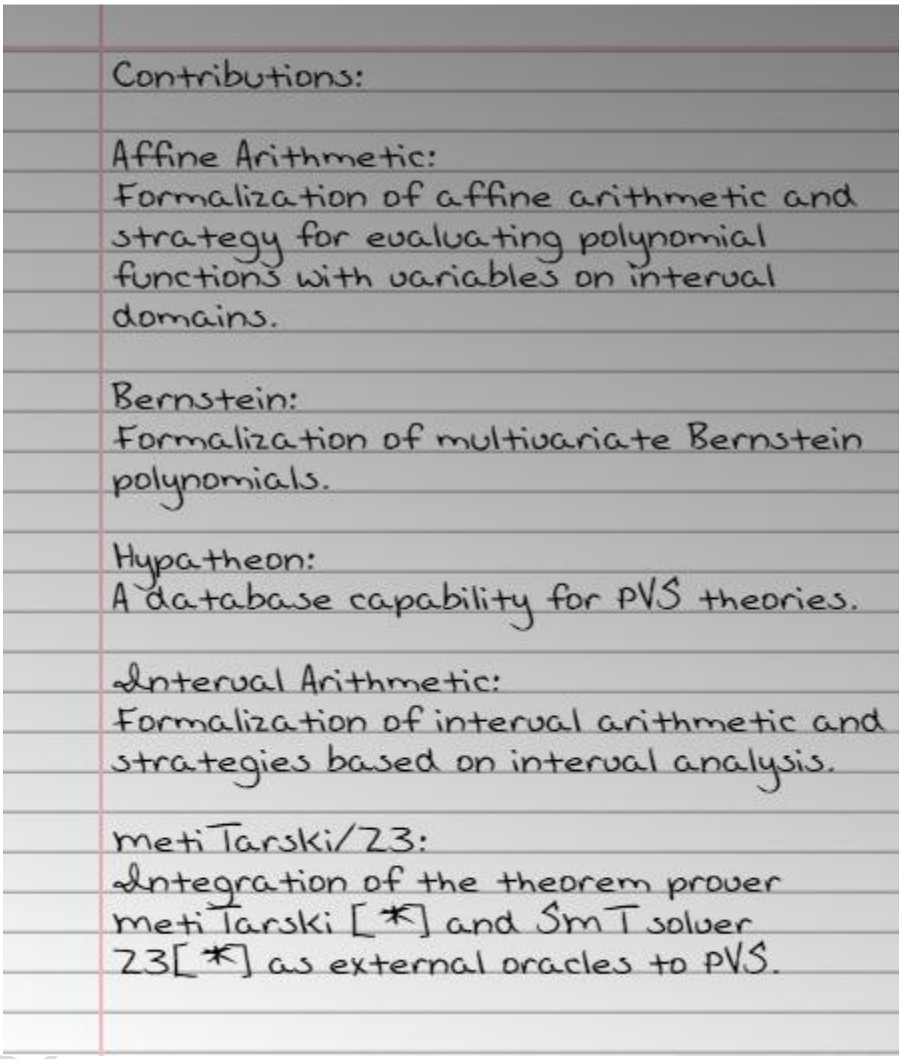


DAA-Displays:
Library of interactive graphical display elements (widgets) for cockpit systems, and simulations tools supporting comparative analysis of cockpit displays.
DA&DALUS:
(Detect and Avoid Alerting Logic for Unmanned Systems): Library of formally verified detect and avoid algorithms for Unmanned Aircraft Systems.

Goals and Strategy Of Our Program:
The major goals of our research program are:
=> to advance the state-of-the-art in formal methods, making it practical for use on life-critical systems developed by the aerospace industry in the United States
=> to orchestrate the transfer of this technology to industry through use of carefully designed demonstration projects
=> Our basic strategy is to apply formal methods to the technically



challenging areas of digital flight-control systems design that are currently beyond the state-of-the-art and to initiate demonstration projects on problem domains in which current formal methods are adequate.



Contributions:

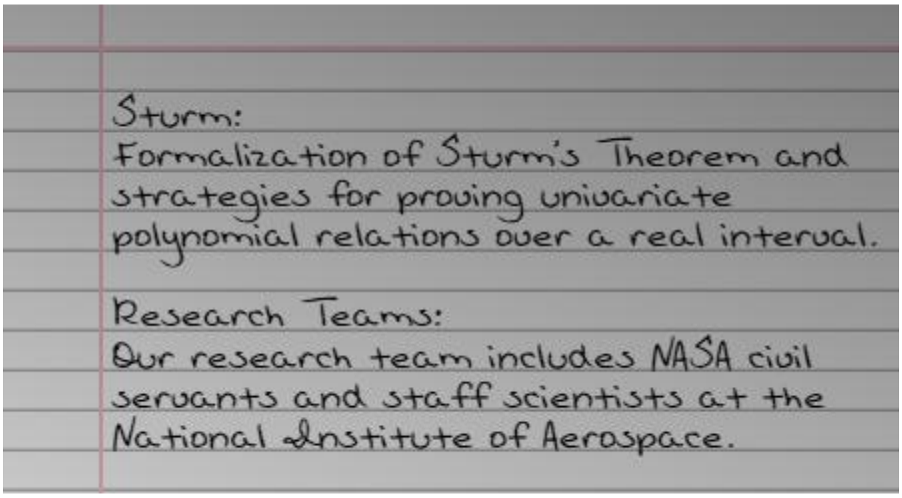
Affine Arithmetic:
Formalization of affine arithmetic and strategy for evaluating polynomial functions with variables on interval domains.

Bernstein:
Formalization of multivariate Bernstein polynomials.

Hypatheon:
A database capability for PVS theories.

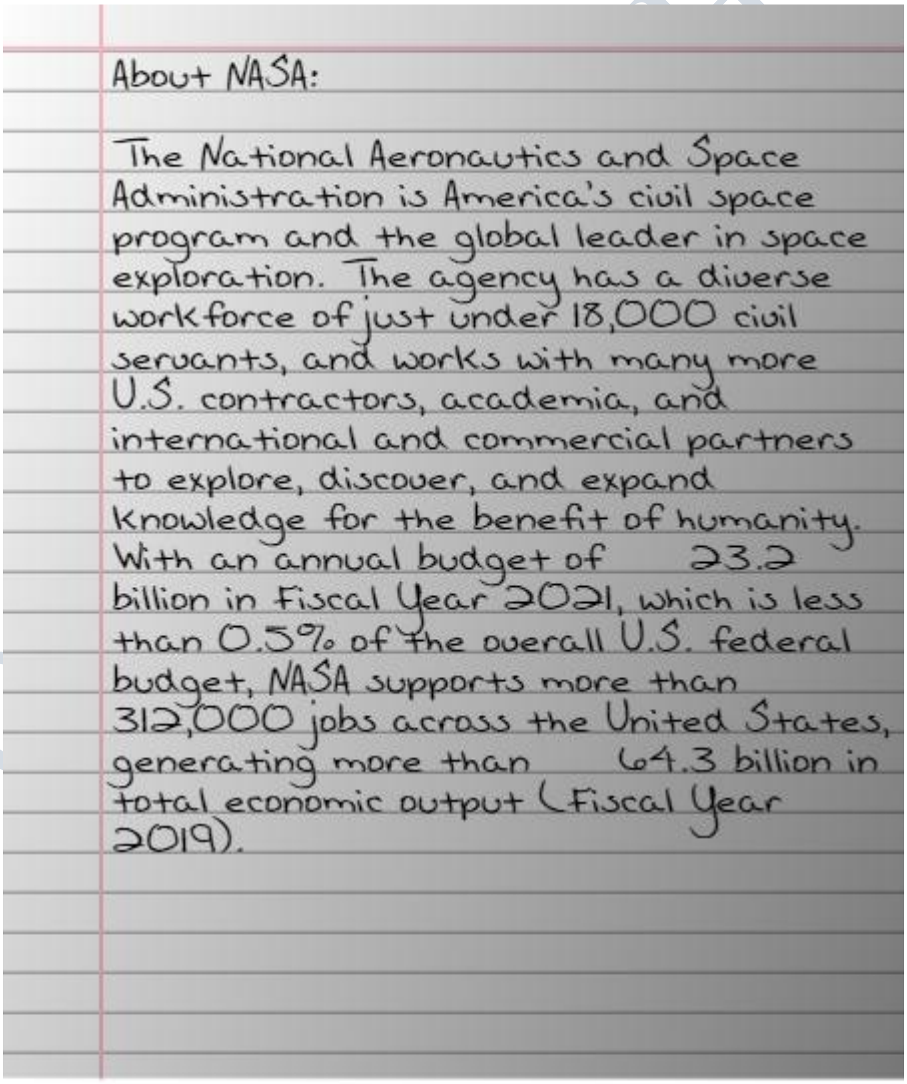
Interval Arithmetic:
Formalization of interval arithmetic and strategies based on interval analysis.

metiTarski/Z3:
Integration of the theorem prover metiTarski [*] and SmT solver Z3[*] as external oracles to PVS.



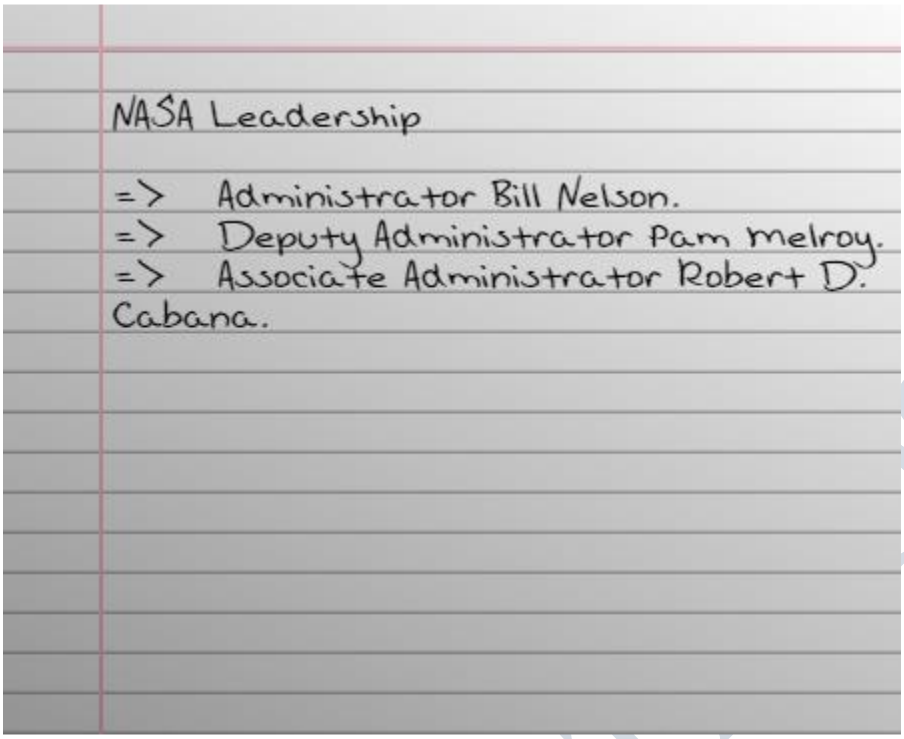
Sturm:
Formalization of Sturm's Theorem and strategies for proving univariate polynomial relations over a real interval.

Research Teams:
Our research team includes NASA civil servants and staff scientists at the National Institute of Aerospace.



About NASA:

The National Aeronautics and Space Administration is America's civil space program and the global leader in space exploration. The agency has a diverse workforce of just under 18,000 civil servants, and works with many more U.S. contractors, academia, and international and commercial partners to explore, discover, and expand knowledge for the benefit of humanity. With an annual budget of 23.2 billion in Fiscal Year 2021, which is less than 0.5% of the overall U.S. federal budget, NASA supports more than 312,000 jobs across the United States, generating more than 64.3 billion in total economic output (Fiscal Year 2019).



NASA Leadership

=> Administrator Bill Nelson.
=> Deputy Administrator Pam melroy.
=> Associate Administrator Robert D. Cabana.