Asteroid Approach Final Report
15-424 Foundations of Cyber-Physical Systems

Kerry Snyder

Abstract

The recent identification of near earth objects with the potential to either harm earth or provide boundless wealth has lead to an uptake in the number of space missions directed at asteroids and comets by both public entities and private companies. One key need shared between all of these missions is the ability to safely approach and land on an asteroid. This research tackles the problem of safely and efficiently controlling a spacecraft to softly touchdown on an asteroid so that a wide variety of scientific and commercial tasks can be accomplished. Safety conditions in a reduced dimension space are derived from physical equations and then proven using the logical verification tool KeYmara. Then, efficiency conditions are explored and compared to fuel use information from an actual asteroid landing mission.

Introduction

In 1986, the ESA's Giotto spacecraft returned the first close up images of a comet or asteroid, passing within 596 km of Halley's Comet. The NEAR Shoemaker mission, which was launched by NASA ten years later, studied the asteroids 253 Mathilde and 433 Eros and ended its mission by successfully soft-landing on Eros. More recently, the Asteroid Redirect Mission has been proposed by NASA to move an asteroid into lunar orbit to be studied by humans. All of these missions share a common theme which is a small but very expensive spacecraft approaching a very large misshapen rock. It is therefore imperative that these missions can safely approach and function in close proximity with an asteroid.

This work studies the logical verification of various aspects of an asteroid probe mission. Such verification has a broad impact in the field of space robotics. The recent Rosetta comet landing mission by ESA cost a total of 1.6 billion EUR or almost 2 billion USD. Further, it took almost a month for the team to plan and execute a rendezvous with the comet, a very challenging mission with a somewhat disappointing ending. The older NEAR mission only cost 224 million, but spent over a year orbiting EROS before its final soft touchdown was planned and executed. Finally, the Asteroid Redirect Mission requires human safe operations, so verifiable safety is of utmost importance.

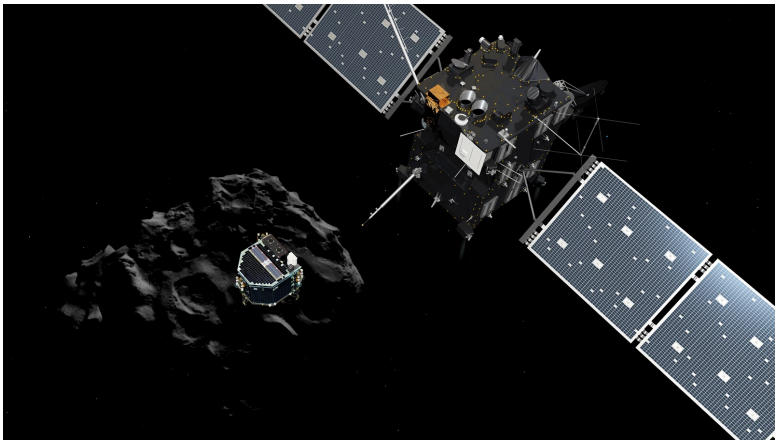

Figure 1: Rosetta probe and Philae Lander near Comet 67P/Churyumov-Gerasimenko. Credit: ESA

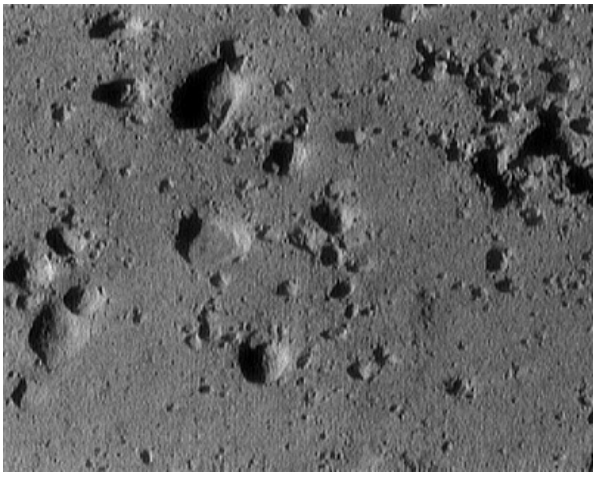

Figure 2: Regolith from the asteroid 433 Eros, imaged by NEAR Shoemaker during its descent to the surface. Credit: NASA

The Asteroid Redirect Mission Concept of Operations describes many of the key phases of an asteroid approach mission. Once the vehicle has come within 100-200km of the target, it spends some time orbiting and surveying the target until enough knowledge is gained to make a safe approach. This knowledge includes size, shape, rotational rate, albedo, and gravity. Once a trajectory has been planned, the vehicle begins its “descent” with some degree of remote monitoring and control and eventually completes its landing or approach. As the distance between the satellite and the asteroid decreases, the risk of damage increases, which is why the planning process typically takes months rather than hours.

Prior Work

In the past, probabilistic methods have been the standard means of verification of spacecraft systems, particularly monte carlo experiments. These methods involve simulating the system and controller for a certain amount of time from a distribution of input conditions and then fitting a distribution to the output states in order to determine expected performance and dispersion[2]. In order to compute a statistically significant posterior distribution, hundreds of thousands to tens of millions of runs of the simulation and controller are necessary which takes significant time and computational power. This method has been applied to the study of the probability of collision of satellites rendezvousing in orbit, a similar problem, with 50,000 to 500,000 runs taking hours to days to run[3]. It also has heritage in the Apollo missions, such as determining crew safety in an early launch abort [4].

In recent years, formal verification of Cyber-Physical Space Systems has been studied with increasing effort. A chinese team considered model checking and theorem proving in the study of the descent guidance of a lunar lander and were able to verify a variety of safety properties during one of six phases of descent to the lunar surface[5]. Another study looked again at the problem of satellite rendezvous, from the perspective of model checking rather than monte carlo analysis[6]. This publication focused in particular on orbital dynamics for satellite operation in earth orbit and was able to verify safety in circular orbits in the presence of sensing and thrust uncertainties. The primary difference between this prior work and the work of this research is the location and relative sizes in the approach. For the approach of an asteroid, the gravity and orbit of the earth is often minimal whereas the gravity of the target itself is not. This introduces challenges as the spacecraft is always accelerating towards the target. These challenges and others are addressed in this research.

Developments

Model Development

The first step in verifying an asteroid-satellite cyber-physical system is developing a physical model of the continuous time dynamics and the discrete control system. The dynamical model was developed with many simplifying assumptions. First, motion is only considered in two axes, the vector of approach between the asteroid and satellite and “roll” rotation about that axis. This covers the primary control objective of the asteroid redirect mission is to approach very close to an asteroid, match its rotational rate, and then either capture it or retrieve a sample. Next, acceleration due to gravity was modeled as a single constant value. In reality, most asteroids have a very noncircular shape and highly nonuniform density, both of which contribute to what is known as a “lumpy” gravity model. In order to properly navigate and plan a guidance trajectory, these differences are very important. However, for the actual control, a simplified gravitational acceleration is sufficient. This also leads to straightforward differential equation solutions in the initial system, greatly simplifying the initial safety proof.

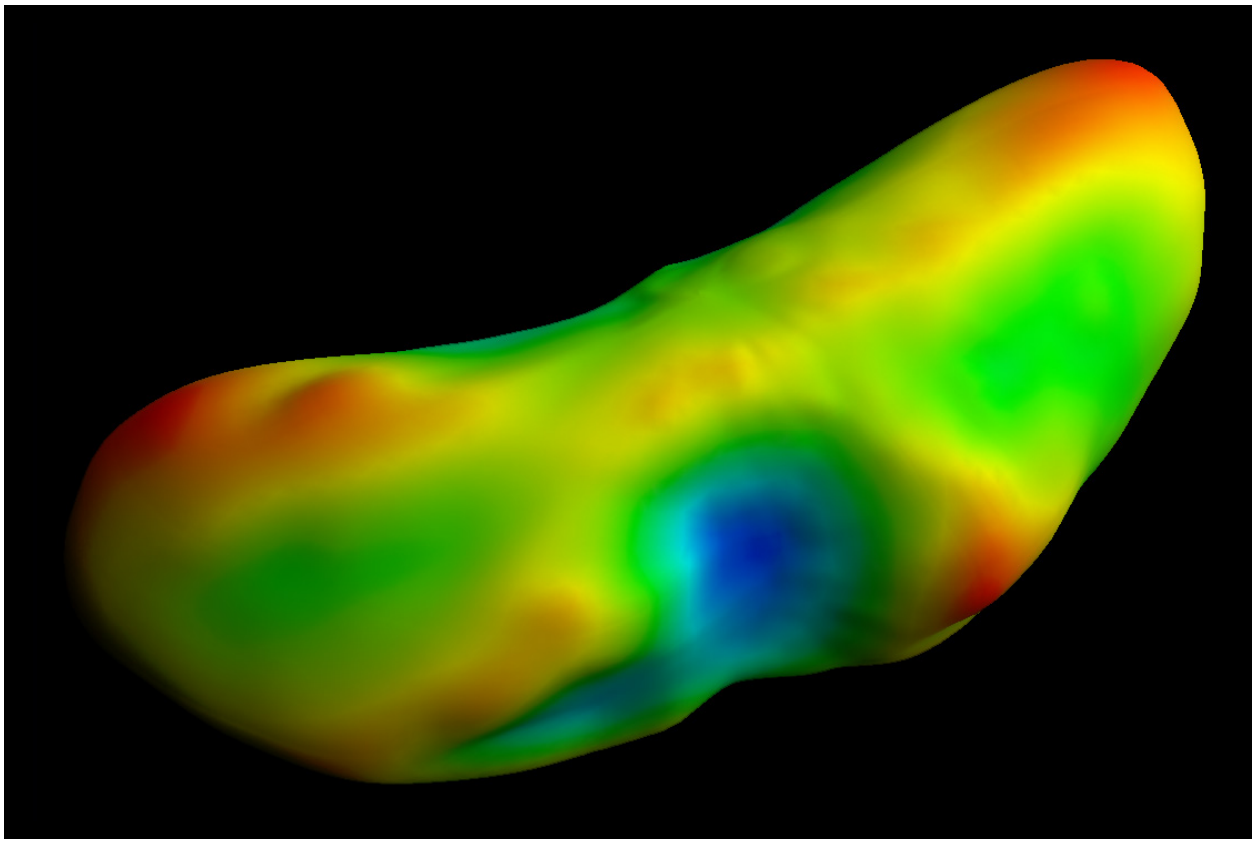

Figure 3: Gravitational Topography model of the asteroid 433 Eros computed by the NEAR mission. Credit: NASA

For the discrete part of the hybrid system, a time triggered controller was developed to match a realistic real-time satellite control system. At a fixed but arbitrary time constant, the controller uses perfect knowledge of the state of the system to decide whether or not it is necessary to brake. To do so, it determines the distance that it will accelerate due to gravity over the next time step and compares this to the amount of distance that it would take to brake at that end velocity. If the distance traveled is beyond the braking threshold distance, the asteroid will chose to brake over the next time step. If it is not, it will be able to safely

accelerate and take control after a full time step. Since the controller is time triggered, this decision is repeated and a loop invariant is required for non-trivial proofs.

$$p - v * T - \frac{1}{2}gT^2 > \frac{-(v+g*T)^2}{2(g-B)}$$

Equation 1: Control Decision, the true case is acceleration and the false case is braking

The final consideration that I had planned was the inclusion of an evolution domain in the differential equations describing the state. The evolution constraint was that the controller ceases as soon as velocity reaches zero. In a real system, an approach would consist of multiple temporary pauses, potentially with the satellite moving opposite the direction of the target asteroid. The other evolution domain constraints are more realistic, as the final touchdown (at $p = 0$) should complete the operation of the controller and safety, such that this is not a crash, must be considered separately. In the development of this model, one constraint that I did not initially consider is the relative magnitude of the braking acceleration versus the gravitational acceleration of the asteroid. In retrospect, it makes sense that the braking acceleration must be strictly greater than the gravitational acceleration in order for the vehicle to come to a stop as it must cancel the gravity of the asteroid and also decrease its velocity.

Safety Condition

Due to the aforementioned evolution domain constraints, a stronger safety condition that accounts for both position and velocity is needed. Since we will know nothing about time, this condition must be invariant of any knowledge about the time so far or the time remaining. This naturally leads to the following well known equation of motion: $v_f^2 = v_o^2 + 2(g - B)(p_f - p_o)$. From this equation, we can fill in the properties of our single dimension asteroid-satellite system and find an invariant on the evolution of the system that leads to a safety proof. The initial velocity v_i is the current velocity of the spacecraft. The final velocity v_f is zero, as the satellite must come to a complete stop. The acceleration is the net acceleration when braking, which is simply $g - B$. The final position p_f is the surface of the asteroid, located at $p = 0$, and the initial position p_i is the current position of the spacecraft, p. Finally, for clarity, this equation is solved for p, which yields $p \geq \frac{-v^2}{2(g-B)}$.

This safety condition also serves as part of the loop invariant since it provides a convenient abstraction of the relationship between position and velocity necessary for safety to be maintained. This loop invariant and the solutions to the differential equations are enough to verify this same condition as a safety property and validate the overall hybrid system automatically in KeYmara. This yields a solid base system that is further iterated in the following sections.

Rotation Matching

The next control operation that is needed for an asteroid approach mission is rotation rate matching. Many near earth asteroids have been observed to rotate at a variety of rates, typically with a period of “between one hour and one day”[7]. This is rather slow in comparison to the thrust capabilities of space probes, which typically either use reaction wheels or

monopropellant thrusters. Reaction wheels use flywheels and the conservation of angular momentum to impart changes in rotational velocity, which allows for very precise pointing. Thrusters impart an offset force tangent to the desired rotation axis and can be modulated at different lengths of time to produce varying magnitudes of thrust. Either of these methods can can produce a somewhat arbitrary change in rotational velocity over a given period of time. For this reason, the rotation matching part of the controller computes the thrust necessary to match rates with the asteroid over the next time step and then applies that thrust. Proof of this property becomes trivial with two additions: adding a precondition that we are at least one time step away from the asteroid and adding a test after the differential equation that only allows physics to run for exactly the time step duration. Although these conditions are limiting, they are valid for a real world system. Both of the aforementioned rotational actuators can vary their angular acceleration output and most control systems run as a hard real-time fixed rate control loop with (verifiably) no possibility of other time steps. Finally, as modeled the asteroid rotation rate must be greater than the satellite rotation rate, since these cases mirror each other. Proving both at the same time only compounds the branch space without yielding any new knowledge.

An alternative model that was implemented but not proven was moving the thrust velocity physics to the discrete portion of the cyber-physical system. Instead of imparting an angular acceleration over a certain amount of time, this system would represent an instantaneous change in angular velocity. This more closely matches the profile of the cold-gas thruster than the previous model, although differential mechanics would probably also be necessary for a complete system model. The precondition for such a model would be that the distance to the asteroid will not be covered in fewer than n timesteps, where the difference between the rotational rates of the asteroid and probe differ by less than $n * T$.

Fuel Use

The next critical modeling concern in an asteroid-satellite system is that of fuel use. Typically, the dry mass of a satellite or deep space probe is less than half of the total mass at takeoff, with the rest taken up by fuel. Any accurate model of spacecraft dynamics must consider changing mass, as the acceleration due to the thrust of a rocket engine depends on both the theoretically constant force output of the engine and the current instantaneous mass. For these reasons, dynamic mass and fuel use were the next modeling and proving challenges that I tackled.

The dynamic mass system requires a variety of new variables (only one of which actually varies over time) which I will define first for clarity. First, m tracks the actual current mass of the satellite, which varies over time due to fuel use. The value of m at the beginning of operation is defined as mi, which also serves as an upper bound for m throughout the propagation of this model. Both m and mi are initialized to the sum of dm and M, which are dry mass and fuel mass, respectively. The dry mass of the system is the mass of the physical components of the satellite and empty fuel tanks and serves as a lower bound on m. The fuel mass shall be initialized based the stopping requirements.

Some other new variables are necessary to replace the constant braking acceleration used in the previous model. First, the force output of the engine is defined as f, which is modeled as a constant value. Although noise, vacuum, and ramp-up effects exist that can vary this value, these changes are out of scope of this project and can be reasonably approximated with a constant value. Next, the specific impulse I_{sp} of the engine must be modeled. Specific impulse is an efficiency measure that relates mass of fuel used to the firing time and force output of the engine. As this value is typically computed with respect to earth gravity, its constant value is also included and initialized.

Based on this concept of mass, we can begin modifying the original physics model to account for changing mass. The first change is in the acceleration value. Braking is no longer a fixed acceleration constant but rather it is defined as the force output of the engine divided by the current mass: $\frac{a*f}{m}$. Since mass is also changing with time, this immediately complicates the differential equations and implies that a proof will need to use invariant based methods rather than the direct ODE solution. The actual change in mass over time depends on the thrust force of the engine, its specific impulse, and the gravitational acceleration of earth: $\frac{dm}{dt} = \frac{-a*f}{I_{sp}*g_e}$. One note is that a has been changed to a binary flag deciding whether or not the spacecraft should thrust, so that these differential equations have symbolic access to the changing variables rather than constant access. Next, all other references to the old constant braking acceleration of B are changed to $\frac{f}{mi}$. This is a good lower bound on the braking acceleration as mass can only decrease, causing this acceleration value to increase. An increase in braking acceleration is strictly safer for the satellite probe system as it will more quickly be able slow its velocity. Once important note is that this model no longer includes the rotation matching controls. This was done primarily to simplify the proof process, as the only coupling between the two are the distance needed to match rates. This is also valid from the standpoint of fuel use for rotation and pointing as it typically consists of less than five percent of the overall fuel budget. These are all of the changes needed for the model specifically, next we will look at the changes in proof invariants.

As discussed, we can no longer take advantage of the ODE Solve proof rule and must rather use differential invariants to close this safety proof. The first invariant that we must track is that mass does not increase from its initial value. In reality, mass must either decrease or stay the same over a given time period, but this condition is sufficient to prove safety. Since the initial mass is constant, the application of differential invariant says that the derivative of m must be zero or negative, which it is by definition. Next, the position-velocity constraint that was previously derived for safety is added as a differential invariant as well, which if true trivially proves the invariant and therefore the safety condition. The differential invariant proof of this condition is not as obvious as the mass property, but it does also close.

There is one remaining key issue with this proof: the addition of $m \geq dm$ to the differential equation evolution domain constraints. This essentially ceases operation of the system when the satellite runs out of fuel, no matter what. Any any state that satisfies the velocity-position constraint when it runs out of fuel will be considered “safe”. In a sense, this is reasonable since a satellite typically ends operation once it runs out of fuel. However, this is decidedly unhelpful if you want to prove that you can safely land on an asteroid rather than

safely be around it until you run out of fuel. For a realistic case, you need to know something about efficiency.

Efficiency

If you want to design a system to safely approach an asteroid, you must not only show that you are always safe but that you also have enough fuel to successfully reach the surface in a controlled manner. This can be formulated as an efficiency constraint that will be violated if the spacecraft runs out of fuel before reaching within a certain distance of the target. Although I was not able to prove such a property, I made some effort to derive a reasonable bound on position, velocity, mass, and engine performance such that the spacecraft would always have enough fuel to land. To do so, I started by calculating the maximum velocity that the spacecraft could reach if it does not brake. This can be derived from the same equation as our safety condition: $v_f^2 = v_i^2 + 2a(p_f - p_i)$ by setting the initial position and velocity to the current position and velocity of the spacecraft, the final position to zero, and the acceleration to the gravitational pull of the asteroid. This yields: $v_f = \sqrt{v^2 + 2ap}$. Next, we can calculate the amount of fuel needed to slow from that velocity to zero, through the intermediate variable of time: $v = v_o - g * t, m = \frac{-ft}{I_{sp}g_e}$, $m = \frac{-f}{I_{sp}*g_e} * \frac{v_f - v_0}{-g}$. If we could simply plug in the maximum velocity value into this equation, we could get a conservative bound and safety condition for fuel mass. Unfortunately, we cannot write a square root in our proof system. I made some attempts to encode this constraint in a provable way but was unable to do so. My belief was that creative squaring of certain parts of this constraint could yield a workable invariant but I was stymied by the inequality

Future Work

The application of formal verification methods to space systems has a wide variety of future applications to which I have given much thought through the duration of this project. The key issue with this project as-is is the lack of efficiency statements, which make that an obvious next step in the continuation of this project. Once that property has been validated, an easy next step would be to apply this to past missions asteroid missions to see if the bounds have any link to the fuel margin of safety used in reality. For example, NASA makes the assumption of an I_{sp} of 325 seconds for an asteroid sample return mission[8] and the NEAR probe carried about 300kg of fuel with a dry mass of 478kg and a primary engine force of 450N[9]. With our very conservative safety property, this would require about 735kg of fuel, over twice the amount that the mission carried. While this demonstrates that optimal efficiency conditions are very difficult to derive, it also shows that this condition provides an order-of-magnitude correct fuel value using relatively simple and very safe assumptions.

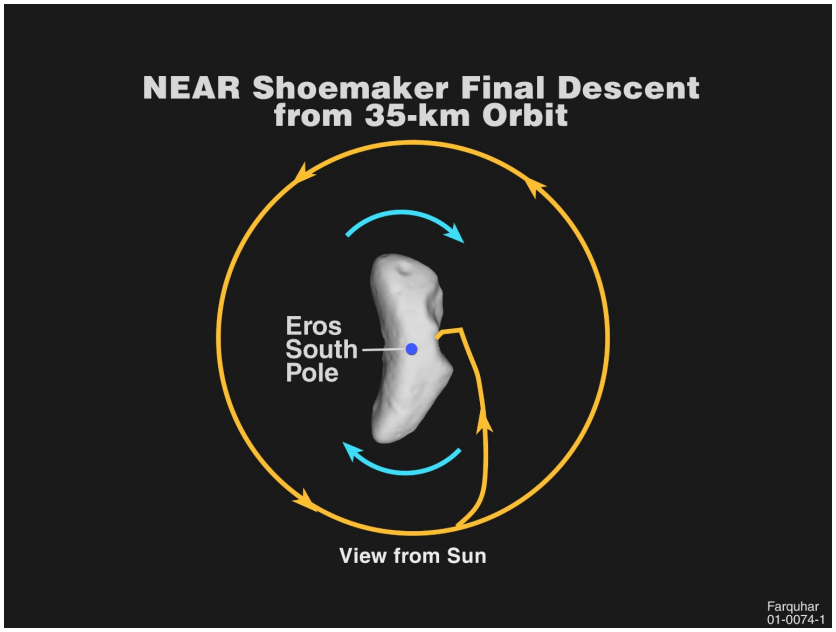

Figure 4: Actual descent trajectory of NEAR to the surface of 433 Eros. Credit: JHU APL

Many other improvements to this model could also be made in order to converge on a more correct hybrid system. The nonuniform gravitational field of many asteroids could better be approximated by bounds around a constant average, which would increase proof difficulty in that safety would have to apply for any change within that bound. Another important consideration is increasing the dimensionality of the system and integrating orbital mechanics. For a truly useful model, you would need to account for orbital gravity effects around both the sun and the target asteroid. Furthermore, a distribution of noise exists around almost every variable in this system, and all of this noise should be handled in a controller running a real mission.

Conclusion

Formal safety verification of hybrid systems is an important technique in designing and implementing cyber-physical systems that we can trust with either millions of dollars or human lives. In space, these challenges are compounded by communications delays, limited processing power, expensive launch costs, and little to no chance of a rescue mission. For these reasons, the logical verification of a spacecraft's asteroid approach could save significant time and money for a variety of space missions. And as missions to asteroids become more and more common, a valid safe approach will become more and more necessary. This project does so by verifying a fuel limited spacecraft can safely approach an asteroid, and makes movement towards a safe and efficient asteroid approach controller.

A verified safe approach and landing controller will have a broad impact in the field of space robotics. Asteroid mining has the potential to be a billion dollar industry that will help fuel the next generation of deep space missions. These methods naturally apply to larger

airless bodies such as the moon and other dwarf planets and could be extended to apply to objects with an atmosphere as well. Precise approach and landing is necessary in many other areas on earth, in orbit, and beyond and may be the key to making human life multi-planetary.

References

[1]: “Asteroid Redirect Mission Reference Concept.” NASA.
[2]: Castet, Jean and Saleh, Joseph. “Spacecraft Reliability and Multi-State Failures: A Statistical Approach.” Book (2011).
[3]: Phillips, Michael. “Spacecraft Collision Probability Estimation for Rendezvous and Proximity Operations.” Masters Thesis (2012).
[4]: Chenoweth, H. B. “Monte Carlo Simulation of the Apollo Command Module Land Landing.” *Journal of Spacecraft and Rockets*. Vol 8, #10 (1971).
[5]: Zhao, H. et. al. “Formal Verification of a Descent Guidance Control Program of a Lunar Lander.” *Formal Methods*, LNCS Volume 8442 (2014).
[6]:Johnson, Taylor T. et. al. “Satellite Rendezvous and Conjunction Avoidance: Case Studies in Verification of Nonlinear Hybrid Systems.” *Formal Methods*, LNCS Volume 7436 (2012).
[7]:Cardall, C. and Daunt, S. “Astronomy 161 Lecture Notes.” University of Texas Knoxville.
[8]:Morimoto, M. et. al. “Trajectory Design of Multiple Asteroid Sample Return Missions.” *Advances in Space Research*. Vol 34 (2004).
[9]:Holdridge, Mark E. “NEAR Shoemaker Spacecraft Mission Operations.” *Johns Hopkins APL Technical Digest*. Vol 23, #1 (2002).