Abort-Safe Spacecraft Motion: Reachability Theory and Predictive Control

by

Daniel Aguilar Marsillach

M.S., Georgia Institute of Technology, 2017

B.Eng., University of Manchester, 2015

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Aerospace Engineering Sciences

2021

Committee Members:

Marcus Holzinger, Chair

Hanspeter Schaub

Jay McMahon

Morteza Lahijanian

Avishai Weiss

Aguilar Marsillach, Daniel (Ph.D., Aerospace Engineering Sciences)

Abort-Safe Spacecraft Motion: Reachability Theory and Predictive Control

Thesis directed by Prof. Marcus Holzinger

The increased usage of autonomous systems and vehicles will certainly improve societal transportation and infrastructure in terms of overall performance and safety. For widespread adoption, such systems have to ensure safety under the presence of various faults, conditions and unknown environments. Additionally, vehicle operations need to be robust with respect to potential actuator or path-planning, navigation, and control system failures.

This thesis develops an operationally useful and realistic framework for vehicle motion-planning and control algorithms that ensure safe, collision-free trajectories under various actuator failure scenarios. The results are general and applicable to systems with linear time-varying dynamics, but here, the benefits of the approach are shown for various spacecraft relative motion case studies. The methodology makes use of backwards reachable sets, which are used to characterize the unsafe region of state space from which, in the presence of a failure, a collision between a chaser and a target vehicle cannot be avoided. That is, in this region of state space no feasible evasive collision-avoidance maneuvers exist. Additionally, the passively unsafe state space or the sets of states that result in free-drift collisions with the target, due to total loss of control actuation, are characterized.

A chaser spacecraft is guided towards a target body via a model predictive control trajectory generation scheme that ensures abort-safety by avoiding the a-priori computed unsafe region of state space. To ensure problem tractability in real-time, the original non-convex motion-planning problem is convexified online using local half-space that separate the chaser spacecraft from the unsafe region of state space. This ensures that the chaser approaches its target in an inherently abort-safe manner. Simulations of the rendezvous planning and control policy on various orbits demonstrate how the approach ensures passive

and active aborts that are safe in the event of various thruster failures.

Finally, the developed work used to characterize the regions of state space that are passively unsafe, are described using orbital elements differences, which has a few benefits. Such sets have reduced linearization errors ensuring higher accuracy when characterizing the passively unsafe regions of state space compared with the same sets expressed using Cartesian coordinates. As such, the linear domain in which the safety analysis is performed is enlarged. Naturally, these sets are mostly useful for formation flying scenarios where the controlled vehicle is close to the target region. However, we provide insights as to how such sets can be used for the purposes of both safe formation and constellation design.

Dedication

To my family.

Acknowledgements

I would like to thank my advisor Professor Marcus Holzinger for his support and mentorship. He welcomed me into his lab at Georgia Tech and advised me on my masters project, which eventually resulted in me embarking on my Ph.D. journey. I sincerely appreciate his guidance throughout this journey. Within the VADeR lab, I specifically want to thank Shez Virani, who taught me a lot, made me a better engineer, and changed my life one Saturday afternoon.

I would like to thank all of the committee members: Professors Hanspeter Schaub, Jay McMahon, Morteza Lahijanian and Dr. Avishai Weiss for their time and suggestions. I had the pleasure of taking Prof. Schaub and Prof. McMahon's courses, which helped me internalize and understand fundamental knowledge related to spacecraft formation flying, guidance, and control. Thank you all for being great role models and for giving students the tools to succeed in this field.

Special thanks to the team at Mitsubishi Electric Research Laboratories (MERL), which include Avishai Weiss, Stefano Di Cairano, Uroš Kalabić, and Abraham Vinod, for their help, insights, time, and guidance. Thank you for your mentorship and collaboration on many of the presented topics. I want to particularly thank Avishai Weiss, who has been an excellent advisor and mentor to me; I sincerely thank him for everything. The first internship with Avishai paved the way for this thesis and everything that came after, so thank you for perturbing my trajectory in the best of ways.

Finally, thank you to my other collaborators and colleagues.

Contents

Chapter

Tables

Table

Figures

Figure

Chapter 1

Introduction

Spacecraft guidance, navigation, and control algorithms are among the highest-priority technologies for future autonomous spacecraft missions [1] and have to meet strict criteria prior to flight due to mission cost and lack of repair opportunities [2]. From a controls perspective, this results in vehicles needing to demonstrate robust operation in various conditions and unknown environments [2]. Missions also need to be robust with respect to potential guidance, navigation, and control system failures. This is typically accounted for in the mission and approach trajectory design process [3, 4]. The research herein is also motivated by the increased usage and utility of spacecraft proximity operations. Examples of such missions include orbital servicing and maintenance technology matures among others [5]. Recently, servicing missions were completed by the Mission Extension Vehicle-1 and 2, which successfully extended the life of GEO telecommunication satellites [6]. Evidently, as the number of orbiting satellites increases and missions become more autonomous and complex, the need to develop novel autonomous and safe spacecraft motion-planning algorithms and techniques is also greater [2, 7].

Depending on the mission type, different levels of safety are required. For example, in spacecraft rendezvous, approaches must guarantee several degrees of safety as seen in [3, 4, 8]. Initially, the approaching spacecraft, called the chaser or deputy, must remain passively safe with respect to a target body, sometimes called the chief, for a specified amount of time. An approach is passively safe if free-drift trajectories from some initial state do not

enter an unsafe region or set. Upon closer proximity to the target, active-safety must be maintained whereby the chaser must be able to perform a powered-abort maneuver to avoid colliding with the target [9]. Both passive and active safety can be generally denoted by what we call **abort safety**. Then, a spacecraft is in the abort safe region of state space if a passive or active abort exists from its current state. Naturally, such safety guarantees are of interest to general formation flying and relative proximity operations (RPO). The design of safe spacecraft rendezvous approaches or relative motion has been achieved using a number of techniques. Due to the non-convex nature of collision avoidance and abort safety constraints, optimization or sampling-based trajectory optimization techniques are appropriate for handling such problems [7]. In this thesis, we utilize optimization-based control methods, specifically, model predictive control (MPC), in conjunction with reachability analysis to develop techniques that steer a chaser spacecraft around such unsafe regions. This allows for the successful completion of an RPO mission while satisfying the abort-safety constraints.

The safe region of state space can be approximated using reachability theory. A reachable set is the exact or approximate set of states that can be reached by a system, given initial/final states, a time-horizon, inputs, and the model parameters. The use of reachable sets is fundamental to formally and rigorously verify the safety of a system [10, 11]. Most of the prior work in this area focuses on computing controlled reachable sets, which theoretically can be done using optimal control methods, including the well known Hamilton-Jacobi-Bellman (HJB) reachability level-set technique [12, 13]. However, for high dimensional systems, HJB methods are computationally intractable [11, 14]. As a result, numerous other techniques that are applicable to nonlinear systems have been developed that over and under-approximate the reachable sets obtained using HJB methods [15, 13, 16, 17, 18]. Many of these techniques have also been extended to consider disturbances, dynamical uncertainty and noise [19, 20, 10]. In terms of the application of reachability theory to spacecraft motion, linear reachability theory is often used since spacecraft relative proximity operations generally occur in the linearizable domain about a reference trajectory of a real (or fictitious)

target. Hence, most of the literature involving spacecraft RPO and docking (RPO&D) along with reachability analysis do not utilize the full nonlinear dynamics models.

The reachable sets form the backbone of the work proposed in this thesis. While a lot of the literature currently focuses on computing reachable sets, particularly in the controlled cases, as far as the authors know, limited work has been doing using reachability theory to compute both passive and active abort-safe regions. This thesis develops a framework which utilizes abort-safe reachable sets and then discusses how the reachable sets can be used to guarantee the safety of a chaser (or deputy) with respect to a target spacecraft (or chief) using model predictive control. Being able to characterize these regions has other interesting implications in the astrodynamics domain. It can help inform and improve the spacecraft trajectory design problem. A more specific use case of this work lies in space traffic management, which is a generalization of the multi-disciplinary field of space situational and domain awareness [21, 22]. Such applications are considered in the last chapter of the thesis where the problems of safe formation and constellation organization are discussed.

One of the challenges remains computing and utilizing these reachable sets in a computationally tractable manner for distinct spacecraft motion scenarios. Prior research in passively-safe spacecraft relative motion uses geometric constraints that can be overly-conservative, shooting-like methods resulting in large optimization problems, or overly-constrained orbital parameters, limiting the types of relative motion that are considered safe. Active abort-safety is a relaxation of the passively-safe case but has been investigated much less [9]. The focus of this thesis lies in planning the motion of spacecraft in an inherently passive abort-safe (PAS) and active abort-safe (AAS) manner for arbitrary initial conditions. The resulting methods and algorithms enable safer, more complex, and robust autonomous spacecraft relative motion.

Thesis Statement: Abort-safe spacecraft relative motion can be guaranteed and generalized using reachability analysis, predictive control methods, and set-based constraints, fundamentally improving spacecraft RPO safety, initial trajectory design, online implementation and vehicle autonomy.

1.1 Abort-Safe Spacecraft Rendezvous on Generic Elliptical Orbits

Initially, an approaching spacecraft, called the chaser, must remain passively safe with respect to a target body, called the target, for a pre-specified amount of time. A rendezvous approach is passively safe if instantaneous free-drift trajectories emanating from the approach do not enter an avoidance region around the target. In other words, by nominally following a passively safe approach trajectory, in the event of a total loss of propulsion, the chaser spacecraft will naturally drift clear of the target. Upon closer proximity to the target, active safety must be maintained at all times along the approach trajectory, whereby in the event of a partial loss of propulsion, the chaser must be able to perform a powered-abort maneuver with its remaining functional thrusters to avoid colliding with the target. Allowing for active abort maneuvers relaxes the safety requirements compared to the passive case, permitting trajectories more pertinent to the final approach phase of a rendezvous mission for which an entirely passive approach may not be feasible or desirable.

Classically, spacecraft relative motion is guaranteed to be passively safe by exploiting orbital mechanics knowledge and constraining the chaser's trajectory via an open-loop guidance generation that is computed on the ground. In recent years, interest in more autonomous, online-generated passive safety techniques has increased, e.g., by constraining the relative motion using orbital elements [23], or by using receding-horizon optimization, where collision avoidance constraints are placed on future free-drift states via a state transition matrix [24, 9, 25, 26]. Breger and How developed a method for online generation of nominal trajectories that, in the event of partial thruster failure, can switch to a safe input sequence

to avoid collision [9]. To guarantee the existence of such a sequence, the method expands the size of the optimization problem by solving for both nominal and abort sequences concurrently given an initial condition for which the method is feasible. These methods, however, do not compute the region of state space in which feasible passive or active abort maneuvers exist. The safe state space can be approximated using reachability theory which generalizes the methods discussed above and allows one to construct safe approaches from arbitrary safe initial conditions. The focus of this contribution lies in characterizing the unsafe state space, whether for passive or powered abort, which is then utilized for the development of an online model predictive control (MPC) policy that ensures abort-safe approaches.

Contribution 1: The characterization of the passive and active abort-safe state space using linear reachability theory and the development of a model predictive control-based algorithm to maintain abort-safety during RPO.

1.2 Abort-Safe Spacecraft Rendezvous with State and Dynamical Uncertainty

An important aspect of the viability of the algorithm for actual space missions is that it must be able to perform well in unknown and uncertain environments [2]. The aim of this contribution is to maintain abort-safety while being robust to unmodeled perturbations, state uncertainty, and simultaneously, provide an increasingly fuel-efficient solution compared to the method developed in the prior contribution. Motivated by increasingly complex rendezvous missions such as NASA's Lunar Orbital Platform-Gateway (LOP-G) concept [27], this work considers rendezvous with a target body in perturbed environments while including state or navigation uncertainty.

This contribution generalizes the prior one, which assumed unperturbed and deterministic states, by incorporating both dynamical, state, and input uncertainty into the abort-safety problem. While robust control methods may be used to characterize the unsafe regions

of state space and to ensure the spacecraft satisfies any safety constraints robustly, we choose to perform the analysis using stochastic methods because robust methods can be overly conservative [11, 28]. This is the case because worst-case uncertainty is often considered. In the stochastic sense, probabilistic guarantees can be made about the safety of the system, i.e., the safety constraints are satisfied to a certain degree of likelihood. Stochastic methods allow us to study varying degrees of safety, from the practically absolutely safe scenario, similar to a robust approach, to a mildly safe one. Additionally, since GN&C algorithms ingest state estimate information from a filter, it makes sense to use a probabilistic framework. In this work, we are interested in ensuring that the chaser remains in the likely abort-safe region of state space, where the probability of an abort existing is high. This implies that if an active or a passive abort is required, there is a probability associated with the existence of that abort maneuver. Moreover, due to the presence of navigation or state uncertainty, we want the confidence that the algorithm is steering the chaser around the probabilistically unsafe regions to be high as well, which is demonstrated using chance-constraints.

There is a wealth of literature on the topic of stochastic reachability, which include forward and backward analysis using Fourier transforms [29], occupancy functions [30, 20], chance-constraints [31, 32, 33], approximate dynamic programming [34], and particle filters [35], among others. For active abort-safety with noise or disturbances, optimal controllers need to be considered because such controllers provide the maximal or largest reachable sets [36]. In our problem, an optimal controller will truly characterize where a feedback policy, that is subjected to noise, may be safe or unsafe. A common assumption then is to assume a Markov control policy is used for analysis and design purposes, i.e., the controller acts on a current estimate of the state and the state follows a random process in which the Markov property holds. Then, in theory, the stochastic reachable sets can be computed via dynamic programming (DP) [37, 38]. As stated previously though, such methods are computationally intractable for high-dimensional systems like ours, which resulted in prior work that over and under-approximates the sets obtained with DP [39].

The problem of stochastic reachability of a target tube, first introduced in [40], considers safety specifications which are captured via a finite collection of time-varying sets within which the nominal state must remain [41]. This generalizes notions of the terminal hitting-time stochastic reach-avoid [42] and the stochastic viability problems [39, 19]. A mild modification of the target tube framework in [39] is used to characterize the regions of state space for which the probability of a safe active abort-maneuver existing is low. These regions are deemed probabilistically unsafe. Moreover, in this work, we additionally consider the impact of linearization errors on these unsafe regions, which if ignored can compromise the safety of the system even within the linearization regime of interest over longer periods of time.

Aside from generalizing the prior contribution to the stochastic case, we are interested in developing a method that reduces fuel consumption and yields sparse thrust signals while maintaining abort-safety. Thruster signal sparsity implies that the on-board thrusters are engaged less often, which is important to protect on-board instrumentation as well as for preventing stuck-on thrusters. In the absence of state or safety constraints, one can choose to solve the optimal ΔV maneuver by solving the standard optimal control problem [43, 44, 45]. When convex or non-convex state or input constraints are present, a multitude of techniques can be employed to optimize a trajectory in an online or offline manner. Some examples include model-predictive-control [2, 25, 46, 47, 48], local and global collocation [49, 50], shooting methods [51], successive convexification[52, 53], among others. The differences between these methods typically lie in the transcription process, i.e., the discretization of the continuous-time system and the enforcement of constraints. Another alternative for improving ΔV performance is to replace a quadratic cost function with an L1-norm [54] or regularized linear-quadratic cost function [55].

Solving the full ΔV optimal control that is abort-safe requires solving a nonlinear program with a multitude of non-convex constraints, presenting a challenge for real-time implementation. If on-off control input constraints are incorporated, yielding a mixed-integer

nonlinear program, the optimization becomes increasingly difficult. This motivates an approach that yields abort-safe trajectories that can be used in an online manner while reducing thruster on-off switches and the total ΔV consumed. To this end, a solution that exploits the natural dynamics better is demonstrated by means of predictive coasting arcs, i.e., regions where the spacecraft's thrusters can be disengaged while moving safely towards a goal region. The developed technique leverages passive reachability theory, resulting in a methodology that engages thrusters less often and can reduce the total ΔV of the maneuver.

Contribution 2: The development of an abort-safe online trajectory generation algorithm that utilizes coasting arcs for improved control performance while accounting for state, input, and dynamical uncertainty.

1.3 Passive Abort-Safe Spacecraft Motion using Orbital Element Differences

The prior contributions focus on computing the passive and active abort-safe regions of state space using a Cartesian coordinate description which is valid near the target or chief spacecraft. The goal of this contribution is to characterize these sets using orbital element differences, which are useful for arbitrary relative motion and eventually, as will be discussed, for initial safe formation and constellation design. There are a number of reasons for characterizing the unsafe regions of state space in terms of orbital element differences. By construction, using differential orbital elements captures eccentric chief orbits [56]. Depending on the orbital element model used, the resulting passive backwards reachable sets (PBRS) are much simpler to describe as only a subset of the coordinates are time-varying. Additionally, the dynamics of relative states in terms orbital element differences have smaller linearization errors compared to relative Cartesian representations [57, 58], which is beneficial when propagating Gaussian uncertainty. Additionally, the linearizable domain around the chief or target's reference trajectory is enlarged too, which allows us to ensure safety

for even longer time-horizons compared to the Cartesian analogue. Finally, performing the analysis in terms of orbital element differences can help facilitate formation and constellation design as mission constraints of interest are often in terms of spacecraft orbital elements.

Given future LEO mega-constellations missions and concepts, that are placing thousands of spacecraft within a constellation, there is a warranted concern for the safety of spacecraft "near" such constellations [22]. To guarantee the safety of future spacecraft missions, several improvements in space traffic management standards need to be made that minimize collision risk between active and inactive spacecraft [59]. It is estimated that conjunction events will increase in frequency by the simple introduction of the upcoming mega-constellations in low Earth orbit (LEO) [60, 61]. In the constellation design scenario, orbits are typically chosen to satisfy mission requirements, which depend on ground observation or communications constraints [62, 63, 64]. In these instances, passive safety is a by product of the phasing of the constellation and the number of satellites in it, since up until recently, constellations have not been densely packed. The work in this contribution helps inform how satellites should be organized and how many could fit in a particular regions of state space while explicitly satisfying safety constraints or requirements. We propose using reachable sets as a method of defining a generic orbital slot, which can inform and aid our understanding of the safe holding capacity of the near-Earth space environment.

Not surprisingly, there is a lot of literature that discusses techniques for maintaining passive safety using orbital element differences or relative orbital elements. From a theoretical perspective, the related prior work in the literature usually considers passively-safe relative motion under the assumption that the deputy and chief spacecraft have a matched period. Some of these constrain the chosen relative orbit elements to ensure a minimum amount of separation between the deputy and chief spacecraft in the radial/along-track plane [65, 66, 23, 67], which guarantees passive safety. The notion of walking and stationary safety ellipses are discussed in [68], where passively-safe drifting and periodic relative orbits are used to ensure consistent separation between a deputy and chief spacecraft. These configurations

have the specific property of not intersecting the chief's along-track axis or its Keplerian orbit. For formation design, another important constraint is that the relative motion between the spacecraft remains bounded [69], which is typically of interest for spacecraft within the same constellation as well, as the relative geometry should remain stationary to satisfy mission requirements.

The formulations and safety constraints in the literature are derived from orbital mechanics and geometry. In [23], a safe minimum separation constraint is derived which relies on the assumption that the chief is in an unperturbed circular or near-circular orbit. While relative orbits have been designed for chief spacecraft with arbitrary eccentricity [69], there is limited work on generic passive safety constraints for chiefs with arbitrary eccentricity that are subject to perturbations. This is derived and shown in this contribution as a special case of the reachable set analysis. Moreover, the passive safety constraints in the literature do not easily generalize to all possible kinds of relative motion around the chief, which is possible using passive backwards reachability analysis, at the expense of more computation.

As such, in this contribution, we first characterize the regions of state space that are passively unsafe with respect to a chief using orbital element differences. The passive backwards reachable sets here can be directly used for arbitrary relative motion scenarios such as rendezvous using the same algorithms in the first two contributions. We demonstrate how analyzing slices of these sets for the sake of formation and constellation design can help reduce the dimensionality of the problem, greatly simplifying the safe formation and constellation design problems. Additionally, such slices of the reachable sets eventually yield geometrical safety constraints, similar to ones in prior work. In summary, this contribution presents initial results and insights as to how reachability theory can be used for the purposes of maintaining safety between spacecraft in formations and constellations.

Contribution 3: The characterization of passively unsafe regions of state space for a deputy spacecraft with respect to a chief in terms of orbital element differences and its applications to formation flying and initial constellation design.

1.4 Contributions and Outline

The contributions in this work focus on the applicability of reachability theory to ensure relative motion that is inherently safe with respect to partial or full loss of thruster capability. In chapter 2, preliminaries and background theory are introduced. Chapter 3 discusses how backwards reachable sets are used to characterize regions of state space where a passive or active abort allows a chaser spacecraft to successfully avoid collision with a terminal set. The second contribution, presented in Chapter 4, generalizes this concept while accounting for state and dynamical uncertainty. Additionally, a set-based coasting arc method is presented that can yield more fuel-efficient solutions than the nominal safe policy. Finally, Chapter 5 leverages a coordinate change from Cartesian to orbit element differences to characterize the passively unsafe state space, which is useful for formation and initial constellation design. The thesis focuses on reachability analysis to acquire the abort-unsafe regions of state space and their corresponding application to demonstrates how such sets can be used.

1.5 Thesis-Related Publications

Some of the research leading to this thesis has appeared previously in research papers. Moreover, this work has contributed to the development of patents and inventions, submitted to the United States Patent Office (USPTO).

1.5.1 Journal Articles

[1] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Abort-Safe Spacecraft Rendezvous on Generic Elliptic Orbits. IEEE Trans. on Control Systems Technology, Submitted May 2021.

[2] Aguilar Marsillach, Daniel, Vinod, Abraham, Di Cairano, Stefano, Holzinger, Marcus, Kalabic, Uros, and Weiss, Avishai. Abort-Safe Spacecraft Rendezvous with State and Dynamical Uncertainty. J. Guidance, Control, and Dynamics, Planned Dec. 2021.

[3] Aguilar Marsillach, Daniel, and Holzinger, Marcus. Passively Safe Spacecraft Motion using Orbit Element Differences. J. Spacecraft and Rockets, Planned Dec. 2021.

1.5.2 Conference Papers

[1] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Fail-safe Rendezvous Control on Elliptic Orbits using Reachable Sets. In Proc. American Control Conf., 4920-4925, 2020.

[2] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Abort-Safe Spacecraft Rendezvous in case of Partial Thrust Failure. In Conf. Decision and Control, 1490-1495, 2020.

[3] Aguilar Marsillach, Daniel, Di Cairano, Stefano,Kalabic, Uros, and Weiss, Avishai. Fail-Safe Spacecraft Rendezvous on Near-Rectilinear Halo Orbits. In Proc. American Control Conf.,2980–2985, 2021.

1.5.3 Patents

[1] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Fail-Safe Vehicle Rendezvous in Case of Total Control Failure. USPTO, Submitted 2020.

[2] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Abort-Safe Vehicle Rendezvous in Case of Partial Control Failure. USPTO, Submitted 2020.

[3] Aguilar Marsillach, Daniel, Di Cairano, Stefano and Weiss, Avishai. Drift-based Rendezvous Control. USPTO, Submitted 2020.

Chapter 2

Preliminaries

2.1 Notation

$\mathbb{R}$, $\mathbb{R}_{\geq 0}$, $\mathbb{R}^n$, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Z}_{0+}$ are the sets of real numbers, non-negative real numbers, the Euclidean space, natural numbers, integers, and non-negative integers, respectively. For intervals, we use notations such as $\mathbb{Z}_{[a,b)} = \{z \in \mathbb{Z} : a \leq z < b\}$. Vectors are shown in boldface.

A reference frame, $\mathrm{F_x}$, is defined at an origin and consists of three orthonormal dextral basis vectors $\{\hat{\boldsymbol{\imath}}, \hat{\boldsymbol{\jmath}}, \hat{\boldsymbol{k}}\}$. The angular velocity vector of frame $\mathrm{F_x}$ with respect to $\mathrm{F_y}$ is denoted by $\boldsymbol{\omega}_{\mathrm{x/y}}$. A derivative as seen by the inertial frame $\mathrm{F_e}$ is denoted by $\overset{e.}{(\cdot)}$ whereas a derivative as seen by another frame $\mathrm{F_v}$ is denoted by $\overset{\mathrm{v.}}{(\cdot)}$. Such vector derivatives seen are obtained using the transport theorem. A vector resolved in frame $\mathrm{F_x}$ is denoted ${}^{\mathrm{x}}(\cdot)$, any unit vector is denoted by $\hat{(\cdot)}$. The position of a point c with respect to a point b is given by $\boldsymbol{r}_{\mathrm{c/b}}$.

Given a continuous time signal $x(t)$ sampled with period ΔT, we denote the value at time instant $k\Delta T$, $k \in \mathbb{Z}_{0+}$, by $\boldsymbol{x}_k = \boldsymbol{x}(k\Delta T)$, and $\boldsymbol{x}_{j|k}$ denotes the value of $\boldsymbol{x}$ predicted j steps ahead from k. The discrete-time state transition matrix is from time index i-to-j is denoted $\Phi(i,j)$ in time-step form or $\Phi(t_i,t_j)$ when using absolute times.

Given a matrix H, $[H]_i$ denotes the i^{th} row of the matrix and $H^{\frac{1}{2}}$ denotes its matrix square root. I_n denotes the n-dimensional identity matrix. The matrix M that is a function of τ is enclosed with brackets and denoted $[M(\tau)]$. The Euclidean norm of a vector is given by $||\cdot||$.

2.2 Convex Sets & Operations

The hyperplane representation ($\mathcal{H}$-rep) of the polyhedron $\mathcal{P} \subseteq \mathbb{R}^n$ is $\mathcal{P}(H, \boldsymbol{k}) = \{\boldsymbol{x} \in \mathbb{R}^n : H\boldsymbol{x} \leq \boldsymbol{k}\}$ with $H \in \mathbb{R}^{p \times n}$, $\boldsymbol{k} \in \mathbb{R}^p$. An ellipsoid centered at $\boldsymbol{d} \in \mathbb{R}^n$ with shape matrix D, is defined as $\mathcal{E}(\boldsymbol{d}, D) \triangleq \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{x} - \boldsymbol{d})^\top D^{-1}(\boldsymbol{x} - \boldsymbol{d}) \leq 1\}$ or equivalently, $\{D^{\frac{1}{2}}\boldsymbol{v} + \boldsymbol{d} \in \mathbb{R}^n : \|\boldsymbol{v}\|_2 \leq 1\}$. The set of all subsets of $\mathcal{X}$ is denoted as $2^{\mathcal{X}}$, and the cardinality of a set $\mathcal{X}$ is $|\mathcal{X}|$. The complement of a set $\mathcal{X}$ is given by $\mathcal{X}^{\mathrm{c}}$.

For two sets, $\mathcal{X} \in \mathbb{R}^n$, $\mathcal{Y} \in \mathbb{R}^n$, the Minkowski sum is denoted by $\mathcal{X} \oplus \mathcal{Y}$, and is defined as

$$\mathcal{X} \oplus \mathcal{Y} = \{\boldsymbol{x} + \boldsymbol{y} \in \mathbb{R}^n : \boldsymbol{x} \in \mathcal{X}, \boldsymbol{y} \in \mathcal{Y}\}. \tag{2.1}$$

The Pontryagin difference is denoted $\mathcal{X} \ominus \mathcal{Y}$, which is

$$\mathcal{X} \ominus \mathcal{Y} = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} + \boldsymbol{y} \in \mathcal{X}, \forall \boldsymbol{y} \in \mathcal{Y}\} \tag{2.2}$$

and finally, the set difference $\mathcal{X} \setminus \mathcal{Y}$ is defined as

$$\mathcal{X} \setminus \mathcal{Y} = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} \in \mathcal{X}, \boldsymbol{x} \notin \mathcal{Y}\}. \tag{2.3}$$

Let $\mathcal{S} \subseteq \mathbb{R}^n$ be a convex set, the support function of $\mathcal{S}$, denoted $\rho_{\mathcal{S}}$ is defined as

$$\rho_{\mathcal{S}}(\boldsymbol{l}) = \max_{\boldsymbol{x} \in \mathcal{S}} \ \boldsymbol{l}^{\mathsf{T}}\boldsymbol{x} \tag{2.4}$$

and the convex set $\mathcal{S}$ can be uniquely determined by the support function

$$\mathcal{S} = \bigcap_{\boldsymbol{l} \in \mathbb{R}^n} \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{l}^{\mathsf{T}}\boldsymbol{x} \leq \rho_{\mathcal{S}}(\boldsymbol{l})\}. \tag{2.5}$$

The Minkowski sum of convex sets $\mathcal{A}$ and $\mathcal{B}$, using support functions is given as

$$\rho_{\mathcal{A} \oplus \mathcal{B}}(\boldsymbol{h}) = \rho_{\mathcal{A}}(\boldsymbol{h}) + \rho_{\mathcal{B}}(\boldsymbol{h}) \tag{2.6}$$

The image of the convex set $\mathcal{C} \subseteq \mathbb{R}^n$ through matrix $A \in \mathbb{R}^{m \times n}$ is a convex set $A\mathcal{C} = \{A\boldsymbol{x} \in \mathbb{R}^m : \boldsymbol{x} \in \mathcal{C}\}$. The preimage of the convex set $\mathcal{C} \subseteq \mathbb{R}^m$ through matrix $A \in \mathbb{R}^{m \times n}$ is a convex set $\mathcal{C}A = \{\boldsymbol{x} \in \mathbb{R}^n : A\boldsymbol{x} \in \mathcal{C}\}$. The indicator function of a non-empty set $\mathcal{S}$ is given by $\mathbb{1}_{\mathcal{S}}(\bar{\boldsymbol{x}})$ where $\mathbb{1}_{\mathcal{S}}(\bar{\boldsymbol{x}}) = 1$ if $\bar{\boldsymbol{x}} \in \mathcal{S}$ and is zero otherwise.

2.3 Probability

The probability density function (PDF) of a random vector $\boldsymbol{v}$ is denoted as $\psi_{\boldsymbol{v}} \in \mathbb{R}_{\geq 0}$. The evaluation of the PDF at a vector $\bar{\boldsymbol{v}}$ is given as $\psi_{\boldsymbol{v}}(\bar{\boldsymbol{v}})$. The tilde notation is used to denote that a random vector belongs to a certain distribution, i.e., $\boldsymbol{v} \sim \psi_{\boldsymbol{v}}$. The expected value of a random vector $\boldsymbol{v}$ is given by $\mathbb{E}[\boldsymbol{v}]$ and its covariance matrix is given by $\Sigma^{\boldsymbol{v}} = \mathbb{E}\big[(\boldsymbol{v} - \mathbb{E}[\boldsymbol{v}])(\boldsymbol{v} - \mathbb{E}[\boldsymbol{v}])^{\mathsf{T}}\big]$. If $\boldsymbol{v}$ is normally distributed, then, $\psi_{\boldsymbol{v}}(\bar{\boldsymbol{v}}) = \mathcal{N}(\bar{\boldsymbol{v}}; \mathbb{E}[\boldsymbol{v}], \Sigma^{\boldsymbol{v}})$. Given a set $\mathcal{S}$, the probability that a random vector $\boldsymbol{v}$ is inside set $\mathcal{S}$ given by

$$\mathbb{P}_{\boldsymbol{v}}\{\boldsymbol{v} \in \mathcal{S}\} = \int_{\mathcal{S}} \psi_{\boldsymbol{v}}(\bar{\boldsymbol{v}}) d\bar{\boldsymbol{v}} \tag{2.7a}$$

$$= \int_{\mathbb{R}^n} \psi_{\boldsymbol{v}}(\bar{\boldsymbol{v}}) \cdot \mathbb{1}_{\mathcal{S}}(\bar{\boldsymbol{v}}) d\bar{\boldsymbol{v}} \tag{2.7b}$$

$$= \mathbb{E}\big[\mathbb{1}_{\mathcal{S}}(\boldsymbol{v})\big] \tag{2.7c}$$

where the subscript in $\mathbb{P}_{\boldsymbol{v}}\{\cdot\}$ denotes the random vector used to compute the probability measure. Note that computing the probability in (2.7a) generally requires performing a numerical quadrature. When the set $\mathcal{S}$ is axis-aligned and $\boldsymbol{v}$ is normally distributed, this quadrature is greatly simplified.

Without loss of generality, we denote the probability that an initial state $\bar{\boldsymbol{x}}_0$ at index $k = 0$ reaches $\mathcal{S}$ in N steps, using a control policy $\pi \in \mathcal{M}$ as $\mathbb{P}_{\boldsymbol{x}}^{\bar{\boldsymbol{x}}_0, \pi}\{\boldsymbol{x}_N \in \mathcal{S}\}$. Here, $\boldsymbol{x}_N$ is stochastic due to the process noise, even if $\bar{\boldsymbol{x}}_0$ is deterministic. The policy $\pi = [\mu_0(\cdot), \mu_1(\cdot), \ldots, \mu_{N-1}(\cdot)]$ consists of state-feedback functions $\mu : \mathcal{X} \mapsto \mathcal{U}$.

2.4 Spacecraft Dynamics & Kinematics

Since the majority of the results in this thesis pertain to the unperturbed and perturbed two-body problem, here, we highlight the related dynamics models. Other models used can be found in Appendix A. Consider a target and a chaser in orbit around a central body, e.g., Earth. The frame $\mathrm{F_e}$ is the Earth-Centered Inertial (ECI) frame. The chaser's center of mass is denoted by c and has a chaser-fixed frame $\mathrm{F_c}$. The target's center of mass is

denoted by t and has a target-fixed frame $\mathrm{F_t}$. The target's orbit frame $\mathrm{F_o} = \{\hat{\boldsymbol{\imath}}_r, \hat{\boldsymbol{\imath}}_\theta, \hat{\boldsymbol{\imath}}_h\}$ is Hill's frame with radial, along-track, and cross-track basis vectors. The vector $\hat{\boldsymbol{\imath}}_r$ is parallel to the target spacecraft position vector, $\hat{\boldsymbol{\imath}}_h$ points in the direction of the orbit's angular momentum, and $\hat{\boldsymbol{\imath}}_\theta$ completes the right-hand rule. The chaser is controlled and assumed to be rigid. All external forces acting on the target and chaser are assumed to act on their respective centers of mass. During the active abort-safety phase of the approach, we assume the chaser frame $\mathrm{F_c}$ is aligned with the target's orbital frame $\mathrm{F_o}$, i.e., $\boldsymbol{\omega}_{\mathrm{c/o}} = \mathbf{0}$ due to the presence of directional navigation sensors.

The translational equations of motion for the target and the chaser relative to the inertial frame $\mathrm{F_e}$ are given by

$$\overset{\mathrm{e}}{\boldsymbol{r}}_{\mathrm{t/b}} = -\mu \frac{\boldsymbol{r}_{\mathrm{t/b}}}{\|\boldsymbol{r}_{\mathrm{t/b}}\|^3} + \frac{\boldsymbol{f}_{\mathrm{t}}}{m_{\mathrm{t}}}, \tag{2.8a}$$

$$\overset{\mathrm{e}}{\boldsymbol{r}}_{\mathrm{c/b}} = -\mu \frac{\boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3} + \frac{\boldsymbol{f}_{\mathrm{c}}}{m_{\mathrm{c}}}, \tag{2.8b}$$

where $\boldsymbol{r}_{\mathrm{t/b}}, \boldsymbol{r}_{\mathrm{c/b}}$ are the position vectors of the target and chaser's center of mass relative to the center of the Earth, given by a point b, $m_{\mathrm{t}}, m_{\mathrm{c}}$ are the target and chaser masses, μ is Earth's gravitational parameter, and $\boldsymbol{f}_{\mathrm{t}}$, $\boldsymbol{f}_{\mathrm{c}}$ represent external forces acting on the target and chaser, respectively. The external forces include orbital perturbations as well as control actions.

Given a target and chaser spacecraft, and a point b coincident with the origin of the inertial frame, the position of the chaser relative to the target is given by

$$\boldsymbol{r}_{\mathrm{c/t}} = \boldsymbol{r}_{\mathrm{c/b}} - \boldsymbol{r}_{\mathrm{t/b}}. \tag{2.9}$$

Taking the derivative of the relative position (2.9) with respect to the target's orbital frame $\mathrm{F_o}$ yields

$$\overset{\mathrm{t}}{\boldsymbol{r}}_{\mathrm{c/t}} = \overset{\mathrm{e}}{\boldsymbol{r}}_{\mathrm{c/b}} - \overset{\mathrm{e}}{\boldsymbol{r}}_{\mathrm{t/b}} - \boldsymbol{\omega}_{\mathrm{o/e}} \times \boldsymbol{r}_{\mathrm{c/t}}. \tag{2.10}$$

Taking the derivative of of the relative velocity (2.10) with respect to the target's orbital

frame $\mathrm{F_o}$ yields [69]

$$\overset{\mathrm{t..}}{\boldsymbol{r}}_{\mathrm{c/t}} = \overset{\mathrm{e..}}{\boldsymbol{r}}_{\mathrm{c/b}} - \overset{\mathrm{e..}}{\boldsymbol{r}}_{\mathrm{t/b}} - \overset{\mathrm{e.}}{\boldsymbol{\omega}}_{\mathrm{o/e}} \times \boldsymbol{r}_{\mathrm{c/t}} - \boldsymbol{\omega}_{\mathrm{o/e}} \times (\boldsymbol{\omega}_{\mathrm{o/e}} \times \boldsymbol{r}_{\mathrm{c/t}}) - 2\boldsymbol{\omega}_{\mathrm{o/e}} \times \overset{\mathrm{t.}}{\boldsymbol{r}}_{\mathrm{c/t}} \,. \tag{2.11}$$

Chapter 3

Abort-Safe Rendezvous on Generic Elliptical Orbits

3.1 Introduction

In this chapter, we construct active and passive abort-safe regions of state space using reachability theory, which allows us to compute safe approach trajectories from arbitrary safe initial conditions. A reachable set is the set of states that can be reached by a system, given initial/final states, a time-horizon, a set of input sequences, and the model parameters. Reachable sets have previously been used for spacecraft relative proximity operations and docking. Several nonlinear reachability techniques have been developed for general relative motion dynamics [70, 13, 16]. Of these, Hamilton-Jacobi methods in particular quickly become computationally intractable for high-dimensional systems, while other techniques over and under-approximate the "true" reachable sets in a tractable way [71]. Moreover, because spacecraft proximity operations occur near the target, linearized relative motion dynamics are often sufficiently accurate, permitting the use of linear reachability techniques [72, 30, 39, 36, 73]. In [72], backwards reachable sets of the linear time-invariant (LTI) Clohessey-Wiltshire (CW) equations of relative motion determine successful initial conditions for docking, whereas [30, 39, 36] compute reach-avoid sets, that is, sets of states that can be reached while avoiding obstacle sets.

Here, we compute backwards reachable sets (BRS) that characterize the unsafe state space in which passive or active aborts are infeasible. In order to generate abort-safe rendezvous on generic orbits, we linearize the nonlinear relative equations of motion resulting

in linear time-varying (LTV) equations. Due to the LTV nature of the system and Becausethe reachable set is usually non-convex over a finite time interval [74], we construct the set as the union of convex BRS for different initial and final times along the target's periodic orbit. The union represents the unsafe state space to be avoided. As avoiding the union of BRS results in non-convex constraints, we convexify the problem by computing half-spaces that cover a local region of the BRS along the trajectory, and use the half-spaces as safety constraints. We incorporate the safety constraints in a model predictive control (MPC) policy to generate rendezvous approaches that remain outside of the union of BRS, i.e., in the abort-safe region of state space, which guarantees that, in the event of various thruster failure scenarios, safe passive or active aborts exist. The approach of separating state space into safe and unsafe regions in the event of thrust failure distinguishes this work from much of the literature on spacecraft collision avoidance, which occurs under nominal thrust conditions. For nominal thrust collision avoidance using constrained trajectory optimization techniques, model predictive control (MPC), or robotic motion planning algorithms, see [9, 75, 76, 77, 78]. Continuous-time reactive-control policies that use artificial potential functions to avoid areas of state space are developed in [79]. For additional sources on MPC for spacecraft rendezvous under nominal propulsion conditions, see [80, 47, 48, 81, 46, 82] and references therein.

In [83, 84] we presented preliminary research related to this contribution. With respect to the early contributions, this chapter provides a complete treatment of the method, including refined algorithms, for instance by constructing hyperplanes from multiple ellipsoidal sets, and a deeper analysis, e.g., on the thrust failure effects on admissible and backwards reachable sets and on the trade-offs between polytopic and ellipsoidal sets. Furthermore, we provide a more complete validation, including a rendezvous mission scenario to the International Space Station (ISS) that shows the behavior of an entire mission using different approaches for different mission phases, and we demonstrate the robustness of the approach to unmodeled perturbations via set inflation. Thus, this chapter presents design improve-

ments, deeper analysis, more details and discussions, and a more precise validation in a realistic mission scenario.

The chapter proceeds in Section 3.2 with a description of the safe rendezvous problem and an introduction of the spacecraft model and admissible control sets. Section 3.3 highlights robust backwards reachable set theory and its use for abort safety. Section 3.4 discusses the MPC prediction model, cost function, and the convexification of the safety constraints for polytopic and ellipsoidal sets. Section 3.5 presents algorithmic and computational details related to the offline and online formulation of the problem. Section 3.6 presents a variety of simulations and results for both abort and passive safety.

3.2 Abort-Safe Rendezvous

In **safe rendezvous** a chaser spacecraft must approach a target in an abort-safe manner such that in the event of partial or total loss of propulsion, the chaser spacecraft can perform an active or passive abort that avoids collision with the target.

Adopting NASA's convention for safety regions surrounding the ISS, the chaser must first maintain passive abort-safety with respect to two regions centered at the target's center of mass, referred to as the approach ellipsoid (AE) and keep-out-sphere (KOS), resulting in two phases of passive safety requirements. As seen in Figure 3.1a, the KOS is a proper subset of the AE. Passive safety is first maintained with respect to the AE, and subsequently, as the chaser nears the AE, with respect to the KOS. A **passively unsafe state** is such that the natural unforced dynamics from such an initial state enters the AE, or, in the second phase, the KOS, at some future time step, while a **passively safe state** results in a natural trajectory that does not enter the corresponding region. During the passive abort-safe approach, if the chaser suffers a catastrophic loss of propulsion or other system anomaly and chooses to power off all thrusters, the chaser is guaranteed to follow a trajectory that avoids collision with the target.

The final approach phase of the mission is initiated if no failures or anomalies occur

along the chaser's passively safe approach. At this stage, when the chaser is in very close proximity to the target and intends to dock or berth, passive aborts may no longer be feasible and active abort-safety with respect to a target region approximating the target's physical shape must be maintained, as depicted in Figure 3.1b. An **active abort-unsafe state** is such that, after partial loss of thrust, any trajectory from such an initial state enters the target region regardless of the control actions applied with the remaining thrust. Conversely, an **active abort-safe state** is one in which there exists at least one control sequence using the remaining thrust that allows the chaser to avoid entering the target region. During the active abort-safe approach, if the chaser suffers a partial thrust failure, it will be able to use its remaining thrust to execute a trajectory that avoids collision with the target.

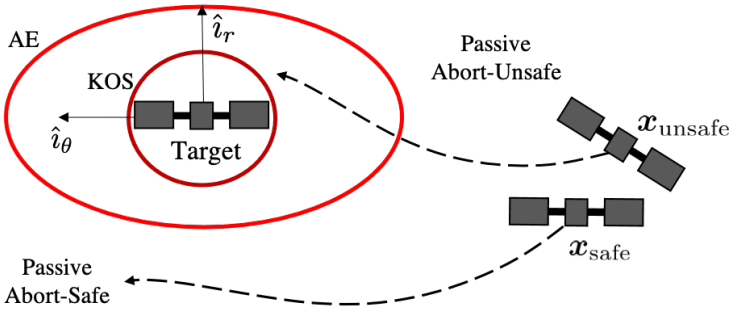
Passive abort-safety is classically guaranteed by designing mission-specific passively safe trajectories offline and then tracking them online. For active abort-safety, redundant thrusters are often engaged in a predetermined active collision avoidance maneuver (CAM) in the event of thruster anomalies in proximity to the target [8]. In the subsequent development, no mission-specific passively safe trajectories or CAMs are precomputed. Instead, we characterize offline the region of state space as abort-safe or abort-unsafe, which then enables online planning of rendezvous trajectories that remain in the abort-safe region as the chaser approaches the target. Thus, we guarantee the existence of passive or active aborts in various thrust failure scenarios. The characterization of state space into safe and unsafe regions opens up the possibility of automating the safe rendezvous problem in a future where rendezvous is frequent and routine while allowing for online computation of fuel optimized, and often non-intuitive, safe trajectories.

3.2.1 Spacecraft Model

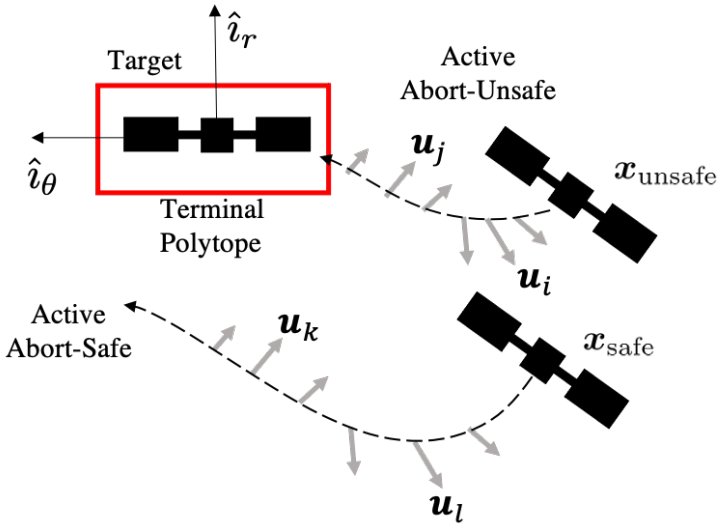
Substituting (2.8) into (2.11) yields the full nonlinear relative equations of motion, which can be linearized about the target's trajectory when $\|\boldsymbol{r}_{\mathrm{c/t}}\| \ll \|\boldsymbol{r}_{\mathrm{t/b}}\|$, and resolved in

Figure 3.1: Passive and active abort-safety illustrations.

(a) Natural dynamics takes the chaser into the AE and KOS if passively unsafe, and clears the regions if passively safe.



(b) At the active abort-unsafe state $\boldsymbol{x}_{\text{unsafe}}$, no control signal exists to avoid the target region while at $\boldsymbol{x}_{\text{safe}}$, it does.



the target's orbital frame $\mathrm{F_o}$, resulting in [85]

$$\begin{aligned}
\delta\ddot{x} - \left(\tfrac{2\mu}{r_\mathrm{t}^3} + \tfrac{h^2}{r_\mathrm{t}^4}\right)\delta x + \left(\tfrac{2\overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}\cdot\boldsymbol{r}_{\mathrm{t/b}}}{r_\mathrm{t}^4}h\right)\delta y - \left(\tfrac{2h}{r_\mathrm{t}^2}\right)\delta\dot{y} &= \tfrac{u_x}{m_\mathrm{c}}, \\
\delta\ddot{y} + \left(\tfrac{\mu}{r_\mathrm{t}^3} - \tfrac{h^2}{r_\mathrm{t}^4}\right)\delta y - \left(\tfrac{2\overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}\cdot\boldsymbol{r}_{\mathrm{t/b}}}{r_\mathrm{t}^4}h\right)\delta x + \left(\tfrac{2h}{r_\mathrm{t}^2}\right)\delta\dot{x} &= \tfrac{u_y}{m_\mathrm{c}}, \\
\delta\ddot{z} + \left(\tfrac{\mu}{r_\mathrm{t}^3}\right)\delta z &= \tfrac{u_z}{m_\mathrm{c}},
\end{aligned} \tag{3.1}$$

where ${}^{\mathrm{o}}\boldsymbol{r}_{\mathrm{c/t}} = [\delta x\ \delta y\ \delta z]^\mathsf{T} \in \mathbb{R}^3$ is the relative position resolved in $\mathrm{F_o}$, $r_\mathrm{t} = \|\boldsymbol{r}_{\mathrm{t/b}}\|$, $h = \|\boldsymbol{r}_{\mathrm{t/b}} \times \overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}\|$ is the inertial specific angular momentum of the target's orbit, and $\boldsymbol{u} \triangleq {}^{\mathrm{o}}\boldsymbol{f}_\mathrm{c} = [u_x\ u_y\ u_z]^\mathsf{T} \in \mathbb{R}^3$ is the control input applied to the chaser resolved in $\mathrm{F_o}$.

As r_t varies along the orbit, the equations of motion (3.1) result in the LTV system

$$\dot{\boldsymbol{x}}(t) = \tilde{A}(t)\boldsymbol{x}(t) + \tilde{B}\boldsymbol{u}(t), \tag{3.2}$$

where $\boldsymbol{x} \triangleq [\delta x\ \delta y\ \delta z\ \delta\dot{x}\ \delta\dot{y}\ \delta\dot{z}]^\mathsf{T} \in \mathbb{R}^6$. We sample (3.2) with sampling period ΔT, which is assumed to be small enough to not lose significant behavior between samples

$$\boldsymbol{x}_{k+1} = \boldsymbol{f}(k, \boldsymbol{x}_k, \boldsymbol{u}_k) = A_k\boldsymbol{x}_k + B_k\boldsymbol{u}_k. \tag{3.3}$$

The discrete-time LTV model (3.3) is used as a prediction model for our controller and for the reachable set calculations. The model for closed-loop simulations is obtained by time discretizing the nonlinear relative equations (2.11), (2.8) with an even finer sampling period.

While the spacecraft model used in this work is based on a Keplerian orbit around a central body, the equations of motion (3.3) are LTV and the proposed control design can be applied to relative motion about other orbits or reference trajectories that can be modeled in such way, e.g., perturbed or 3-body orbits.

3.2.2 Thrusters and Failure Modes

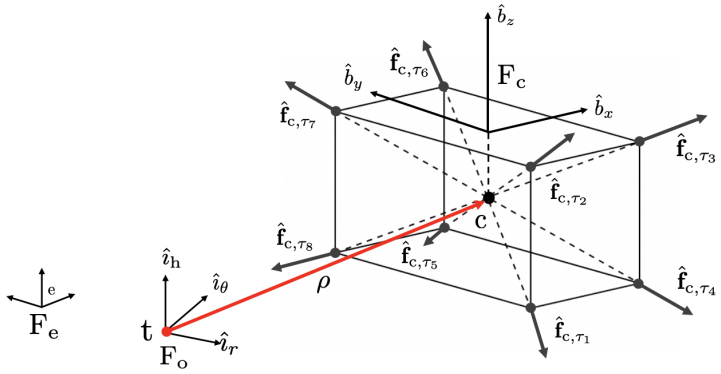
The chaser spacecraft, depicted in Figure 3.2, has eight thrusters rigidly fixed with respect to $\mathrm{F_c}$ that provide thrust in lines coincident with their positions and the center of mass of the spacecraft such that they do not impart any torque. The total force applied to

the chaser resolved in $\mathrm{F_o}$ is

$$\boldsymbol{u} = {}^{\mathrm{o}}\boldsymbol{f}_{\mathrm{c}} = \sum_{j=1}^{8} \gamma_j {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j}, \tag{3.4}$$

where $\gamma_j \in [0, u_{\mathrm{m},j}]$ is the magnitude of thruster j, $u_{\mathrm{m},j}$ is the maximum thrust of thruster j, and ${}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j}$ is the chaser-fixed thrust direction of thruster j resolved in $\mathrm{F_o}$.

Figure 3.2: Chaser model and thruster configuration. The inertial, target orbital (Hill), and chaser frames, $\mathrm{F_e}, \mathrm{F_o}, \mathrm{F_c}$ are shown.

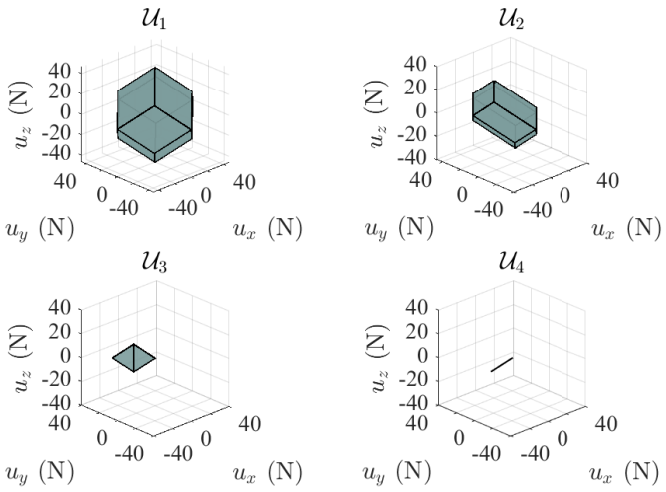


During the execution of a rendezvous maneuver, any number of thrusters may fail. Given the set of thruster indices $\mathcal{I} = \{1, 2, \ldots, 8\}$, the set of working thruster combinations is $\mathcal{M} = 2^{\mathcal{I}}$, $n_{\mathrm{F}} = |\mathcal{M}|$. The set $\mathcal{M}_i \in \mathcal{M}$ denotes a specific set of functional thrusters, also called a thrust mode. $\mathcal{M}_i = \mathcal{I}$ indicates nominal operation of all thrusters, and $\mathcal{M}_i = \emptyset$ indicates total loss of propulsion. The set of all possible failure modes is $\mathcal{FM} = \mathcal{M} \setminus \mathcal{I}$. The admissible control set $\mathcal{U}_i \subset \mathbb{R}^3$ associated with thrust mode $\mathcal{M}_i \in \mathcal{M}$ is

$$\mathcal{U}_i = \bigoplus_{j \in \mathcal{M}_i}^{|\mathcal{M}_i|} \{\gamma_j {}^{\mathrm{o}}\hat{\boldsymbol{f}}_{\mathrm{c},\tau_j} : \gamma_j \in [0, u_{\mathrm{m},j}]\}, \tag{3.5}$$

which is the Minkowski sum of various line (thrust) segments. As a result of the variable thrust assumption and the positioning of each thruster, the sets $\mathcal{U}_i$ are polytopes, for which four examples are shown in Figure 3.3.

Figure 3.3: Sample admissible control sets for different thrust modes. Upper left: all thrusters functional $\mathcal{M}_i = \mathcal{I}$. Upper right: thrusters 1, 2, and 3 working, $\mathcal{M}_i = \{1, 2, 3\}$. Bottom left: thrusters 7 and 8 are functional, $\mathcal{M}_i = \{7, 8\}$. Bottom right: only thruster 8 is functional, $\mathcal{M}_i = \{8\}$.



3.2.3 Problem Statement

Consider a given avoidance set $\tilde{\mathcal{S}} \subset \mathbb{R}^3$, which may represent the AE, KOS, or an over-approximation of the target's physical geometry. The set $\tilde{\mathcal{S}}$ is lifted to include the chaser's admissible operational velocities, yielding $\mathcal{S} \subset \mathbb{R}^6$. This defines a region in state space that the chaser must avoid in the event of total or partial thruster failure.

The objective of the safe spacecraft rendezvous problem is for the chaser to approach the target in a manner that is passively safe with respect to the AE when far, passively safe with respect to the KOS when near, and abort-safe with respect to the target region before docking. In the different phases, the approach is such that in the corresponding events of total or partial thruster failures, $\mathcal{M}_i \in \mathcal{FM}$, at a generic time instant $t_{\text{fail}} = k_{\text{fail}}\Delta T$ there exists, respectively, an uncontrolled (passive) or controlled (active) N-step abort sequence such that the chaser trajectory does not enter $\mathcal{S}$ for all discrete times $k \in \mathbb{Z}_{[k_{\text{fail}}, k_{\text{fail}}+N]}$. That is, there exists $\boldsymbol{u}_{k_{\text{fail}}}, \ldots, \boldsymbol{u}_{k_{\text{fail}}+N-1} \in \mathcal{U}_i$ such that $\boldsymbol{x}_k \notin \mathcal{S}$ for $k \in \mathbb{Z}_{[k_{\text{fail}}, k_{\text{fail}}+N]}$. In practice, N is significantly larger than what can be used for prediction horizon in a control design.

3.3 Robust Reachable Sets and Abort Safety

We enforce abort safety by maintaining the chaser outside of the unsafe region of state space, that is, the region where, if a failure occurs, a collision cannot be avoided. We construct the unsafe region from the robust backwards reachable sets (RBRS) of the target set with respect to the after-failure input set, that is, the set of states that will enter the target set regardless of the applied inputs, among those that are available after the failure. Thus, when the failure occurs and the state is in the RBRS, no admissible control exists that avoids collision at a specified final time.

Definition 3.3.1. *Given $\boldsymbol{x}_{k+1} = \boldsymbol{f}(k, \boldsymbol{x}_k, \boldsymbol{u}_k)$, a convex admissible control set $\mathcal{U}$ where $\boldsymbol{u} \in \mathcal{U}$, and final time step k_{f}, the N-step robust backward reachable set $\mathcal{R}_b(N; \mathcal{S}, \mathcal{U}, k_{\text{f}})$ of*

target region $\mathcal{S} \subset \mathbb{R}^n$ *is*

$$\mathcal{R}_b(0;\mathcal{S},\mathcal{U},k_\mathrm{f}) = \mathcal{S}, \tag{3.6a}$$

$$\mathcal{R}_b(j;\mathcal{S},\mathcal{U},k_\mathrm{f}) = \{\boldsymbol{x} \in \mathbb{R}^n : \tag{3.6b}$$

$$\boldsymbol{f}(k_\mathrm{f}-j,\boldsymbol{x},\boldsymbol{u}) \in \mathcal{R}_b(j-1;\mathcal{S},\mathcal{U},k_\mathrm{f}), \forall \boldsymbol{u} \in \mathcal{U}\},$$

$$\forall j = \{1,\ldots,N\}.$$

The N-step RBRS is the set of initial conditions at time $t_0 = t_\mathrm{f} - N\Delta T$ from which the chaser will not be able to avoid the target region $\mathcal{S}$ at time t_f, regardless of the admissible control sequence applied.

Definition 3.3.2. *The robust backwards reachable set over the discrete-time interval* $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ *(RBRSI), where* $k_0 = k_\mathrm{f} - N$*, is the union of the* j*-step RBRS for* $j = \{1,\ldots,N\}$*,*

$$\mathcal{R}_N(\mathcal{S},\mathcal{U},k_\mathrm{f}) = \bigcup_{j=0}^{N} \mathcal{R}_b(j;\mathcal{S},\mathcal{U},k_\mathrm{f}). \tag{3.7}$$

The RBRSI denotes the set of states $\bar{\boldsymbol{x}}$ such that from $\boldsymbol{x}_k = \bar{\boldsymbol{x}}$, $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$ the chaser will not be able to avoid the target region $\mathcal{S}$ at time step k_f, regardless of the admissible control sequence applied. [1]

Next, we account for changing final time, considering that the orbit, and hence the LTV system, is periodic. To this end, the orbit-RBRSI is the union of the RBRSI over $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, $k_0 = k_\mathrm{f} - N$, for k_f that varies along one orbit

$$\bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U}) = \bigcup_{k_\mathrm{f}=k_\mathrm{p}+1}^{2k_\mathrm{p}} \mathcal{R}_N(\mathcal{S},\mathcal{U},k_\mathrm{f}), \tag{3.8}$$

where k_p is the orbital period in time steps, and we assume that $N < k_\mathrm{p}$ due to the length of the desired spacecraft maneuver. By taking the union of the RBRSI for changing final time

[1] All discrete time representations of RBRS and RBRSI are in fact approximations for the actual continuous-time behavior. However, these approximations can be made sufficiently accurate by an appropriate choice of the sampling period ΔT.

around one orbit, (3.8) contains sets of states for which there exists a time in the target's periodic orbit such that a collision will necessarily occur after at most N steps. The union ensures the target state is evaluated at discrete points along an orbital period, yielding a set of final states

$$X_f = \left\{ \begin{bmatrix} \boldsymbol{r}_{\mathrm{t/b}}(t_\mathrm{f}) \\ \overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}\,(t_\mathrm{f}) \end{bmatrix}, \ldots, \begin{bmatrix} \boldsymbol{r}_{\mathrm{t/b}}(t_\mathrm{f} + k_\mathrm{p}\Delta T) \\ \overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}\,(t_\mathrm{f} + k_\mathrm{p}\Delta T) \end{bmatrix} \right\}, \tag{3.9}$$

which is equivalent to evaluating $\boldsymbol{r}_{\mathrm{t/b}}$, $\overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}}$ at different true anomalies $\theta \in [0, 2\pi]$, Because$k, t \propto \theta$.

Remark 1. *We arrive at the construction of $\bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})$ "backwards," by first fixing the final time and considering all initial times within N steps in* (3.7)*, and then considering all final times within the orbit in* (3.8)*, which models where along the orbit the collision will occur. An alternative, yet completely equivalent, approach is to first define the set of states that necessarily collide with the target within N steps for a fixed initial time and then take the union for all t_0 within the orbit.*

Remark 2. *Typically RBRS are the set of states that enter the target set for all disturbances in a set $\mathcal{W}$. Here, we use RBRS to determine the set of states where abort maneuvers that avoid the target set do not exist. Hence, we use the control set $\mathcal{U}$ instead of the disturbance set $\mathcal{W}$ in the RBRS computation.*

3.3.1 Abort-Safe Sets

Consider a discrete-time interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ and a target set $\mathcal{S}$ constant in such an interval. Given the state at an initial time step k_0, the state at any time step $k > k_0$ is given by

$$\boldsymbol{x}_k = \Phi(k, k_0)\boldsymbol{x}_0 + \mathcal{C}\tilde{\boldsymbol{u}}, \tag{3.10}$$

where $\mathcal{C}$ is the controllability matrix of the LTV system (3.3), $\tilde{\boldsymbol{u}}^\mathsf{T} = \begin{bmatrix} \boldsymbol{u}_{k-1}^\mathsf{T} & \ldots & \boldsymbol{u}_{k_0}^\mathsf{T} \end{bmatrix}$, and $\Phi(k, k_0) = A_k A_{k-1} \cdots A_{k_0}$ is the k_0-to-k transition matrix. For the sake of notation let

$$\boldsymbol{x}_k = \boldsymbol{\phi}(k; \boldsymbol{x}_0, \tilde{\boldsymbol{u}}, k_0), \tag{3.11}$$

where $\tilde{\boldsymbol{u}} \in \mathcal{U}^h$, and, with a little abuse of notation, $h \geq k - k_0$, i.e., we may include more inputs in $\tilde{\boldsymbol{u}}$ even though the ones with indexes $j > k-1$ have no impact on $\boldsymbol{x}_k$. Letting $k_\mathrm{f} - k_0 = N$, we define the safe set $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S},\mathcal{U})$ as the set of initial conditions that can be made to not collide with $\mathcal{S}$ within a desired discrete-time interval, i.e., $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S},\mathcal{U}) = \{\boldsymbol{x} \in \mathbb{R}^n : \ \exists \tilde{\boldsymbol{u}} \in \mathcal{U}^N, \ \boldsymbol{\phi}(k;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},k_0) \notin \mathcal{S}, \ \forall k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}\}$.

Proposition 3.3.1. *Let $\boldsymbol{x}_0 \in \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})^c$. Then, for any k_0 and $k_\mathrm{f} = k_0 + N$, there exists $\tilde{\boldsymbol{u}} \in \bar{\mathcal{U}}^N$, such that $\boldsymbol{\phi}(k;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},k_0) \ \notin \mathcal{S}$, for all $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$. Hence,*

$$\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S},\mathcal{U}) = \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})^c. \tag{3.12}$$

Proof. By construction of (3.7) and (3.8), $\bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})$ contains all the initial conditions $\boldsymbol{x}_0$ such that for all $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ there exists $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$ such that $\boldsymbol{\phi}(k;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},k_0) \ \in \mathcal{S}$. Thus, the complement $\bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})^c$ contains the initial conditions $\boldsymbol{x}_0$ such that there exists $\tilde{\boldsymbol{u}} \in \mathcal{U}^N$ such that for all $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$, $\boldsymbol{\phi}(k;\boldsymbol{x}_0,\tilde{\boldsymbol{u}},k_0) \ \notin \mathcal{S}$, which is the desired safety condition. The validity for any k_0 is due to (3.6) and to including in (3.8) the RBRSI for all $k_\mathrm{f} \in \mathbb{Z}_{[k_\mathrm{p}+1,2k_\mathrm{p}]}$, which covers all the time instants by considering that the LTV system is periodic with period k_p. Thus, $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S},\mathcal{U}) = \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U})^c$. □

Due to the definition of $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S},\mathcal{U})$, if the state is kept inside it, the existence of a control sequence that avoids $\mathcal{S}$ in any interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ is guaranteed.

We construct the unsafe set as the union of the orbit-RBRSI in (3.8) over the input sets (3.5). Becausesome failure modes may not need to be considered, e.g., the spacecraft may be re-oriented to change the configuration of the faulty thrusters, the unsafe set is constructed from the input sets (3.5) of some pre-specified $q \leq n_\mathrm{F}$ failure modes of interest

$$\bar{\mathcal{U}} = \bigcup_{i=1}^{q} \mathcal{U}_i. \tag{3.13}$$

Then, the set of unsafe states is the union over the failure modes of interest

$$\mathcal{X}_{N,q}^{\mathrm{unsafe}}(\mathcal{S},\bar{\mathcal{U}}) = \bigcup_{\mathcal{U}_i \in \bar{\mathcal{U}}} \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U}_i). \tag{3.14}$$

Hence the safe set with respect to q failure modes is

$$\mathcal{X}_{N,q}^{\text{safe}}(\mathcal{S},\bar{\mathcal{U}}) = \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})^{\text{c}}. \tag{3.15}$$

The above equations provide general expressions for the unsafe sets that rely only on a compact target set. For actual computation of these sets, we need to assume a particular form for the target set, e.g., a polytope or an ellipsoid.

Remark 3. *The sets in $\bar{\mathcal{U}}$ are constructed under the assumption that* $\mathrm{F_c}$ *is aligned with* $\mathrm{F_o}$*. Even if this were not the case after a failure, the chaser spacecraft may be reoriented by the attitude control system to align itself with the orientation used to compute $\mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})$, ensuring active abort-safety. Such an attitude maneuver can generally be completed much faster than the required rendezvous orbital maneuver. For passive abort-safety, $\bar{\mathcal{U}} = \emptyset$, the unsafe set $\mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})$ is independent of the orientation of* $\mathrm{F_c}$*.*

3.3.2 Active Safety based on Polytopes

When the dynamics are linear as in (3.3) and the target set $\mathcal{S}$ is a polytope, the RBRS is also a polytope and is computed by solving linear programs (LPs) [86]. Hence, the unsafe set is the union of polytopes that take into account the LTV nature of the equations of relative motion as well as well as several admissible input sets that capture multiple failure modes. Consider the target set $\mathcal{S} \triangleq \mathcal{P}_{\text{f}} = \mathcal{P}(H_{\text{f}}, \boldsymbol{l}_{\text{f}})$. Let the j-step RBRS from final time t_{f} be $\mathcal{R}_b(j;\mathcal{P}_{\text{f}},\mathcal{U},k_{\text{f}}) = \mathcal{P}(H_j,\boldsymbol{l}_j)$, the $j+1$-step RBRS is $\mathcal{R}_b(j+1;\mathcal{P}_{\text{f}},\mathcal{U},k_{\text{f}}) = \{\boldsymbol{x} \in \mathbb{R}^n : H_{j+1}\boldsymbol{x} \leq \boldsymbol{l}_{j+1}\}$, where

$$H_{j+1} = H_j A_{k_{\text{f}}-(j+1)}, \tag{3.16a}$$

$$[\boldsymbol{l}_{j+1}]_i = \min_{\boldsymbol{u}\in\mathcal{U}} \quad [\boldsymbol{l}_j]_i - [H_j]_i B_{k_{\text{f}}-(j+1)}\boldsymbol{u}. \tag{3.16b}$$

Redundant hyperplanes for obtaining a minimal representation of $\mathcal{P}(H_j,\boldsymbol{l}_j)$ are removed by solving LPs. In terms of set operations, (3.16) is given by $\big(\mathcal{P}(H_j,\boldsymbol{l}_j) \ominus B_{(\cdot)}\,\mathcal{U}\big)A_{(\cdot)}$. Because$\mathcal{S}$

is a polytope, each RBRS in (3.16) will also be a polytope, while the RBRSI, $\bar{\mathcal{R}}_N(\mathcal{P}_\mathrm{f},\mathcal{U})$, is a union of polytopes, which may be non-convex.

The RBRS is expected to be smaller the larger the range is of available control after a failure, because the vehicle can perform abort maneuvers from more initial states $\boldsymbol{x}_0 \in \mathbb{R}^n$.

Proposition 3.3.2. *Given a final time step k_f and two control sets $\mathcal{U}_v$ and $\mathcal{U}_y$, such that $\mathcal{U}_y \subseteq \mathcal{U}_v$, the RBRSs at $k_\mathrm{f} - j + 1$, for $\mathcal{U}_v$ and $\mathcal{U}_y$ satisfies*

$$\mathcal{R}_b(j;\mathcal{P}_\mathrm{f},\mathcal{U}_v,k_\mathrm{f}) \subseteq \mathcal{R}_b(j;\mathcal{P}_\mathrm{f},\mathcal{U}_y,k_\mathrm{f}). \tag{3.17}$$

Proof. When considering two sets, such that $\tilde{\mathcal{G}} \subseteq \mathcal{G}$, it follows that $\big(\mathcal{F} \ominus \mathcal{G}\big) \subseteq \big(\mathcal{F} \ominus \tilde{\mathcal{G}}\big)$. Aside from the input sets $\mathcal{U}_y$ and $\mathcal{U}_v$, the RBRS at $k_\mathrm{f} - (j+1)$ are constructed using the same matrices, $A_{k_\mathrm{f}-j}$ and $B_{k_\mathrm{f}-j}$. Then, the input sets affect the RBRS computation through the Pontryagin difference $\mathcal{P}(H_j,\boldsymbol{l}_j) \ominus B_{(\cdot)}\mathcal{U}$. Thus, if $\mathcal{U}_y \subseteq \mathcal{U}_v$, then $\mathcal{R}_b(j;\mathcal{P}_\mathrm{f},\mathcal{U}_v,k_\mathrm{f}) \subseteq \mathcal{R}_b(j;\mathcal{P}_\mathrm{f},\mathcal{U}_y,k_\mathrm{f})$. □

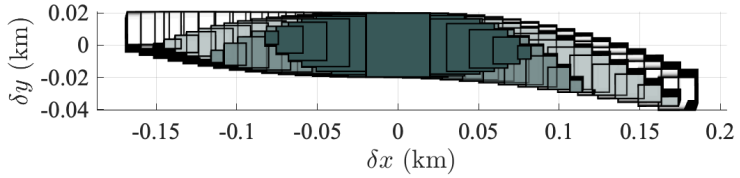
Additionally, if $\mathcal{U}_v \subseteq \mathcal{U}_y$, then $\bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U}_y) \subseteq \bar{\mathcal{R}}_N(\mathcal{S},\mathcal{U}_v)$ due to (3.8). As such, the unsafe region of state space gets larger as the spacecraft loses actuation due to thruster failures.

Figure 3.4a shows slices of the RBRSI for increasingly severe failure modes. The darker the set, the fewer thrusters have failed. Slices are taken for $\delta z = \delta\dot{y} = \delta\dot{z} = 0$ and $\delta\dot{x} \in \{-1.5,\ 0,\ 1.5\} \times 10^{-6}$ km/s. Figure 3.4b shows the projection of the same RBRSI sets onto the orbital plane, δx, δy. The sets in the RBRSI get larger as the spacecraft becomes increasingly under-actuated, indicating that a larger region of state space is unsafe. When the RBRS is computed for total propulsion failure, i.e, $\mathcal{M}_i = \emptyset$ and $\mathcal{U}_i = \emptyset$, the result is the set of passively unsafe states, i.e., the initial conditions for which free-drift trajectories enter $\mathcal{S}$. The passively unsafe set is the largest Because$\mathcal{R}_b(j;\mathcal{S},\mathcal{U}_i \neq \emptyset,k_\mathrm{f}) \subseteq \mathcal{R}_b(j;\mathcal{S},\emptyset,k_\mathrm{f})$.

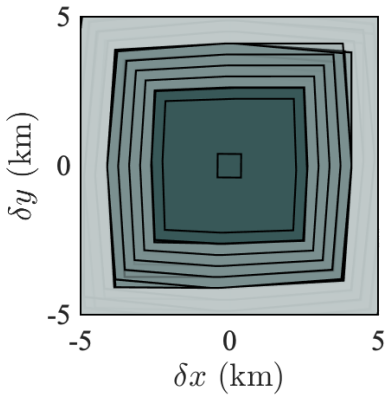
Maintaining passive safety ensures a collision free rendezvous under the worst possible propulsion failure mode. Spacecraft rendezvous missions are often staged to maintain passive

Figure 3.4: RBRSI illustrations, from dark to light: we reduce the number of functional thrusters, therefore, less safe state space.

(a) Slices of the RBRSI



(b) Projections of the RBRSI



safety first, as a chaser approaches but is still far from the target, and active safety later, as the chaser comes into close proximity to the target. Because$\tilde{\boldsymbol{u}} = \mathbf{0}_{3h\times 1} \in \mathcal{U}^h$, the computation of the RBRS are greatly simplified. For this special case, the RBRS is denoted Passive Backwards Reachable Sets (PBRS) as control is no longer considered.

Computing the PBRS is computationally much less demanding than the RBRS as no LPs need to be solved, other than those for removing redundant hyperplanes. If $k_j = k_\mathrm{f} - j$, the j-step PBRS polytope is

$$\mathcal{R}_b(j; \mathcal{P}_\mathrm{f}, \emptyset, k_\mathrm{f}) = \{\boldsymbol{x} \in \mathbb{R}^n : H_\mathrm{f}\Phi(k_\mathrm{f}, k_\mathrm{f} - j)\boldsymbol{x} \leq \boldsymbol{l}_\mathrm{f}\}. \tag{3.18}$$

3.3.3 Passive Safety based on Ellipsoids

For passive safety, an alternative is to consider an ellipsoidal target set $\mathcal{S} \triangleq \mathcal{E}_\mathrm{f} = \mathcal{E}(\mathbf{0}, P)$ centered at the origin with shape matrix P. Since $\mathcal{E}_\mathrm{f}$ is an ellipsoid, the discrete-time dynamics (3.3) are linear time-varying, and $\boldsymbol{u}_k = 0$, the j-step PBRS (3.6)

$$\mathcal{R}_b(j; \mathcal{E}_\mathrm{f}, \emptyset, k_\mathrm{f}) = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x}^\top \Phi(k_\mathrm{f}, k_\mathrm{f} - j)^\top \; P^{-1} \; \Phi(k_\mathrm{f}, k_\mathrm{f} - j) \; \mathbf{x} \leq 1\}, \tag{3.19}$$

are also ellipsoids Becauseellipsoids are closed under affine transformations. The N-step PBRSI $\mathcal{R}_N(\mathcal{E}_\mathrm{f}, \emptyset, k_\mathrm{f})$ is not an ellipsoid, but is the union of a finite set of ellipsoids. The orbit-PBRSI $\bar{\mathcal{R}}_N(\mathcal{E}_\mathrm{f}, \emptyset)$ is similarly obtained by taking the union of the N-step PBRSI over k_f that varies along one orbit.

3.4 Abort-Safe Rendezvous Control

Next, we develop an abort-safe control policy that enforces the state to remain in the safe set (3.15). Specifically, we develop a model predictive control (MPC) policy that minimizes a cost function designed based on performance metrics, while constraining the trajectory to remain within (3.15), and hence outside its complement (3.14) where, in presence of failures, collisions with the target are unavoidable.

At every time step k, the MPC policy solves the finite horizon optimal control problem

$$\min_{\boldsymbol{U}_k} \quad F(\boldsymbol{x}_{N_\mathrm{p}|k}) + \sum_{j=0}^{N_\mathrm{p}-1} L(\boldsymbol{x}_{j|k}, \boldsymbol{u}_{j|k}) \tag{3.20a}$$

$$\text{s.t.} \quad \boldsymbol{x}_{j+1|k} = A_{j|k}\boldsymbol{x}_{j|k} + B_{j|k}\boldsymbol{u}_{j|k} \tag{3.20b}$$

$$\boldsymbol{g}_k(\boldsymbol{x}_{j|k}, \boldsymbol{u}_{j|k}) \leq 0 \tag{3.20c}$$

$$u_{j|k} \in \mathcal{U}(k) \tag{3.20d}$$

$$\boldsymbol{x}_{0|k} = \boldsymbol{x}_k \tag{3.20e}$$

where $N_\mathrm{p} \ll N$ is the prediction horizon length, the prediction model (3.20b) is (3.3), (3.20c) is the safety constraint ensuring that collision can be averted in the presence of propulsion system failures, and $\mathcal{U}(k) \in \{_i\}_i$ is the input set at time step k, which depends on the propulsion system condition according to (3.5). The MPC control law is given by

$$\boldsymbol{u}_k = \kappa_\mathrm{mpc}(\boldsymbol{x}_k) = \boldsymbol{u}^*_{0|k}, \tag{3.21}$$

where $\boldsymbol{U}^*_k = (\boldsymbol{u}^*_{0|k} \dots \boldsymbol{u}^*_{N_\mathrm{p}-1|k})$ is the optimizer of (3.20).

3.4.1 Cost Function

We design the stage cost and the terminal cost in (3.20a) as

$$L(\boldsymbol{x}, \boldsymbol{u}) = \boldsymbol{x}^\top Q \boldsymbol{x} + \boldsymbol{u}^\top R \boldsymbol{u}, \tag{3.22a}$$

$$F(\boldsymbol{x}) = \boldsymbol{x}^\top M \boldsymbol{x}, \tag{3.22b}$$

where the weight matrices $Q = Q^\top \geq 0$, $R = R^\top > 0$, $M = M^\top > 0$ are selected to achieve the desired performance, resulting in a linear quadratic MPC for which (3.20) is a quadratic program (QP). The weight Q affects the primary objective, which is to approach the target, i.e., reaching zero position and velocity. The weight R affects the secondary objective, which is to minimize the total required propellant by minimizing the thrust. The terminal cost M

is usually chosen to obtain stability properties, although here the main focus is on ensuring safety in case of a thruster failure. Non-quadratic cost functions can also be used as in [55], while still achieving active safety due to the constraint (3.20c).

3.4.2 Polytopic Safety Constraint

Implementing (3.20c) directly as $x_{j|k} \in \mathcal{X}_{N,q}^{\text{safe}} = \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{P}_{\text{f}}, \bar{\mathcal{U}})^c$ renders (3.20) non-convex and hard to solve. We convexify the problem by imposing convex constraints that exclude (3.14) from the feasible space of (3.20) based on the following result.

Result 1. *([86, Prop.3.31]) Given polytopes $\mathcal{P}_1(H_1, \boldsymbol{l}_1)$, $\mathcal{P}_2(H_2, \boldsymbol{l}_2)$, then $\mathcal{P}_2(H_2, \boldsymbol{l}_2) \supset \mathcal{P}_1(H_1, \boldsymbol{l}_1)$ if and only if there exists a non-negative matrix Λ such that*

$$\begin{aligned} \Lambda H_1 &= H_2 \\ \Lambda \boldsymbol{l}_1 &\leq \boldsymbol{l}_2. \end{aligned} \tag{3.23}$$

Given a subset of the polytopes $\{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, l_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$ within $\mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{P}_{\text{f}}, \bar{\mathcal{U}})$, where $H_i^{\bar{\mathcal{R}}} \in \mathbb{R}^{n_{ci} \times n}$, we use Result 1 to construct a halfspace $\mathcal{P}_h(\boldsymbol{h}, 1) = \{\boldsymbol{x} \in \mathbb{R}^n : \ \boldsymbol{h}\boldsymbol{x} \leq 1\}$ such that $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, \boldsymbol{l}_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$. Given $\bar{\boldsymbol{x}} \in \mathbb{R}^n$, let $\boldsymbol{h}^*(\bar{\boldsymbol{x}})$, $\{\boldsymbol{\lambda}_i^*(\bar{\boldsymbol{x}})\}_{i=1}^{\ell}$, $s^*(\bar{\boldsymbol{x}})$ be the solution of

$$\min_{s, \boldsymbol{h}, \{\boldsymbol{\lambda}_i\}_{i=1}^{\ell}} \quad -s \tag{3.24a}$$

$$\text{s.t.} \quad s \geq 0 \tag{3.24b}$$

$$\boldsymbol{h}\bar{\boldsymbol{x}} \geq 1 + s \tag{3.24c}$$

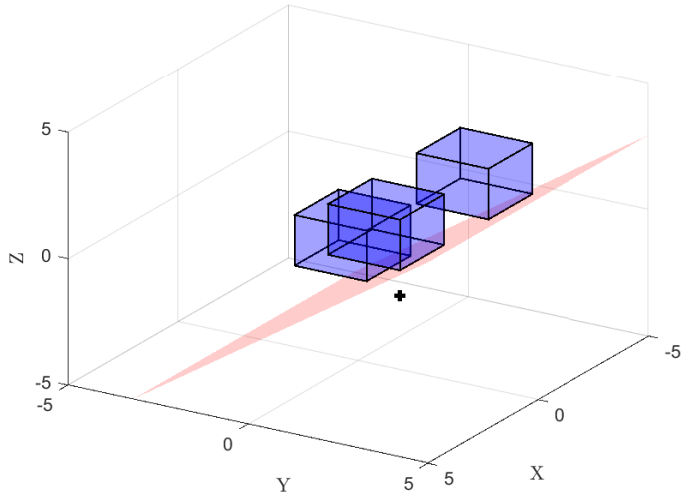
$$[\boldsymbol{\lambda}_i]_j \geq 0, \quad j = 1, \ldots, n_{ci} \tag{3.24d}$$

$$\boldsymbol{\lambda}_i H_i^{\bar{\mathcal{R}}} = \boldsymbol{h} \tag{3.24e}$$

$$\boldsymbol{\lambda}_i \boldsymbol{l}_i^{\bar{\mathcal{R}}} \leq 1, \quad i = 1, \ldots, \ell \tag{3.24f}$$

where $\boldsymbol{\lambda}_i \in \mathbb{R}^{1 \times n_{ci}}$, for all $i = 1, \ldots, \ell$. Any feasible solution of the LP (3.24) is such that $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, \boldsymbol{l}_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$. Furthermore, any feasible solution of (3.24) is such that $\bar{\boldsymbol{x}} \notin \mathcal{P}_h(\boldsymbol{h}, 1)$, and the cost function (3.24a) maximizes the clearance of $\bar{\boldsymbol{x}}$ to the half space $\mathcal{P}_h(\boldsymbol{h}^*, 1)$.

Figure 3.5: A 3D demonstration of Result 1. The blue polytopes represent sets to be avoided in 3D space while the red hyperplane separates the state marked by the black cross from the polytopes.



At time k, we construct (3.20c) from the optimal trajectory according to (3.20) at time $k-1$, $(\boldsymbol{x}^*_{0|k-1} \dots \boldsymbol{x}^*_{N_\mathrm{p}|k-1})$. Given $\boldsymbol{x}^*_{j|k-1}$, $j \in \{1, \dots, N_\mathrm{p}\}$, we select the ℓ closest polytopes in $\mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{P}_\mathrm{f}, \bar{\mathcal{U}})$ by

$$\begin{aligned} \mathrm{d}(\boldsymbol{x}^*_{j|k-1}, S_i) = \min_{\boldsymbol{y}} \quad & \|\boldsymbol{x}^*_{j|k-1} - \boldsymbol{y}\|_2 \\ \text{s.t.} \quad & \boldsymbol{y} \in S_i. \end{aligned} \tag{3.25}$$

Then, we compute $\boldsymbol{h}_{j|k} = \boldsymbol{h}(\boldsymbol{x}^*_{j+1|k-1})$ from (3.24) based on the selected $\{\mathcal{P}_i\}_{i=1}^{\ell}$ and implement (3.20c) as its complement

$$-\boldsymbol{h}_{j|k}\boldsymbol{x}_{j|k} \leq -1 - \rho, \tag{3.26}$$

where $\rho > 0$ is an arbitrarily small constant, in order for (3.20c) to determine a closed set excluding (3.14). Because$\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}_i\}_{i=1}^{\ell}$, (3.26) does not intersect $\cup_{i=1}^{\ell}\mathcal{P}_i$.

Remark 4. *If ℓ is chosen to include all polytopes of $\mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{P}_\mathrm{f}, \bar{\mathcal{U}})$, the feasible set of* (3.26) *is contained in $\mathcal{X}^{\mathrm{safe}}_{N}(\mathcal{P}_\mathrm{f}, \bar{\mathcal{U}})$. We allow to include only the subset of closest polytopes to take advantage of the receding horizon nature of* (3.21) *to reduce the computational burden of* (3.20) *and* (3.24)*, and to avoid being excessively conservative. In fact, $\mathcal{X}^{\mathrm{unsafe}}_{N,q}(\mathcal{P}_\mathrm{f}, \bar{\mathcal{U}})$ considers all terminal times around the orbit, while the final approach of the rendezvous maneuver considered here terminates in a small, albeit difficult to predict, fraction of the orbital period.*

Cost function (3.24a) is meant to increase the residual of $\boldsymbol{x}^*_{j|k-1}$ in satisfying (3.26), so that the chaser has more clearance to maneuver and select an optimal trajectory without riding on or near the constraint.

3.4.3 Ellipsoidal Safety Constraint

Similar to Result 1, a half-space constraint can be constructed for avoiding ellipsoidal sets.

Result 2. *([87, Section 2.5]) Given $j+k$ ellipsoids*

$$\mathcal{E}_i = \{Q_i^{\frac{1}{2}}\boldsymbol{v} + \boldsymbol{q}_i \in \mathbb{R}^n \ : \|\boldsymbol{v}\|_2 \leq 1\}, \tag{3.27}$$

where $Q_i = Q_i^{\mathsf{T}} \succ 0$, a hyperplane, defined by $\boldsymbol{a}^\top \boldsymbol{x} = b$, that strictly separates $\bigcup_{i=1}^{j} \mathcal{E}_i$ from $\bigcup_{i=k+1}^{j+k} \mathcal{E}_i$ is computed by solving the second-order cone program (SOCP)

$$-\|Q_i^\top \boldsymbol{a}\|_2 + \boldsymbol{a}^\top \boldsymbol{q}_i - b \geq \alpha, \quad i = 1, \ldots, j \tag{3.28}$$

$$\|Q_i^\top \boldsymbol{a}\|_2 + \boldsymbol{a}^\top \boldsymbol{q}_i - b \leq -\alpha, \quad i = j+1, \ldots, j+k. \tag{3.29}$$

Given a subset of the ℓ closest ellipsoids $\{\mathcal{E}(\boldsymbol{q}_i^{\bar{\mathcal{R}}}, Q_i^{\bar{\mathcal{R}}})\}_{i=l}^{\ell}$ within $\mathcal{X}_N^{\text{unsafe}}(\mathcal{E}_\text{f}, \emptyset)$, we use Result 2 to construct a halfspace $\mathcal{P}(\boldsymbol{a}^{\mathsf{T}}, 1) = \{\boldsymbol{x} \in \mathbb{R}^n \ : \ \boldsymbol{a}^{\mathsf{T}}\boldsymbol{x} \leq 1\}$ such that $\mathcal{P}_a(\boldsymbol{a}^{\mathsf{T}}, 1) \supset \{\mathcal{E}(\boldsymbol{q}_i^{\bar{\mathcal{R}}}, Q_i^{\bar{\mathcal{R}}})\}_{i=l}^{\ell}$. We separate ℓ ellipsoids from the state $\boldsymbol{x}$ and for each ellipsoid $\mathcal{E}_i$, we require that

$$\sup_{\|\boldsymbol{v}\| \leq 1} \boldsymbol{a}^{\mathsf{T}}(Q_i^{\frac{1}{2}}\boldsymbol{v} + \boldsymbol{q}_i) - b \leq -\alpha \tag{3.30}$$

where the supremum argument is

$$\boldsymbol{v}^* = \frac{Q_i^{\frac{1}{2}}\boldsymbol{a}}{\|Q_i^{\frac{1}{2}}\boldsymbol{a}\|}. \tag{3.31}$$

Substituting (3.31) into (3.30), yields the convex safety constraint for the ellipsoidal case. Thus, given $\bar{\boldsymbol{x}} \in \mathbb{R}^n$, let $\boldsymbol{a}^*(\bar{\boldsymbol{x}})$, $s^*(\bar{\boldsymbol{x}})$ be the solution of

$$\min_{s,\boldsymbol{a}} \quad -s \tag{3.32a}$$

$$\text{s.t.} \quad s \geq 0 \tag{3.32b}$$

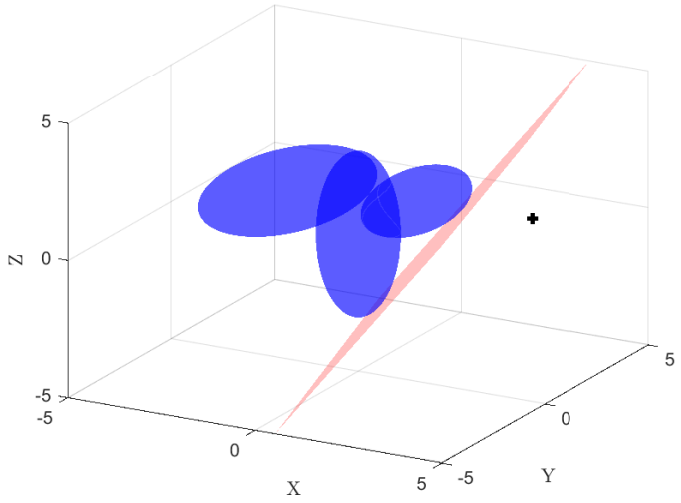
$$\boldsymbol{a}^{\mathsf{T}}\bar{\boldsymbol{x}} \geq 1 + s \tag{3.32c}$$

$$\|Q_i^\top \boldsymbol{a}\|_2 + \boldsymbol{a}^\top \boldsymbol{q}_i \leq b - \alpha, \quad i = 1, \ldots, \ell \tag{3.32d}$$

where $\alpha = 0$ as strict separation is not necessary and $b = 1$. Any feasible solution to the SOCP is such that $\mathcal{P}_a(\boldsymbol{a}, 1) \supset \{\mathcal{E}(\boldsymbol{q}_i^{\bar{\mathcal{R}}}, Q_i^{\bar{\mathcal{R}}})\}_{i=l}^{\ell}$.

Thus, in the ellipsoidal case we compute $\boldsymbol{a}_{j|k} = \boldsymbol{a}(\boldsymbol{x}^*_{k+1|t-1})$ from (3.32) by considering the ℓ closest ellipsoids to the previosuly computed trajectory in a manner similar to (3.25),

Figure 3.6: A 3D demonstration of Result 2. The blue ellipsoids represent sets to be avoided in 3D space while the red hyperplane separates the state marked by the black cross from the ellipsoids.



and replace (3.26) with

$$-\boldsymbol{a}_{j|k}^{\mathsf{T}}\boldsymbol{x}_{j|k} \leq -1-\rho. \tag{3.33}$$

Remark 5. *In the case that a single ellipsoid is used for the safety constraint, i.e., $\ell = 1$, the closest (more conservative) ellipsoid is used. The hyperplane can also be constructed by projecting the current state radially onto the ellipsoid and taking the tangent at that point, which does not require the solution of SOCPs [83]. See below for more details.*

3.4.3.1 Simplifying Heuristic

An alternative approach is to let $\ell = 1$, so that only the nearest ellipsoid is used to convexify the problem for a particular $\boldsymbol{x}_{j|k-1}$. The avoidance of each ellipsoid is then described by non-convex constraints

$$\boldsymbol{v}^{\top}(Q_i^{\bar{\mathcal{R}}})^{-1}\boldsymbol{v} \geq 1, \tag{3.34}$$

where $\boldsymbol{v}$ represents a generic state vector here. Instead of obtaining the closest sets by solving various QCQP, here, we approximately compute the closest set by taking a radial projection. A half-space is constructed using the tangent at the projected point of the ellipsoid, which removes the need to compute an optimization problem, saving computational time.

The squared radial "distance" from the state $\boldsymbol{x}$ to the surface of the ellipsoid $\mathcal{E}_i$ is

$$\rho^2 = \boldsymbol{v}^{\top}(Q_i^{\bar{\mathcal{R}}})^{-1}\boldsymbol{v}. \tag{3.35}$$

Normalizing the state $\boldsymbol{v}$ by ρ, results in a point on the ellipsoid's surface

$$\bar{\boldsymbol{v}} = \frac{\boldsymbol{v}}{\rho}, \tag{3.36}$$

because $\bar{\boldsymbol{v}}^{\top}(Q_i^{\bar{\mathcal{R}}})^{-1}\bar{\boldsymbol{v}} = 1$. The tangent hyperplane to the ellipsoid surface at $\bar{\boldsymbol{v}}$ is parameterized by the normal vector

$$\boldsymbol{a} = 2(Q_i^{\bar{\mathcal{R}}})^{-1}\bar{\boldsymbol{v}}, \tag{3.37}$$

since $Q_i^{\bar{\mathcal{R}}} = (Q_i^{\bar{\mathcal{R}}})^\top$. Then, the hyperplane is defined by all $\boldsymbol{x}$ in the following set

$$\{\boldsymbol{x} \in \mathbb{R}^6 : \boldsymbol{a}^\top \boldsymbol{x} = b\}, \tag{3.38}$$

where $b = \mathbf{a}^\top \bar{\boldsymbol{v}}$.

Given a state $\boldsymbol{x}$ at time t, we compute the projections $\bar{\boldsymbol{v}}$ to all ellipsoids $\mathcal{E}_i \in \mathcal{X}_N^{\text{unsafe}}(\cdot)$. Due to the possibly large number of ellipsoids, rather than imposing half-space constraints for all of them, we only enforce the one that seems to be most conservative, i.e., the one that is most exterior to the center of the ellipsoids, in our case the origin, by selecting i such that

$$\bar{\boldsymbol{v}}_i^* = \arg\max_i \ \|\bar{\boldsymbol{v}}_i\|, \ i = 1, \ldots, n_s, \tag{3.39}$$

where n_s is the number of sets in $\mathcal{X}_N^{\text{unsafe}}(\mathcal{E}_\text{f}, \emptyset)$. As before, the constraints along the MPC horizon are updated based on these half-spaces.

3.5 Implementation and Practical Aspects

Next, we introduce practical information related to the implementation of the approach and discuss the various safety constraints in terms of computational burden.

3.5.1 Implementation

Algorithm 1 summarizes the approach for abort-safe rendezvous, where the safe set computation is performed offline Becauseit does not require real-time data and is computationally demanding. When the spacecraft engages the final approach phase, the safety constraints are removed to allow for berthing or docking.

The algorithm is initialized by separating $\boldsymbol{x}_0$ from the nearest unsafe sets along the entire MPC window. Then, the constrained MPC problem is solved, and the states along the prediction horizon are used to re-compute half-space constraints at each step $k \in \{0, 1, ..., N-1\}$. This is repeated for some fixed number of iterations, finally resulting in an initial half-

Algorithm 1 Abort-Safe Rendezvous Control

Offline: Compute the unsafe set (3.14) using polytopic or ellipsoidal target sets
1: **input:** $\boldsymbol{x}_k$
2: **repeat**
3: Select ℓ polytopes (ellipsoids) of $\mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})$ closest to $\boldsymbol{x}_{j|k}$ by (3.25) for $j = 1,\dots,N$
4: Convexify safety constraint along MPC horizon using Results 1, 2
5: Solve optimal control problem (3.20)
6: Apply control policy (3.21) to the chaser spacecraft
7: **until** Final approach is activated

space constraint sequence. After initialization, the constraint sequence is iteratively updated with the new predicted states in receding horizon.

The following proposition summarizes the abort-safe rendezvous approach using polytopic sets.

Proposition 3.5.1. *At any time step k, let the convex safety constraint* (3.20c) *be* (3.26) *for ℓ such that $\{\mathcal{P}_i\}_{i=1}^{\ell} = \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})$. Let $\boldsymbol{x}_0$ be any state such that $\boldsymbol{x}_0 = \boldsymbol{x}_{j|v}$ for some $v = 0,\dots,N_{\text{p}}-1$, where $\{\boldsymbol{x}_{j|v}\}_{v=0}^{N_{\text{p}}}$ is any feasible trajectory of* (3.20). *Then, there exists an abort control sequence $\boldsymbol{u}^a(x_0) = \{\boldsymbol{u}_{j|k+v}(x_0)\}_{j=0}^{N-1}$ such that when applied from $\boldsymbol{x}_0$, the trajectory $\boldsymbol{x}^a(x_0,\boldsymbol{u}^a(x_0)) = \{\boldsymbol{x}_{j|k+v}\}_{j=0}^{N}$, where $\boldsymbol{x}_{0|k+v} = \boldsymbol{x}_0$, does not enter the target set, i.e, $\boldsymbol{x}_{j|k+v} \notin \mathcal{S},\ \forall j \in \{0,\dots,N\}$.*

Proof. Since (3.26) are such that their complement $\mathcal{P}_h(\boldsymbol{h},1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}},\boldsymbol{l}_i^{\bar{\mathcal{R}}})\}_{i=1}^{n_{\text{s}}} = \mathcal{X}_{N,q}^{\text{unsafe}}(\mathcal{S},\bar{\mathcal{U}})$, any feasible solution of (3.20) ensures $\boldsymbol{x}_{j|k} \in \mathcal{X}_{N,q}^{\text{safe}}$. Then per Proposition 3.3.1, for every $\boldsymbol{x_0} = \boldsymbol{x}_{j|k}$ there exists at least one abort sequence $\boldsymbol{u}^a(x_0) = \{\boldsymbol{u}_{j|k+v}(x_0)\}_{j=0}^{N-1}$ that results in a trajectory $\boldsymbol{x}_{j|k+v} \notin \mathcal{S}$ for all $j = 0,\dots,N$. Therefore, the chaser will avoid entering the target set $\mathcal{S}$ for at least N steps. □

In the passive safety case, $\{\boldsymbol{u}_{j|k+v}\}_{j=0}^{N-1} = \{\boldsymbol{0}\}_{v=0}^{N-1}$ and thus, proposition 3.5.1 applies to the ellipsoidal passive safety scenario using (3.33) instead of (3.26). Usually, $\ell \ll n_{\text{s}}$ to reduce the computational burden. However, by choosing ℓ large enough and selecting the sets based on distance, e.g., (3.25), we only remove sets that are far away from the spacecraft.

Constructing the hyperplanes (3.26) or (3.33) based on the closest sets often results in separating the spacecraft trajectory also from the neglected ones so that Proposition 3.5.1 still holds in practice.

When the chaser approaches the border of a particular target set, i.e., the AE, KOS, or target polytope, the next phase of the the maneuver can be triggered. These phase changes occur when the distance to the set is below designed thresholds, that is, $d(\boldsymbol{x}_{0|k}, \mathcal{S}_i) < d_i$, where d_i is the distance to the target set in phase i, and possibly, after additional checks are done on the spacecraft. Phasing is used because the safety constraints change along the different parts of the mission and including state-triggered constraints in the MPC [88] is outside of the scope of the current work.

3.5.2 Comparison of Various Safety Constraints

This chapter presents three methods to enforce passive and active safety based on polytopic and ellipsoidal sets. The LP and SOCP methods require solving optimizations within the MPC loop while the heuristic for ellipsoids in rem 5 does not. In all cases, the MPC problem (3.20) results in a QP. Table 3.1 highlights the number and type of optimization problem that each convexification method requires, including the determination of the ℓ closest sets and the construction of the hyperplanes. For ellipsoidal passive safety, the heuristic may be desirable for online application, as it significantly reduces the computational complexity compared to its SOCP counterpart while resulting in a similar degree of safety. If separation from multiple sets is required, the polytopic approach may be more effective than the ellipsoidal one BecauseLPs and QPs are simpler to solve, in general, than SOCPs. Table 3.1 primarily reports the types of problems to be solved, that determine what solvers need to be included in the spacecraft embedded computing platform. In terms of computational speed, the size of each problem also has impact.

Table 3.1: Online numerical optimization problems solved at each step for the different approaches of enforcing safety.

Variations	LPs	QPs	SOCP
$\mathcal{P}$ Active safety	N_p	$n_\mathrm{s}+1$	0
$\mathcal{P}$ Passive-Safety	N_p	$n_\mathrm{s}+1$	0
$\mathcal{E}$ Passive-Safety	0	1	$N_\mathrm{p}+n_\mathrm{s}$
$\mathcal{E}$ Passive-Safety Heuristic	0	1	0

3.5.3 Approach Velocities

In the polytopic case, we construct the target set as $\mathcal{P}_\mathrm{f} = \mathcal{P}(H_\mathrm{f}, \boldsymbol{l}_\mathrm{f})$, where $H_\mathrm{f} = \begin{bmatrix} I_6 & -I_6 \end{bmatrix}^\mathsf{T}$, and $\boldsymbol{l}_\mathrm{f}$ defines the upper and lower position and velocity bounds of the set, e.g., $\boldsymbol{l}_\mathrm{f} = \begin{bmatrix} p_\mathrm{m}\mathbb{1}_{1\times 3} & v_\mathrm{m}\mathbb{1}_{1\times 3} & p_\mathrm{m}\mathbb{1}_{1\times 3} & v_\mathrm{m}\mathbb{1}_{1\times 3} \end{bmatrix}^\mathsf{T}$. Similarly, the ellipsoidal target set is given by $\mathcal{E}_\mathrm{f} = \mathcal{E}(\mathbf{0}, P)$, where

$$P = \begin{bmatrix} P_\mathrm{p} & 0_{3\times 3} \\ 0_{3\times 3} & P_\mathrm{v} \end{bmatrix} \in \mathbb{R}^{6\times 6}, \tag{3.40}$$

$P_\mathrm{p} = P_\mathrm{p}^\mathsf{T} \succ 0$, and $P_v = P_v^\mathsf{T} = v_\mathrm{m} I_3 \succeq 0$. As the approach velocity bounds are increased, $v_\mathrm{m} \to \infty$, both $\mathcal{P}_\mathrm{f}$ and $\mathcal{E}_\mathrm{f}$ are unbounded in the velocity subspace, resulting in RBRSI that contain the states which enter the target set in N steps, or less, **at any relative velocity** $\dot{\boldsymbol{\rho}}$. Practically, we select $v_\mathrm{m} \gg 0$ to include the chaser's admissible operational velocities, permitting the usage of Results 1 and 2, which require $\mathcal{P}_i$ or $\mathcal{E}_i$ to be compact.

3.5.4 Robustness to unmodeled perturbations

The safety constraints in (3.20c) and the prediction model (3.20b) are designed based on (3.1), which applies to Keplerian orbits, i.e, they ignore perturbations such as Earth's non-spherical and unequal mass distribution, air-drag effects in low-Earth orbits, third-body effects, and more [69]. In practice, the use of exclusion regions such as the AE or KOS allow for the effects of these perturbations to be ignored at design time, while still ensuring safety of the target in the event of chaser propulsion failures. If the spacecraft under the nominal

model does not enter the exclusion region, when subject to non-Keplerian dynamics for short time-horizons, it will not collide with the target although it may enter the exclusion region. That is, the exclusion region works as a safety margin against unmodeled perturbations.

If one wants to achieve robust avoidance of the entire exclusion area, such as the AE or KOS, our approach provides multiple options. From a purely algorithmic perspective, the techniques presented in Section 3.3 can be extended to account for a set $\mathcal{W}$ bounding the unmodeled perturbations. This amounts to computing robust controllable sets, since in order to avoid a given region in case of propulsion failures, the trajectory must not enter the set of states for which there exists at least one disturbance sequence that results in entering the given region for all the admissible sequences of command inputs, according to the propulsion fault condition. However, that is numerically challenging because computing each step in the set iteration requires projection of a set of states and disturbances, i.e., a subset of $\mathbb{R}^{n+d}$, onto a set of states, i.e., a subset of $\mathbb{R}^n$ [89], where the projection algorithm has in general non-polynomial complexity even for polytopes.

A simple to implement, although suboptimal, approach is to inflate the unsafe sets (3.14) by a margin $\gamma > 1$, which in turn shifts the linear constraints (3.26), (3.33) that implement (3.20c). For ellipsoids and polytopes, the inflated sets are $\cup_{i=1}^{n_s}\{\boldsymbol{x} \in \mathbb{R}^6,\ \boldsymbol{x}^\top P_i^{-1}\boldsymbol{x} \leq \gamma\}$ and $\cup_{i=1}^{n_s}\mathcal{P}_i(H_i, \gamma \boldsymbol{l}_i)$, respectively. The inflation parameter γ can be selected in general by high-precision orbital simulations that characterize the impact of the disturbances, although in some cases, analytical over approximation is possible.

3.6 Simulation Results

We first present ellipsoidal passive abort safety results along with a robustness study to determine how Algorithm 1 behaves when subjected to unmodeled perturbations. Then, we report simulations that validate the polytopic active abort safety. Finally, the proposed method is demonstrated on a phased, full mission scenario of abort-safe rendezvous with

the ISS. We define an AE around the target of size $\begin{bmatrix}1 & 2 & 1\end{bmatrix}$ km in the radial, along-track, and out-of-plane directions, and a KOS of size $\begin{bmatrix}100 & 100 & 100\end{bmatrix}$ m. With approach velocities $v_{\mathrm{m}} = 0.1$km/s, these ellipsoidal sets are given by $\mathcal{E}_{\mathrm{AE}}$ and $\mathcal{E}_{\mathrm{KOS}}$, respectively. The sampling period $\Delta T = 30$s. The mass of the chaser spacecraft is $m_{\mathrm{c}} = 4000$ kg. Each thruster can apply a maximum thrust of $u_{\mathrm{m}} = 0.02$ kN. Where relevant, we discuss the performance trade-off between enforcing safety and not enforcing safety using delta-V, which is the mass-independent propellant consumption of the maneuver $\Delta V = \sum_{k=0}^{N-1} \|\tilde{B}\boldsymbol{u}_k\| \cdot \Delta T$. We run the discrete-time MPC (3.21) in closed-loop with the continuous-time model (2.11),(2.8) resolved in $\mathrm{F_o}$.

3.6.1 Ellipsoidal Passive Abort Safety

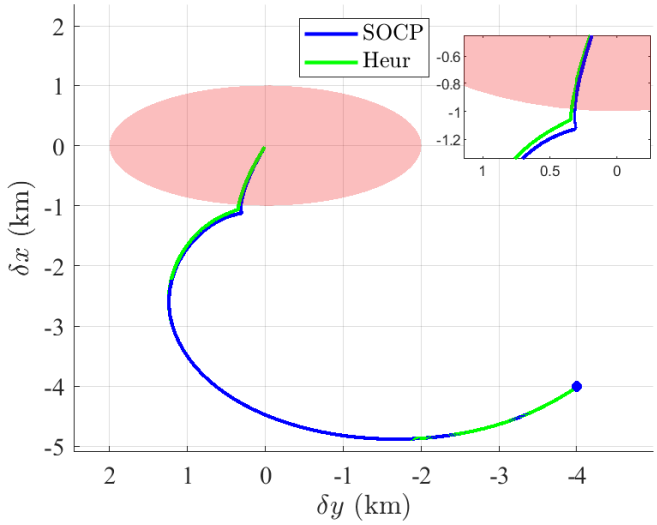
3.6.1.1 Heuristic vs. SOCP

We compare the radial projection heuristic of Remark 5 with the SOCP-based safety constraint (3.33) for a target in a circular Earth-orbit. For circular orbits, the relative equations of motion (3.1) simplify to the well-known Clohessy-Wiltshire (CW) equations [69]. Becausethe CW equations are linear time-invariant, the RBRSI are invariant along the orbit and only (3.7) is necessary for passive safety. The safety horizon N corresponds to a length of three orbital periods, $N = \frac{3k_{\mathrm{p}}}{\Delta T}$, that is, by remaining in $\mathcal{X}_N^{\mathrm{safe}}(\mathcal{S}, \emptyset)$, the chaser will not passively drift into the AE given by $\mathcal{S} \triangleq \mathcal{E}_{\mathrm{AE}} \subset \mathbb{R}^6$ for at least three subsequent orbital revolutions. The target's orbit is defined by the classical orbital elements $\begin{bmatrix}a & e & i & \omega & \Omega & f\end{bmatrix}^\top = \begin{bmatrix}6738\mathrm{km} & 0 & 51.64^\circ & 94.07^\circ & 302.37^\circ & 0^\circ\end{bmatrix}^\top$, see [69] to relate orbital elements to inertial states.

The SOCP-based method separates the chaser spacecraft from $\ell = 3$ ellipsoids at every time step in the MPC horizon, whereas the radial projection heuristic separates the chaser from $\ell = 1$ ellipsoid. Figure 3.7 shows that the approaches are similar in this simulation. Although the similar trajectories are not necessarily guaranteed for all initial conditions, the

simulation shows the benefits of using the radial-projection heuristic as it requires much less computation and can achieve similar safe approaches.

Figure 3.7: Comparing the approaches resulting from SOCP and heuristic-based safety constraints.

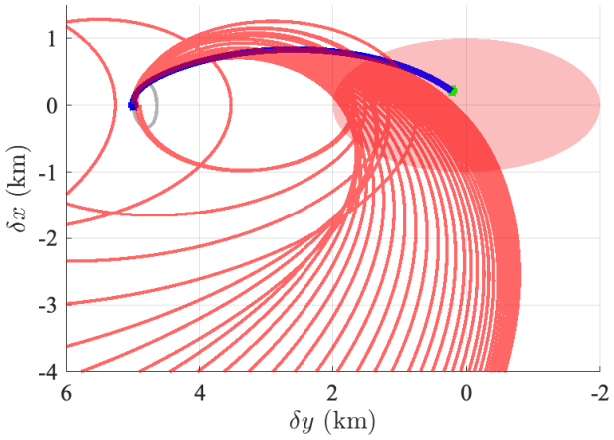


3.6.1.2 V-bar Approach

Next, we consider an along-track, also called V-bar, approach such that the initial position is purely in the $\hat{\imath}_\theta$ direction (positive δy). We compare a passively safe control policy to a simulation where the passive safety constraints are removed, i.e., a passively unsafe policy. Passive safety is enforced via the heuristic of rem 5. The target is in an eccentric Earth-orbit with the classical orbital elements $\begin{bmatrix} a & e & i & \omega & \Omega & f \end{bmatrix}^\top = \begin{bmatrix} 7420\text{km} & 0.1 & 0.01^\circ & 0^\circ & 0^\circ & 145^\circ \end{bmatrix}^\top$. The resulting orbital period of the target body is $t_\text{p} = 106.02 \text{ min} = 6361.2 \text{ s}$.

The number of steps in the MPC horizon is $N_\text{p} = 30$. The safety horizon N corresponds to three orbital periods, which is more than 20 times the length of the prediction horizon. The safety phases with respect to the AE and KOS share the same state and control penalties,

Figure 3.8: Passively Unsafe approach with respect to the AE from the along-track direction for a target in an eccentric orbit. States along the trajectory enter the AE under natural dynamics.



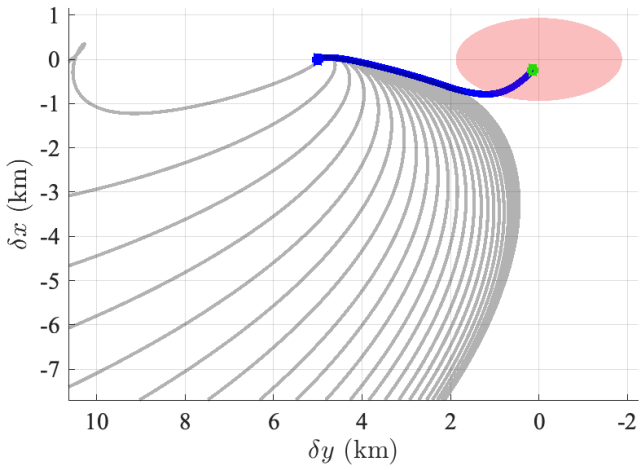
$Q = I_6$, $R = 1.3 \cdot 10^4 I_3$, and terminal cost $M = 10^2 I_6$. The initial state is $\boldsymbol{x}_0 = \begin{bmatrix} \boldsymbol{p}_0^\mathsf{T} & \boldsymbol{v}_0^\mathsf{T} \end{bmatrix}^\mathsf{T}$ where $\boldsymbol{p}_0^\mathsf{T} = \begin{bmatrix} 0 & 5 & 0 \end{bmatrix}$km and $\boldsymbol{v}_0^\mathsf{T} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ km/s.

The results are shown in Figures 3.8–3.10, where, the initial condition is represented by a blue circle, the trajectory of the relative position of the chaser with respect to the target as seen in the target's orbital frame F_o is shown in blue. The sampled free-drift trajectories propagated forward without control to verify passive safety are shown in gray. The sampled free-drift trajectories that enter the AE or the KOS are shown in red.

As a baseline, we apply the MPC policy (3.21) that does not enforce the passive safety constraints. The resulting maneuver is shown in Figure 3.8 and requires $\Delta V_\mathrm{unsafe} = 0.0134$ km/s. The spacecraft enters the AE orbit-PBRSI prior to reaching the target set boundary and thus, sampled free-drift trajectories along the nominal rendezvous maneuver intersect the AE and are unsafe (shown in red). Then, we run the same simulation while enforcing the passive safety constraint, which yields the maneuver shown in Figure 3.9. Clearly, enforcing the passive safety constraints results in a passively safe trajectory towards the AE with $\Delta V_\mathrm{safe} = 0.0206$ km/s.

Once the chaser chaser is near the AE, the maneuver proceeds towards the target

Figure 3.9: Passively safe approach with respect to the AE, in red, from the along-track direction for a target in an eccentric orbit. Sampled states do not enter the AE under natural dynamics within the safety horizon N.



while maintaining passive safety with respect to the KOS. The resulting maneuver is shown in Figure 3.10.

3.6.1.3 Robustness to Unmodeled Perturbations

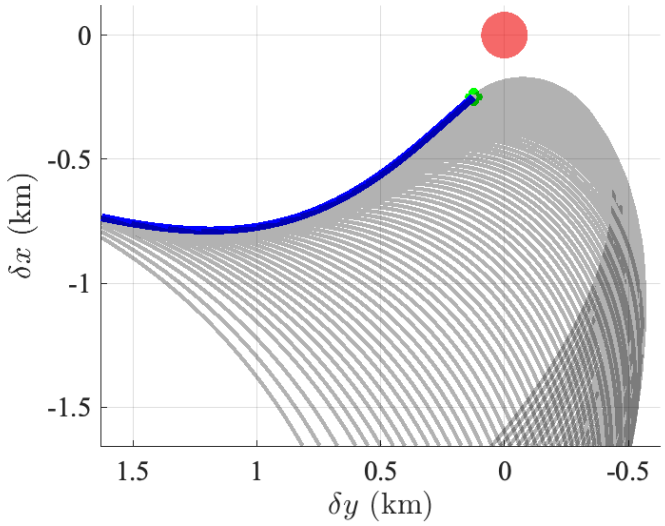
In order to evaluate the proposed control policy when subjected to realistic perturbations, we consider the target and chaser spacecraft to be perturbed by Earth's oblateness, captured by the J2 zonal harmonic acceleration, and third body gravitational disturbances from the sun and the moon. The perturbations are nonlinear functions of the inertial position, $\boldsymbol{r}$, and are denoted $\boldsymbol{a}_{J2}(\boldsymbol{r})$, $\boldsymbol{a}_{\mathrm{s}}(\boldsymbol{r})$, and $\boldsymbol{a}_{\mathrm{m}}(\boldsymbol{r})$, respectively. Though other perturbations can be included, these are the dominant ones for most near-Earth orbital regimes. The inertial acceleration model (2.8) is modified to include the perturbations,

$$\boldsymbol{r}_{\mathrm{t}}'' = -\mu \frac{\boldsymbol{r}_{\mathrm{t}}}{\|\boldsymbol{r}_{\mathrm{t}}\|^3} + \boldsymbol{a}_{J2}(\boldsymbol{r}_{\mathrm{t}}) + \boldsymbol{a}_{\mathrm{s}}(\boldsymbol{r}_{\mathrm{t}}) + \boldsymbol{a}_{\mathrm{m}}(\boldsymbol{r}_{\mathrm{t}}), \tag{3.41a}$$

$$\boldsymbol{r}_{\mathrm{c}}'' = -\mu \frac{\boldsymbol{r}_{\mathrm{c}}}{\|\boldsymbol{r}_{\mathrm{c}}\|^3} + \frac{\boldsymbol{u}}{m_{\mathrm{c}}} + \boldsymbol{a}_{J2}(\boldsymbol{r}_{\mathrm{c}}) + \boldsymbol{a}_{\mathrm{s}}(\boldsymbol{r}_{\mathrm{c}}) + \boldsymbol{a}_{\mathrm{m}}(\boldsymbol{r}_{\mathrm{c}}), \tag{3.41b}$$

yielding orbits that are no longer Keplerian. While the simulation model (2.11) is perturbed, we retain (3.2) for constructing the RBRS and as the MPC prediction model (3.20b).

Figure 3.10: Passively safe approach with respect to the KOS, in red, from the along-track direction for a target in an eccentric orbit. Sampled states do not enter the AE under natural dynamics within the safety horizon N.



As discussed in Section 3.5.4, under perturbations the proposed safe rendezvous method is no longer guaranteed to provide abort-safe trajectories that avoid the original target sets. However, we expect the chaser trajectories to only cross the border of the exclusion zone, hence staying away from the actual target position, so that collisions are avoided thanks to the exclusion zone margin.

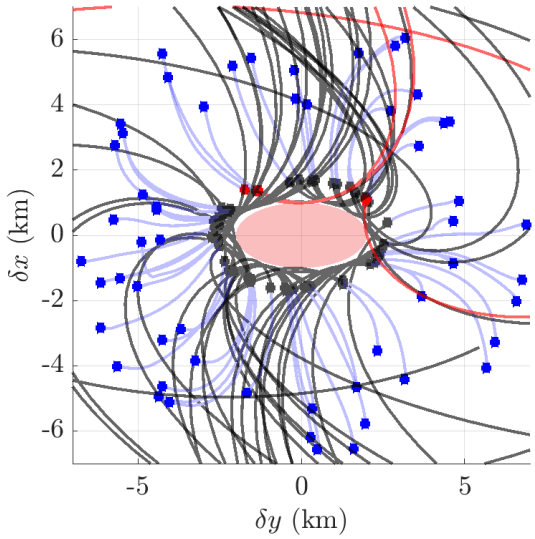
Figure 3.11 shows $N_{\text{sim}} = 55$ closed-loop simulations of passive safety with respect to the AE, where the total loss of propulsion occurs close to the boundary of the AE. In Figure 3.11, the portions of the approach where the propulsion system operates nominally are shown in blue, while the free-drift trajectories after the failures are in black. The black marks show the states at which the thrust is fully lost, and the trajectories that enter the AE are shown in red.

Figure 3.11a shows the results for various random initial conditions when the nominal PBRSs are used, i.e., $\gamma = 1$. In this case, 3 out of 55 simulations result in trajectories that enter the AE. However, such trajectories cross the AE near the edge, clearing the target by kilometers. As expected, the AE provides a sufficient margin to avoid the target, when used in conjunction with our proposed approach.

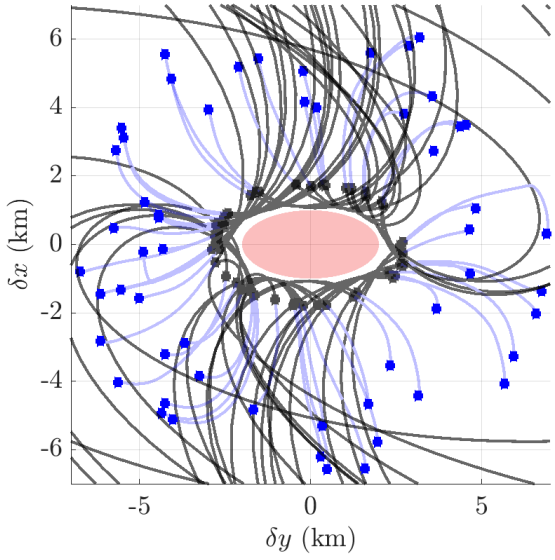
As discussed in Section 3.5.4, to ensure that the trajectories remain outside of the exclusion zone even under perturbations, the unsafe sets can be inflated, while still using the nominal safe controller. Figure 3.11b shows the trajectories for the same initial conditions and failure times as in Figure 3.11a where the RBRSs are inflated by a factor $\gamma = 1.1$. In these cases, none of the trajectories enter the AE, showing that a relatively small inflation and minor modification to the nominal sets, allows us to retain the same RBRS computation and nominal controller while maintaining robustness of the entire exclusion zone in the presence of perturbations.

Figure 3.11: Closed-loop simulations of rendezvous in presence of perturbations.

(a) Approaches from various initial conditions with nominal prediction model and nominal RBRS, i.e., $\gamma = 1$. Passively safe approaches (blue), free drift trajectories (black), failure events (black marker); 3/55 trajectories entered (briefly) the AE (red).



(b) Approaches from various initial conditions with nominal prediction model and inflated RBRS, $\gamma = 1.1$, roughly 4.9%. Passively safe approaches (blue), free drift trajectories (black), failure events (black marker). No trajectory is entering (even briefly) the AE.



3.6.2 Polytopic Active Abort-Safety

For active abort-safety, the weight matrices in the cost function (3.20a) are $Q = 10^3 \cdot I_6$, $R = I_3$, $M = Q$. The target set is defined by a polytope $\mathcal{P}(H_\mathrm{f}, \boldsymbol{l}_\mathrm{f})$ where $H_\mathrm{f} = \begin{bmatrix} I_6 & -I_6 \end{bmatrix}^\mathsf{T}$ and $\boldsymbol{l}_\mathrm{f} = \begin{bmatrix} p_\mathrm{m}\mathbb{1}_{1\times 3} & v_\mathrm{m}\mathbb{1}_{1\times 3} & p_\mathrm{m}\mathbb{1}_{1\times 3} & v_\mathrm{m}\mathbb{1}_{1\times 3} \end{bmatrix}^\mathsf{T}$, $p_\mathrm{m} = 0.02$ km, and $v_\mathrm{m} = 6.0 \times 10^{-3}$ km/s. The target initial conditions are defined by the classical orbit elements $\begin{bmatrix} a & e & i & \omega & \Omega & f \end{bmatrix}^\mathsf{T} = \begin{bmatrix} 7420\text{km} & 0.1 & 0.01^\circ & 0^\circ & 0^\circ & 140^\circ \end{bmatrix}^\mathsf{T}$, which yields an orbital period of 106.2 min. The number of steps in the MPC horizon is $N_\mathrm{p} = 8$. The safety horizon is a quarter of the orbital period, $N = \lceil \frac{t_\mathrm{p}}{4\Delta T} \rceil + 1 = 54$, almost 8 times larger than N_p. The failure occurs at t_fail, when the state is x_{k_fail}, so that for $k < k_\mathrm{fail}$, $\boldsymbol{u}_k \in \mathcal{U}_1$, which corresponds to $\mathcal{M}_1 \triangleq \mathcal{I}$, i.e., nominal control. For $k \geq k_\mathrm{fail}$, $\boldsymbol{u}_k \in \mathcal{U}_i$ where $\mathcal{M}_i \in \mathcal{FM}$, i.e., some thrusters have failed, where we recall the thruster layout in Figure 3.2. For $k \geq k_\mathrm{fail}$ we set $Q, M = 0_{6\times 6}$ so that the only objective is to avoid the target.

Next, we show the behavior of the **safe controller** (3.21) that enforces $\boldsymbol{x} \in \mathcal{X}_N^\mathrm{safe}(\mathcal{P}_\mathrm{f}, \mathcal{U})$ and compare it with a standard design, called the **unsafe controller**, that only enforces $\boldsymbol{x} \notin \mathcal{P}_\mathrm{f}$. We show two cases with differing thruster anomalies. We compare the behavior of the controllers before and after the failure time, $t_\mathrm{fail} = 240$s. In these simulations $q = 1$ so safety is only maintained with respect to one failure mode in each approach.

In the first case, only thruster τ_1 fails and thus $\mathcal{M}_2 \triangleq \mathcal{I} \setminus \{1\} \in \mathcal{FM}$. Initially, $\boldsymbol{u}_k \in \mathcal{U}_1$, where $\mathcal{U}_1$ is the nominal control set. After the failure occurs, $\boldsymbol{u}_k \in \mathcal{U}_2$ for the remainder of the simulation. The initial state in the target's Hill frame is $\boldsymbol{x}_0 = \begin{bmatrix} \boldsymbol{p}_0^\mathsf{T} & \boldsymbol{v}_0^\mathsf{T} \end{bmatrix}^\mathsf{T}$ where $\boldsymbol{p}_0^\mathsf{T} = \begin{bmatrix} -75.7 & 95.1 & -54.7 \end{bmatrix} \times 10^{-3}$ km and $\boldsymbol{v}_0^\mathsf{T} = \begin{bmatrix} 1.0 & -1.1 & 0.7 \end{bmatrix} \times 10^{-3}$ kms^{-1} for both controllers. The trajectories for the safe and unsafe controllers are shown in Figure 3.12a, while the control histories are shown in Figure 3.12b. Indeed, while the unsafe controller cannot avoid colliding with the target, when the safe controller is used, an avoidance maneuver is possible. The command of the unsafe controller after the failure time saturates

while attempting but failing to avoid collision. Not surprisingly, the safe approach is more costly in terms of delta-V since $\Delta V_{\text{safe}} = 5.8 \times 10^{-3}$ km/s and $\Delta V_{\text{unsafe}} = 2.8 \times 10^{-3}$ km/s.

The same behavior is observed when only thruster τ_8 remains functional after failure, i.e., $\mathcal{M}_3 \triangleq \{8\} \in \mathcal{FM}$. Then, after the failure occurs, $\boldsymbol{u}_k \in \mathcal{U}_3$, which is a single line segment. The initial condition for both controllers is $\boldsymbol{x}_0 = \begin{bmatrix} \boldsymbol{p}_0^\mathsf{T} & \boldsymbol{v}_0^\mathsf{T} \end{bmatrix}^\mathsf{T}$ where $\boldsymbol{p}_0^\mathsf{T} = \begin{bmatrix} -32.8 & -83.0 & -177.1 \end{bmatrix} \times 10^{-3}$ km and $\boldsymbol{v}_0^\mathsf{T} = \begin{bmatrix} 0.3 & 0.9 & 2 \end{bmatrix} \times 10^{-3}$ km/s The trajectories for the safe and unsafe controllers are shown in Figure 3.13a, while the control histories are shown in Figures 3.13b, respectively. Indeed, while the unsafe controller cannot avoid colliding with the target, the safe controller can. Again, this comes at the cost of increased propellant consumption, as the ΔV for the safe controller, $\Delta V_{\text{safe}} = 1.8 \times 10^{-3}$ km/s, is larger than the unsafe controller $\Delta V_{\text{unsafe}} = 1.0 \times 10^{-3}$ km/s.

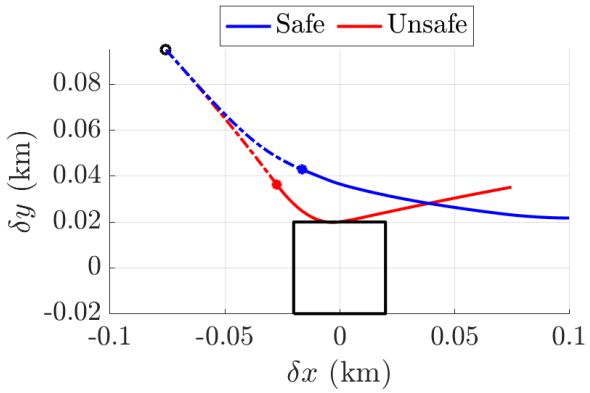
3.6.3 Varying Initial Conditions

For simplicity and clarity, we consider a scenario of a planar rendezvous, $\delta z, \delta \dot{z} = 0$. Here, the failure mode considered is defined by $\mathcal{M}_3 \triangleq \{8\} \in \mathcal{FM}$, such that thrusters τ_1 through τ_7 simultaneously fail. In these simulations, the failure occurs at $k_{\text{fail}} = 0$, and as a consequence $\boldsymbol{u}_k \in \mathcal{U}_3$, for all $k \geq 0$. We generate random initial conditions $\boldsymbol{x}_0^{\text{safe,i}} \in \mathcal{X}_{N,1}^{\text{safe}}(\mathcal{P}_{\text{f}}, \mathcal{U}_3)$ and $\boldsymbol{x}_0^{\text{unsafe,i}} \in \tilde{\mathcal{R}}_N(\mathcal{P}_{\text{f}}, \mathcal{U}_3, k_{\text{f}}) \subset \mathcal{X}_{N,1}^{\text{unsafe}}$ in a small region around the target.

Figure 3.14a shows that all of the initial conditions within the safe set can use the remaining thruster to stay away from the target for the remainder of the simulation. For comparison, Figure 3.14b shows the resulting trajectories when the unsafe controller attempts to only avoid the target set, i.e., $\boldsymbol{x}_{j|k} \notin \mathcal{P}_{\text{f}},\ \forall j = \{1, \ldots, N_p\}$ given initial conditions within the unsafe set $\tilde{\mathcal{R}}_N(\mathcal{P}_{\text{f}}, \mathcal{U}_3, k_{\text{f}})$. In this case, the unsafe controller is unable to avoid the target polytope due to the unsafe initial conditions, as expected by the construction of (3.6).

Figure 3.12: Comparison of the safe and unsafe controllers when only thruster, τ_1, fails, i.e., $\mathcal{M}_2 = \mathcal{I} \setminus \{1\}$.

(a) Approaches to the target set, in black, for the controllers. The black circle and marks are the the initial and failure states, respectively. Dashed and solid lines are states before and after attempted abort.



(b) Control histories for the controllers. Vertical dash line marks t_{fail}.

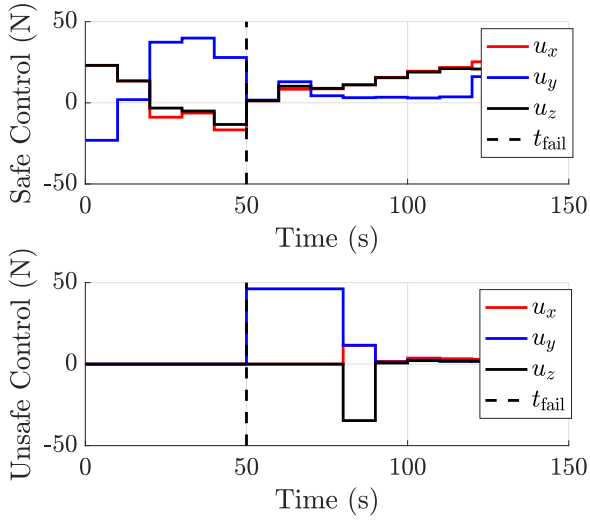
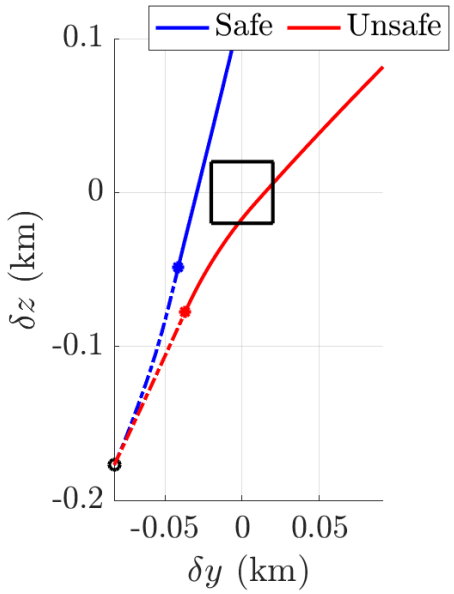


Figure 3.13: Comparison of the safe and unsafe controllers when thrusters $\tau_1 - \tau_7$ fail, i.e., $\mathcal{M}_3 = \{8\}$.

(a) Approaches to the target set, in black, for the controllers. The black circle and marks are the the initial and failure states, respectively. Dashed and solid lines are states before and after attempted abort.



(b) Control histories for the controllers. Vertical dash line marks t_{fail}.

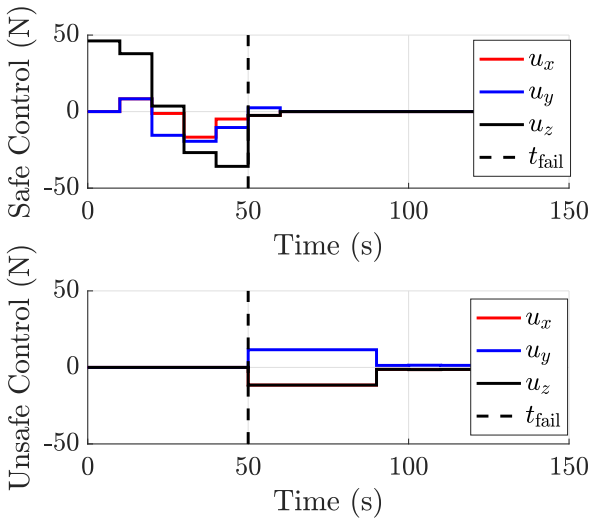
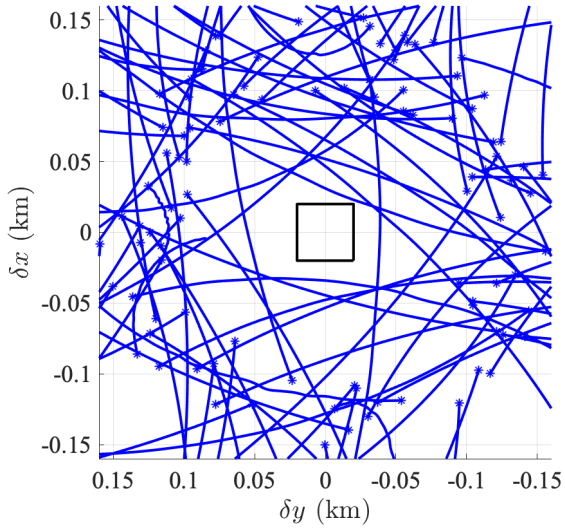
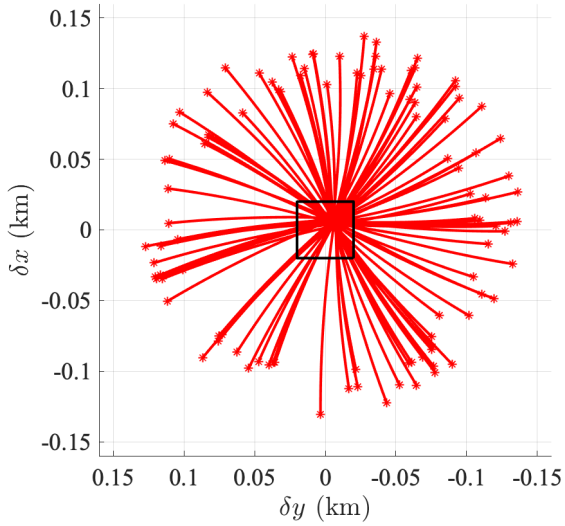


Figure 3.14: Various initial conditions for the case when only 1 thruster remains functional after the failure, i.e., $\mathcal{M}_3 = \{8\}$.

(a) Simulations with safe controller for multiple safe initial conditions, $\boldsymbol{x}_0 \in \mathcal{X}_{N,1}^{\text{safe}}(\mathcal{P}_\text{f}, \mathcal{U}_3)$. Collisions with the target $\mathcal{P}_\text{f}$ can be avoided.



(b) Simulations with the unsafe controller, which attempts to avoid $\mathcal{P}_\text{f}$ at all times, for multiple unsafe initial conditions $\boldsymbol{x}_0 \in \mathcal{X}_{N,1}^{\text{unsafe}}(\mathcal{P}_\text{f}, \mathcal{U}_3)$. The chaser cannot avoid entering target set $\mathcal{P}_\text{f}$.



3.6.4 Full Mission Simulation - ISS Rendezvous

We consider a realistic mission scenario where the chaser rendezvous with a target in a circular low Earth orbit. In this scenario, the mission incorporates both passive and active safety in a a phased sequence. Initially, passive safety is necessary with respect to the approach ellipsoid. As the chaser closes in on the AE, the next phase where passive safety is maintained with respect to the KOS is initiated. Upon closer proximity, the active safety phase is initiated. We consider a target representing the international space station (ISS) in a circular orbit with orbital elements given in Section 3.6.1.1. Active safety is maintained with respect to all thruster failure combinations, yielding $n_{\mathrm{F}} = 255$ failure modes. As a result of the LTI dynamics, all of these failure modes can be considered concurrently since $n_{\mathrm{s}} = 2527$, while it would be much larger in the LTV case.

We consider the relative initial state $\boldsymbol{x}_0 = \begin{bmatrix} \boldsymbol{p}_0^{\mathsf{T}} & \boldsymbol{v}_0^{\mathsf{T}} \end{bmatrix}^{\mathsf{T}}$ where $\boldsymbol{p}_0^{\mathsf{T}} = \begin{bmatrix} 0 & 5 & 0 \end{bmatrix}$ km and $\boldsymbol{v}_0^{\mathsf{T}} = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ km/s. As before, passive safety is maintained in both the AE and KOS phases of the rendezvous simulation. Figure 3.15 shows the corresponding approach with the annotated mission phases. Starting from the left, the first green circle shows the initial state and where passive safety is maintained with respect to $\mathcal{E}_{\mathrm{AE}}$. Immediately to the right, at $\delta y \approx 2$km, the mission progresses to the next phase and passive safety is maintained with respect to $\mathcal{E}_{\mathrm{KOS}}$. Then, the active abort-safety phase begins. Finally, the green circle closest to $\mathcal{E}_{\mathrm{KOS}}$ shows the activation of the final approach, i.e., where the chaser converges to the origin, $\boldsymbol{x} \to 0$.

We can confirm that safety is maintained with respect to the various phases by checking if any of the states along the approach are inside each phases' corresponding unsafe sets. Figure 3.16 shows that the chaser only enters the prior phases' unsafe sets after the phase switching times, i.e., after it has permission to advance to the next phase. These transition times are shown by the black dashed vertical lines. Similarly, the phases switches are evident in the history of the MPC control signals in Figure 3.17.

Figure 3.15: Safe approach for a full mission scenario with annotated safety specifications per phase. Each phase begins at a green circle.

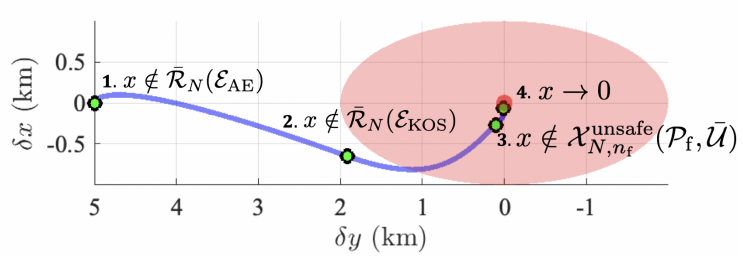


Figure 3.16: States only enter a particular phase's unsafe sets after explicitly being commanded to do so.

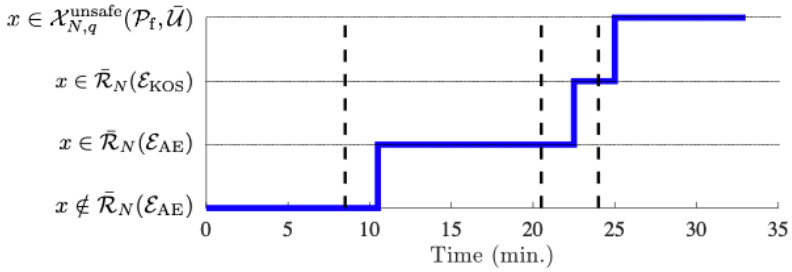
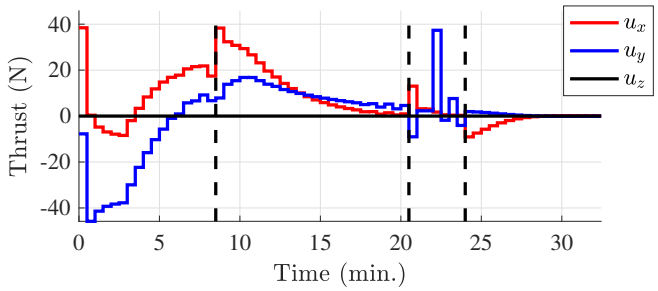


Figure 3.17: Control over the various phases of the mission.



Chapter 4

Fuel-Efficient Abort-Safe Spacecraft Rendezvous with State and Dynamics Uncertainty

In the previous chapter, a deterministic abort-safe rendezvous model predictive control policy and analysis is presented. In this chapter, the focus lies on improving control performance in terms of ΔV to develop more fuel-efficient solutions. Additionally, we generalize our prior work on abort-safe rendezvous to consider stochastic disturbances in the dynamics as well as input uncertainty. Though we focus on the rendezvous problem in this chapter, the methods developed are applicable to general formation flying scenarios.

4.1 Introduction

As discussed in chapter 3, fail-safe spacecraft rendezvous can be cast as a trajectory generation and control problem that avoids unsafe regions of state space in which collision is guaranteed under total or partial thrust failure. The unsafe regions can be characterized using reachability theory [84, 86, 90]. Recall that spacecraft missions often seek to minimize ΔV, which provides a measure of the total propellant consumed throughout a maneuver [54]. When introducing non-convex safety constraints, it becomes difficult to solve for the optimal ΔV maneuver in a computationally efficient manner [91]. As such, the non-convex constraints are often locally approximated as convex constraints, yielding a feasible sub-optimal solution that remains fuel efficient. These convexified constraints have been exploited to maintain passive safety using MPC [9, 55, 83, 84]. Moreover, thruster on-time may be

reduced by incorporating thruster on-off integer decision variables in the optimization [92]. Combining safety and thruster on-off decision variables requires solving a non-convex mixed-integer program, which is challenging for on-board implementation. Thus, a computationally tractable approach that satisfies the safety constraints while improving performance in terms of ΔV and reduced thruster on-time is desirable. For shortness, we call an input signal where thrusters are off more often, per given time, than another input signal, one that is sparser.

As mentioned in the introduction, chapter 1, stochastic reachability analysis has been studied extensively in the literature [29, 30, 20, 31, 32, 33, 34]. When analyzing active cases, a common assumption is to assume that a Markov control policy is being used for the sake of reachability and design purposes. This allows for the theoretical characterization of the active stochastic reachable sets via dynamic programming (DP) [37, 38]. As stated previously though, such methods are computationally intractable for high-dimensional systems like ours, which motivated prior work that over and under-approximates the sets obtained with DP [39]. We leverage such work in this chapter to characterize the probabilistically unsafe regions of state space. Moreover, the impact of linearization errors in the dynamics function is also considered. This is particularly important for longer duration missions because ignoring these errors can compromise the safety of the system, even within the linearization regime of interest.

Here, for the initial approach where passive safety is typically required, we propose a solution that can improve fuel-efficiency by leveraging natural orbital dynamics using stochastic PBRS (SPBRS). The resulting methodology allows the chaser to enter a coasting-arc during which no control is required to safely coast toward the target of interest. This expands our prior work on passive and abort-safe spacecraft rendezvous about time-varying reference trajectories in chapter 3 by improving control performance and reducing thruster usage. First a goal set is defined near the original avoidance set. Then, offline, the backwards reachable sets of the goal set are computed, resulting in the sets of states that naturally drift into the goal set in a certain number of time-steps. We call these (S)PBRS emanating from

the goal set **coasting sets**. An MPC policy is then developed that targets the appropriate coasting set in an online manner, so that once the correct set is entered, the chaser can disengage its thrusters and passively coast toward the goal set. In the stochastic case, the coasting and unsafe sets are computed under the assumption that the dynamical uncertainty is modeled as additive white gaussian noise (AWGN). To compensate for state uncertainty due to imperfect measurements and process noise, chance-constraints are utilized [93].

The results in this chapter focus on a rendezvous mission concept for a target orbiting a single central body. However, we provide an example of how such a framework is used for a target in NRHO. Prior work for NRHO rendezvous has considered the design of safe approach trajectories in an offline manner [94, 95]. As for online trajectory generation, stochastic and robust MPC has been applied using chance-constraints and tube-MPC [96], [82]. This work however does not consider safety with respect to failure modes and also do not use high-fidelity NRHO target references. Our simulations demonstrate a reduction in maneuver ΔV and a significant reduction of thruster on-time compared to our prior work.

This chapter is structured as follows. Section 4.2 introduces the spacecraft model and dynamics. Section 4.3 presents the relevant reachable set theory and its relation to safety, while in Section 4.4, nonlinear reachability analysis is performed under some particular assumptions. In Section 4.5, the coasting set method is presented. Section 4.6 discusses how the stochastic passive-unsafe and abort-unsafe sets are used to develop the stochastically safe rendezvous control policy. Finally, results of the approach are shown in Section

hp2sec:simulatioN$_c$*hp*2

4.2 Stochastic Model

As before, the spacecraft are assumed to be rigid bodies such that all exogenous forces act on their centers of mass and the target spacecraft is assumed to be uncontrolled. In the two-body case, the nonlinear relative equations of motion as seen by the target are linearized while including perturbations [69]. The linearized equations of relative motion are provided

in Appendix A. Theses include some perturbations of interest, though more can be added following the same methodology. In the NRHO scenario, discussed later, the equations of motion are derived and expressed in the Synodic frame $\mathrm{F_S}$ and the related dynamics are also given in Appendix A.

Here, we denote the target's inertial state by $\boldsymbol{z}(t)$ and the chaser's relative state with respect to the target as $\boldsymbol{x}(t)$, as in Chapter 3. The stochastic nonlinear equations of relative motion are of the form

$$\dot{\boldsymbol{x}}(t) = \tilde{\boldsymbol{f}}(\boldsymbol{x}(t), \boldsymbol{z}(t)) + B\boldsymbol{u}(t) + B\delta\boldsymbol{u}(t) + \boldsymbol{q}(t) \tag{4.1}$$

where $\tilde{\boldsymbol{f}}(\boldsymbol{x}(t), \boldsymbol{z}(t))$ are the natural continuous-time dynamics of the system, the input or control uncertainty is given by $\delta\boldsymbol{u}(t) \sim \mathcal{N}(\mathbb{E}[\delta\boldsymbol{u}(t)], \Sigma^{\boldsymbol{u}}(t))$, and $\boldsymbol{q}(t) \sim \mathcal{N}(\mathbb{E}[\boldsymbol{q}(t)], \Sigma^{\boldsymbol{q}}(t))$ is the dynamical process noise in the system. The uncertainty in control may be modeled using thruster misalignment or magnitude errors as well as attitude errors. We also assume that the input uncertainty and process noise at different time steps are independent and uncorrelated, i.e., white noise.

Because linearized dynamics dominate around some nominal trajectory, we approximate the relative motion of the chaser with respect to the target (4.1) about the target's nominal trajectory using the resulting LTV system

$$\dot{\boldsymbol{x}}(t) = \tilde{A}(t)\boldsymbol{x}(t) + \tilde{B}\boldsymbol{u}(t) + \tilde{B}\delta\boldsymbol{u}(t) + \boldsymbol{q}(t), \tag{4.2}$$

where $\boldsymbol{u} \triangleq {}^{\mathrm{o}}\boldsymbol{f}_{\mathrm{c}}$ is the chaser's control input expressed in the target's orbital Hill frame $\mathrm{F_o}$. Here, the linearized domain around the chief's nominal trajectory, where the rendezvous is performed, is denoted by $\mathcal{X} \subseteq \mathbb{R}^n$. In this work we consider a discrete time formulation of (4.2) with sampling period ΔT, which is assumed to be small enough to not lose significant behavior between samples, yielding

$$\boldsymbol{x}_{k+1} = A_k\boldsymbol{x}_k + B_k(\boldsymbol{u}_k + \boldsymbol{\delta u}_k) + \boldsymbol{q}_k, \tag{4.3}$$

where $\boldsymbol{\delta u}_k \sim \mathcal{N}(\mathbb{E}[\delta \boldsymbol{u}_k], \Sigma_k^{\boldsymbol{u}})$ and $\boldsymbol{q}_k \sim \mathcal{N}(\mathbb{E}[\boldsymbol{q}_k], \Sigma_k^{\boldsymbol{q}})$ is the discrete-time process noise. The stochastic discrete-time LTV model (4.3) is used as a prediction model for our controller and for the reachable set calculations. For simplicity, in the active or controlled case, we combine the process noise and input uncertainty, yielding

$$\boldsymbol{x}_{k+1} = A_k \boldsymbol{x}_k + B_k \boldsymbol{u}_k + \boldsymbol{w}_k \tag{4.4a}$$

$$\boldsymbol{w}_k = B_k \boldsymbol{\delta u} + \boldsymbol{q}_k \tag{4.4b}$$

where $\boldsymbol{w}_k \sim \mathcal{N}(\mathbb{E}[\boldsymbol{w}_k],\ \Sigma_k^{\boldsymbol{w}})$, $\mathbb{E}[\boldsymbol{w}_k] = B_k \mathbb{E}[\boldsymbol{\delta u}] + \mathbb{E}[\boldsymbol{q}_k]$ and $\Sigma_k^{\boldsymbol{w}} = \Sigma_k^{\boldsymbol{q}} + \Sigma_k^{\boldsymbol{u}}$. In this work, we assume $\mathbb{E}[\delta \boldsymbol{u}_k] = \mathbf{0}$ and $\mathbb{E}[\boldsymbol{w}_k] = \mathbf{0}$. The relative state covariance or uncertainty at step k is denoted $\Sigma_k^{\boldsymbol{x}}$, and depends on prior state, control, and process noise. This is used for future covariance propagation using the Kalman recursion

$$\begin{aligned} \Sigma_{k+1|t}^{\boldsymbol{x}} &= A_{j|k} \Sigma_{j|k}^{\boldsymbol{x}} A_{j|k}^{\mathsf{T}} + B_{j|k} \Sigma_{j|k}^{\boldsymbol{u}} B_{j|k}^{\mathsf{T}} + \Sigma_{j|k}^{\boldsymbol{q}} \\ &= A_{j|k} \Sigma_{j|k}^{\boldsymbol{x}} A_{j|k}^{\mathsf{T}} + \Sigma_{j|k}^{\boldsymbol{w}}, \end{aligned} \tag{4.5}$$

because $\Sigma_{j|k}^{\boldsymbol{w}} = B_{j|k} \Sigma_{j|k}^{\boldsymbol{u}} B_{j|k}^{\mathsf{T}} + \Sigma_{j|k}^{\boldsymbol{q}}$. Though not shown here, a filter is used to get a-posteriori mean and uncertainty estimates as well. This model allows us to combine uncertainty in the target and chaser's inertial states in a way that either both bodies or one of them can be considered stochastic. That is, either both vehicles or one of them is modeled using stochastic dynamics, resulting in a random relative state vector.

In this work, we assume that the target's trajectory is well understood such that the linearized relative dynamics are accurate to first order. This assumption is made because any significant uncertainty in the target vehicle's state or dynamics results in uncertainty in the model matrices $A_{j|k}$ and $B_{j|k}$. Hence, any error in the estimates of $\boldsymbol{z}_k$ result in error matrices of the form ΔA_k and ΔB_k, which can be absorbed by a new process noise model, i.e., $\tilde{\boldsymbol{w}}_k = \boldsymbol{w}_k + \Delta A_k \boldsymbol{x}_k + \Delta B_k (\boldsymbol{u}_k + \delta \boldsymbol{u}_k)$. In this work, we assume that such errors are small and that the a-priori knowledge of the system matrices are accurate to first-order. Any deviations of the target from it's nominal trajectory are captured through the nominal process noise $\boldsymbol{q}_k$.

4.2.1 Problem Statement

We consider the problem of driving a spacecraft safely to a target location while avoiding a known region around the target, using minimum fuel. The maneuver is performed using a receding horizon control framework where the relative state of the chaser is partially observable through measurements. In order to account for unmodelled perturbations as well as sensor limitations, the dynamics and sensor outputs are perturbed by stochastic disturbances. For both the passive and active abort-safe scenarios, we construct over (outer) approximations of the stochastically unsafe regions of state space, which include an assumed form of dynamical uncertainty, i.e., process noise. Such regions are computed under an assumed probability of collision. Avoidance of this region of state space guarantees that a passive or active abort maneuver exists with a minimum amount of probability.

4.2.2 State Estimation and Cost

A model predictive, receding horizon, control framework is used with a planning horizon N_p. At every step $k \in \mathbb{N}$ of the receding horizon control, an estimate of the chaser's random state is available, which has distribution $\boldsymbol{x}_k \sim \mathcal{N}(\mathbb{E}[\boldsymbol{x}_k], \Sigma_k^{\boldsymbol{x}})$. The mean and covariance are updated by means of a Kalman filter, though the a-priori and a-posteriori estimates are not explicitly differentiated in the notation. In the absence of measurement and process noise, we obtain the deterministic abort-safe motion problem. The cost of the mission is denoted $J : \mathcal{X}^N \times \mathcal{U}^N \to \mathbb{R}$, is a function of the trajectory and controller. The cost of interest here attempts to reduce fuel-consumption while having desirable closed-loop or coasting properties.

4.2.3 Thruster Configuration

As shown in chapter 3, for given a thruster configuration, we can construct a general polytopic and compact admissible control set

$$\mathcal{U} = \{\boldsymbol{u} \in \mathbb{R}^3 : H_u \boldsymbol{u} \leq \boldsymbol{k}_u\}, \tag{4.6}$$

where $\mathbf{0} \in \mathcal{U}$. For simplicity, in this chapter the control vector is constrained only by lower and upper bounds, $\boldsymbol{u}_l$ and $\boldsymbol{u}_u$, respectively. Hence, $\boldsymbol{k}_u$ in (4.57) is completely determined by $\boldsymbol{u}_l$ and $\boldsymbol{u}_u$. Let $\boldsymbol{k}_{u,i}$ correspond to the admissible control set $\mathcal{U}_i$. When accounting for safety with respect to partial or total loss of thrust, it is sufficient to consider distinct $\boldsymbol{k}_{u,i}$ for different failure modes. The set of possible failure modes, $\mathcal{FM}$ is therefore given by $\mathcal{FM} = \{\boldsymbol{k}_{u,1}, \ldots, \boldsymbol{k}_{u,n_\mathrm{F}}\}$, where $n_\mathrm{F} = |\mathcal{FM}|$ is the total number of failure modes under consideration. We let $\mathcal{U}_i$ denote the admissible control set corresponding to failure mode $\mathcal{FM}_i \in \mathcal{FM}$. These failure modes are used to construct the set of states for which all control actions lead to collision with a polytopic terminal set [84].

4.3 Stochastic Reachable Sets

The introduction of stochastic noise into the computation of the unsafe regions of state space requires extending the work done in chapter 3. We characterize the abort-unsafe regions of state-space that include dynamics model uncertainty in both the passive and active abort scenarios. In the active abort-safety scenario, uncertainty in the control itself impacts the safety of possible abort maneuvers. When characterizing the passive abort sets, uncertainty in the control is not required as once the chaser ceases to engage its thrusters, the uncertainty in the state is purely driven by the nominal process noise injected into the system. For both cases, these sets define regions in which the probability of entering a final set $\mathcal{S}$ is above some threshold, i.e., the probability of collision is lower-bounded.

In this chapter, we introduce some new notation that will simplify the descriptions of the unsafe regions of state space. Most of the prior work computes controlled stochastic

backwards reachable sets based on the following one-step controlled backwards reach set [18, 40, 86, 97].

Definition 4.3.1 (One-step controlled backwards reach set)**.** *The one-step controlled backward reachable from a set $\mathcal{S} \subset \mathcal{X}$, using admissible controls $\mathcal{U}$, is defined as*

$$\tilde{\mathcal{R}}_{1,k}(\mathcal{S},\mathcal{U}) = \{\boldsymbol{x} \in \mathcal{X} : \exists \boldsymbol{u} \in \mathcal{U}, \exists \boldsymbol{y} \in \mathcal{S}, \boldsymbol{y} = A_k\boldsymbol{x} + B_k\boldsymbol{u}\}. \tag{4.7}$$

This defines all of the states that can reach a set $\mathcal{S}$ using a control action from $\mathcal{U}$ without any noise.

Unlike the controlled reach set above, for abort-safety, we compute the set of states for which all controls enter a set $\mathcal{S}$. This set was introduced in chapter 3 as the RBRS.

Definition 4.3.2 (One-step RBRS)**.** *The one-step RBRS, i.e., abort-unsafe backward reachable set, is defined as*

$$\mathcal{R}_{1,k}(\mathcal{S},\mathcal{U}) = \{\boldsymbol{x} \in \mathcal{X} : \forall \boldsymbol{u} \in \mathcal{U}, \exists \boldsymbol{y} \in \mathcal{S}, \boldsymbol{y} = A_k\boldsymbol{x} + B_k\boldsymbol{u}\}, \tag{4.8}$$

which we have seen in (3.6)*, and yields states for which all control actions result in entrance of $\mathcal{S}$, without any noise.*

4.3.1 Abort-unsafe Sets Given a Fixed Final Time

Before computing the unsafe stochastic sets for the generic LTV system (4.4a), we characterize the regions of state space for which all controls enter a set $\mathcal{S}$ at a specific final time t_f or time-step N, with some probability. For simplicity, we use the acronym SBRS to indicate the stochastic version of RBRS. We use the method in [39] to characterize such regions. For the sake of the SBRS computation, the process noise at a step k is treated as a disturbance belonging to a bounded set $\mathcal{W}_k$, such that $\mathbb{P}\{\boldsymbol{w}_k \in \mathcal{W}_k\} \geq \alpha$. Because the noise is assumed to be AWGN here, the disturbance set is constructed based on the super-level sets of a Gaussian PDF. Thus, the set $\mathcal{W}$ is an α-probability ellipsoid and we recall that if $\boldsymbol{w}$

is AWGN, then $\boldsymbol{w}_i$ and $\boldsymbol{w}_j$ are independent $\forall i, j$. Treating the process noise as a disturbance greatly simplifies the SBRS computation.

The set of states that enter $\mathcal{S}$ at a specific final time step N can be obtained from dynamic programming [39]. In this case, it is assumed that the vehicle uses a stochastic and Markov feedback control policy $\pi \in \mathcal{M}$, where $\mathcal{M}$ is the set of Markov control policies and $\mathcal{M} \subseteq \mathcal{U}$. Such policies are used to characterize the SBRS. Then, the probability that an initial state $\boldsymbol{x}_0$ at index $k = 0$ reaches $\mathcal{S}$ in N steps using a Markov policy $\pi \in \mathcal{M}$ is given by the probability measure $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_0,\pi}\{\boldsymbol{x}_N \in \mathcal{S}\}$.

In [39], the probability measure $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_0,\pi}\{\boldsymbol{x}_N \in \mathcal{S}\}$ is maximized as the objective is to find a control policy that has a high chance of satisfying the reachability goal. This results in doing a conventional stochastic controlled reachability analysis, which leverages (4.7). In the abort-safety case, we want to obtain regions of state space which enter $\mathcal{S}$ with some minimum probability, which will leverage (4.8). Successful avoidance of these probabilistically unsafe regions then ensures that an abort maneuver exists with a minimum probability. Such probability thresholds are left as design variables that depend on the application of interest.

In summary, we seek to find the policy π that minimizes $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_0,\pi}\{\boldsymbol{x}_N \in \mathcal{S}\}$. We denote the minimum probability of reaching set $\mathcal{S}$ under optimal policy π^* as $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_0,\pi^*}\{\boldsymbol{x}_N \in \mathcal{S}\}$. Using dynamic programming, the β super-level stochastic reachable set consists of all states at a step k that satisfy the reachability objective, i.e., entering $\mathcal{S}$ at step N, with minimum probability of β. The set of states at index k that enters $\mathcal{S}$ at N with at least β probability is then given by

$$\mathcal{L}_k^{\pi^*}(\beta, \mathcal{S}) = \{\boldsymbol{x}_k \in \mathcal{X} : \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k,\pi^*}\{\boldsymbol{x}_N \in \mathcal{S}\} \geq \beta\}. \tag{4.9}$$

These sets are theoretical in nature for high-dimensional systems due to the previously mentioned computational intractability. Naturally, letting $k = 0$, yields the set of initial states $\boldsymbol{x}_0$ that enters $\mathcal{S}$ at N, which is given by $\mathcal{L}_0^{\pi^*}(\beta, \mathcal{S})$.

Leveraging the prior work in [39, 97], we construct over-approximations of (4.9) to

ensure safety in the "right direction" while ensuring computationally tractability. Here, we over-approximate the sets at variable $k \in \mathbb{Z}_{[0,N]}$, where N represents the safety horizon. In this work, we over-approximate the sets $\mathcal{L}_k^{\pi^*}(\beta, \mathcal{S})$ with a set denoted $\text{Reach}_k^+(\mathcal{S}, N)$. The latter is constructed using set-based (Lagrangian) methods to characterize the over-approximation of the true reach set [18, 39], which we used in chapter 3.

Definition 4.3.3 (SBRS)**.** *The SBRS over-approximation over the discrete-time interval* $\mathbb{Z}_{[0,N]}$ *are given by the backwards recursion*

$$\mathit{Reach}_k^+(\mathcal{S}, N) = \mathcal{X} \cap \mathcal{R}_{1,k}\Big(\mathit{Reach}_{k+1}^+(\mathcal{S}, N) \oplus (-\mathcal{W}_k),\ \mathcal{U}\Big), \tag{4.10}$$

where $\mathit{Reach}_N^+(\mathcal{S}, N) = \mathcal{S}$ *and* $k = N-1, \ldots, 0$*. Starting from the final time step, we work our way to the initial time step. While* (4.10) *explicitly depends on* $\mathcal{W}_k$ *and* $\mathcal{U}$*, the dependence is dropped for notational simplicity.*

Proposition 4.3.1. *The set* $\mathit{Reach}_k^+(\mathcal{S}, N)$ *over-approximates the set* $\mathcal{L}_k^{\pi^*}(\beta, \mathcal{S})$*, i.e.,* $\mathcal{L}_k^{\pi^*}(\beta, \mathcal{S}) \subseteq \mathit{Reach}_k^+(\mathcal{S}, N)$*.*

Proof. The proof follows from [39, Thm. 2]. Let $\boldsymbol{x}_k \in \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N)$. We need to show that

$$\boldsymbol{x}_k \in \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N) \implies \boldsymbol{x}_k \in \mathcal{X} \setminus \mathcal{L}_k^{\pi^*}(\beta, \mathcal{S}). \tag{4.11}$$

The set in (4.10) is given by

$$\begin{aligned} \text{Reach}_k^+(\mathcal{S}, N) = \{\boldsymbol{x} \in \mathcal{X} : \forall j \in \mathbb{Z}_{[k,N-1]}, \forall \boldsymbol{u}_j \in \mathcal{U}, \exists \boldsymbol{w}_j \in \mathcal{W}_j, \\ \boldsymbol{x}_{j+1} = A_j \boldsymbol{x}_j + B_j \boldsymbol{u}_j + \boldsymbol{w}_j, \boldsymbol{x}_N \in \mathcal{S}\} \end{aligned} \tag{4.12}$$

The admissible complement of (4.12) is

$$\begin{aligned} \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N) = \{\boldsymbol{x} \in \mathcal{X} : \exists j \in \mathbb{Z}_{[k,N-1]}, \exists \boldsymbol{u}_j \in \mathcal{U}, \forall \boldsymbol{w}_j \in \mathcal{W}_j, \\ \boldsymbol{x}_{j+1} = A_j \boldsymbol{x}_j + B_j \boldsymbol{u}_j + \boldsymbol{w}_j, \boldsymbol{x}_N \notin \mathcal{S}\} \end{aligned} \tag{4.13}$$

This set defines the regions outside of the over-approximating SBRS. The set $\mathcal{X} \setminus \mathcal{L}_k^{\pi^*}(\beta, \mathcal{S})$, is given as

$$\mathcal{X} \setminus \mathcal{L}_k^{\pi^*}(\beta, \mathcal{S}) = \{\boldsymbol{x} \in \mathcal{X} : \inf_{\pi \in \mathcal{M}} \ \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \in \mathcal{S} | \boldsymbol{x}_k\} < \beta\}, \tag{4.14a}$$

$$= \{\boldsymbol{x} \in \mathcal{X} : \exists \pi \in \mathcal{M}, \ \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \in \mathcal{S} | \boldsymbol{x}_k\} < \beta\}, \tag{4.14b}$$

$$= \{\boldsymbol{x} \in \mathcal{X} : \exists \pi \in \mathcal{M}, \ \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k\} > 1 - \beta\}, \tag{4.14c}$$

that is, $\mathcal{X} \setminus \mathcal{L}_k^{\pi^*}(\beta, \mathcal{S})$ is characterized by the set of states for which there exists at least one Markov control (feedback) policy that does not enter the final set $\mathcal{S}$ in N steps, with at least probability $1 - \beta$.

Let the the augmented disturbance vector $\bar{\boldsymbol{w}} \in \bar{\mathcal{W}} = \mathcal{W}_k \times \cdots \mathcal{W}_{N-1}$. Then, we expand the term $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k\}$ in (4.14c) using the law of total probability to consider disturbances sampled from inside and outside of $\bar{\mathcal{W}}$ in the analysis. As such, the probability that a state $\boldsymbol{x} \in \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N)$ does not enter $\mathcal{S}$ at step N using a policy $\pi \in \mathcal{M}$, is given by

$$\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k\} = \tag{4.15a}$$

$$\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} \cdot \mathbb{P}_{\boldsymbol{w}}\{\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} + \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k, \bar{\boldsymbol{w}} \notin \bar{\mathcal{W}}\} \cdot \mathbb{P}_{\boldsymbol{w}}\{\bar{\boldsymbol{w}} \notin \bar{\mathcal{W}}\}$$

$$\geq \mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} \cdot \mathbb{P}_{\boldsymbol{w}}\{\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} = \mathbb{P}_{\boldsymbol{w}}\{\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\}$$

because $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} = 1$. We can truncate the augmented stochastic noise vector using a probability threshold β, such that $\mathbb{P}_{\boldsymbol{w}}\{\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}\} = 1 - \beta$, and thus,

$$\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_k \in \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N)\} \geq 1 - \beta. \tag{4.16}$$

This indicates that states that are outside $\text{Reach}_k^+(\mathcal{S}, N)$ are less likely to enter $\mathcal{S}$ at step N than states outside of $\mathcal{L}_k^{\pi^*}(\beta, \mathcal{S},)$, which completes the proof. □

In summary, the probability that a maneuver can avoid entering $\mathcal{S}$ at N in the region $\mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N)$ is greater than or equal to $1 - \beta$. From (4.16), it follows that $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k, \pi}\{\boldsymbol{x}_N \in$

$\mathcal{S}|\boldsymbol{x}_k \in \mathcal{X} \setminus \text{Reach}_k^+(\mathcal{S}, N)\} < \beta$. As $\beta \to 0$, we obtain a high degree of active abort-safety with respect to a specific final step N.

Remark 6. *If $\mathcal{U} = \emptyset$, then the resulting sets characterize the passively unsafe states, i.e, where passive abort-maneuvers are unsafe using probability level β.*

For a linear dynamics model (4.4a), the over-approximated stochastic backwards reachable sets (4.10) are given by

$$\mathcal{R}_{1,k}\big(\text{Reach}_{k+1}(\mathcal{S}, N) \oplus (-\mathcal{W}_k), \mathcal{U}\big) = \tag{4.17a}$$

$$\{\boldsymbol{x} \in \mathcal{X} : \forall \boldsymbol{u} \in \mathcal{U}, \exists \boldsymbol{y} \in \text{Reach}_{k+1}(\mathcal{S}, N) \oplus (-\mathcal{W}_k), \boldsymbol{y} - \boldsymbol{w}_k = A_k\boldsymbol{x} + B_k\boldsymbol{u}\}$$

$$= \{\boldsymbol{x} \in \mathcal{X} : A_k\boldsymbol{x} \in (\text{Reach}_{k+1}(\mathcal{S}, N) \oplus (-\mathcal{W}_k)) \ominus B_k\mathcal{U}\} \tag{4.17b}$$

$$= \mathcal{X} \cap \big((\text{Reach}_{k+1}(\mathcal{S}, N) \oplus (-\mathcal{W}_k)) \ominus B_k\mathcal{U}\big)A_k, \tag{4.17c}$$

for all $k = N-1, \ldots, 0$. These define the sets of states that enter $\mathcal{S}$ under disturbances contained in $\bar{\mathcal{W}}$, no matter the admissible controls $\mathcal{U}$, at step N. We enforce abort-safety by maintaining the chaser outside of this over-approximated unsafe region of state space. Because the sets in (4.17) are computed using $\mathcal{U} \supset \mathcal{M}$, this analysis holds for **general** control policies, which include which include Markov feedback controllers.

Taking the union of these sets along an interval of interest yields the SBRSI.

Definition 4.3.4. *The stochastic robust backwards reachable set over the discrete-time interval $\mathbb{Z}_{[0,N]}$ (SBRSI) is the union of the j-step SBRS for $j = \{0, \ldots, N-1\}$,*

$$\mathit{UnionReach}^+(\mathcal{S}, N) = \bigcup_{j=0}^{N} \mathit{Reach}_j^+(\mathcal{S}, N), \tag{4.18}$$

which denotes the set of states $\boldsymbol{x}_k = \bar{\boldsymbol{x}}$, $k \in \mathbb{Z}_{[0,N]}$ for which the chaser will not be able to avoid the target region $\mathcal{S}$ at time step N, regardless of the admissible control sequence applied, with probability β.

4.3.2 Abort-unsafe Sets for Varying Final Time

Above, we computed the sets of abort-unsafe states given a fixed final time step, that is we found probabilistically unsafe regions that enter $\mathcal{S}$ at a specific future time step. Here, we generalize this to varying final times due to the LTV nature of (4.4a), because a perturbed target orbit is not in a periodic orbit. To this end, the LTV-SBRSI is the union of various SBRSI for variable horizon $N \in \mathbb{Z}_{[0,k_\mathrm{f}]}$, where k_f defines the full safety horizon of interest. Thus, we introduce the set

$$\mathrm{UnionReachLTV}(\mathcal{S}, k_\mathrm{f}) = \bigcup_{N=0}^{k_\mathrm{f}} \mathrm{UnionReach}^{+}(\mathcal{S}, N), \tag{4.19}$$

which provides the union for increasing time horizons so that safety is maintained with respect to the LTV system. If only a single control set $\mathcal{U}_i$ is considered, then,

$$\mathrm{SafeSet} = \mathrm{UnionReachLTV}(\mathcal{S}, k_\mathrm{f})^c, \tag{4.20}$$

and naturally, $\mathrm{UnsafeSet} \triangleq \mathrm{UnionReachLTV}(\mathcal{S}, k_\mathrm{f})$.

As in chapter 3, to be safe with respect to various failure modes, the union of the LTV-SBRSI has to be taken over various input sets. The **abort-unsafe sets** are constructed from q input sets as

$$\mathrm{UnsafeSet} = \bigcup_{i=1}^{q} \mathrm{UnionReachLTV}(\mathcal{S}, k_\mathrm{f})\big|_{\mathcal{U}_i}, \tag{4.21}$$

where the correponding failure mode controls $\mathcal{U}_i$ are used. The safe set with respect to q failure modes is then simply given by

$$\mathrm{SafeSet} = \mathrm{UnionFail}^{\mathrm{c}}. \tag{4.22}$$

The above expressions for abort-unsafe are general and rely only on compactness of the terminal set.

4.3.3 Fixed Final Time Under-approximation of the SPBRS

It is of interest to compute under-approximations of the passive SBRS, such that, no matter the disturbance set $\mathcal{W}$ affecting the system, the initial states contained in the under-approximation will enter a desired target set, denoted $\mathcal{G} \subset \mathcal{X}$, with some probability. That is, the states are likely to enter the desired set, regardless of the disturbances affecting the system.

Definition 4.3.5. *Given $\boldsymbol{x}_{k+1} = A_k\boldsymbol{x}_k + B_k\boldsymbol{u}_k$ and final time step N, the j-step under-approximation of the passive SBRS from a goal set $\mathcal{G} \subset \mathcal{X}$ is*

$$Reach_j^-(\mathcal{G}, N) = \{\boldsymbol{x} \in \mathcal{X} : \forall \boldsymbol{w}_j \in \mathcal{W}_j, A_j\boldsymbol{x} + \boldsymbol{w}_j \in Reach_{j+1}^-(\mathcal{G}, N)\} \tag{4.23a}$$

$$= \big(Reach_{j+1}^-(\mathcal{G}, N)\} \ominus \mathcal{W}_j\big)A_j \tag{4.23b}$$

where $j = \{N-1, \ldots, 0\}$. Such sets yield states that have a likelihood of entering $\mathcal{G}$ in the N-step horizon.

Definition 4.3.6. *The inner-approximations of the passive SBRS over the discrete-time interval $\mathbb{Z}_{[0,N]}$ (passive SBRSI) is the union*

$$UnionCoast^-(\mathcal{G}, N) = \bigcup_{j=0}^{N} Reach_j^-(\mathcal{G}, N). \tag{4.24}$$

If $\boldsymbol{x}_0 \in \text{Reach}_0^-(\mathcal{G}, N)$, and the augmented disturbance set $\bar{\mathcal{W}} = \mathcal{W}_0 \times \cdots \mathcal{W}_N$, then by the law of total probability

$$\mathbb{P}(\boldsymbol{x}_N \in \mathcal{S} | \boldsymbol{x}_0) =$$

$$\mathbb{P}(\boldsymbol{x}_N \in \mathcal{G} | \boldsymbol{x}_0, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) \cdot \mathbb{P}(\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) + \mathbb{P}(\boldsymbol{x}_N \in \mathcal{G} | \boldsymbol{x}_0, \bar{\boldsymbol{w}} \notin \bar{\mathcal{W}}) \cdot \mathbb{P}(\bar{\boldsymbol{w}} \notin \bar{\mathcal{W}}) \tag{4.25a}$$

$$\geq \mathbb{P}(\boldsymbol{x}_N \in \mathcal{G} | \boldsymbol{x}_0, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) \cdot \mathbb{P}(\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) \tag{4.25b}$$

$$\geq \mathbb{P}(\bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) = \beta, \tag{4.25c}$$

because $\text{Reach}_0^-(\cdot)$ was constructed using $\bar{\mathcal{W}}$ and thus, $\mathbb{P}(\boldsymbol{x}_N \in \mathcal{G} | \boldsymbol{x}_0, \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}) = 1$, $\forall \bar{\boldsymbol{w}} \in \bar{\mathcal{W}}$, $\boldsymbol{x}_N \in \mathcal{G}$. As such, the higher the lower bound β, the higher the probability of naturally

coasting into the set $\mathcal{G}$. As the set $\bar{\mathcal{W}}$ gets larger, the passive SBRS inner approximations become "smaller" and thus the odds of entering $\mathcal{G}$ under natural dynamics are higher.

4.3.4 Over-Approximation of LTV Abort-Unsafe Sets

In general, a large number of sets characterize the union in UnionReachLTV($\mathcal{S}, k_{\mathrm{f}}$). For a single control mode $\mathcal{U}$, the number of abort-unsafe n_{s} throughout an N-step horizon is at most the sum of consecutive integers

$$n_{\mathrm{s,max}} = \frac{N(N+1)}{2}. \tag{4.26}$$

In the passive case, $n_{\mathrm{s}} = n_{\mathrm{s,max}}$, while in the active case, $n_{\mathrm{s}} \leq n_{\mathrm{s,max}}$ due to the Pontryagin difference. In chapter 3 and [84] we used ℓ nearby sets to compute a local convex constraint, but this still requires computing n_s QPs at every step in the MPC horizon to understand what unsafe regions are near the predicted state. Hence, the number of sets n_s strongly affects the computational tractability of the online approach, i.e., as N increases significantly, maintaining safety becomes intractable.

We briefly discuss a method used to over-approximate the number of passive sets such that only $N+1$ sets are needed to cover UnionReachLTV($\mathcal{S}$,$\mathcal{U}$), greatly reducing the computational load for online separation of a vehicle from the unsafe regions of state space. The proposed algorithm applies generally but is most accurate for cases where the dynamics matrix $A_i \approx A_j$.

In an N-step horizon, the j-steps SBRS are computed $N-j$ times. We over-approximate the j-steps SBRS with a single set using support functions. The result is a single set $\mathrm{Reach}_j^{\#} \supseteq \cup_j \mathrm{Reach}_j^{+}(\mathcal{S}, N-j)$ that over-approximates the relevant j-steps SBRS. This allows us to cover UnionReachLTV($\mathcal{S}, k_{\mathrm{f}}$) with $N+1$ sets.

Given a matrix $H \in \mathbb{R}^{n_r \times n}$ of direction vectors with n_r rows, the over-approximation is given by

$$\mathrm{Reach}_j^{\#} = \bigcap_{i=1}^{n_r} \Big\{ \; [H]_i \boldsymbol{x} \leq \max_{j \in \mathbb{Z}_{[0,N]}} \rho_{\mathrm{Reach}_j^{+}(\cdot)}([H]_i) \Big\}. \tag{4.27}$$

Then, we compute the over-approximation $\text{UnionReachLTV}^{\#}(\mathcal{S}, k_{\text{f}}) = \cup_{j=0}^{N}\text{Reach}_j^{\#}$ which consists of $N+1$ sets that cover the unsafe region of state space. Naturally, for LTV systems, $\text{UnionReachLTV}^{\#}(\mathcal{S}, k_{\text{f}}) \supset \text{UnionReachLTV}(\mathcal{S}, k_{\text{f}})$ while for LTI systems, the resulting sets are identical, i.e., $\text{UnionReachLTV}^{\#}(\mathcal{S}, k_{\text{f}}) \equiv \text{UnionReachLTV}(\mathcal{S}, k_{\text{f}})$. Algorithm 2 shows the logical flow of this over-approximation.

Algorithm 2 Support function-based over-approximations of **UnionReachLTV** for LTV systems

Input: $H, \mathcal{S}, \mathcal{W}_k, \mathcal{U}, k = 0, \ldots, N$,
Output: $\textbf{UnionReachLTV}^{\#}$
repeat
    For variable j, compute all j-step $\text{Reach}_j^{+}(\mathcal{S}, N-j)$ using (4.17).
    Compute $\text{Reach}_j^{\#}$ by retaining maximum $\rho_{(\cdot)}([H]_i)$, i.e., solving (4.27).
until All j-step SBRS are computed for all k

4.4 Nonlinear Reachability: Linearization Error Compensation

Though the LTV dynamics model (4.3) is generally accurate in $\mathcal{X}$, the accumulation of the model errors due to linearization can compromise the safety of the system. We are interested in compensating for such errors when characterizing **UnSafeSet** to ensure that safety is maintained **despite** the neglected higher order terms in the dynamics linearization. This is particularly important for the far-rendezvous portion of a mission, where in the event of a failure, feedback can not be used to maintain safety. Essentially, the goal is to ensure that the chaser is safe under the full nonlinear dynamics model (4.1).

Similarly, in the coasting scenario, we want to guarantee that the nonlinear system enters the desired goal set at the final time. As will be shown, neglecting such errors can result in the chaser missing the goal set $\mathcal{G}$. In [71], forward reachable sets are computed for generic nonlinear dynamical system by over-approximating the instantaneous Lagrange remainder, which is the linearization error of the multivariate dynamics function, and treating these errors as an input in a conventional linear reachability analysis. That is, the nonlinear

problem is analyzed from the perspective of a linear one in addition to some "extra" input that corresponds to the possible linearization errors.

In this work, we first specify a region of interest, namely $\mathcal{X}$, which represents the allowable domain of the chaser. In this region, the worst-case linearization errors are estimated for a chaser spacecraft in $\mathcal{X}$, which is the case for rendezvous and other formation flying missions. By first specifying the domain $\mathcal{X}$, we can correctly over-approximate the linearization error of interest, and then utilize the method in [71] to characterize the unsafe region of state space.

We denote the solution to the state equation using nonlinear and linear dynamics under a control signal $\boldsymbol{u}(t)$ for $t \in [t_0, t_f]$ as

$$\boldsymbol{x}^{\mathrm{nl}}(t) = \boldsymbol{\phi}^{\mathrm{nl}}(t; \boldsymbol{x}_0, t_0, \boldsymbol{u}(t)), \ t \in [t_0, t_f] \tag{4.28a}$$

$$\boldsymbol{x}^{\mathrm{l}}(t) = \boldsymbol{\phi}^{\mathrm{l}}(t; \boldsymbol{x}_0, t_0, \boldsymbol{u}(t)), \ t \in [t_0, t_f] \tag{4.28b}$$

and the error between the system models at t as

$$\boldsymbol{e}(t) = \boldsymbol{x}^{\mathrm{nl}}(t) - \boldsymbol{x}^{\mathrm{l}}(t). \tag{4.29}$$

Due to the affine control and disturbance in (4.1), the control and process noise do not contribute to the linearization errors under this model. For each row i of the multivariate dynamics function $\tilde{\boldsymbol{f}}(\cdot)$, the Lagrange remainder represents the exact error, and as such

$$[\dot{\boldsymbol{x}}^{\mathrm{nl}}(t)]_i = [A(t)]_i \boldsymbol{x}(t) + [B(t)]_i \boldsymbol{u}(t) + [\boldsymbol{w}(t)]_i + \mathcal{L}_i(\boldsymbol{x}(t)), \tag{4.30}$$

meaning the i^{th} component of the dynamics belongs to a set made of the linear model and the error term $\mathcal{L}_i(t)$, which is given by the Lagrange remainder.

Definition 4.4.1. *Let the continuous-time state and linearization point for* (4.1) *be* $\boldsymbol{x}(t)$ *and* $\boldsymbol{x}_{\mathrm{r}}(t)$*, respectively. The Lagrange remainder, or linearization error, for basis component*

i at a state $\boldsymbol{x}$ is given by

$$\mathcal{L}_i(\boldsymbol{x}) = \frac{1}{2}(\boldsymbol{x}-\boldsymbol{x}_{\mathrm{r}})^{\mathsf{T}}\frac{\partial^2 \tilde{\boldsymbol{f}}_i(\boldsymbol{\xi},\boldsymbol{z})}{\partial^2 \boldsymbol{x}}(\boldsymbol{x}-\boldsymbol{x}_{\mathrm{r}})^{\mathsf{T}} \tag{4.31}$$

$$= \frac{1}{2}\boldsymbol{x}^{\mathsf{T}}\frac{\partial^2 \tilde{\boldsymbol{f}}_i(\boldsymbol{\xi},\boldsymbol{z})}{\partial^2 \boldsymbol{x}}\boldsymbol{x} \tag{4.32}$$

where $\boldsymbol{x}_{\mathrm{r}} = \mathbf{0}_{n\times 1}$, $\boldsymbol{\xi} = \gamma\boldsymbol{x}, \gamma \in [0,1]$.

Remark 7. *Here, we linearize about the origin of the Hill frame, thus, $\boldsymbol{x}_{\mathrm{r}}(t) = \mathbf{0}_{n\times 1}$.*

Generally, the point at which the remainder is exactly computed, $\boldsymbol{\xi}$ is unknown, and hence has to be estimated. The state-space dynamical systems considered in this chapter are such that the first $n/2$ dynamics are simply the velocities i.e. $\tilde{\boldsymbol{f}}_i = \boldsymbol{v}_i,\ i = \{x, y, z\}$. Consequently, their Hessian matrices are zero-matrices, $\frac{\partial^2 \tilde{\boldsymbol{f}}_i(\boldsymbol{\xi},\boldsymbol{z}_k)}{\partial^2 \boldsymbol{x}} = 0_{n\times n}$ so that there is no need to compute the Lagrange remainder for half of the Cartesian basis components of interest.

To obtain a conservative estimate of the remainder, we follow the reasoning in [71], where we seek to maximize the remainder's norm $L_i(\boldsymbol{x}) \triangleq \|\mathcal{L}_i(\boldsymbol{x})\|$ in the region $\mathcal{X}$ for each basis component i at an instant in time t

$$L_i(\boldsymbol{x}^*) = \max_{\boldsymbol{x},\gamma} \left\| \frac{1}{2}\boldsymbol{x}^{\mathsf{T}}\frac{\partial^2 \tilde{\boldsymbol{f}}_i(\gamma\boldsymbol{x},\boldsymbol{z}(t))}{\partial^2 \boldsymbol{x}}\boldsymbol{x} \right\|, \tag{4.33}$$

$$\text{s.t. } \boldsymbol{x} \in \mathcal{X}, \gamma \in [0,1],$$

which is bounded by

$$0 \leq L_i(\boldsymbol{x}^*) \leq \frac{1}{2}\|\boldsymbol{x}^*\| \left\| \frac{\partial^2 \tilde{\boldsymbol{f}}_i(\gamma\boldsymbol{x}^*,\boldsymbol{z}(t))}{\partial^2 \boldsymbol{x}} \right\| \|\boldsymbol{x}^*\|, \tag{4.34a}$$

$$L_i^u(\boldsymbol{x}) = \frac{1}{2}\|\boldsymbol{x}^*\| \left\| \frac{\partial^2 \tilde{\boldsymbol{f}}_i(\gamma\boldsymbol{x}^*,\boldsymbol{z}(t))}{\partial^2 \boldsymbol{x}} \right\| \|\boldsymbol{x}^*\|. \tag{4.34b}$$

Because the continuous-time nonlinear dynamics are linearized and then discretized with sampling period ΔT and the Lagrange remainder over-approximation only holds at an instantaneous time t, we require an over-approximation $\tilde{L}_i$ of Lagrange remainder $\mathcal{L}_i(\boldsymbol{x}(t))$

over an interval of time $\tau \in [t_k, t_k + \Delta T]$, i.e,

$$L_i^u(\boldsymbol{x}(\tau)) \leq \tilde{L}_i, \ \forall \tau \in [t_k, t_k + \Delta T] \tag{4.35}$$

Such an over-approximation of the Lagrange remainder in the interval of interest in (4.35) can be found numerically. Then, we can obtain a vector of worst-case linearization errors $\bar{L}_k = \begin{bmatrix} \tilde{L}_4(t_k) & \tilde{L}_5(t_k) & \tilde{L}_6(t_k) \end{bmatrix}^\mathsf{T}$. These errors are used to create a fictitious disturbance set E_k which can be incorporated into the linear reachability analysis to make claims about the nonlinear system. The over-approximating error set in interval $[t_k, t_{k+1}]$ is constructed using

$$E_k = \{\boldsymbol{y} \in \mathbb{R}^m \ : \ H_e \boldsymbol{y} \leq \boldsymbol{k}_e\} \tag{4.36}$$

where, $H_e = [I_m, -I_m]^\mathsf{T}$ and $\boldsymbol{k}_e = [\bar{L}_k^\mathsf{T}, \bar{L}_k^\mathsf{T}]^\mathsf{T}$.

Finally, as in [71], the over-approximating linearization error set E_k at t_k is incorporated as a known disturbance on the original linear reachability analysis. As such, the nonlinear reachable states are related to the linear ones by

$$\boldsymbol{x}^{\text{nl}}(t_{k+1}) \in \{A_k \boldsymbol{x} + B_k(\boldsymbol{u} + \boldsymbol{e}_k)\}, \boldsymbol{e}_k \in E_k \tag{4.37a}$$

$$\boldsymbol{x}^{\text{nl}}(t_{k+1}) \in \{\boldsymbol{x}^{\text{l}}(t_{k+1})\} \oplus B_k E_k, \tag{4.37b}$$

where $B_k E_k$ is the error disturbance mapped into the state space. Here, provided the linear and nonlinear trajectories remain in $\mathcal{X}$, so that the errors are correctly accounted for, the reachable states of the nonlinear system are correctly captured. No guarantees can be made if the state leaves $\mathcal{X}$ as the linearization errors are then unaccounted for.

4.4.1 Over-Approximation of the Nonlinear Abort-Unsafe Sets

In the absence of stochastic noise, treating the linearization error as disturbance can result in having to perform facet and vertex enumeration, due to the Minkowski sum, which is computationally not desirable [86, 89]. Instead, we again use support functions in the

backwards recursion to compute an over-approximation of the passive and active abort-unsafe sets of the deterministic nonlinear system.

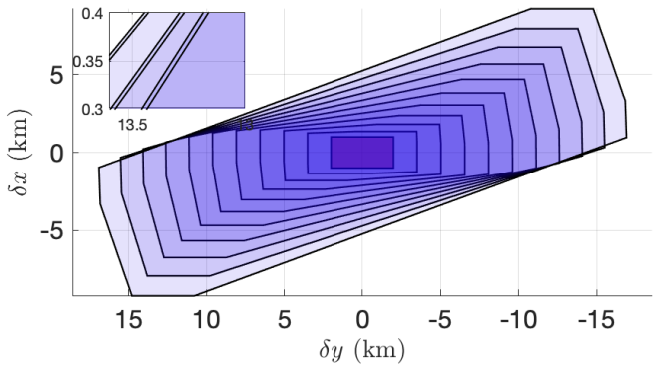
Definition 4.4.2. *The N-step over-approximation of the nonlinear RBRS from a set $\mathcal{S} \subset \mathcal{X}$ is given by*

$$\begin{aligned} \mathit{Reach}_k^{\mathrm{nl},+}(\mathcal{S}, N) &= \{\boldsymbol{x} \in \mathcal{X} : \forall \boldsymbol{u} \in \mathcal{U},\ \exists \boldsymbol{e}_k \in E_k, A_k\boldsymbol{x} + B_k\boldsymbol{u} + \boldsymbol{e}_k \in \mathit{Reach}_{k+1}^{+}(\mathcal{S}, N)\} \\ &= \big(\big(\mathit{Reach}_{k+1}^{\mathrm{nl},+}(\mathcal{S}, N)\} \oplus (-E_k)\big) \ominus \mathcal{U}\big) A_k \end{aligned} \tag{4.38a}$$

where again $\mathit{Reach}_N^{\mathrm{nl},+}(\mathcal{S}, N) = \mathcal{S}$ and $k = \{N-1, \ldots, 0\}$.

Figure 4.1 shows how the PBRS from a set $\mathcal{S}$ that include the linearization errors are larger than the ones obtained through the nominal linear analysis. Here, the sets are projected to the along-track and radial plane of the target's Hill frame. The set $\mathcal{S}$ is shown in red, in the center.

Figure 4.1: Projection of the inflated PBRS compensating for linearization errors and the nominal linear PBRS in the $x - y$ plane. The nonlinear sets over-approximate and envelop the linear ones.



4.4.2 Combined Linearization Error and Process Noise

Generally, because the true dynamics of the system are nonlinear, it is difficult to assert probabilistic statements about the safety of the stochastic nonlinear system. A nonlinear transformation of a random vector is required when propagating the current PDF of the chaser's state forward or backward in time, thus a PDF that is initially Gaussian will no longer remain so. However, because the linearization errors are small, the chaser's estimated PDF in $\mathcal{X}$ is well-approximated by a Gaussian distribution, despite the linearization errors.

We briefly discuss a couple of methods that satisfy the probabilistic safety constraints we desire for the original nonlinear system. First, we naively assume the linearization errors have negligible impact on the chaser's PDF, that is, the nonlinearities do not affect the PDF propagation. The second method incorporates the linearization errors as additional process noise to the stochastic linear model. These methods provide good approximations for the nonlinear system but have no guarantees due to the issue raised above.

Due to linearity, the linearization errors can be incorporated by modifying the disturbance set $\mathcal{W}_k$. We define a set $\widetilde{\mathcal{W}}_k \triangleq \mathcal{W}_k \oplus E_k$ that accounts for both stochastic disturbances and linearization disturbances in the original reachability analysis. Let $\tilde{\boldsymbol{w}}_k = \boldsymbol{w}_k + \boldsymbol{e}_k,\ \boldsymbol{w}_k \in \mathcal{W}_k, \boldsymbol{e}_k \in E_k \implies \tilde{\boldsymbol{w}} \in \widetilde{\mathcal{W}}_k = \mathcal{W}_k \oplus E_k$, where

$$\mathbb{P}\{\tilde{\boldsymbol{w}}_k \in \widetilde{\mathcal{W}}_k\} = \mathbb{P}\{\boldsymbol{w}_k + \boldsymbol{e}_k \in \widetilde{\mathcal{W}}_k\}, \tag{4.39}$$

$$= \mathbb{P}\{\boldsymbol{w}_k \in \mathcal{W}_k\}, \tag{4.40}$$

because the linearization error is treated as a deterministic disturbance and **stochasticity** enters through $\mathcal{W}_k$. Then, to be safe with respect to both random noise and linearization errors, we avoid the sets $\text{Reach}_k^{\text{nl},+}(\mathcal{S}, N)$ computed with the new disturbance sets such that $\mathbb{P}_{\boldsymbol{x}}^{\boldsymbol{x}_k,\pi}\{\boldsymbol{x}_N \notin \mathcal{S} | \boldsymbol{x}_0 \in \mathcal{X} \setminus \text{Reach}_k^{\text{nl},+}(\mathcal{S}, N)\} \geq 1 - \beta$. Similarly, we can under-approximate the passive backwards reachable set by replacing $\mathcal{W}_j$ in (4.23b) with $\widetilde{W}_j$. The tightening effect of the linearization error compensation compared to the nominal deterministic coasting sets is clear in Figure 4.2, where in the nominal case some trajectories miss the goal set $\mathcal{G}$

altogether.

An alternative method for compensation of the linearization errors is to model the linear process noise based on the linearization errors. Specifically, the linearization error can be modeled as a random vector with an assumed distribution, e.g., $\boldsymbol{e}_k \sim \mathcal{N}(\mathbf{0}, \Sigma_k^e)$ with covariance

$$\Sigma_k^e = \gamma \text{diag}([\tilde{L}_4^2, \tilde{L}_5^2, \tilde{L}_6^2]), \tag{4.41}$$

such that the support of the corresponding probability ellipsoid sufficiently captures the linearization error. Then, the expected value of the state is

$$\mathbb{E}[\boldsymbol{x}_{j+1|k}] = \mathbb{E}[A_{j|k}\boldsymbol{x}_{j|k} + B_{j|k}\boldsymbol{u}_{j|k} + \boldsymbol{w}_{j|k} + B_{j|k}\boldsymbol{e}_{j|k}], \tag{4.42a}$$

$$\mathbb{E}[\boldsymbol{x}_{j+1|k}] = A_{j|k}\mathbb{E}[\boldsymbol{x}_{j|k}] + B_{j|k}\mathbb{E}[\boldsymbol{u}_{j|k}], \tag{4.42b}$$

and the state uncertainty is

$$\tilde{\Sigma}_{j+1|k}^{\boldsymbol{x}} = A_{j|k}\Sigma_{j|k}^{\boldsymbol{x}}A_{j|k}^{\mathsf{T}} + B_{j|k}(\Sigma_{j|k}^{\boldsymbol{u}} + \Sigma_{j|k}^{\boldsymbol{e}})B_{j|k}^{\mathsf{T}} + \Sigma_{j|k}^{\boldsymbol{q}}, \tag{4.43}$$

which accounts for control uncertainty, process noise, and linearization errors in the system. By modeling the process noise in this way, we lose theoretical guarantees about the nonlinear reachability of the system. However, in practice, the process noise can be appropriately tuned such that the support of the noise sufficiently captures the linearization errors as well as alternative sources of process noise. Another benefit of this approach, is that we do not have to compute the SBRS as if an input was acting on the system. Doing so results in less conservatism compared to modelling it as an explicit input, as shown in Figures 4.3-4.4. In these figures, the stochastic forward reachable sets from an initial condition in the positive along-track direction are computed using the two linearization error compensation methods. It is clear that adding the linearization error into the process noise results in much less conservatism, the validity of which is confirmed in Figure 4.5. Figure 4.5 shows, in black, states that are propagated using the nonlinear dynamics with AWGN, which remain inside the projected confidence ellipsoids calculated using (4.43).

Figure 4.2: Initial states, shown by the green and blue squares, that enter and miss the desired goal set with stochastic coasting arcs relative to a target in LEO. In blue: trajectories that do not compensate for linearization error and process noise and miss the goal set $\mathcal{G}_{\mathrm{f}}$. In green, trajectories that are robust to noise and linearization error and enter $\mathcal{G}_f$. The trajectories are for a time-horizon of $t_f - t_0 = 50$ min., roughly half an orbital period of a target in LEO. Safe initial states not considered here.

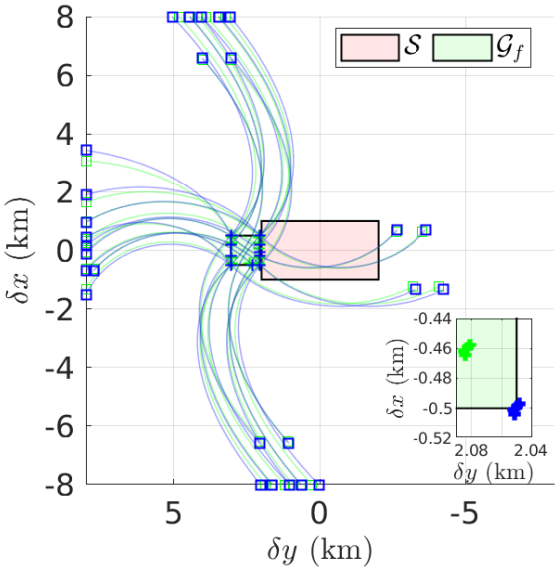
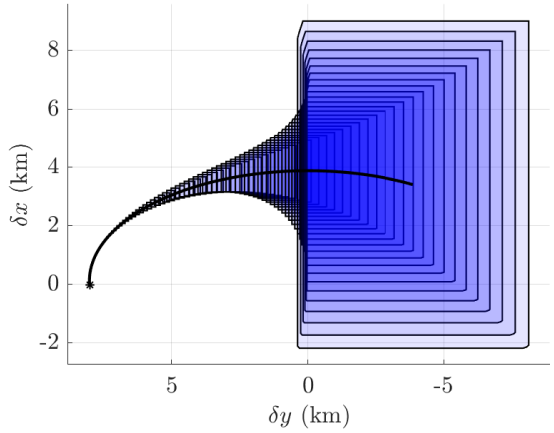


Figure 4.3: Comparison of the stochastic forward reachable sets when the linearization error is incorporated as an additive disturbance vs. as process noise to the nominal model. Propagation time is 40 min, about a third of the target's orbital period.

(a) In blue, the stochastic passive forward reach sets from an initial condition using the additive disturbance method. In black, the expected trajectory is shown.



(b) In blue, the stochastic passive forward reach sets assuming the linearization error is incorporated into the process noise. In black, the expected trajectory is shown.

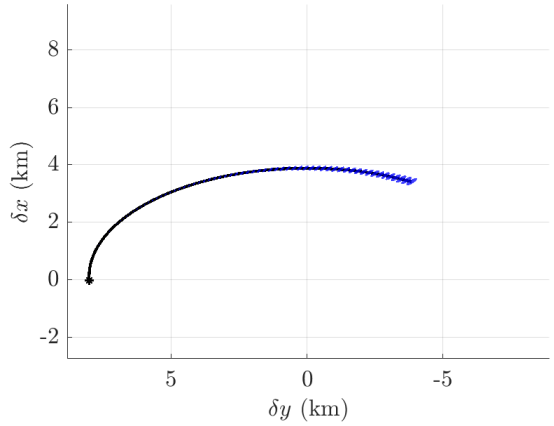
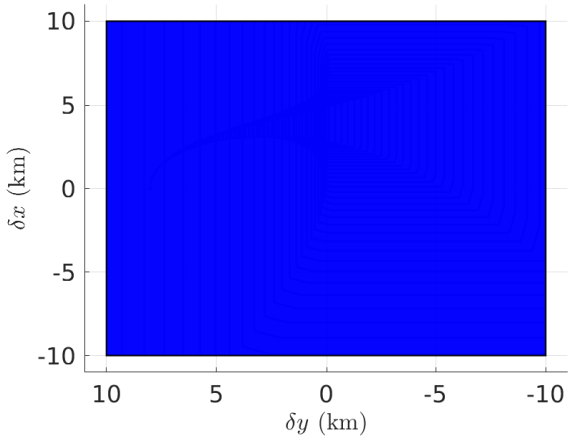


Figure 4.4: Comparison of the nonlinear stochastic forward reachable set: additive disturbance or process noise over longer horizon. Propagation time is 80 minutes, about a third of the target's orbital period. After 80 minutes, the additive disturbance method shows that the entire position subspace $\mathcal{X}$ is reachable.

(a) In blue, the stochastic passive forward reach sets from an initial condition using the additive disturbance method, which occupies the entire position subspace of $\mathcal{X}$.



(b) In blue, the stochastic passive forward reach sets assuming the linearization error is incorporated into the process noise. In black, the expected trajectory is shown.

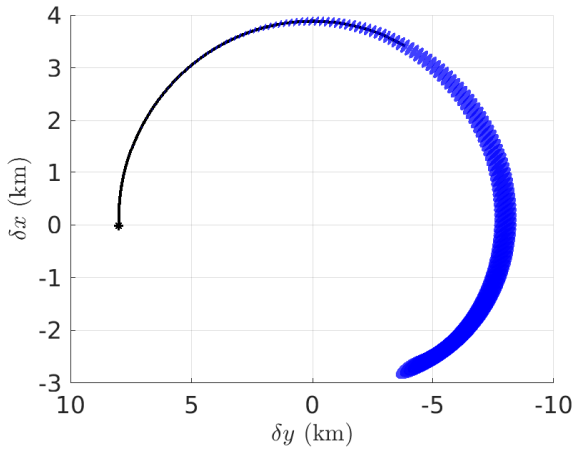
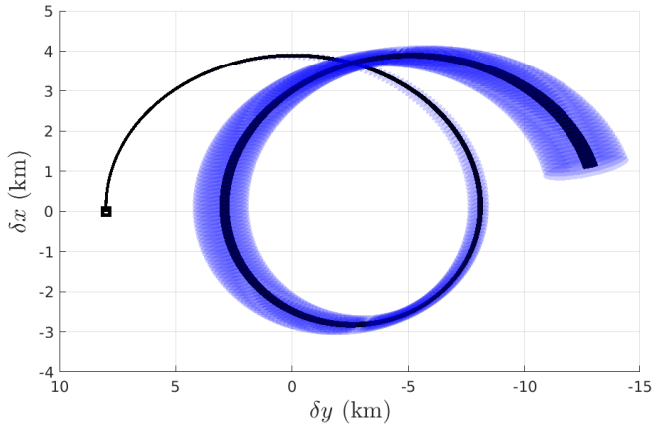


Figure 4.5: Sample trajectories propagated forward in time using the nonlinear stochastic model based on $\Sigma_k^{\boldsymbol{q}} + \Sigma_k^{\boldsymbol{e}}$. All trajectories lie well within the 0.95 confidence ellipsoids, thus, linearization erros can be incorporated as process noise.



4.5 Safe Coasting Arcs

Section 4.3.3 introduced how under-approximations of the stochastic passive backwards reachable sets are obtained. We call such sets **coasting sets** for obvious reasons, we desire to enter such a set to exploit the natural dynamics, leading to possible reductions in maneuver ΔV and thruster on-time. In summary, we define the goal set as $\mathcal{G}$, and we desire that the chaser arrives at $\mathcal{G}$ in at most N_c coasting steps, i.e., $\boldsymbol{x}_{N_\mathrm{c}} \in \mathcal{G}$. For the deterministic nonlinear case, it is sufficient to compute $\cup_{k=0}^{N_\mathrm{c}} \mathcal{R}_{1,k}(\mathcal{G}, E_k)$ to obtain the sets of states that enter in N_c steps or at a specific final time step k_c, no matter the linearization errors present. The stochastic version is highlighted in (4.23b) and for simultaneous compensation of the linearization errors and the process noise effects, we can again use sets such as $\widetilde{\mathcal{W}}_k = \mathcal{W}_k \oplus E_k$ in the backwards recursion. In summary,

$$\mathrm{CoastingSets} = \cup_{j=0}^{N_\mathrm{c}} \mathrm{Reach}_j^-(\mathcal{G}, N_\mathrm{c}). \tag{4.44}$$

The goal set is defined such that its intersection with $\mathcal{S}$ is empty, i.e., $\mathcal{G} \cap \mathcal{S} = \emptyset$. Naturally, the states in $\mathrm{Reach}_k^-(\mathcal{G}, N_\mathrm{c})$ need not be passively safe. That is, for some $\delta t > 0$, there may exist a state $\boldsymbol{x}(t) \in \mathcal{G}$ such that $\boldsymbol{x}(t + \delta t) \in \mathcal{S}$ or vice-versa, there may exist a state $\boldsymbol{x}(t) \in \mathcal{S}$ such that $\boldsymbol{x}(t + \delta t) \in \mathcal{G}$. In general then,

$$\mathcal{G} \cap \mathrm{Reach}_k^+(\mathcal{S}, N_\mathrm{c}) \neq \emptyset \tag{4.45}$$

$$\implies \mathrm{Reach}_k^-(\mathcal{G}, N_\mathrm{c}) \cap \mathrm{Reach}_k^+(\mathcal{S}, N_\mathrm{c}) \neq \emptyset. \tag{4.46}$$

Note that if $\mathrm{Reach}_k^-(\mathcal{G}, N_\mathrm{c}) \cap \mathrm{Reach}_k^+(\mathcal{S}, N_\mathrm{c}) = \emptyset$, then one can drive the chaser into $\mathrm{Reach}_k^-(\mathcal{G}, N_\mathrm{c})$ without passive safety constraints. Because this is not the case for spacecraft dynamical problems, as (4.46) is in general non-empty, we formulate a method for the chaser spacecraft to enter the passively safe portion of CoastingSets, denoted as SafeCoastingSets, where

$$\mathrm{SafeCoastingSets} = \mathrm{CoastingSets} \setminus \mathrm{UnSafeSet}. \tag{4.47}$$

However, for computational reasons, we wish to not compute this set difference explicitly. SafeCoastingSets is made up of a union of passively safe coasting sets that arrive at $\mathcal{G}$ in N_c steps or less. If the rendezvous approach is constrained to be passively safe for N steps, we require $N_\mathrm{c} \leq N$ for the resulting coasting-arc to have a safety-horizon $N\Delta t$.

Remark 8. *Provided the Pontryagin difference* $\left(Reach^{-}_{j+1}(\mathcal{G}, N_\mathrm{c}) \ominus \mathcal{W}_j\right) \neq \emptyset$*, which appears in* (4.23b)*, then there exists a coasting arc of at least* $j\Delta t$ *seconds.*

4.5.1 Linear Time-Varying Case

To obtain a successful coasting arc, we specify a fixed final coasting time k_c at which we seek to enter the goal set $\mathcal{G}$. The coasting maneuver is planned such that the maximum duration it can be is $t_m = t_\mathrm{c} - t_0$, where t_0 is the initial time. We generally pick $t_c < t_f$ such that there is an additional amount of time after the coasting is complete in which the safety of the vehicle can be guaranteed. Then, the resulting maximum number of coasting steps is $N_\mathrm{c} = \frac{t_m}{\Delta T}$. This is a time-dependent problem where the relative state of the chaser $\boldsymbol{x}_{N_\mathrm{c}-j}$ has to enter $\mathrm{Reach}^{-}_{N_\mathrm{c}-j}(\mathcal{G}, N_\mathrm{c})$ to ensure a successful coasting arc from an initial time step $N_\mathrm{c}-j$ to a final time step of interest N_c. That is, if $\boldsymbol{x}_{N_\mathrm{c}-j} \notin \mathrm{Reach}^{-}_{N_\mathrm{c}-j}(\mathcal{G}, N_\mathrm{c})$ there are no guarantees that $\boldsymbol{x}_{N_\mathrm{c}} \in \mathcal{G}$ due to the LTV nature of the system because the coasting sets from two different final times k_i and k_j, are not the same, i.e., $\mathrm{Reach}^{-}_{j}(\mathcal{G}, k_i) \neq \mathrm{Reach}^{-}_{j}(\mathcal{G}, k_j),\ \forall k_i, k_j$. Thus, to enforce a coasting arc, we require

$$\boldsymbol{x}_j \in \mathrm{Reach}^{-}_{j}(\mathcal{G}, N_\mathrm{c}),\ j \in \{0, \ldots, N_\mathrm{c} - 1\}. \tag{4.48}$$

Because initially $\boldsymbol{x}_0 \notin \mathrm{Reach}^{-}_{0}(\mathcal{G}, N_\mathrm{c})$, the constraints (4.48) are softened to avoid infeasibility. Once (4.48) is satisfied, the chaser has entered a coasting set for step j and then it will passively coast to $\mathcal{G}$ in $N_\mathrm{c} - j$ steps with a probability associated with the construction of the sets $\widetilde{\mathcal{W}}$.

4.5.2 Linear Time-Invariant Case

For a linear time-invariant (LTI) system, there is additional flexibility in designing a coasting arc from an initial time to a specified final time. Though the same method as in section 4.5.1 is applicable, where a fixed final time is chosen, the LTI dynamics allow us to relax the timing problem above, yielding a free final time method. That is, because $A_k = A$, $\forall k$, given any two final times k_i and k_j, the coasting sets are identical, i.e., $\text{Reach}_0^-(\mathcal{G}, k_i) = \text{Reach}_0^-(\mathcal{G}, k_j), \forall k_i, k_j$. Thus, if $\boldsymbol{x}_j \in \text{Reach}_0^-(\mathcal{G}, N_\text{c})$, the chaser is guaranteed to enter the $\mathcal{G}$ in N_c steps even though $j \neq k_\text{c} - N_\text{c}$, which is not the case for an LTV system. Though this does not apply for eccentric orbits or general perturbed trajectories, it does apply to targets in unperturbed circular orbits and may yield a good approximation for near circular target orbits over short horizons.

4.6 Rendezvous Control

Next, we develop an abort-safe control policy that enforces the state to remain in **SafeSet**. Specifically, we develop a SMPC policy that minimizes a cost function designed based on performance metrics, while constraining the trajectory to remain within **SafeSet**, and hence outside its complement (4.21). For the entire rendezvous mission, we consider two controllers: the first one steers the spacecraft from the initial position towards the target while enforcing passive safety and exploiting coasting arcs. The second controller is engaged when the spacecraft enters the final approach corridor while enforcing active abort-safety. Both controllers are implemented using SMPC, where the only the imposed constraints are changed.

Because the SMPC prediction model used is LTV, it does not capture the effects of any linearization errors. As such, additional process noise is given to the SMPC policy based on (4.43) to further tighten any constraints of interest, e.g. safety and coasting constraints. Alternatively, we could use nonlinear SMPC to obtain nonlinear state updates, but in doing

so we may lose convergence guarantees.

4.6.1 Stochastic Optimal Control Problem

The **non-coasting** SMPC policy yields a constrained trajectory that is safe while driving the chaser to approach the target. Conversely, the **coasting** SMPC, appends the coasting set constraints in the initial rendezvous phase to the **non-coasting** SMPC formulation. At every time step k, the SMPC policy solves the finite horizon optimal control problem

$$\min_{\boldsymbol{U}_k} \quad \mathbb{E}\big[F(\boldsymbol{x}_{N_\mathrm{p}|k}) + \sum_{j=0}^{N_\mathrm{p}-1} S(\boldsymbol{x}_{j|k}, \boldsymbol{u}_{j|k})\big] \tag{4.49a}$$

$$\text{s.t.} \quad \boldsymbol{x}_{j+1|k} = \mathbb{E}[A_{j|k}\boldsymbol{x}_{j|k} + B_{j|k}\boldsymbol{u}_{j|k}] \tag{4.49b}$$

$$\mathbb{P}\{\boldsymbol{g}_k(\boldsymbol{x}_{j|k}, \boldsymbol{u}_{j|k}) \leq 0\} \geq \alpha \tag{4.49c}$$

$$u_{j|k} \in \mathcal{U}(k) \tag{4.49d}$$

$$\boldsymbol{x}_{0|k} = \mathbb{E}[\boldsymbol{x}_k] \tag{4.49e}$$

where $N_\mathrm{p} \ll N$ is the prediction horizon length, the prediction model (4.49b) is (4.3), (4.49c) is the chance constraint ensuring that collision can be averted in the presence of propulsion system failures as well as the coasting constraint, if desired. $\mathcal{U}(k)$ is the input set at time step k, which depends on the propulsion system condition, i.e., before or after a failure. The MPC control law is given by

$$\boldsymbol{u}_k = \kappa_\mathrm{mpc}(\mathbb{E}[\boldsymbol{x}_k]) = \boldsymbol{u}^*_{0|k}, \tag{4.50}$$

where $\boldsymbol{U}^*_k = (\boldsymbol{u}^*_{0|k} \dots \boldsymbol{u}^*_{N_\mathrm{p}-1|k})$ is the optimizer of (4.49).

4.6.2 Cost Function

We design the stage and terminal cost in (4.49a) as

$$S(\boldsymbol{x}, \boldsymbol{u}) = \boldsymbol{x}^\top Q \boldsymbol{x} + \boldsymbol{u}^\top R \boldsymbol{u}, \tag{4.51a}$$

$$F(\boldsymbol{x}) = \boldsymbol{x}^\top M \boldsymbol{x}, \tag{4.51b}$$

where the weight matrices $Q = Q^\top \geq 0$, $R = R^\top > 0$, $M = M^\top > 0$ are selected to achieve the desired performance, resulting in a linear quadratic MPC for which (4.49) is a quadratic program (QP). The weight Q affects the primary objective, which is to approach the target, i.e., reaching zero position and velocity. The weight R affects the secondary objective, which is to minimize the total required propellant by minimizing the thrust. M is usually chosen to obtain stability properties, although here the main focus is on ensuring safety in case of a thruster failure. Non-quadratic cost functions can also be used as in [55], while still achieving active safety due to the constraint (4.49c).

4.6.3 Constraints

Here, we briefly discuss the relevant constraints of the SMPC problem.

4.6.3.1 Safety

For both passive and active abort-safety, we impose these constraints on the state to remain outside of the abort-unsafe sets UnionReachLTV($\mathcal{S}, k_\mathrm{f}$) (4.19) by computing a half-space that excludes UnionReachLTV($\mathcal{S}, k_\mathrm{f}$) based on Result 1 in Chapter 3. Specifically, a set of nearby polyhedra $\{\mathcal{P}(H_i, k_i)\}_{i=1}^{\ell} \subset$ UnionReachLTV($\mathcal{S}, k_\mathrm{f}$) are used to construct a halfspace $\mathcal{P}_h(\boldsymbol{h}, 1) = \{\boldsymbol{x} \in \mathbb{R}^n : \ \boldsymbol{h}^\mathsf{T}\boldsymbol{x} \leq 1\}$ such that $\mathcal{P}_h(\boldsymbol{h}, 1) \supset \{\mathcal{P}(H_i^{\bar{\mathcal{R}}}, \boldsymbol{k}_i^{\bar{\mathcal{R}}})\}_{i=1}^{\ell}$. That is, a half-space that contains a subset of UnionReachLTV($\mathcal{S}, k_\mathrm{f}$) is constructed and its complement is used to maintain abort-safety. Given $\bar{\boldsymbol{x}} \in \mathbb{R}^n$, the required half-space normal $\boldsymbol{h}^*(\bar{\boldsymbol{x}})$ is obtained by solving a linear program [84, 86]. These half-space constraints are computed based on the previously predicted state trajectory, given by the MPC policy. Let $(\boldsymbol{x}_{0|k-1} \dots \boldsymbol{x}_{N_p|k-1})$ be the trajectory computed at time $k-1$, we compute half-space normal vectors $\boldsymbol{h}_{j|k-1}$, and use this at the next MPC iteration such that $\boldsymbol{h}_{j|k-1}^\mathsf{T}\boldsymbol{x}_{j|k} \leq 1, \ \forall j = 0, \dots, N_p$. For **passive abort-safety**, we use passive system to compute UnionReachLTV($\mathcal{S}, k_\mathrm{f}$) while we use the active ones for **active abort-safety**.

4.6.3.2 Navigation Uncertainty

When constructing the UnionReachLTV($\cdot$), initial state uncertainty is neglected, because only the effects of process noise are considered to compute the unsafe sets. In reality, the chaser will have initial state uncertainty as a result of uncertain measurements and dynamics, i.e., $\boldsymbol{x}_0 \sim \psi_{\boldsymbol{x}}(\boldsymbol{x})$ is a random vector. Incorporating state uncertainty for the general controlled or linearization error compensated backwards reachable sets is difficult, but is more easily done in the purely passive case. Incorporating initial state uncertainty results in a predicted covariance of

$$\tilde{\Sigma}^{\boldsymbol{x}}_{j|k} = \Phi(j,k)\ \Sigma^{\boldsymbol{x}}_{k}\ \Phi(j,k)^{\mathsf{T}} + \Sigma^{\boldsymbol{x}}_{j|k}, \tag{4.52}$$

where $\Sigma^{\boldsymbol{x}}_{j|k}$ is the component purely due to process noise. Moreover, because the state uncertainty changes throughout the course of a maneuver, it is preferable to compensate for any state uncertainty in a way that does not require a full re-computation of the unsafe or coasting sets. This motivates the use of chance-constraints, which provides a measure of confidence for the satisfaction of a constraint under state uncertainty. Thus, we arrive at the following condition for safety

$$\mathbb{P}\{\boldsymbol{x}_{j|k} \notin \text{UnionReachLTV}(\mathcal{S}, k_{\text{f}})\} \geq \alpha \tag{4.53a}$$

$$\impliedby \mathbb{P}\{\boldsymbol{x}_{j|k} \in \cup_i \{p_i^{\mathsf{T}} \boldsymbol{x}_{j|k} \leq q_i\}\} \geq \alpha \tag{4.53b}$$

$$\impliedby \max_i \mathbb{P}\{\boldsymbol{x}_{j|k} \in \{p_i^{\mathsf{T}} \boldsymbol{x}_{j|k} \leq q_i\}\} \geq \alpha \tag{4.53c}$$

$$\iff \mathbb{P}\{\boldsymbol{x}_{j|k} \in \{p_i^{\mathsf{T}} \boldsymbol{x}_{j|k} \leq q_i\}\} \geq \alpha, \quad \exists i \tag{4.53d}$$

$$\iff \Phi\left(\frac{q_i - p_i^{\mathsf{T}} \mathbb{E}[\boldsymbol{x}_{j|k}]}{(p_i^{\mathsf{T}} \Sigma^{\boldsymbol{x}}_{j|k} p_i)^{\frac{1}{2}}}\right) \geq \alpha, \quad \exists i \tag{4.53e}$$

$$\iff p_i^{\mathsf{T}} \mathbb{E}[\boldsymbol{x}_{j|k}] \leq q_i - \Phi^{-1}_{\text{cdf}}(\alpha)\,(p_i^{\mathsf{T}} \Sigma^{\boldsymbol{x}}_{j|k} p_i)^{\frac{1}{2}}, \quad \exists i \tag{4.53f}$$

which suggests that we have a confidence α that the true chaser state satisfies the locally convex safety constraints. Recall that when outside of the unsafe region of state space, a safe abort will exist with a minimum probability of $1-\beta$. Thus, we can claim to have α confidence

that we are safe with probability $1-\beta$. Additionally, if $\Sigma^{\boldsymbol{x}}_{j|k} = 0_{n\times n}$, i.e., we have no state uncertainty, we recover the original safety constraints $p_i^\mathsf{T}\mathbb{E}[\boldsymbol{x}_{j|k}] \leq q_i \implies p_i^\mathsf{T}\boldsymbol{x}_{j|k} \leq q_i$. Generally, the chance-constraint pushes the chaser away from the unsafe region of state space, reducing the effective probability of collision.

Remark 9. *Computing the effective probability of collision from a given state using α and $1-\beta$ is not readily possible; the set UnionReachLTV itself contains states with varying degrees of safety and without further analysis, the actual measure of safety is unclear.*

4.6.3.3 Coasting Arcs

The coasting constraints throughout the horizon are given by (4.48). We let $\mathcal{G} = \mathcal{P}(H_\mathrm{g}, \boldsymbol{k}_\mathrm{g})$ be a polytope such that the passive SBRS are given by polytopes. Given the current time step k, the appropriate coasting set is targeted by enforcing

$$\boldsymbol{x}_{j|k} \in \mathrm{Reach}^-_{k+j}(\mathcal{G}, N_\mathrm{c}), \tag{4.54}$$

for $j = 0, \ldots, N_p$, which is a linear constraint of the form

$$H_\mathrm{c}\boldsymbol{x}_{j|k} \leq \boldsymbol{k}_\mathrm{c} + \mathbb{1}s_{j|k} \tag{4.55}$$

where the slack variable $s_{j|k}$ is used to avoid infeasibility because $\boldsymbol{x}_0 \notin \mathrm{Reach}^-_0(\mathcal{G}, N_\mathrm{c})$. The cost function penalty on the slack variables $s_{j|k}$ minimizes the infeasibility, which results in driving the chaser into the coasting set. If navigation or state uncertainty is included, then as before, a chance-constraint is utilized such that

$$\mathbb{P}\{\boldsymbol{x}_{j|k} \in \mathrm{Reach}^-_{k+j}(\mathcal{G}, N_\mathrm{c})\} \geq \alpha \tag{4.56a}$$

$$\impliedby \mathbb{P}\{\boldsymbol{x}_{j|k} \in \cap_i\{[H_\mathrm{c}]_i^\mathsf{T}\boldsymbol{x}_{j|k} \leq [\boldsymbol{k}_\mathrm{c}]_i\}\} \geq \alpha \tag{4.56b}$$

$$\iff \Phi\left(\frac{[\boldsymbol{k}_\mathrm{c}]_i - [H_\mathrm{c}]_i^\mathsf{T}\mathbb{E}[\boldsymbol{x}_{j|k}]}{([H_\mathrm{c}]_i^\mathsf{T}\Sigma^{\boldsymbol{x}}_{j|k}[H_\mathrm{c}]_i)^{\frac{1}{2}}}\right) \geq \alpha, \quad i = 0, \ldots, n_r \tag{4.56c}$$

$$\iff [H_\mathrm{c}]_i^\mathsf{T}\mathbb{E}[\boldsymbol{x}_{j|k}] \leq [\boldsymbol{k}_\mathrm{c}]_i - \Phi^{-1}_\mathrm{cdf}(\alpha)([H_\mathrm{c}]_i^\mathsf{T}\Sigma^{\boldsymbol{x}}_{j|k}[H_\mathrm{c}]_i)^{\frac{1}{2}}, \quad i = 0, \ldots, n_r, \tag{4.56d}$$

which suggests that we have α-confidence that the state $\boldsymbol{x}_{j|k} \in$ the coasting set $\text{Reach}^{-}_{k+j}(\mathcal{G}, N_\text{c})$.

4.6.3.4 Line-of-sight

A LOS constraint is added for the final active abort-safety phase which maintains the chaser spacecraft within a corridor that leads to an assumed docking port on the target. This constraint requires the state of the chaser to remain within a cone $A_\text{los}\boldsymbol{x}_{j|k} \leq \boldsymbol{b}_\text{los}$. Additionally, the goal set is constructed to be contained within the LOS cone, i.e., $\mathcal{G} \subset \mathcal{P}(A_\text{los}, \boldsymbol{b}_\text{los})$. Again, when incorporating state uncertainty, we utilize a chance-constraint.

4.6.3.5 Control

As shown in [84], for given a thruster configuration, we can construct a general polytopic admissible control set at step k

$$\mathcal{U}(k) = \{\boldsymbol{u} \in \mathbb{R}^3 : H_u\boldsymbol{u} \leq \boldsymbol{k}_u\}. \tag{4.57}$$

The set $\mathcal{U}(k)$ can present nominal control or for example a back-up set of thrusters, which will be assumed in the active safety phase of the approach.

4.6.3.6 Summary

Because the coasting-arc is useful when the chaser is far relative to the target, these coasting constraints are only used in the initial rendezvous phase where passive safety is required. Conversely, the LOS constraints are only necessary when the chaser is heading towards a docking port. Thus, for the initial approach, we can write the passively safe path constraints, $\boldsymbol{g}_p$ as

$$\boldsymbol{g}_p(\boldsymbol{x}_{j|k}, s_{j|k}) = \begin{bmatrix} -\boldsymbol{h}_{j|k}^\intercal \boldsymbol{x}_{j|k} + 1 + \Phi_\text{cdf}^{-1}(\alpha)\left(p_i^\intercal \Sigma_{j|k}^{\boldsymbol{x}} p_i\right)^{\frac{1}{2}} \\ H_c\boldsymbol{x}_{j|k} - \mathbb{1}s_{j|k} - \boldsymbol{k}_c - \bar{\boldsymbol{c}} \end{bmatrix} \leq \boldsymbol{0}.$$

where, $[\bar{\boldsymbol{c}}]_i = \Phi_{\text{cdf}}^{-1}(\alpha)([H_{\text{c}}]_i^{\mathsf{T}}\Sigma_{j|k}^{\boldsymbol{x}}[H_{\text{c}}]_i)^{\frac{1}{2}}$. When a coasting set is entered, control is switched off, so the passively safe control policy is summarized by

$$\boldsymbol{u}_k = \begin{cases} \kappa_{mpc}(\mathbb{E}[\boldsymbol{x}_k]) \in \mathcal{U}, & \mathbb{E}[\boldsymbol{x}_k] \notin \text{Reach}_k^-(\mathcal{G}, N_{\text{c}}) \\ \mathbf{0} \in \mathbb{R}^3, & \mathbb{E}[\boldsymbol{x}_k] \in \text{Reach}_k^-(\mathcal{G}, N_{\text{c}}) \end{cases} \tag{4.58}$$

For active safety, we replace the passive safety constraints with the abort-safety constraints. Additionally, the coasting constraints are exchanged for the LOS cone, yielding

$$\boldsymbol{g}_a(\boldsymbol{x}_{j|k}) = \begin{bmatrix} -\boldsymbol{h}_{j|k}^{\mathsf{T}}\boldsymbol{x}_{j|k} + 1 + \Phi_{\text{cdf}}^{-1}(\alpha)\,(p_i^{\mathsf{T}}\Sigma_{j|k}^{\boldsymbol{x}}p_i)^{\frac{1}{2}} \\ A_{\text{los}}\boldsymbol{x}_{j|k} - \boldsymbol{b}_{\text{los}} - \bar{\boldsymbol{l}} \end{bmatrix} \leq \mathbf{0}. \tag{4.59}$$

where $[\bar{\boldsymbol{l}}]_i = \Phi_{\text{cdf}}^{-1}(\alpha)([A_{\text{los}}]_i^{\mathsf{T}}\Sigma_{j|k}^{\boldsymbol{x}}[A_{\text{los}}]_i)^{\frac{1}{2}}$.

4.7 Results

Now, results pertaining to the safe SMPC, with and without coasting, are presented.

4.7.1 Stochastic Rendezvous with Near-Earth Targets

We consider a target in a near circular target orbit with $e_{\text{t}} = 0.0001$ and a semi-major axis of 7578km. In this simulation, we include J_2, lunar, and solar third body effects on both the chaser and the target. We compute the passively unsafe regions of state space with a safety horizon of 3 orbital periods. The deputy is initially in the negative along-track direction from the target. In the loop, we update the relative states and PDF of the chaser with respect to the target using a simple linear Kalman filter with noisy relative position measurements.

Initially, passive safety is maintained with respect to a polytopic set $\mathcal{S}$ while a coasting set is targeted. The developed method is compared to a non-coasting MPC policy in terms of maneuver ΔV and input signal sparsity. The total ΔV of a maneuver is given by $\Delta V = \sum_{i=0}^{N-1} ||B(\cdot)\boldsymbol{u}_i|| \cdot \Delta T$. In the simulations, a sampling time of $\Delta T = 30$s is used, and the

nominal admissible control set $\mathcal{U}_n$, i.e., without any loss of thrust, is such that $\boldsymbol{u}_u = -\boldsymbol{u}_l = \mathbb{1}_{3\times 1} \cdot 50\text{N}$. Passive safety is maintained with respect to a polytopic set of size where $1.5 \times 3.5 \times 1.5$ km^3 in the position subspace and we consider impact velocities of up to 100m/s.

4.7.1.1 No Coasting

First, we consider the case where the safe SMPC method is used. Here, the chance-constraints are used to ensure the chaser does not enter the passively unsafe regions of state space. The resulting approach is visible in Figure 4.6. The expected states along the approach trajectory are sampled and propagated forward passively to confirm passive safety, which is clear because none of the trajectories enter $\mathcal{S}$, shown in red. In Figure 4.7, samples are taken from the relative state's distribution at a particular time index and propagated forward in time, yielding a "tube" shown in black. None of these samples enter $\mathcal{S}$, which indicates the chance-constraint is working as designed and expected. For the chosen parameters, this SMPC uses a total maneuver $\Delta V = 27.7463$ m/s. The expected relative position, velocities, and corresponding control signals are given in Figure 4.8.

Figure 4.6: Passively safe rendezvous without a coasting arc. The expected SMPC trajectory is shown in blue while the expected passive failure trajectories are shown in black.

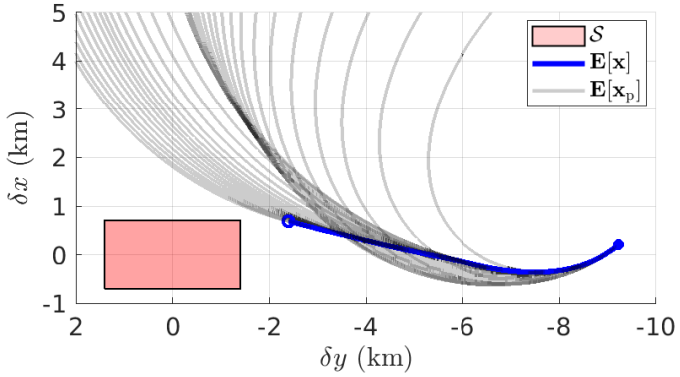


Figure 4.7: Passively safe rendezvous without a coasting arc. The expected MPC trajectory is shown in blue. In black, random samples at t_i from $\mathcal{N}(\mathbb{E}[\boldsymbol{x}_i], \Sigma_i^{\boldsymbol{x}})$. The samples are from a 0.99 confidence ellipsoid around the mean.

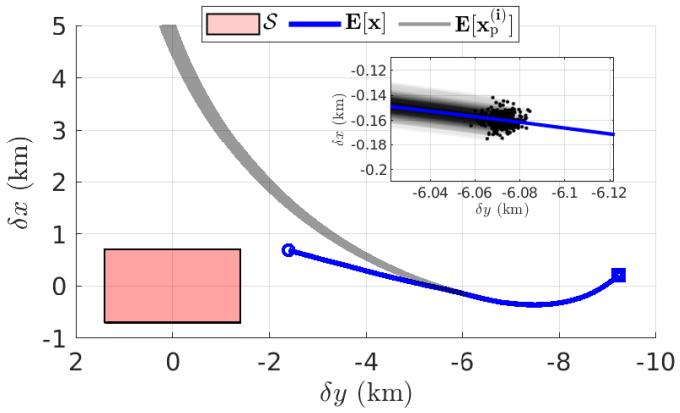
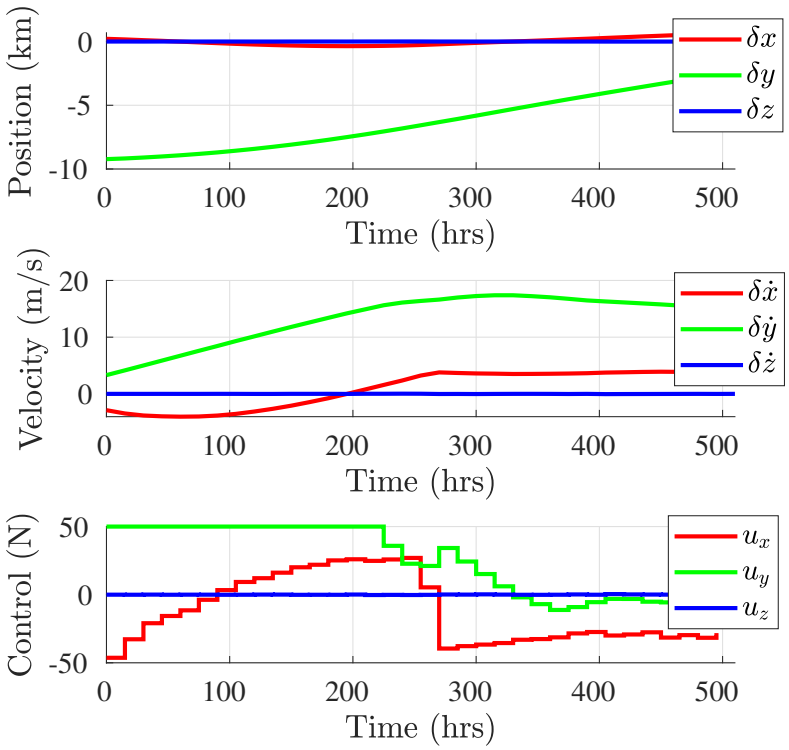


Figure 4.8: Relative position, velocity, and control trajectories for a passively safe non-coasting rendezvous maneuver.



4.7.2 Passively safe coasting

Next, we consider the case where the coasting safe SMPC method is used to obtain coasting arc of a quarter period in duration. Here, the chance-constraints are used to ensure the chaser does not enter the passively unsafe regions while simultaneously targeting the interior regions of the coasting sets of interest. Once inside the coasting set, the chaser turns off it's thrusters and coasts into $\mathcal{G}$. The geometry of interest is shown in Figure 4.9. The goal set $\mathcal{G}$ is an enlarged version of the approach polytope $\mathcal{S}$. This allows for the SMPC to consider multiple approach locations around the target. The resulting approach is visible in Figure 4.9, where the expected states along the approach are sampled and propagated forward passively to confirm passive safety, which is clear because none of the trajectories enter $\mathcal{S}$. After only three steps, the chaser enters a coasting set and arrives at $\mathcal{G}$ approximately a quarter period later, as designed. In Figure 4.10, samples are taken from the relative state's distribution at the third index, after shutting off the thursters, and propagated forward in time. None of these samples enter $\mathcal{S}$, which indicates the chance-constraint is working as designed and expected, i.e., passive safety is maintained while the goal set is reached even when subjected to unmodeled accelerations (process noise). Figure 4.11 shows the expected relative position, velocity, and control of the chaser for the rendezvous approach, where the initial short burn required at the beginning is visible. This maneuver saturates the controller at $50N$. Then, after entering the coasting set, the thrusters are disengaged. This solution has a total maneuver $\Delta V = 3.7061$ m/s, which is clearly much more fuel-efficient than the conventional safe SMPC method.

4.7.3 Active Safety

The active abort-safety scenario considered here is one where the chaser is assumed to start in the center of an approach corridor in the positive along-track direction from the target, as is frequently done in current missions [8]. The corrider is given by a LOS

Figure 4.9: Safe rendezvous with a coasting arc. The expected SMPC trajectory is shown in blue while the expected passive failure trajectories are shown in black.

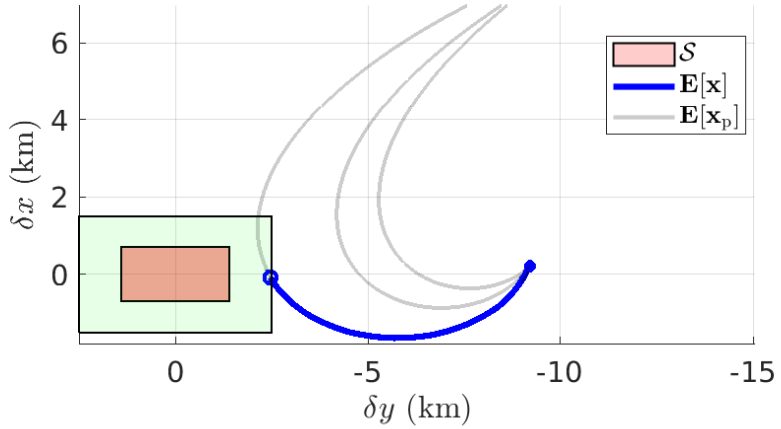


Figure 4.10: Safe rendezvous with a coasting arc. The expected SMPC trajectory is shown in blue. In black, random samples at t_i from $\mathcal{N}(\mathbb{E}[\boldsymbol{x}_i], \Sigma_i^{\boldsymbol{x}})$. The samples are from a 0.99 confidence ellipsoid around the mean.

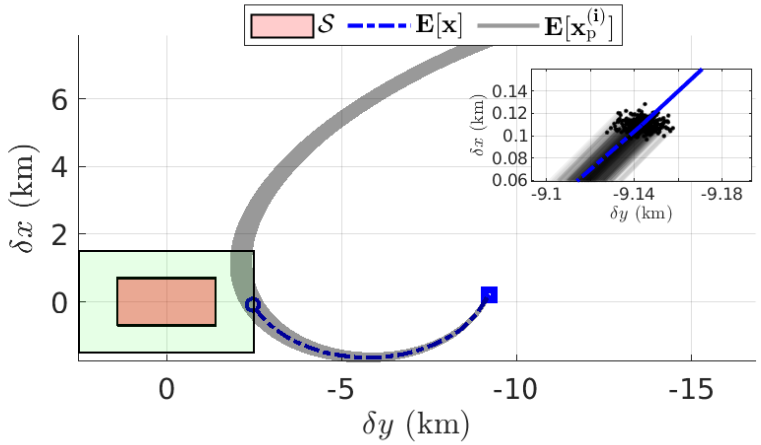
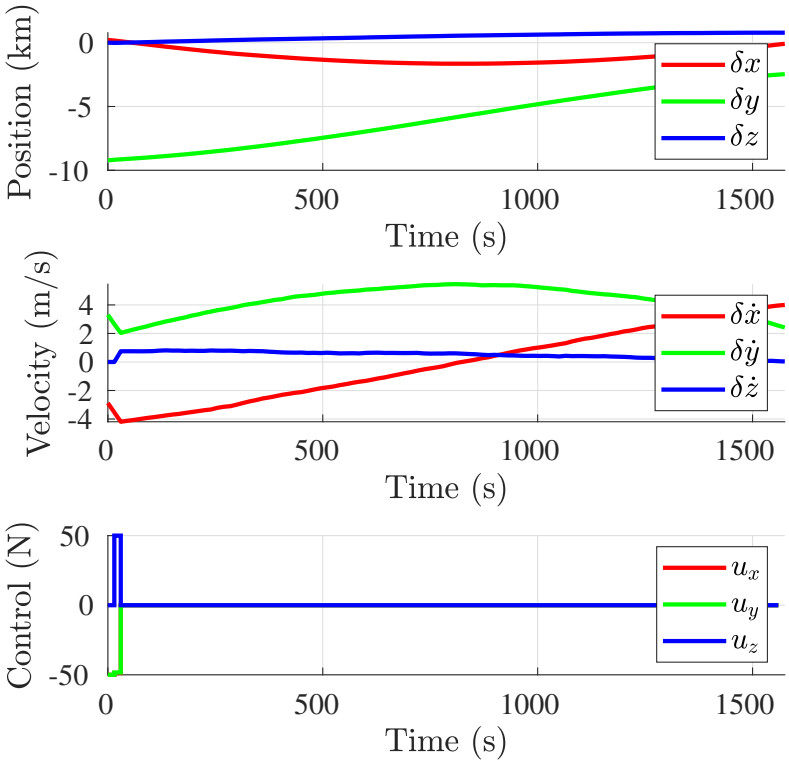
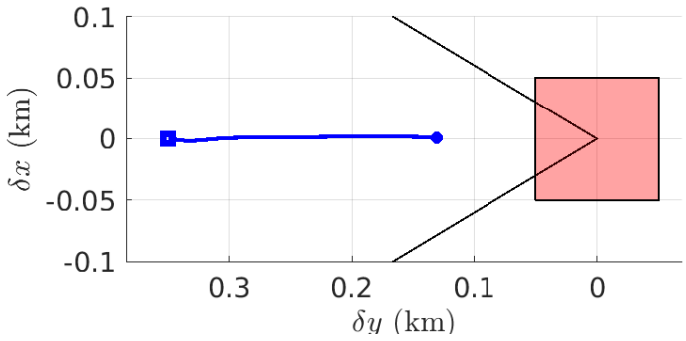


Figure 4.11: Relative position, velocity, and control trajectories for a passively safe coasting rendezvous maneuver.



constraint, as shown in Figure 4.12. We aim to be active abort-safe with respect to a polytopic set $\mathcal{P}_{\mathrm{f}}$, which is a box that tightly over-approximates an assumed target's physical size. The resulting abort-safe trajectory is the one shown in Figure 4.12, where the chaser essentially cancels out deviations from the along-track direction, as designed with the SMPC weights. The resulting relative states and control are visible in Figure 4.13. High penalties have been placed on δx and δz deviations, the consequences of which are seen in Figure 4.13, where the chaser predominantly moves along δy.

Figure 4.12: Actively-safe rendezvous in the LOS cone. The expected MPC trajectory is shown in blue while the expected passive failure trajectories are shown in black.



At a point just over 50m from the surface of the avoidance region $\mathcal{P}_f$, we assume a failure occurs with the primary thruster system, such that the back-up thrusters must perform an abort-maneuver which has not been planned for. By remaining inside the safe region of state space, the SMPC is able to find an abort-maneuver that avoids the set $\mathcal{P}_f$. At this assumed failure time, samples are drawn from the chaser's relative state distribution, and aborts are simulated for each one to determine whether or not the chance-constraints ensured that the majority of the chaser's PDF remains in the safe part of state-space. As is shown in Figure 4.14, all of the drawn samples successfully avoid the set $\mathcal{P}_f$. The abort maneuvers for each sample are pretty similar as shown in Figure 4.15.

Figure 4.13: Positions, velocities, and control during an actively-safe rendezvous.

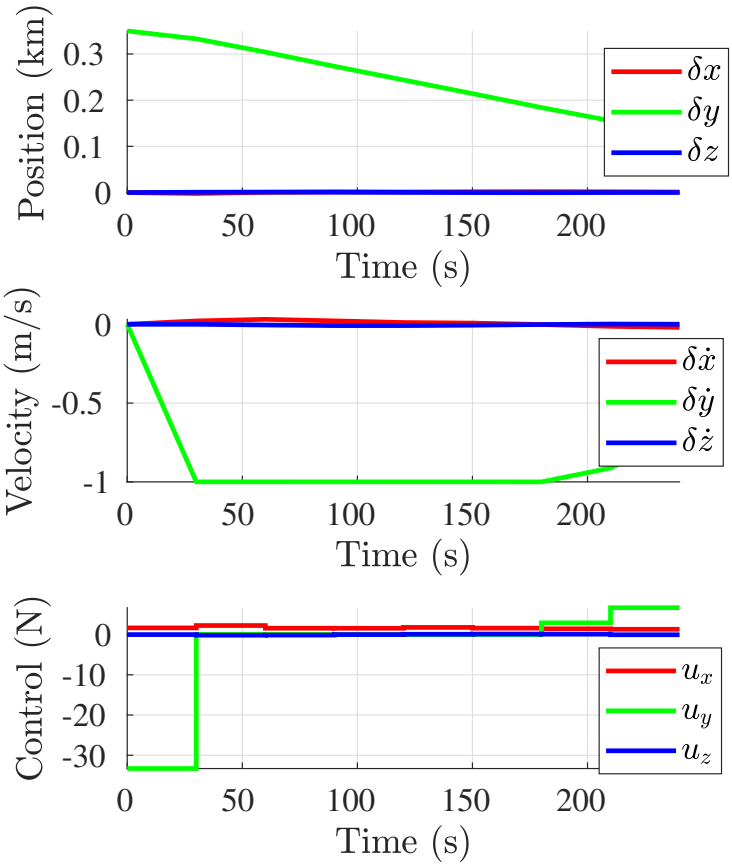


Figure 4.14: Abort trajectories for various samples drawn from the posterior distribution at an assumed failure time. The states are sampled from the 0.99 confidence ellipsoid of the distribution. All states are in the abort-safe region of state space and thus miss the target, represented by the red polytope $\mathcal{P}_f$.

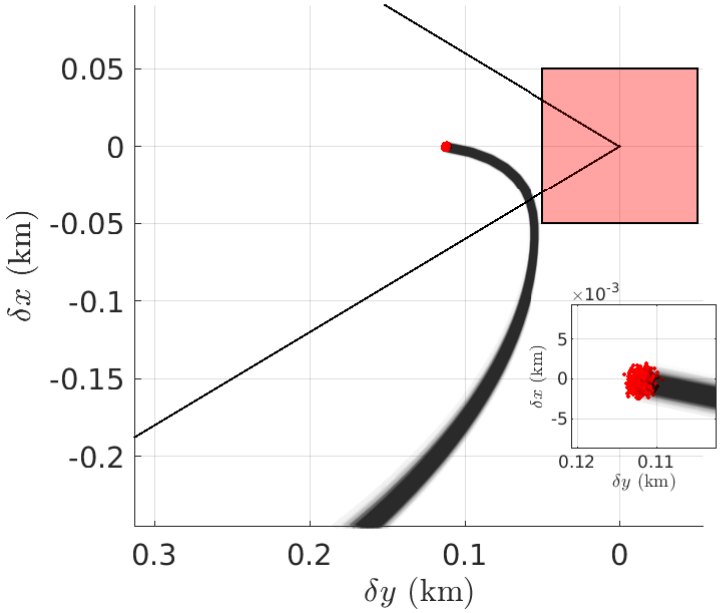
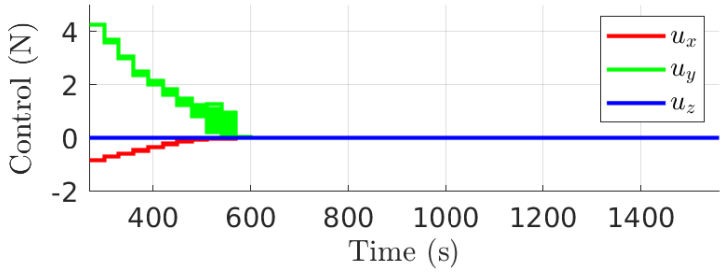


Figure 4.15: Abort control for all samples drawn from the posterior distribution at an assumed failure time.



4.7.4 Deterministic Lunar Gateway Rendezvous

We additionally demonstrate some results of the developed approach for a target in NRHO, representing the Lunar Gateway, and a chaser spacecraft that aims to rendezvous with the target. These results were first presented in [98]. The dynamics are assumed to be deterministic and the full state is known. The deterministic case is studied here to understand more about abort-safe rendezvous missions to NRHO targets. The equations of motion of the target in the resulting near-stable quasi-periodic orbit are linearized, resulting in a linear-time varying (LTV) system from which the passive-unsafe and abort-unsafe sets are computed. Initially, when far from the target, passive-safety is maintained and coasting arcs are exploited. Once the chaser enters a final approach corridor given by an LOS cone, abort-safety with respect to an assumed failure mode is considered.

The target NRHO used in this work is constructed using a full ephemeris model and dominant perturbations [99], which yields a more realistic, i.e., lower maintenance-energy, orbit. The NRHO is defined by a $4:1$ sidereal resonance, i.e., one for which the target completes four orbits for every lunar orbit around the system barycenter. The trajectory in the Synodic frame is shown in Figure 4.16. For additional works related to orbit navigation and maintenance about NRHO, see [99, 100], and references therein. At perilune, the dynamics along the NRHO are the fastest and coupled in all three Cartesian directions, resulting in non-intuitive coasting trajectories. At apolune, the dynamics are slow and the dynamics resemble a double integrator. The passive BRS, when projected onto the position subspace, using dynamics at apolune are shown in Figure 4.17. The double integrator-like dynamics result in the sets being approximately "concentric."

Initially, passive safety is maintained with respect to an ellipsoidal set $\mathcal{E}_f$ while a coasting set is targeted. After coasting into the goal set, abort-safety is maintained with respect to a polytopic set $\mathcal{P}_f$. The developed method is compared to a non-coasting MPC policy in terms of maneuver ΔV and input signal sparsity. In the simulations, $\Delta t_{\text{MPC}} =$

Figure 4.16: Target NRHO quasi-periodic orbit with 4:1 sidereal resonance, as seen in the Synodic frame $\mathrm{F_s}$, with radius of perilune $R_p = 4000$km. Moon visible in gray, Earth neglected for illustrative purposes.

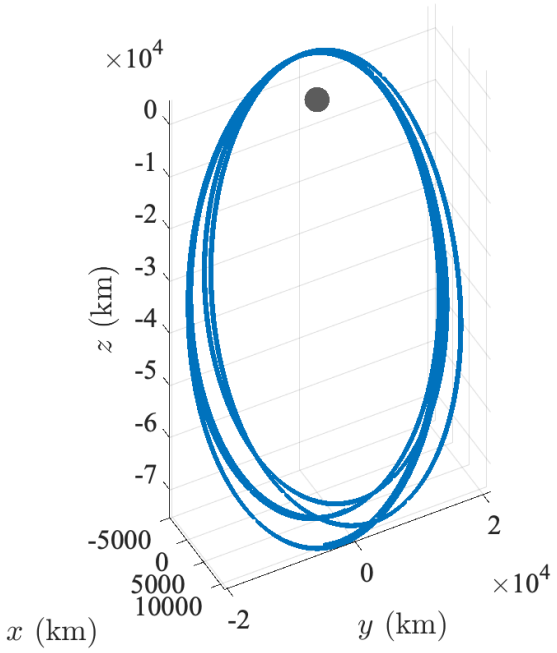
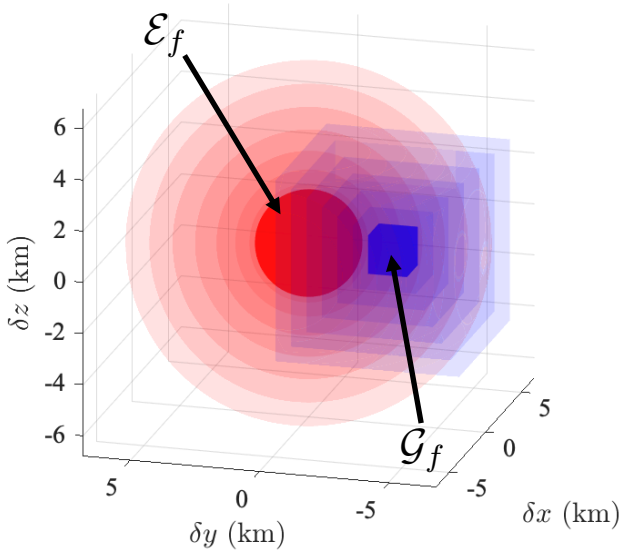


Figure 4.17: Projection of the coasting sets (blue) and the passively unsafe sets (red) onto the 3D position subspace for an NRHO target.



$\Delta t_{\text{RBRS}} = 30$s, and the nominal admissible control set $\mathcal{U}_n$, i.e., without any loss of thrust, is such that $\boldsymbol{u}_u = -\boldsymbol{u}_l = \mathbb{1} \cdot 30\text{N}$. Passive safety is maintained with respect to an ellipsoidal set where $P = \text{diag}(\begin{bmatrix} 2^2 \cdot \mathbb{1}_{1\times 3} & 0.1^2 \cdot \mathbb{1}_{1\times 3} \end{bmatrix}^{\mathsf{T}})$, i.e., an ellipsoid with position and velocity of major-axes of 2km and 0.100km/s, respectively. The goal set $\mathcal{G}$ is a box with ± 1.5km in the positions and ± 5m/s in velocities. The coasting maneuver is $t_m = 6$ hours. The initial condition is randomly sampled from the safe region of state space and is also outside of the computed coasting sets. The initial conditions are shown by red marks in the subsequent plots, the projection of the goal set $\mathcal{G}$ onto the position subspace is shown as a green polytope, while the LOS cone, which is a superset of the goal set $\mathcal{G}$, is shown in light blue.

4.7.4.1 Passive Abort-Safety at Perilune

The resulting approach trajectories are shown in Figure 4.18, the solution without coasting in red, and the solution with coasting arc in blue. The corresponding control signals are shown in Figures 4.19a-4.19b. For the case with coasting arc, only two input steps are required to enter a nearby coasting set. This results in an impulse-like input as shown in Figure 4.19a, leading the chaser into a coasting arc after two discrete-time steps. The states and entire passively safe control signal for the duration of the coasting arc are visible in Figure 4.20. The resulting trajectory is almost entirely driven by the natural dynamics and the chaser enters $\mathcal{G}$ with an approach velocity well below the designed approach velocity limits. Moreover, Figure 4.21 shows samples along the controlled-arc of the maneuver, which are propagated naturally for the considered safety-horizon, to show that the chaser is indeed passively safe. Once the chaser has entered a coasting-arc in a safe manner, the coasting-arc will also be safe, see the trajectory of Figure 4.21 that enters $\mathcal{G}$, shown in green. Conversely, Figure 4.19b shows the resulting control signal for the non-coasting MPC solution. The resulting maneuver length is much shorter; it takes roughly 1.2 hours to enter a bounding box around the $\mathcal{E}_f$ with control or thrust being required at all times. The benefit of the design introduced here is clear as the coasting-arc safe MPC gives $\Delta V = 2.657$m/s, while

Figure 4.18: In red, the MPC solution without a coasting arc while, in blue, the MPC with a coasting arc. Both are passively safe.

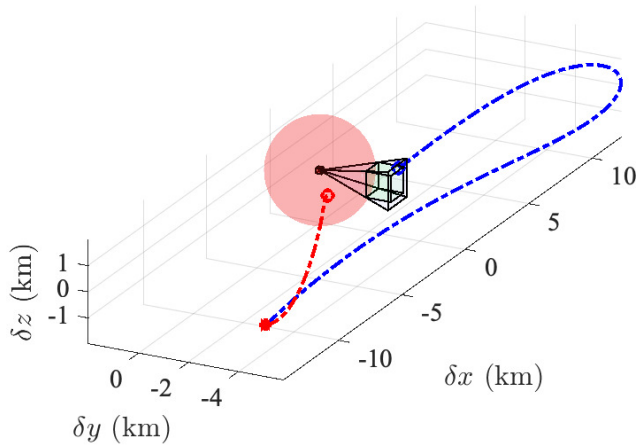
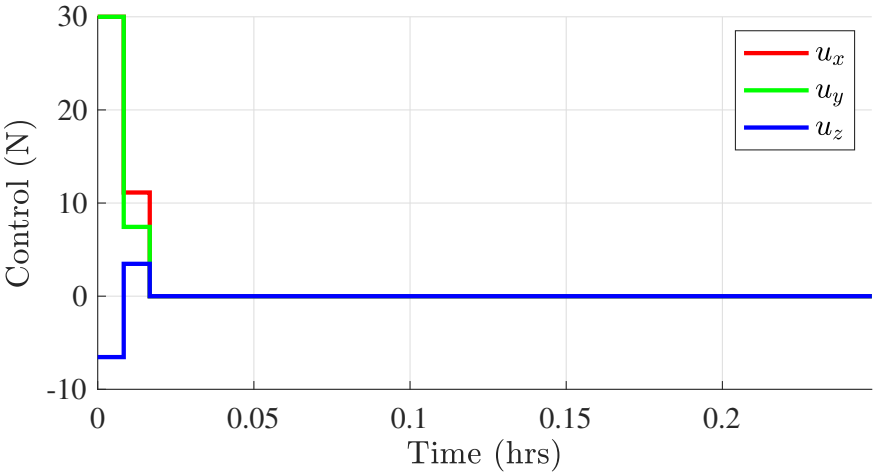
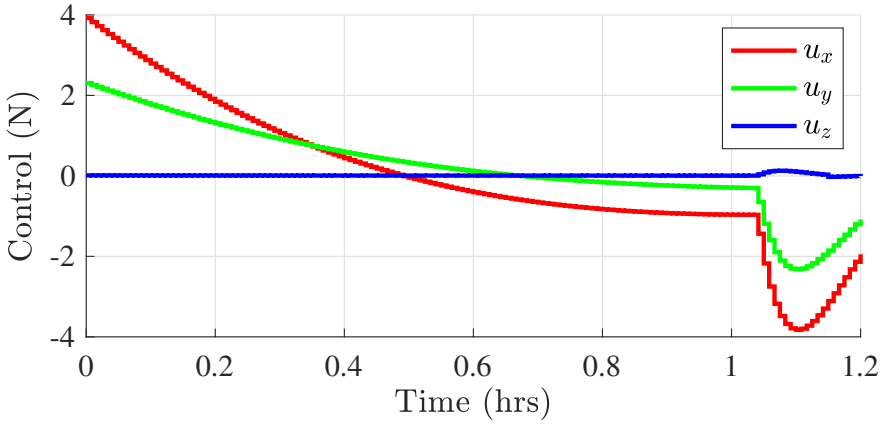


Figure 4.19: Comparison of the safe MPC input signals.



(a) Safe control signal with coasting arcs; only 0.2 hours shown out of the almost 10 hour signal. Resulting $\Delta V = 2.657$ m/s.



(b) Safe control signal without coasting arcs. Resulting $\Delta V = 9.6914$ m/s.

the standard safe MPC approach gives $\Delta V = 9.6914$m/s, yielding a 72.5% reduction in fuel consumption. In addition, the coasting-arc solution has a control signal that is much sparser in time, which is preferable for spacecraft thruster management to reduce propulsion system failures.

For the standard MPC to obtain a trajectory similar to the one with coasting arc, an extremely large prediction-horizon N_p would have to be considered. This would come at the cost of computation as the entire QP-MPC would be much larger and the safety constraints convexification will also involve many more steps. Thus, the coasting-arc MPC that can utilize much shorter N_p seems much more practical for on-board use.

4.7.5 Passive Abort-Safety at Apolune

At apolune, the state transition matrix is close to the identity and control heavily dominates the dynamics. The resulting coasting trajectory and control signal are shown in Figures 4.22-4.23, respectively. In this scenario, $t_m = 6$ hours. The coasting-arc consists of near straight-line motion as seen in Figure 4.22. At apolune, as a consequence of the state transition and control effect matrices, rendezvous approaches are likely safe as long as the relative velocity direction does not point towards $\mathcal{S}$. This phenomena is shown in Figure 4.22. If $\mathcal{G}$ is placed between the given initial condition and $\mathcal{E}_f$, passive-safety would only be possible if the chaser did not approach directly from $+\delta y$. Based on the simulations above, a natural question to pose is where a spacecraft mission should rendezvous with the lunar Gateway. Typically, the chaser is injected into the NRHO at apolune. This, combined with the fact that that control dominates the slower dynamics suggests it is much simpler to maintain safety at apolune, as the PBRS and RBRS are "smaller" compared to perilune.

4.7.6 Active abort-safety at Perilune

Once the spacecraft enters $\mathcal{G}$, the abort-safety phase is initiated. Here, the chaser has to remain outside of the RBRS, constructed with a hypothesized failure mode (additional

Figure 4.20: The position, velocity, and control signal for the initial approach toward an NRHO target with a roughly 6 hour long coasting arc.

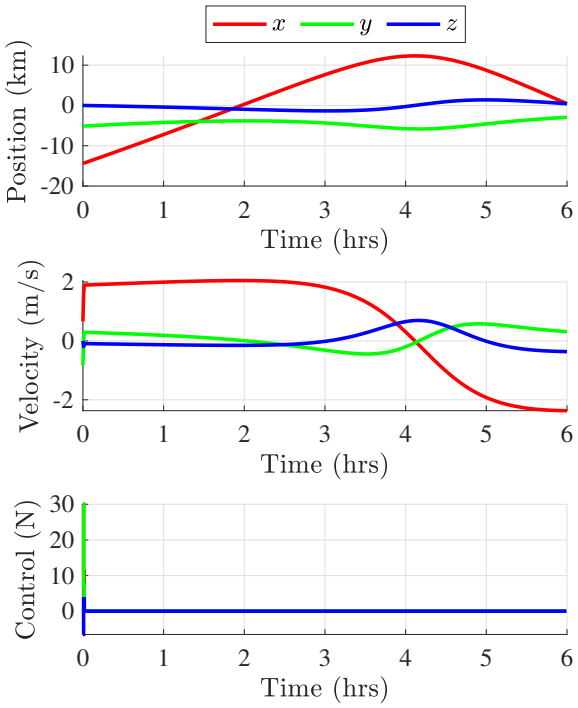


Figure 4.21: Demonstration of passive safety by sampling and propagating states (pre-coasting) along the controlled portion. None enter the red avoidance set.

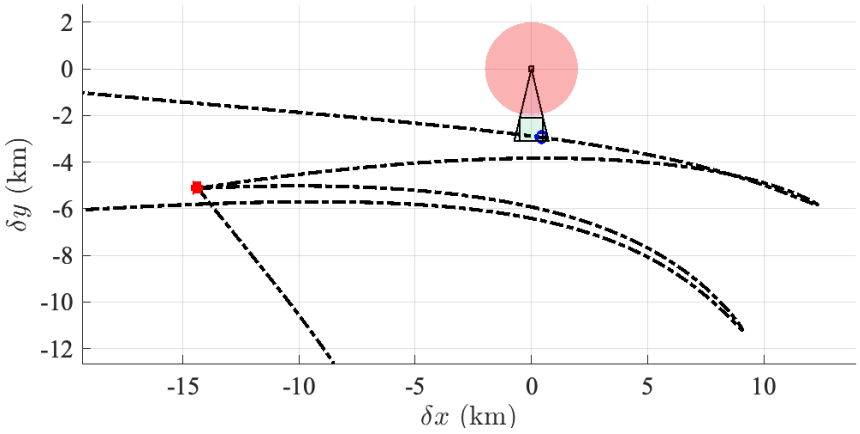


Figure 4.22: A passively safe coasting arc when rendezvous occurs at apolune.

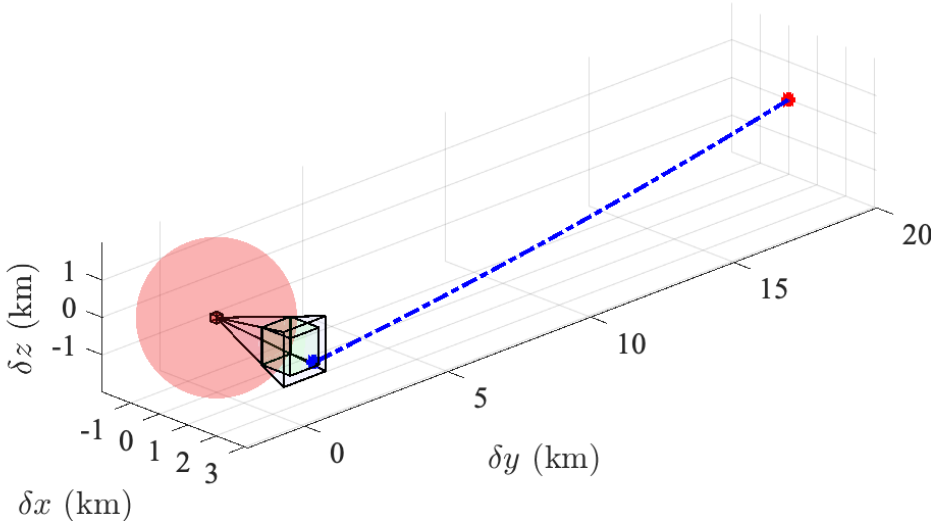
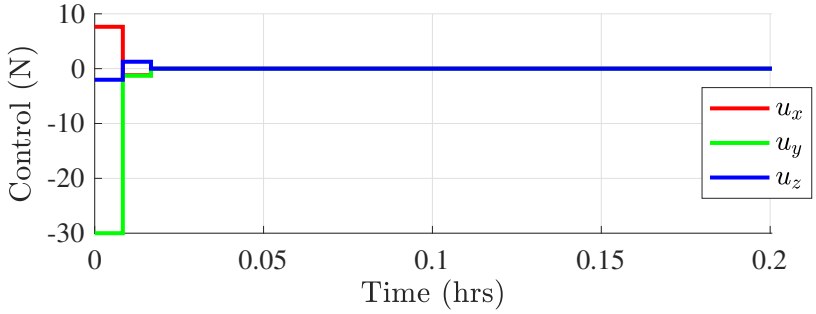


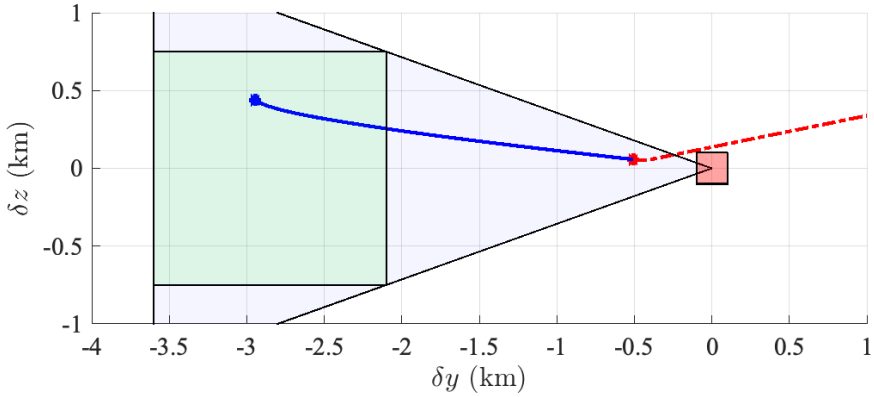
Figure 4.23: Safe control signal with coasting arcs. Only 0.2 hours out of 6 are shown. Resulting $\Delta V = 1.3019$ m/s.



failures can be easily included), such that in the event of a failure, a feasible abort maneuver exists. The incorporation of the LOS constraints severely limits the feasible abort maneuvers and approaches. As seen in Figure 4.24a, the LOS extends towards $-\delta y$. The assumed failure mode is such that $u_x = 0$, $0 \leq u_y \leq 30\text{N}$, $0 \leq u_z \leq 30\text{N}$, i.e., only positive y and z thrusts are available after a failure time t_{fail}. The chaser is able to avoid entering the RBRS while getting close to the target as seen in Figure 4.24a and as such, a viable abort-maneuver exists from t_{fail} onwards. The resulting control signal is shown in Figure 4.24b. A small impulse is applied to avoid collision.

Figure 4.24: Comparison of the safe MPC input signals.

(a) Abort-safe approach from the initial condition in the goal set $\mathcal{G}$ to a state near the terminal polytope $\mathcal{P}_f$. Simulated abort in red.



(b) Control for the abort-safety phase and the simulated abort at t_{fail}.

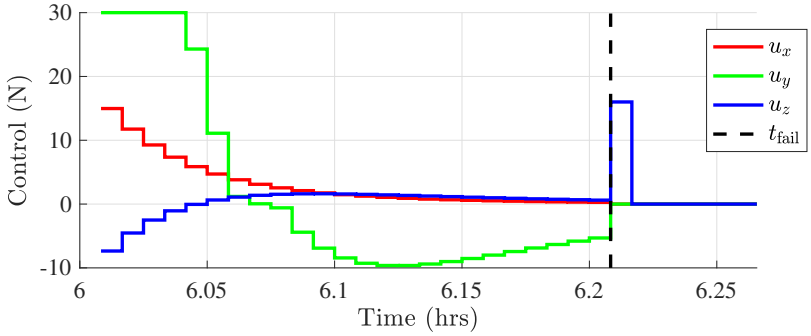
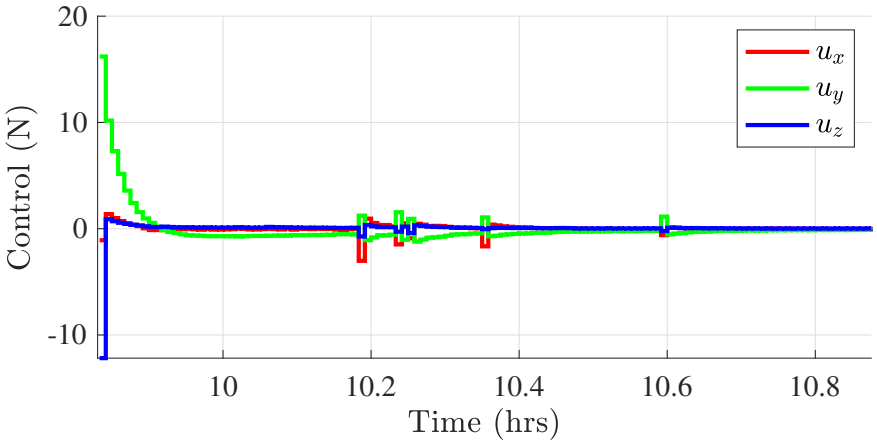


Figure 4.25: The control sequence for the abort-safety phase of the approach. The safety-constraints result in an unsteady control signal.



Chapter 5

Passive Abort-Safe Spacecraft Motion using Orbital Element Differences

5.1 Introduction

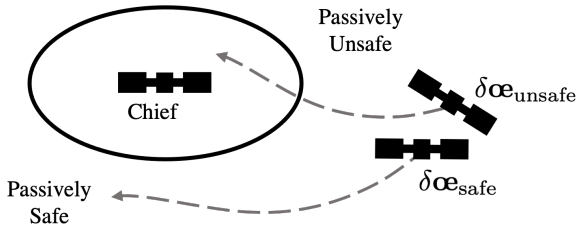
In this chapter, we focus on the problem of passive safety but from a slightly different perspective to the those discussed in chapters 3-4. In the prior chapters, we characterized sets of states that passively drift into a convex set $\mathcal{S}$ using Cartesian coordinates. The dynamics are used correspond to relative states as seen by a target frame, i.e., the sets are computed using the relative equations of motion in the chief or target's orbital Hill frame. Here, we characterize the regions of state space that are passively unsafe with respect to a chief in terms of a different coordinate description, namely, by means of orbital element differences. The orbital elements provide inertial state information of the each spacecraft and their difference yields a relative stat. The passive safety description remains the same but the relative state vector is now different, as seen in Figure 5.1. While the same techniques and algorithms discussed in chapters 3-4 could be used with these "new" BRS, in this chapter, we focus on using such sets for passively safe formation and constellation design.

The limitation of this description is that both spacecraft must be orbiting a single central body, while the Cartesian representation can be used for general dynamics models, i.e., N-body problems. Moreover, by using osculating orbital elements, we can characterize the passively unsafe regions of state space in this new coordinate space while also accounting for known perturbations. However, in this chapter, we will focus on deriving the BRS for the Keplerian dynamics model and the first-order J_2-perturbed mean orbital element

dynamics model. Such models are often used for preliminary design and in the J_2-perturbed mean orbital element representation, the secular effects of the J_2-perturbation are captured [69, 101, 102], which is particularly important for spacecraft in LEO.

For formation flying and constellation design applications, the inclusion of the J_2 secular effects is vital as it greatly improves the accuracy of any preliminary trajectory solutions; tracking or maintaining these "mean" trajectories also has the added benefit of reducing station-keeping or trajectory regulation fuel consumption [69]. These considerations are obviously important in the design of any orbit of interest. The usage of the "mean" element dynamics is useful for controlling the secular drift between satellites in a formation, but does not however, describe the actual motion between spacecraft, due to mapping errors. As such, this model is mostly applicable for formation flying or constellation where highly-accurate positional knowledge is not required. Such a model may not be suitable for active abort-safe rendezvous, where the deputy and chief are closer to each other, but it is useful for station-keeping, general analysis, and design of formations or constellations [103], as will be shown later.

Figure 5.1: Illustration of a passively unsafe and passively safe state. In the former, natural dynamics leads to entry of $\mathcal{S}$ while in the latter, the spacecraft naturally stays clear of $\mathcal{S}$.



5.2 Models

In the general perturbed case, Gauss' variational equations are used which maps the effects of perturbations to the dynamics of each orbital element [69, 104]. In this chapter though, we focus on using classical Keplerian and J_2-perturbed mean orbital element dy-

namics models to further analyze the BRS using models that capture some of the dominant perturbations in LEO, where most of the mega-constellations will be [59]. The equations of interest are available in Appendix A. Such equations are linearized about a reference, given by the chief's trajectory, and discretized for the computation of the BRS. We denote the relative state in terms of the difference between the deputy and chief's orbital elements, i.e., $\delta\boldsymbol{\oe} = \boldsymbol{\oe}_{\mathrm{d}} - \boldsymbol{\oe}_{\mathrm{c}}$. When mean orbital elements are used, we use the bar notation, so that $\delta\bar{\boldsymbol{\oe}} = \bar{\boldsymbol{\oe}}_{\mathrm{d}} - \bar{\boldsymbol{\oe}}_{\mathrm{c}}$ represents the difference in terms of mean orbital elements.

While in the Cartesian case the domain of interest is given by $\mathcal{X} \subseteq \mathbb{R}^6$, when using orbital elements, the domain is a strict subset of the 6-dimensional Euclidean space. This is because of the presence of constrained angular quantities, and we denote this domain as $\mathcal{X}^{\boldsymbol{\oe}} \subset \mathbb{R}^6$. Typically, at least one orbital element is given as an angle that is constrained to belong to a specific interval, e.g., mean anomaly $M \in [0, 2\pi)$. The space $\mathcal{X}^{\boldsymbol{\oe}}$ then consists of the Cartesian product of various intervals, which in general, depend on the orbital element description used, e.g., Keplerian, semi-singular, equinoctial, etc. Since we are considering near-Earth applications, that is, none parabolic and hyperbolic orbits, we constrain the osculating eccentricity and semi-major axis by $e < 1$ and $0 < a < \infty$, respectively.

5.2.1 Keplerian Dynamics

Suppose the following osculating orbital elements are chosen $\boldsymbol{\oe} = [n, e, i, \Omega, \omega, M]^{\mathsf{T}}$. The relative dynamics are then simply given by $\delta\dot{\boldsymbol{\oe}} = [0_{1\times(n-1)}, \delta n]^{\mathsf{T}}$, where [69]

$$\delta n \approx -\frac{3}{2}\sqrt{\frac{\mu}{a_{\mathrm{c}}^5}}\,\delta a, \tag{5.1}$$

and the corresponding plant matrix is

$$A(t) = \begin{bmatrix} 0_{n-1\times 1} & 0_{n-1\times n-1} \\ 1 & 0_{1\times n-1} \end{bmatrix}, \tag{5.2}$$

which is an time invariant and nilpotent. Under this description, the state transition matrix $\Phi(t_{k+1}, t_k) = e^{A(t_{k+1}-t_k)} = I + A\Delta T$, because $A^2 = 0_{6\times 6}$, and $\Delta T = t_{k+1} - t_k$.

5.2.2 J_2-perturbed Mean Orbital Element Dynamics

A large part of the LEO region, where the majority of the upcoming mega-constellations will be [59], is predominantly affected by J_2 perturbations. It is convenient then to analyze the "gross" motion of such orbits with mean orbital elements that capture the secular drift due to J_2 perturbations [69]. Using mean orbital elements and the mean J_2 perturbations, only $\bar{\Omega}, \bar{\omega}$, and $\bar{M}$ change with time. Their rates of change are nonlinear functions of the other mean elements $\bar{a}, \bar{e}$ and $\bar{\imath}$. In [69], the nonlinear dynamics of the mean orbital elements are linearized about a reference $\bar{\mathbf{oe}}_r$, yielding a plant matrix $[A(\bar{\mathbf{oe}}_r)]$ that is LTI and nilpotent. The linearized equations of motion in continuous time are $\delta\dot{\bar{\mathbf{oe}}} = [A(\mathbf{oe}_r(t))]\delta\bar{\mathbf{oe}}$. In discrete-time we have the following dynamics

$$\delta\bar{\mathbf{oe}}_{k+1} = \Phi(t_{k+1}, t_k)\delta\bar{\mathbf{oe}}_k, \tag{5.3a}$$

$$\Phi(t_{k+1}, t_k) = e^{[A(\mathbf{oe}_r(t_k))]\Delta T} = I_6 + [A(\bar{\mathbf{oe}}_{r,k})]\Delta T, \tag{5.3b}$$

where the dynamical plant matrix is

$$[A(\bar{\mathbf{oe}}_r)] = \begin{bmatrix} 0_{3\times3} & 0_{3\times3} \\ [A_{21}(\bar{\mathbf{oe}}_{r,k})] & 0_{3\times3} \end{bmatrix}. \tag{5.4}$$

The block matrix $[A_{21}(\bar{\mathbf{oe}}_{r,k})]$ is a matrix function of $\bar{a}_r, \bar{e}_r, \bar{\imath}_r$ and is given in [69]. The algorithm in [69, Appendix F] which retains the first-order J_2 terms is used to map from osculating to mean orbital elements and vice versa.

5.3 Coordinate Transformations

As in the preceding chapters, we utilize avoidance regions around the chief spacecraft again which are defined by convex sets. Recall that $\mathcal{S} \subset \mathcal{X}$, which represents an avoidance region around the chief and in the Cartesian space. It represents a set of relative positions and impact velocities which the chaser has to avoid entering. Since the avoidance region of interest is defined in $\mathcal{X}$, this set has to be expressed in terms of orbital element differences

some how. That is, the set itself has to be mapped from relative Cartesian space to orbital element space.

In [69], an invertible linear mapping between relative states in the chief's Hill frame and orbit element differences is derived using semi-singular orbit elements. This orbital element set is particularly useful when analyzing inclined near-circular orbits but suffers from singularities when the chief's orbit is equatorial, i.e., $i_c = 0$. The linear mapping is described by the matrix function $[A(\mathbf{oe}_{\mathrm{c}}(t))]$ and transforms orbit element differences into a Cartesian relative state vector expressed in the chief's Hill frame, i.e., $\boldsymbol{x} = [A(\mathbf{oe}_{\mathrm{c}}(t)]\delta\mathbf{oe}$. These types of linear mappings are particularly useful as the image or pre-image of a convex under a linear mapping remains convex.

Without loss of generality, let $\boldsymbol{g} : \mathcal{X}^{\mathbf{oe}} \times \mathcal{X}^{\mathbf{oe}} \mapsto \mathbb{R}^6$ be a mapping that given $\mathbf{oe}_{\mathrm{d}}$ and $\mathbf{oe}_{\mathrm{o}}$, yields a Cartesian relative state vector expressed in the chief's orbital frame F_{o}. Such a mapping is usually nonlinear and is given by the following nonlinear vector function

$$\boldsymbol{x} = \boldsymbol{g}(\mathbf{oe}_{\mathrm{d}}; \mathbf{oe}_{\mathrm{c}}). \tag{5.5}$$

Note that this mapping is invertible, i.e., $\mathbf{oe}_{\mathrm{d}} = g^{-1}(\boldsymbol{x}; \mathbf{oe}_{\mathrm{c}})$. We can uniquely recover the deputy's orbital elements given the Cartesian relative state and knowledge of chief's inertial state. The deputy's state in terms of orbit elements of the chief is given by $\mathbf{oe}_{\mathrm{d}} = \mathbf{oe}_{\mathrm{c}} + \delta\mathbf{oe}$; substituting this into (5.5) while performing a first-order approximation yields

$$\boldsymbol{x} = g(\mathbf{oe}_{\mathrm{c}} + \delta\mathbf{oe}; \mathbf{oe}_{\mathrm{c}}) \tag{5.6a}$$

$$\boldsymbol{x} = g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}}) + \frac{\partial g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}})}{\partial \delta\mathbf{oe}}\delta\mathbf{oe} + O(\delta\mathbf{oe}) \tag{5.6b}$$

$$\boldsymbol{x} \approx g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}}) + \frac{\partial g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}})}{\partial \delta\mathbf{oe}}\delta\mathbf{oe} \tag{5.6c}$$

where $g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}}) = \mathbf{0}_{n\times 1}$, i.e., the relative state of the chief with respect to itself is zero. As such, the first-order mapping is given by the Jacobian matrix

$$[G(\mathbf{oe}_{\mathrm{c}})] \triangleq \frac{\partial g(\mathbf{oe}_{\mathrm{c}}; \mathbf{oe}_{\mathrm{c}})}{\partial \delta\mathbf{oe}}. \tag{5.7}$$

As discussed earlier, such a matrix is provided in [69] for semi-singular elements. This approach generalizes to all orbital element descriptions, including the ones of interest in this Chapter provided the chief's state is not near a singularity.

5.4 Passive Backwards Reachable Sets

We enforce passive safety by ensuring that the deputy remains outside of the passively unsafe region of state space, that is, the region where natural dynamics results in the deputy entering or "colliding" with $\mathcal{S}$. The set $\mathcal{S}$, when expressed in orbital element differences, is clearly dependent on the chief's state at any given time. As such, we slightly change the notation compared to the prior chapters for the purposes of simplification. The set $\mathcal{S}_k^{\boldsymbol{\oe}}$ is the $\mathcal{S}$ expressed in terms of orbital element differences $\delta\boldsymbol{\oe}$ given the chief's state $\boldsymbol{\oe}_{\mathrm{c},k}$ at index k. The subscript highlights the explicit dependency on time, that is, expressing $\mathcal{S}$ in terms of $\delta\boldsymbol{\oe}$ will yield different sets which depend on the chief's state $\boldsymbol{\oe}_{\mathrm{c},k}$. Since the chief's trajectory is assumed to be known a-priori, we parameterize the set as a function of time. We can now introduce the BRS computation using orbital element differences.

Definition 5.4.1 (Backwards Reachable Sets)**.** *Given a discrete-time dynamical system $\delta\boldsymbol{\oe}_{k+1} = \boldsymbol{f}(k, \delta\boldsymbol{\oe}_k)$, and final time step k_f, the N-step backward reachable set $\mathcal{R}_b(N; \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\oe}})$ of $\mathcal{S}_k^{\boldsymbol{\oe}} \subset \mathbb{R}^6$, is found using the backwards recursion*

$$\mathcal{R}_b(0; \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\oe}}) = \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\oe}}, \tag{5.8a}$$

$$\mathcal{R}_b(j; \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\oe}}) = \{\delta\boldsymbol{\oe}_k \in \mathbb{R}^6 : \boldsymbol{f}(k_\mathrm{f} - j, \delta\boldsymbol{\oe}_k) \in \mathcal{R}_b(j-1; \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\oe}})\},\ j = \{1, \ldots, N\}. \tag{5.8b}$$

Here, the discrete-time dynamics function $\boldsymbol{f}(\cdot)$ may in general be nonlinear or linear. In the latter case, convexity of the BRS is preserved.

The function $\boldsymbol{f}(\cdot)$ represents the relative dynamics of the deputy with respect to the chief, which can be nonlinear and include perturbations. Such a nonlinear discrete-time function can be obtained using various numerical quadratures. Alternatively, this dynamical

function may also be a discrete-time version of the first-order approximation of the relative Gauss' variational equations with perturbations, linearized about the chief's trajectory. In this case, $\boldsymbol{f}(\cdot)$ is given by a sequential state transition matrix, obtained by integrating a perturbed Jacobian matrix, similar to that constructed in (A.13). The N-step BRS is the set of initial conditions at time $t_0 = t_\mathrm{f} - N\Delta T$ from which the deputy will not be able to avoid entering $\mathcal{S}_k^{\boldsymbol{\infty}}$ at time t_f, or k_f, under natural dynamics.

Definition 5.4.2 (Backwards Reachable Sets over an Interval)**.** *The backwards reachable set over the discrete-time interval (BRSI) $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, where $k_0 = k_\mathrm{f} - N$, is the union of the j-step BRS for $j = \{1, \ldots, N\}$,*

$$\mathcal{R}(N, \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\infty}}) = \bigcup_{j=0}^{N} \mathcal{R}_b(j; \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\infty}}). \tag{5.9}$$

The BRSI denotes the set of states $\bar{\boldsymbol{x}}$ such that from $\boldsymbol{x}_k = \bar{\boldsymbol{x}}$, $k \in \mathbb{Z}_{[k_0,k_\mathrm{f}]}$ the deputy will enter the avoidance region around the chief, $\mathcal{S}^{\boldsymbol{\infty}}$, at time step k_f under natural dynamics.

Next, even if the target is in a periodic orbit, we must account for the LTV nature of the linearized dynamics. To that end, we introduce the following sets.

Definition 5.4.3 (Periodic orbit-BRSI)**.** *The periodic orbit-BRSI is the union of the BRSI over $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$, where k_f is varied along one orbit*

$$\mathcal{X}_{\mathrm{unsafe}}^{\mathrm{p}}(N) = \bigcup_{k_\mathrm{f}=k_\mathrm{p}+1}^{2k_\mathrm{p}} \mathcal{R}(N, \mathcal{S}_{k_\mathrm{f}}^{\boldsymbol{\infty}}), \tag{5.10}$$

and k_p is the orbital period in time steps. This represents the sets of states that enter $\mathcal{S}$ in N steps or less, no matter where the chief is in its periodic orbit.

In the general perturbed case, the chief's orbit is no longer periodic, and thus we introduce the following set.

Definition 5.4.4 (Non-periodic orbit-BRSI)**.** *If the the chief orbit is not periodic, then, the non-periodic orbit-BRSI is the union over an interval $\mathbb{Z}_{[k_0,k_\mathrm{f}]}$ is given by*

$$\mathcal{X}_{\mathrm{unsafe}}^{\mathrm{np}}(N) = \bigcup_{j=0}^{N} \mathcal{R}(j; \mathcal{S}_{k_0+j}^{\boldsymbol{\infty}}). \tag{5.11}$$

The union is carried out for increasing final times so that safety is maintained with respect to the LTV system over a safety-horizon of N steps from the given initial time step k_0, i.e., the safety-horizon is $N\Delta T$ from the assumed initial time.

As in chapter 3, when the linear dynamics model and a convex terminal set are used, we are able to compute the BRS by performing simple linear-affine transformations of the original terminal set.

Suppose that $\mathcal{S} \subset \mathbb{R}^6$ represents a region in the 6-dimensional Euclidean space around the chief. To first order, this set can be represented in terms of $\delta\boldsymbol{\oe}$ by computing the pre-image of $\mathcal{S}$ with respect to $[G(\boldsymbol{\oe}_{\mathrm{c}})]$, that is, $\mathcal{S}_k^{\boldsymbol{\oe}} = \mathcal{S}[G(\boldsymbol{\oe}_{\mathrm{c},k})]^{-1}$ or

$$\mathcal{S}_k^{\boldsymbol{\oe}} = \{\delta\boldsymbol{\oe} \in \mathcal{X}^{\boldsymbol{\oe}} : \delta\boldsymbol{\oe} = [G(\boldsymbol{\oe}_{\mathrm{c},k})]^{-1}\boldsymbol{x},\ \boldsymbol{x} \in \mathcal{S}\}. \tag{5.12}$$

Because $\boldsymbol{\oe}_{\mathrm{c},k}$ is a function of time step, and is discrete in this work, we denote the set $\mathcal{S}_k^{\boldsymbol{\oe}}$ as the set $\mathcal{S}$ expressed in $\delta\boldsymbol{\oe}$ at time step k. Because (5.12) is a first-order approximation, the set can be inflated to account for any errors in the mapping such that there exists a set $\tilde{\mathcal{S}}_k^{\boldsymbol{\oe}} \supset \mathcal{S}_k^{\boldsymbol{\oe},\mathrm{nl}}$, where $\mathcal{S}_k^{\boldsymbol{\oe},\mathrm{nl}}$ is the non-convex set obtained using the nonlinear coordinate transformation. This set, is given by

$$\mathcal{S}_k^{\delta\boldsymbol{\oe},\mathrm{nl}} = \{\delta\boldsymbol{\oe} \in \mathcal{X}^{\boldsymbol{\oe}} : \delta\boldsymbol{\oe} = g^{-1}(\boldsymbol{x}; \boldsymbol{\oe}_{\mathrm{c},k}),\ \boldsymbol{x} \in \mathcal{S}\}. \tag{5.13}$$

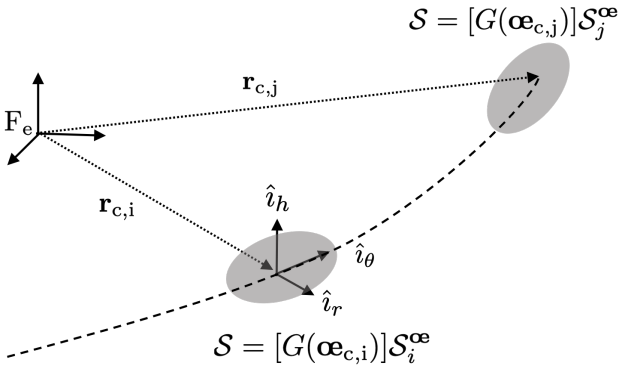
The inflation is done by quantifying the errors in the mapping, constructing an error set $E \subset \mathbb{R}^6$, and letting $\tilde{\mathcal{S}}_k^{\boldsymbol{\oe}} = \mathcal{S}_k^{\boldsymbol{\oe}} \oplus E$.

If the terminal set $\mathcal{S} = \{\boldsymbol{x} \in \mathbb{R}^6 : W\boldsymbol{x} \leq \boldsymbol{w}\}$, then the set is equivalently expressed in terms of $\delta\boldsymbol{\oe}$ as

$$\mathcal{S}_k^{\boldsymbol{\oe}} = \{\delta\boldsymbol{\oe} \in \mathcal{X}^{\boldsymbol{\oe}} : W[G(\boldsymbol{\oe}_{c,k})]\delta\boldsymbol{\oe} \leq \boldsymbol{w}\}, \tag{5.14}$$

using the linear mapping. Evidently, the matrix function $[G(\boldsymbol{\oe}_{c,k}]$ is a function of the osculating orbital elements of the chief. As such, the set $\mathcal{S}_k^{\boldsymbol{\oe}}$ will vary depending on where the chief is in its orbit, in both the unperturbed (Keplerian) and perturbed cases. These "terminal" sets represent the set of $\delta\boldsymbol{\oe}$ which impact with the chief at variable t_{f} or k_{f}.

Figure 5.2: Illustration of the avoidance set $\mathcal{S}$ along the chief's orbit at two t_i and t_j. The set $\mathcal{S}$ is equivalent to two different sets in terms of $\delta\mathbf{oe}$ at different t_i and t_j.



Moreover, suppose one has the BRS expressed in terms of Cartesian Hill frame coordinates, as obtained in chapter 3. The Cartesian j-step BRS $\mathcal{R}_b(j;\mathcal{S},k_{\mathrm{f}})$ in terms of $\delta\mathbf{oe}$, and vice versa, is given by the inverse and affine linear maps

$$\mathcal{R}_b^{\mathbf{oe}}(j;\mathcal{S}_{k_{\mathrm{f}}}^{\mathbf{oe}}) = \mathcal{R}_b(j;\mathcal{S},k_{\mathrm{f}})[G(\mathbf{oe}_{\mathrm{c}}(t_f - j\Delta T)], \tag{5.15a}$$

$$\mathcal{R}_b(j;\mathcal{S},k_{\mathrm{f}}) = [G(\mathbf{oe}_{\mathrm{c}}(t_f - j\Delta T)]\mathcal{R}_b^{\mathbf{oe}}(j;\mathcal{S}_{k_{\mathrm{f}}}^{\mathbf{oe}}), \tag{5.15b}$$

and as such, the sets (5.10) and (5.11) can be described in terms of $\delta\mathbf{oe}$ if the BRS are computed using Cartesian coordinates and STM. However, as will be discussed later, because there are angular quantities in $\mathcal{X}^{\mathbf{oe}}$, one must be careful when mapping the Cartesian sets naively to $\mathcal{X}^{\mathbf{oe}}$.

5.5 Passive Reachability Analysis: Orbit Element Differences

For general nonlinear systems that are conservative in nature, the solution to the discrete-time dynamics function $\boldsymbol{f}(k,\delta\mathbf{oe}_k)$ can be represented by 6 constants of motion, where one is time-varying [105]. The impact on the BRS computation is that only a single variable is changing backwards or forwards in time, leaving $n-1$ time-invariant quantities, simplifying the BRS analysis and computation.

In the Cartesian backward reachable analysis done in [83, 84], the terminal set is not

updated because the Cartesian relative equations of motion are used. Here, we are interested in a set that is defined in the chief's Hill frame expressed in terms of $\delta\mathbf{oe}$.

For Keplerian dynamics, the chief's orbit is periodic and thus $[G(\mathbf{oe}_{c,k}]$ is also periodic. Let k_p be the number of ΔT steps in a chief's orbital period. Then,

$$[G(\mathbf{oe}_{c,k}] = [G(\mathbf{oe}_{c,k+k_\mathrm{p}})], \tag{5.16}$$

For the purposes of passive safety, we wish to characterize the unsafe regions in terms of $\delta\mathbf{oe}$ around the chief. This is achieved by discretizing with sampling period ΔT, and evaluating $\mathcal{S}_k^{\mathbf{oe}}$ for $k = 0, \ldots, N$, where N is the safety horizon of interest. Given a fixed initial time k_0 and $N = k_\mathrm{f}$, we introduce the set

$$\bar{\mathcal{S}} = \bigcup_{i=1}^{N} \mathcal{S}_i^{\mathbf{oe}} = \bigcup_{i=1}^{N} \mathcal{S}[G(\mathbf{oe}_{\mathrm{c},i})], \tag{5.17}$$

which consists of a union of terminal sets, representing all of the avoidance regions in the safety horizon considered. The set $\tilde{S}$ captures all possible $\delta\mathbf{oe}$ along an interval of the possibly perturbed chief's orbit. The BRS using orbital element differences will be of the form

$$\mathcal{R}_b(N; \mathcal{S}_{k_\mathrm{f}}^{\mathbf{oe}}) = \mathcal{X}^{\mathbf{oe}} \cap \mathcal{S}_{k_\mathrm{f}}^{\mathbf{oe}} \Phi(t_f, t_0) \tag{5.18a}$$

$$= \mathcal{X}^{\mathbf{oe}} \cap \Phi(t_f, t_0)^{-1} \mathcal{S}_{k_\mathrm{f}}^{\mathbf{oe}}, \tag{5.18b}$$

that is, the sets are described by an affine or an inverse affine map using the state transition matrix.

5.5.1 The Effect of the Modulo Operator

The angular orbital elements are defined within specific intervals of interest, e.g. $[0, 2\pi)$ in the anomaly angle case, which has important consequences for the BRS computations. The admissible domain of the BRS is given by $\mathcal{X}^{\mathbf{oe}}$ and therefore we take the intersection of $\mathcal{R}_b(\cdot)$ with $\mathcal{X}^{\mathbf{oe}}$ to obtain the admissible reachable states. However, in some cases, the dynamics of certain orbital element angles is one with constant rates, e.g., Keplerian orbital elements with mean anomaly or J_2-perturbed mean orbital elements. The relative

angles grow monotonically with time and then wrap around the domain of interest using the **modulo** operator.

In such cases, the BRS will inevitably leave the admissible domain as more backwards steps are taken, that is, $\mathcal{R}_b(\cdot) \cap \mathcal{X}^{\text{oe}} \neq \emptyset$. The part of the BRS that spills out of $\mathcal{X}^{\text{oe}}$ is given by $\mathcal{R}_b(\cdot) \cap (\mathcal{X}^{\text{oe}})^c$. As will be shown later using some concrete examples, when this occurs, the BRS is effectively split by the modulo operator into the union of convex regions. Denote $\mathcal{X}_+^{\text{oe}} = \{\delta\text{oe} \in \mathcal{X}^{\text{oe}} : [\delta\text{oe}]_i \geq 0,\ i = 1, \ldots, n\}$ as the **positive** side of the admissible orbital element difference domain, while $\mathcal{X}_-^{\text{oe}} = \{\delta\text{oe} \in \mathcal{X}^{\text{oe}} : [\delta\text{oe}]_i \leq 0,\ i = 1, \ldots, n\}$ is the **negative** side of the admissible domain. When the magnitude of the orbital element angles are larger than the maximum allowable difference, e.g. larger then 2π for anomaly angles, the BRS effectively cross into the inadmissible domain $(\mathcal{X}^{\text{oe}})^c$. The j-step BRS at this point need to be adjusted due to the effect of the modulo operator. We consider here the case where the backwards analysis results in a single crossing into the inadmissible domain. In this scenario, the corresponding BRS is given by given by

$$\tilde{\mathcal{R}}_b(j, \mathcal{S}_{k_\text{f}}^{\text{oe}}) = \Big(\mathcal{R}_b(\cdot) \cap \mathcal{X}^{\text{oe}}\Big) \bigcup \Big(\big(\mathcal{R}_b(\cdot) \cap \mathcal{X}_+^{\text{oe}}\big) \oplus \{-\bar{y}_u\}\Big) \bigcup \Big(\big(\mathcal{R}_b(\cdot) \cap \mathcal{X}_-^{\text{oe}}\big) \oplus \{\bar{y}_l\}\Big) \quad (5.19)$$

where $\bar{y}_u, \bar{y}_l \in \mathbb{R}^6$ are the necessary offsets to **re-align** the portion of the BRS that left $\mathcal{X}^{\text{oe}}$ about the origin. That is, the BRS is the union of its original component in the admissible domain and the regions affected by the modulo operator.

Remark 10. *If the backwards time-step is sufficiently large, there can be multiple crossings of this boundary and as such, the BRS is made of the union of many more convex sets.*

Put differently using the vertex representation ($\mathcal{V}$-rep) of the BRS, the single crossing BRS is more simply understood because the modulo operator acts on elements of a vertex (vector) as it is propagated backwards in time. The vertices that make up $\mathcal{S}_k^{\text{oe}}$, denoted $V(k_\text{f})$ may have significantly different δa, which in turn results in different amounts of relative drift between the vertices of the BRS and the chief itself. This naturally affects the propagation of

vertices to the initial time, which is denoted $V(k_0)$. As such, different vertices will be affected by the modulo operator at different times, resulting in the above-mentioned problem. The vertex representation of the BRS after the modulo operator is given by

$$\tilde{\mathcal{R}}_b(j, \mathcal{S}_{k_\mathrm{f}}^{\mathfrak{oe}}) = \mathrm{conv}(V_\mathrm{in}) \cup \mathrm{conv}(V_\mathrm{out}^1) \cup \mathrm{conv}(V_\mathrm{out}^2), \tag{5.20a}$$

$$V_\mathrm{in} = \{\boldsymbol{v}_i(t_0) \in \mathcal{X}^{\mathfrak{oe}}\}_{i=1}^{n_\mathrm{in}}, \tag{5.20b}$$

$$V_\mathrm{out}^1 = \{\tilde{\boldsymbol{v}}_j(t_0) \in \mathcal{X}_+^{\mathfrak{oe}}\}_{j=1}^{n_\mathrm{out}^+}, \tag{5.20c}$$

$$V_\mathrm{out}^2 = \{\tilde{\boldsymbol{v}}_j(t_0) \in \mathcal{X}_-^{\mathfrak{oe}}\}_{j=1}^{n_\mathrm{out}^-}, \tag{5.20d}$$

$$\tilde{\boldsymbol{v}}_j(t_0) = \boldsymbol{v}_j(t_0) \pmod{\bar{\boldsymbol{z}}} \tag{5.20e}$$

where n_in, n_out^+, n_out^- are the number of BRS vertices inside and outside of the admissible domain $\mathcal{X}^{\mathfrak{oe}}$ along the positive and negative regions. The total number of vertices are $n_v = n_\mathrm{in} + n_\mathrm{out}^+ + n_\mathrm{out}^-$. Because of the intersection operation $\mathcal{R}_b(\cdot) \cap \mathcal{X}^{\mathfrak{oe}}$, the number of vertices V_in will necessarily increase. The modulo operator is applied element-wise on $\boldsymbol{v}_j(t_0)$ using the limits $\bar{\boldsymbol{z}}$, which depend on the orbital elements considered.

Remark 11. *The resulting BRS is not simply the convex hull of the vertices after the modulo operation is carried out because this operation does not preserve the convexity of the set.*

An illustrative example considers Keplerian dynamics where an anomaly angle effectively describes the relative state. When the anomaly difference is either more or less than 2π, the modulo operation is required. Beyond this point in time, one obtains states that are unsafe in more than one **relative period**. A deputy state belonging to the BRS has essentially wrapped around the chief's orbit. Despite its proximity in state-space, it would only enter $\mathcal{S}$ after more than one relative period. Given the sets $\mathcal{S}$ assumed in chapters 3-4 and a chief orbiting in LEO, the inadmissible domain is reached in just under 3 days.

In summary, given a sufficiently large backwards time-step, the BRS become non-convex due to the modulo operator and are expressed as the union of the original admissible BRS along with the re-centered component of the BRS that left the admissible domain. It is

for this reason that polytopic sets may be of interest when computing the BRS using orbital element differences as the intersection of a polytope with another yields yet another polytopic set. In the ellipsoidal case, such a set would be difficult to express. In this thesis, we avoid having to compute the non-convex effect of the modulo operator on the BRS using (5.19) by considering scenarios that have not yet reached this point in time during the backwards analysis, e.g., by limiting the relative mean motion of the spacecraft.

One of the benefits of using Cartesian coordinates for the BRS computations is that this issue is avoided entirely.

5.5.2 Keplerian Dynamics and Orbital Elements

We provide the analytic BRS given a deputy and chief subject to Keplerian dynamics whose states are expressed using Keplerian orbital elements. This results in only the mean anomaly difference varying with time through the following relationship: $\delta M = \delta n(t - t_0) + \delta M_0$, while all other orbit elements are time-invariant. For the orbit elements assumed above, the N-step BRS at $k_0 = k_\mathrm{f} - N\Delta T$ is given by

$$\mathcal{R}_b(N; \mathcal{S}^{\mathbf{oe}}_{k_\mathrm{f}}) = \{\delta\mathbf{oe} \in \mathcal{X}^{\mathbf{oe}} : H\Phi(t_f, t_0)\delta\mathbf{oe} \leq \boldsymbol{k}\} \tag{5.21a}$$

$$= \{\delta\mathbf{oe} \in \mathcal{X}^{\mathbf{oe}} : (H + HA(t_f - t_0))\delta\mathbf{oe} \leq \boldsymbol{k}\}, \tag{5.21b}$$

where $H = W[G(\mathbf{oe}_{\mathrm{c},k_\mathrm{f}})]$ and the nilpotent matrix A "isolates" the n^{th} column of H, denoted $\boldsymbol{h}_n$, yielding $HA(t_f - t_0) = [\boldsymbol{h}_n(t_f - t_0), 0_{n\times(n-1)}]$. Therefore,

$$\mathcal{R}_b(N; \mathcal{S}^{\mathbf{oe}}_{k_\mathrm{f}}) = \{\delta\mathbf{oe} \in \mathcal{X}^{\mathbf{oe}} : \tilde{H}\delta\mathbf{oe} \leq \boldsymbol{k}\}, \tag{5.22a}$$

$$\tilde{H} = H + \begin{bmatrix} \boldsymbol{h}_n(t_f - t_0) & 0_{n\times(n-1)} \end{bmatrix}. \tag{5.22b}$$

The column vector $\boldsymbol{h}_n$ and H are fixed and defined at the final time based on (5.14) from which the polytopic BRS are acquired analytically. Similar properties can be derived for an ellipsoidal terminal set $\mathcal{S}$. This makes computation of the BRS particularly simple using $\delta\mathbf{oe}$ as the only $\mathbf{oe}$ that is time-varying is the mean anomaly δM.

However, as discussed in Section 5.5.1, care must be taken because $\delta M \in [-2\pi, 2\pi)$. Since δM cannot span the entire real number line, the modulus operator has to be incorporated into the set calculation. This eventually yields a non-convex representation of the BRS at a particular time step as illustrated in Figure 5.4, which can be expressed as a union of convex sets as seen in (5.19)-(5.20).

Suppose that $H = [I_6, -I_6]^\mathsf{T} \in \mathbb{R}^{12\times 6}$ in (5.21), such that,

$$\mathcal{S}_k^{\mathfrak{oe}} = \{\delta\mathfrak{oe} \in \mathcal{X}^{\mathfrak{oe}} : [I_6, -I_6]^\mathsf{T}\delta\mathfrak{oe} \leq \boldsymbol{k}\} \tag{5.23}$$

then each element in $\delta\mathfrak{oe}$ is bounded from below and above, as given by the rows $[\boldsymbol{k}]_i$. Additionally, assume that the set $\mathcal{S}_k^{\mathfrak{oe}}$ is symmetric about the origin, that is, $[k]_i = [k]_{i+n}$. Using the the Keplerian case, this amounts to $2n-2$ time-invariant constraints if $\mathfrak{oe} = [n, e, i, \Omega, \omega, M]^\mathrm{T}$. As such, the BRS polytope only has two inequalities that change as the considered time-horizon $(t_f - t_0)$ changes, namely, the ones corresponding to δM, given by

$$\delta n(t_f - t_0) + \delta M_0 \leq \delta M_{\max} \tag{5.24a}$$

$$\delta n(t_f - t_0) + \delta M_0 \geq \delta M_{\min}. \tag{5.24b}$$

These inequalities characterize the BRS when the modulo operator is not required. This constrains the initial δM_0 to be within a certain interval while the mean motion difference δn is itself constrained by $\delta n_{\min} \leq \delta n_0 \leq \delta n_{\max}$. Because the terminal set is centrally symmetric, we have $\delta n_{\min} = -\delta n_{\max}$ and $\delta M_{\min} = -\delta M_{\max}$. Here, δn_0 is a variable that is bounded from below and above, but for every δn, there's a specific interval constraining the unsafe δM_0. It is clear that as $\delta n_0 \to 0$, the time it takes for the **modulo** operator to be used increases.

The outer-limits or maximal δM_0 at any time are found by substituting the minimal and maximal δn into (5.24), yielding

$$\delta M_0 \leq \delta M_{\max} - \delta n_{\min}(t_f - t_0) \tag{5.25a}$$

$$\delta M_0 \geq \delta M_{\min} - \delta n_{\max}(t_f - t_0), \tag{5.25b}$$

since $\delta n_{\min}$ and $\delta n_{\max}$ maximize and minimize the upper and lower bounds, respectively. These maximal bounds increase monotonically with the backwards time-horizon considered. When $|\delta M_{\{\max,\min\}} - \delta n_{\{\min,\max\}}(t_f - t_0)| \geq 2\pi$, the modulo operator is used, resulting in a non-convex BRS.

Above, we assumed that $\mathcal{S}_k^{\text{oe}}$ was box-like. Even if it were not, any convex set $\mathcal{S}$ can be over-approximated by a bounding box or hyper-rectangle $\mathcal{B}$. As such, this property can be leveraged to simplify the analysis of the BRS of $\mathcal{S}_k^{\text{oe}}$. By using $\mathcal{B} \supset \mathcal{S}_k^{\text{oe}}$, we obtain a set of the form in (5.23), defined by the shape-matrix $H = [I_6, -I_6]^\mathsf{T}$. By construction then, $\mathcal{B}$ yields a measure of the maximum spread of the set $\mathcal{S}_k^{\text{oe}}$ in each δoe direction. In the Keplerian case, $\mathcal{B}$ maximizes the quantities $|\delta M_{\max}|, |\delta M_{\min}|, |\delta n_{\max}|, |\delta n_{\min}|$. Then, the longest backwards time-horizon that can be considered prior to the **modulo** operator taking effect on the BRS, i.e., when $|\delta M| \geq 2\pi$, is given by

$$t_f - t_0 = \frac{2\pi - \max(|\delta M_{\max}|, |\delta M_{\min}|)}{\max(|\delta n_{\max}|, |\delta n_{\min}|)}, \tag{5.26}$$

and thus the time at which the modulo operation is needed is given by

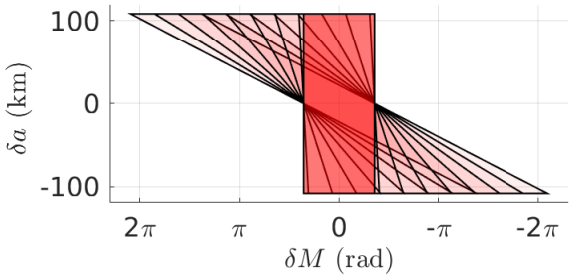
$$t_0^{\text{mod}} \triangleq t_f - \frac{2\pi - \max(|\delta M_{\max}|, |\delta M_{\min}|)}{\max(|\delta n_{\max}|, |\delta n_{\min}|)}. \tag{5.27}$$

The number of backwards steps before the modulo operation is required is then

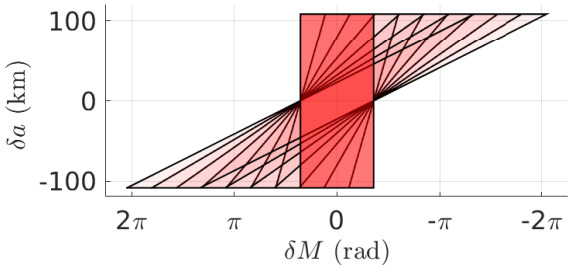
$$N_{\text{mod}} = \frac{t_f - t_0^{\text{mod}}}{\Delta T}. \tag{5.28}$$

Figure 5.4 shows an illustration of the BRS splitting as a result of the modulo operator. We let the time-invariant subspace of δoe be denoted by $\delta\text{oe}_{\mathcal{I}}$. Here, $\delta\text{oe}_{\mathcal{I}} \in \mathbb{R}^5$. The sets are shown at different $\delta\text{oe}_{\mathcal{I}}$ for ease of illustration, but they should be aligned. Here, the original BRS $\mathcal{R}_b(\cdot)$ is split into $\mathcal{R}_b(\cdot)^\alpha$ and $\mathcal{R}_b(\cdot)^\beta$, i.e., the new effective BRS is given by $\tilde{\mathcal{R}}_b(\cdot) = \mathcal{R}_b(\cdot)^\alpha \cup \mathcal{R}_b(\cdot)^\beta$. In this illustration, the original portion of the BRS that is in the admissible domain is $\mathcal{R}_b(\cdot)^\alpha$ while the shifted portion that crossed into the inadmissible one is given by $\mathcal{R}_b(\cdot)^\beta$.

Figure 5.3: Initial states for a passively-safe constellation of 5804 spacecraft distributed along two intersecting orbital planes. A subset of the BRS and PFRS are shown for a single final time. We go backwards and forward for 40 chief periods, i.e., 3 days, and then the crossing of $\pm 2\pi$ occurs.

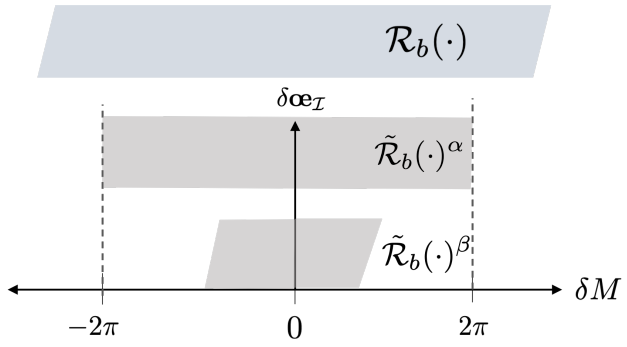


(a) Projected BRS onto δn and δM plane where the BRS projections cross the $(-2\pi, 2\pi)$ domain in terms of δM. These sets require re-initialization after the crossing.



(b) Projected PFRS onto δn and δM plane where the PFRS projections cross the $(-2\pi, 2\pi)$ domain in terms of δM. These sets require re-initialization after the crossing.

Figure 5.4: Illustration of the effect of the mod$(\cdot)$ operation on the BRS, yielding a union of two convex sets.



Again, in this work, we consider scenarios before this problem occurs and hence the BRS are simply given by (5.22). In general, the modulo operation issue can be alleviated by reducing the size of $\mathcal{S}$ for example. Reducing the position bounds and impact velocities will result in one being able to perform a longer backwards analysis prior to having to deal with non-convex BRS.

5.5.3 Mean Elements with J_2 Perturbations

This J_2-perturbed mean orbital element difference STM used to compute the BRS from a generic terminal set $\mathcal{S}^{\bar{\mathbf{oe}}}$ is given in (5.3). Now, only three of the orbital element differences change backwards in time, yielding yet another subspace along which the BRS change. Since the $\mathcal{S}$ is originally defined in the Cartesian Hill frame of the chief, the set is mapped first to osculating orbital element differences and then to mean orbital element differences using a first-order mapping available in [69], based on the work by Brouwer and Lyddane [101, 102]. For mean elements, the N-step BRS at $t_0 = t_f - N\Delta T$ is given by

$$\mathcal{R}_b(N; S_k^{\bar{\mathbf{oe}}}) = \{\delta\bar{\mathbf{oe}} \in \mathcal{X}^{\mathbf{oe}} : (H + H[A(\bar{\mathbf{oe}}_r)](N\Delta T))\delta\bar{\mathbf{oe}} \leq \boldsymbol{k}\}. \tag{5.29}$$

Similar to the Keplerian case, here, the BRS modulo operation can occur with the $\delta\bar{\omega}$, $\delta\bar{\Omega}$, and $\delta\bar{M}$ relative angles.

5.6 Passive Safety Trajectory Design

In equations (5.10) and (5.11), we defined the periodic and non-periodic orbit-BRSI, which characterize the unsafe regions of state space within a time-interval of interest. The former computes the set of states that enter the region $\mathcal{S}$ in N steps or less at any point in the chief's orbit. As such, if a spacecraft is outside of this region, then the spacecraft will not enter $\mathcal{S}$ in at least N steps. The non-periodic orbit-BRSI are similar but only consider states that enter $\mathcal{S}$ within the **next** N steps from an initial time step. A state that is outside of these regions will be safe for the following N steps. In this section, we demonstrate how

the derived BRS and BRSI can be leveraged to guarantee long term safety. Importantly, methods to reduce the dimensionality of the design problem are presented and discussed.

5.6.1 Infinite-Horizon Safety

Using Cartesian relative states expressed in a chief's Hill frame, one can characterize the unsafe regions of state space for a finite time-horizon. Without additional analysis, it is not clear how the methods developed in chapter 3 and 4 can be exploited to guarantee longer term, or infinite-time, safety without computing more sets and increasing the safety-horizon N. When using orbit element differences, such analyses are greatly simplified. This coordinate description allows us to merge classical orbital mechanics and formation flying theory with passive reachability theory, where relative orbits which are safe for a possibly infinite time, for example, fall out as a special case.

5.6.1.1 Keplerian Dynamics

In the Keplerian case, infinite-time safety can be guaranteed by constraining a subset of the deputy's orbital elements, i.e., by considering a subspace of the BRS. We denote the time-invariant subspace of Keplerian orbit elements as $\mathcal{I} \subset \mathbb{R}^5$, which is five-dimensional in nature as the anomaly angle is the only time-varying quantity, that is, $[n, e, i, \Omega, \omega]^\mathsf{T} \in \mathcal{I}$. By projecting the BRS onto the subspace $\mathcal{I}$ of orbital element differences, an interesting property emerges that allows us to guarantee safety for an infinite amount of time in the Keplerian case.

We introduce the projection of a set $\mathcal{S}_k^{\text{oe}}$ onto a lower dimensional subspace here, namely, the time-invariant subspace of orbital elements $\mathcal{I}$. Projecting the terminal set onto $\mathcal{I}$ yields

$$\text{proj}_{\mathcal{I}}(\mathcal{S}_k^{\text{oe}}) = \{\boldsymbol{y} \in \mathbb{R}^5 |\ \boldsymbol{y} = C\boldsymbol{x}, \boldsymbol{x} \in \mathcal{S}_k^{\text{oe}}\} \tag{5.30}$$

where every vector in $\mathcal{S}_k^{\text{oe}}$ is multiplied by a matrix $C = \text{diag}(I_{5\times5}, 0)$. This effectively "marginalizes" the relative anomaly angle.

Suppose the $\mathcal{V}$-rep of $\mathcal{S}_k^{\text{oe}}$ is given by the matrix $V(k_\text{f}) \in \mathbb{R}^{n \times n_v}$, defined at a final time of interest. The columns $\boldsymbol{v}_i$ of $V(k_\text{f})$ are the vertices of $\mathcal{S}_k^{\text{oe}}$ whose convex hull defines the terminal set, that is,

$$\text{conv}(V(k_\text{f})) = \mathcal{S}_k^{\text{oe}}. \tag{5.31}$$

Then, the BRS is given by propagating each vertex backwards in time using $\Phi(k_\text{f}, k_0)^{-1}$, yielding an initial matrix of vertices $V(k_0) = \Phi(k_\text{f}, k_0)^{-1} V(k_\text{f})$. Taking the convex hull of these vertices, under the assumption that the modulo operator is not required yet, the BRS is given by $\mathcal{R}_b(N; \mathcal{S}_{k_\text{f}}^{\text{oe}}) = \text{conv}(V(k_0))$. The projection of the BRS onto the time-invariant subspace of orbit elements is $V_{\mathcal{I}}(t_0) = CV(k_0)$, i.e., the linear map C is applied on each vertex. As such,

$$\begin{aligned}
\mathcal{R}_b^{\mathcal{I}}(N; \mathcal{S}_{k_\text{f}}^{\text{oe}}) &\triangleq \text{proj}_{\mathcal{I}}\big(\mathcal{R}_b(N; \mathcal{S}_{k_\text{f}}^{\text{oe}})\big) && (5.32)\\
&= \text{proj}_{\mathcal{I}}\big(\text{conv}(V(k_0))\big) && (5.33)\\
&= \text{conv}(CV(k_0)) && (5.34)\\
&= \text{conv}(V_{\mathcal{I}}(t_0)) = \text{conv}(V_{\mathcal{I}}(t_f)) && (5.35)
\end{aligned}$$

because $CV(k_0) = CV(k_\text{f})$. As a result, one obtains that the projected BRS onto the subspace $\mathcal{I}$ is equivalent to the projection of the terminal set $\mathcal{S}_k^{\text{oe}}$ onto the same subspace, that is, $\mathcal{R}_b^{\mathcal{I}}(N; \mathcal{S}_{k_\text{f}}^{\text{oe}}) = \text{proj}_{\mathcal{I}}\big(\mathcal{S}_{k_\text{f}}^{\text{oe}}\big)$, for all $k_0 \leq k_\text{f}$.

This projection can be applied to a sequence of sets $\mathcal{S}_k^{\text{oe}}$ where $k \in \mathbb{Z}_{[0,k_\text{p}]}$, that is, the regions $\mathcal{S}$ are evaluated around the chief's periodic orbit, to a certain discretization accuracy, as shown in Figure 5.2. Typically, one evaluates the BRS from a given final time step and works backwards to characterize the sets of states that enter an avoidance region in a certain number of steps. Using orbital element differences, however, we can project the BRS onto the subspace $\mathcal{I}$, which is simply $\mathcal{R}_b^{\mathcal{I}}(N; \mathcal{S}_{k_\text{f}}^{\text{oe}}) = \text{proj}_{\mathcal{I}}\big(\mathcal{S}_{k_\text{f}}^{\text{oe}}\big),\ \forall k_\text{f} \in \mathbb{Z}_{[0,k_\text{p}]}$, to characterize the regions of the time-invariant orbital element subspace that enter $\mathcal{S}$ at any point in time. By projecting onto $\mathcal{I}$, the anomaly difference is marginalized from the passive reachability analysis, yielding the time-invariant orbital element differences which would have entered $\mathcal{S}$

at some future time-step. If a state is outside of this region, it will either not enter $\mathcal{S}$ or it will do so at an impact velocity that is higher than that used to construct $\mathcal{S}$.

The projected sets are evaluated at all times around the chief's orbit and we use the union of these sets

$$\tilde{S}_{\mathcal{I}} = \bigcup_{k=0}^{k_{\mathrm{p}}} \mathrm{proj}_{\mathcal{I}}(\mathcal{S}_k^{\mathfrak{oe}}), \tag{5.36}$$

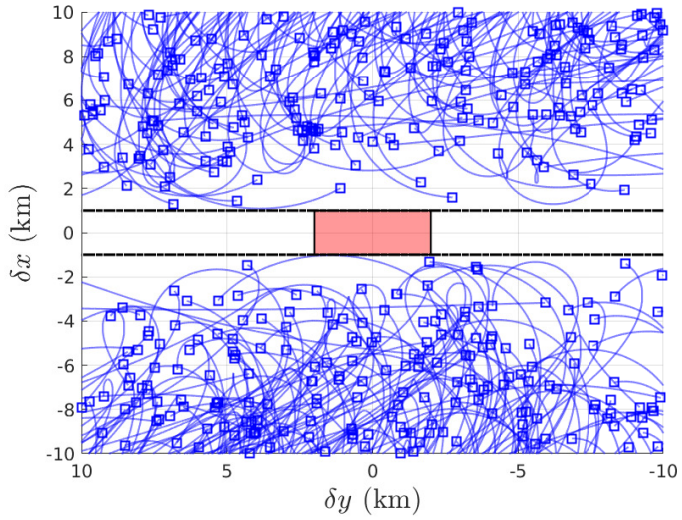
to characterize the regions that a deputy's time-invariant orbital elements must remain outside of to not enter $\mathcal{S}_k^{\mathfrak{oe}}$ at any future step k. This is analogous to characterizing the orbital elements that intersect a solid-sphere that is swept through the chief's orbit in the position subspace, and has particular impact velocities at any point along it in higher dimensions. Thus, if the deputy's relative state with respect to the chief is given by $\delta\tilde{\mathfrak{oe}}$, $C\delta\tilde{\mathfrak{oe}} \notin \tilde{\mathcal{S}}_{\mathcal{I}}$ and $\delta\tilde{\mathfrak{oe}} \in \mathcal{X}^{\mathfrak{oe}}$, then the deputy is said to be passively safe for an infinite amount of time, as its own periodic orbit does not intersect the chief's periodic orbit at any future time.

Such a constraint is conservative as it requires the Keplerian orbits of the chief and deputy to never intersect. Using Cartesian relative Hill coordinates, constraining a trajectory to never intersect the orbit of the chief is quite difficult. Figure 5.5 shows randomly generated initial states $\delta\tilde{\mathfrak{oe}}^{(i)}$ that satisfy the following constraints: $C\delta\tilde{\mathfrak{oe}}^{(i)} \notin \tilde{\mathcal{S}}_{\mathcal{I}}$ and $\delta\tilde{\mathfrak{oe}}^{(i)} \in \mathcal{X}^{\mathfrak{oe}}$. These states are then propagated forward in time and as shown in Figure 5.5; none of the resulting trajectories intersect the orbit of the chief, locally shown by the horizontal black lines in the chief's Hill frame. The safety ellipse, discussed in [68] is also a solution that satisfies this projection constraint, provided the in-plane and cross-track amplitudes are large enough to avoid $\mathcal{S}$.

While this projection constraint may seem impractical and inaccurate, if the deputy and chief have similar physical geometries and are close to each other, then the perturbations acting on both spacecraft are similar in the relative sense and approximately cancel out. As such, this constraint can be used because $\delta\mathfrak{oe} \to 0$, $\boldsymbol{a}_{\mathrm{d}} \to \boldsymbol{a}_{\mathrm{c}}$.

When perturbations are neglected, there is another specific case that results in passive

Figure 5.5: Initial states that are outside of $\text{proj}_{\mathcal{I}}(\bar{\mathcal{S}}^{\text{oe}})$ propagated forward for an orbital period. No trajectory enters $\mathcal{S}$ or $\text{proj}_{\mathcal{I}}(\mathcal{S}_k^{\text{oe}})$, resulting in no intersections of the along-track axis when close to the chief spacecraft.



safety guarantees for an infinite amount of time. This is the case when the deputy spacecraft is in a relative orbit with the chief that does not enter $\mathcal{S}_k^{\text{oe}}$, $\forall k$. This occurs as a result of $\delta a = 0$, i.e., the deputy and chief have matched-periods.

We can design relative orbits or trajectories that do not enter $\mathcal{S}_k^{\text{oe}}$ by considering sections or slices of $\bar{\mathcal{S}}$, the union of $\mathcal{S}_k^{\text{oe}}$ for different k in (5.17), when $\delta n = 0$. When perturbations are neglected, we can design such trajectories that do not intercept $\mathcal{S}$ without ever computing the BRS. We denote such slices as $\bar{\mathcal{S}}\big|_{\delta n=0}$. When we constrain $\delta n = 0$ using Keplerian orbit elements, the BRS cease to change. Slicing $\mathcal{R}_b(\cdot)$ along $\delta\text{oe}_\text{s} = [0, \delta e, \delta i, \delta\Omega, \delta\omega, \delta M]^\mathsf{T}$ yields

$$\mathcal{R}_b(j; \mathcal{S}_{k_\text{f}}^{\text{oe}})\big|_{\delta\text{oe}_\text{s}} = \{\delta\text{oe}_\text{s} \in \mathcal{X}^{\text{oe}} : \tilde{H}\delta\text{oe}_\text{s} \leq \boldsymbol{k}\} \tag{5.37a}$$

$$= \{\delta\text{oe}_\text{s} \in \mathcal{X}^{\text{oe}} : H\delta\text{oe}_\text{s} \leq \boldsymbol{k}\} \tag{5.37b}$$

which is a time-invariant set because $\delta n = 0$ (recall the Keplerian plant matrix in (5.2)). As such, for Keplerian orbit elements, only $\bar{\mathcal{S}}\big|_{\delta\text{oe}_\text{s}}$ has to be evaluated as all $\mathcal{R}_b(j; \mathcal{S}_k^{\text{oe}}) = \mathcal{S}_k^{\text{oe}}$, $\forall j, k$. This is easily verified because the orbital element differences at any future time, given this orbit element set, are $\delta\text{oe}(t) = (I + A(t - t_0))\delta\text{oe}_\text{s} = \delta\text{oe}_\text{s}$. In summary, for unperturbed systems using Keplerian orbit elements, safety with respect to the original set $\mathcal{S}$ is also achieved for an infinite amount of time if

$$\delta\text{oe}_\text{s} \notin \bigcup_{k=0}^{N} \mathcal{S}_k^{\text{oe}}\big|_{\delta\text{oe}_\text{s}} \tag{5.38}$$

where $\delta\text{oe}_\text{s} = [0, \delta e, \delta i, \delta\Omega, \delta\omega, \delta M]^\mathsf{T}$. This will be leveraged for the purposes of formation design in a later section.

This simplication is possible because of the inherent structure of the BRS when considering the orbital element set used here. If one uses semi-singular orbit elements [69], letting $\delta a = 0$ will not result in this property as the BRS depend on other orbit element differences due to the usage of true latitude. The dynamics Jacobian matrix for semi-singular coordinate description depends on variations of true anomaly expressed in terms of the other variables.

In that case, letting $\delta a = 0 \implies \dot{\theta} = 0$, and as such, slices along $\delta a = 0$ of the BRS do not have the same impact as those just shown.

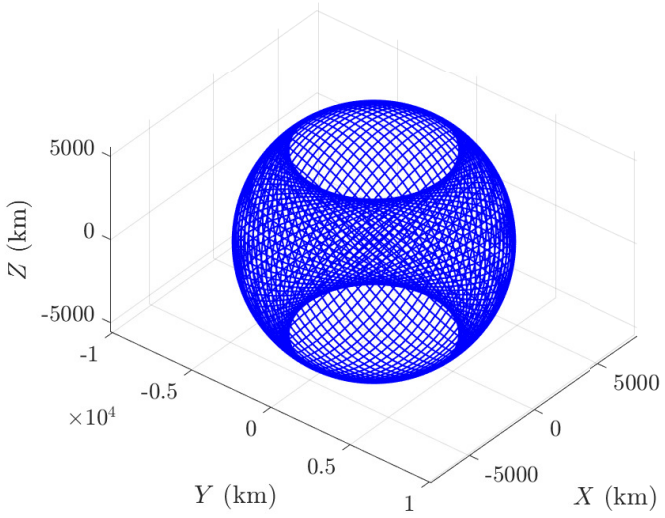
5.6.1.2 Mean Elements with J_2

For discussion purposes, we briefly mention how infinite-horizon safety is achieved under two-body motion with J_2 perturbations. This method, however, does not make use of the BRS analysis and computation done in the rest of this chapter. Beacuse the chief's mean $\bar{a}, \bar{e}$ and $\bar{\imath}$ elements do not change with time under this orbital element set and model, and $\bar{\Omega}, \bar{\omega}, \bar{M}$ vary at a constant rate, the "mean" reachable set of positions can be obtained by performing a volume integral of the changing elements. Without accounting for short and long periodic oscillations, the chief's orbits can be swept for variable $\bar{\Omega}, \bar{\omega}, \bar{M}$. In this chapter though, we map the terminal set $\mathcal{S}$ from the Cartesian Hill frame and express them in terms of $\bar{\mathbf{oe}}$. Under such an analysis, a large number of time steps needs to be considered to fully capture the union $\cup_{k=0}^{k_\mathrm{f}} \mathcal{S}_k^{\bar{\mathbf{oe}}}$ of the unsafe regions of orbital elements, that is, performing the volume integral above with the nominal approach would require a lot of computation.

Suppose that we evaluated the terminal sets for a large enough time-horizon, $k_\mathrm{f} \gg 0$, such that $\mathcal{S}$ is swept across all possible Cartesian states of the chief. Then, following the logic in Section 5.6.1.1, one can compute projections onto the new time-invariant subspace $\mathcal{I} \subset \mathbb{R}^3$, which is 3-dimensional in nature and made up of variable $[a, e, i]^\mathsf{T} \in \mathcal{I}$. The resulting projections are equivalent to projecting the terminal sets onto $\mathcal{I}$, hence, $\mathcal{R}_b^{\mathcal{I}}(N; \mathcal{S}_{k_\mathrm{f}}^{\bar{\mathbf{oe}}}) = \mathrm{proj}_{\mathcal{I}}\big(\mathcal{S}_{k_\mathrm{f}}^{\bar{\mathbf{oe}}}\big)$, for all $k_0 \leq k_\mathrm{f}$. Then, as before, the projected sets are evaluated at all times around the chief's possible inertial Cartesian positions and we use the union of these sets $\tilde{S}_{\mathcal{I}} = \bigcup_{k=0}^{k_\mathrm{p}} \mathrm{proj}_{\mathcal{I}}\big(\mathcal{S}_k^{\mathbf{oe}}\big)$ to characterize the regions that a deputy's time-invariant orbital elements must remain outside of to not enter $\mathcal{S}_k^{\mathbf{oe}}$ at any future step k. This yields orbital elements that intersect the entire orbital shell of the chief, an example of which is depicted in Figure 5.6. Thus, if the deputy's relative state with respect to the chief is given by $\delta\tilde{\mathbf{oe}}$ and if $C\delta\tilde{\mathbf{oe}} \notin \tilde{\mathcal{S}}_{\mathcal{I}}$ and $\delta\tilde{\mathbf{oe}} \in \mathcal{X}^{\mathbf{oe}}$, then the deputy is said to be passively safe

for an infinite amount of time with respect to the secular effects of J_2. Such sets could be inflated to account for variations between osculating and mean orbital elements.

Figure 5.6: The orbital shell resulting from the effects of J_2 perturbations for a near-circular chief in LEO.



There are other ways of achieving infinite-horizon safety which include constraining a deputy's period to be an irrational multiple of the chief's orbital period, which when coupled with a phase difference, at least in the two-body model, results in the spacecraft never intersecting. For the Keplerian and J_2-perturbed models, avoiding the reachable set of positions, which makes up the orbit and shell, respectively, is a sufficient condition for passive safety that is very conservative. For generic formation flying or constellation design, such constraints are not preferable. Intersection of the position reachable sets is possible as long as some phasing-offset is present, as will be shown later.

5.6.2 Finite-Time Safety

In the general case, the sets of states that are unsafe given perturbed and non-periodic orbits in a finite amount of time are found via $\mathcal{X}^{\text{np}}_{\text{unsafe}}(N)$. Constraining a spacecraft to be

outside of $\mathcal{X}^{\text{np}}_{\text{unsafe}}(N)$ results in a finite-time passive safety constraint between the deputy and the chief.

5.7 Utility for Space Traffic Management

In general, enforcing such safety constraints between numerous spacecraft is challenging, which is why formations and constellations are designed with simpler geometric constraints and dynamical arguments. Given the safety constraints derived in this paper, one can use them for a variety of situations, provided the chosen orbital element set makes sense. In this chapter, we focus on the impacts of these constraints on formation and constellation design and organization problems, which is motivated by the space traffic management problem. BRS provide a framework in which regions of state space can be attributed to different spacecraft, like a slot, which can help maintain the safety of orbiting assets and reduce conjunction events.

As mentioned before, one of reasons for expressing these passive safety constraints in terms of $\delta\mathbf{oe}$ are that the linearized dynamics in these spaces are much more accurate than the corresponding Cartesian ones. In fact, in some models the dynamics in terms of orbital elements are simply linear as seen above and therefore there are no linearization errors. Additionally, constellation design is already done with such coordinate sets in mind, and thus, it may be helpful to assess intra and inter-constellation safety using such descriptions. Solving the general passive safety problem that considers multiple spacecraft is quite challenging, if not intractable, and requires the satisfaction of numerous non-convex constraints. One way to constrain N_s spacecraft to be passively safe for N-steps is to enforce

$$\mathcal{X}^{\text{np}}_{\text{unsafe}}(N)\big|_{\mathbf{oe}_{\text{c}_i}} \cap \mathcal{X}^{\text{np}}_{\text{unsafe}}(N)\big|_{\mathbf{oe}_{\text{c}_j}} = \emptyset, \qquad \forall i \neq j = 1, \ldots, N_s. \tag{5.39}$$

This requires N_s non-periodic orbit-BRSI to be disjoint with strict separation, for passive-safety guarantees. This constraint does not allow for overlap of spacecraft avoidance zones,

i.e., $\mathcal{S}_a \cap \mathcal{S}_b = \emptyset$.

As passive safety of multiple spacecraft with respect to each other is desired, we denote the avoidance region around a spacecraft's state $\mathbf{oe}_{\mathrm{c}_i}$ as the set $\mathcal{S}(\mathbf{oe}_{\mathrm{c}_i})$. Instead of enforcing non-overlapping regions in state-space as seen in (5.39), in this work we propose a simpler passive safety constraint given by

$$\mathbf{oe}_{\mathrm{c_i}} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\mathbf{oe}_{\mathrm{c}_j}} \forall i \neq j = 1, \ldots, N_s, \tag{5.40}$$

which allows the avoidance zones $\mathcal{S}(\cdot)$ to overlap but constrains the spacecraft to not enter each other's "terminal" sets. That is, for a pair of spacecraft α and β, we enforce $\mathbf{oe}_{\mathrm{c}_\alpha} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\mathbf{oe}_{\mathrm{c}_\beta}}$ **and** $\mathbf{oe}_{\mathrm{c}_\beta} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\mathbf{oe}_{\mathrm{c}_\alpha}}$ to ensure the chief does not enter the deputy's avoidance zone $\mathcal{S}$, and vice versa. For instance, when the chief and deputy have matched periods and are not perturbed, i.e., $\delta a = 0$, the deputy may be placed infinitesimally close to the set $\mathcal{S}(\mathbf{oe}_{\mathrm{c}})$ with an along-track offset and remain safe for all time. Using the non-overlapping constraint in (5.39), the same can be achieved but the deputy must have a larger anomaly offset to ensure the avoidance sets do not overlap.

In the remainder of this section, we pose the general formation and constellation design packing problems as well as a new definition of an orbital slot. The packing problems are quite complex and as such, we do not present direct solutions to this problem and leave such analyses for future work.

5.7.1 Formations

In this section, we discuss how the derived safety constraints can be used in the formation design process. When fully perturbed dynamics are considered, closed relative orbits that are periodic are not possible to achieve. One can design quasi-periodic orbits by trying to match the deputy's semi major axis a_d with that of the chief a_c, such that $\delta a = a_d - a_c = 0$. In practice, $\delta \dot{a} \neq 0$ as the perturbations between the spacecraft are not identical. However, for spacecraft with similar physical geometries and attitudes, as well as cases where $\delta\mathbf{oe} \to 0$,

one obtains $\delta a \approx 0$ that can be managed with active station-keeping capabilities. Another strategy is to design relative orbits that are "invariant" to perturbations of interest. This can be done for example using mean orbital element differences between spacecraft that are invariant to the secular effects of J_2 perturbations [69].

Remark 12. *The passive safety constraints discussed here can be added to the J_2-invariant ones to obtain relative orbits that do not intersect $\mathcal{S}$.*

The formation design problem can be thought of as an optimization problem whose cost is a function of all spacecraft orbit elements. To guarantee passively safe solutions, one incorporates the safety constraint as well as the matched-period constraint. If the orbital element difference between spacecraft i and j is denoted $\delta\boldsymbol{\alpha}_{i,j}$, then letting the cost function be $J(\delta\boldsymbol{\alpha}_{i,j}) = \|\delta\boldsymbol{\alpha}_{i,j}\|^2$, results in minimizing the deviation of the orbital elements from each other. Such a cost function can be considered for a formation packing problem, i.e., attempting to pack a number of spacecraft as close together as possible.

Definition 5.7.1 (Formation Packing)**.** *We pack a variable number of spacecraft N_s such that they belong to the same formation and have bounded relative motion in the short term, while maintaining passive safety for N steps, by considering solutions to*

$$\min_{\delta\boldsymbol{\alpha}_{i,j},N_s} \quad \sum_{i\neq j=1}^{N_s} \|\delta\boldsymbol{\alpha}_{i,j}\|^2, \tag{5.41a}$$

$$s.t. \quad \boldsymbol{\alpha}_{\mathrm{c_i}} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\boldsymbol{\alpha}_{\mathrm{c}_j}}, \tag{5.41b}$$

$$\delta a_i \approx \delta a_j, \tag{5.41c}$$

$$\boldsymbol{\alpha}_{\mathrm{c}_i} \in \mathcal{X}^{\boldsymbol{\alpha}}, \tag{5.41d}$$

$$i,j = 1,\ldots,N_s,\ i \neq j. \tag{5.41e}$$

If N_s is fixed, this problem is no longer mixed-integer, but it remains nonlinear and non-convex. The inclusion of (5.41b) presents some challenges. These BRS are functions of the current optimization iteration and as such require recomputing within the actual

optimization itself, which can be computationally burdensome for large safety-horizons. If Keplerian dynamics are used, then this problem is greatly simplified as the $\delta a_i = \delta a_j$ results in the BRS collapsing to slices of the terminal set, as described earlier. That is, the problem dimensionality is reduced from six to three dimensions. Formation design with such constraints is much more tractable as only slices of $\mathcal{S}_k^{\text{oe}}$ need to be "separated."

In the event that J_2-invariant orbits are desired, we swap (5.41c) with the constraints that result in the spacecraft having matching mean orbit element rates, which then avoids relative secular growth between the spacecraft in the formation. The simple method to achieve such invariant orbits is by letting $\delta\bar{a} = \delta\bar{e} = \delta\bar{\imath} = 0$, but this restricts the admissible geometries. Other geometries can be considered by constraining $\dot{\bar{\Omega}}_{\text{d}} = \dot{\bar{\Omega}}_{\text{c}}$ and $\dot{\bar{M}}_{\text{d}} + \dot{\bar{\omega}}_{\text{d}} = \dot{\bar{M}}_{\text{c}} + \dot{\bar{\omega}}_{\text{c}}$, following the work in [69], which yields two equations and three unknowns or design variables.

5.7.2 Constellation Design

The general constellation design problem is particularly challenging, even with using the methods developed in this chapter. This is because when considering intersecting constellations, the potential impact velocities are on the order of km/s. As a result, mapping the set $\mathcal{S}$ from the Cartesian Hill frame to the orbital element difference space, $\mathcal{S}_k^{\text{oe}}$, is non-trivial. In this case, the nonlinearities cannot be neglected, which is done in the formation flying and design cases above. Given the rising interest in LEO constellations, there is a clear need to understand how densely a given constellation or a region of space could be packed while satisfying safety constraints. The general constellation packing problem, which aims to fit as many spacecraft in a constellation as possible while satisfying passive safety constraints, is defined below.

Definition 5.7.2 (Constellation Packing)**.** *The general N-step passively-safe constellation*

packing problem is given by

$$\min_{\boldsymbol{\mathfrak{oe}}_{\mathrm{c,i}},N_s} \quad \sum_{i\neq j=1}^{N_s} J(\delta\boldsymbol{\mathfrak{oe}}_{i,j}) \tag{5.42a}$$

$$s.t. \quad \boldsymbol{\mathfrak{oe}}_{\mathrm{c_i}} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\boldsymbol{\mathfrak{oe}}_{\mathrm{c}_j}}, \tag{5.42b}$$

$$\boldsymbol{c}(\boldsymbol{\mathfrak{oe}}_{\mathrm{c},i}) \leq \mathbf{0} \tag{5.42c}$$

$$\boldsymbol{\mathfrak{oe}}_{\mathrm{c},i} \in \mathcal{X}^{\boldsymbol{\mathfrak{oe}}} \tag{5.42d}$$

$$i,j = 1,\ldots,N_s \tag{5.42e}$$

where the number of spacecraft in the constellation N_s is variable and $J(\delta\boldsymbol{\mathfrak{oe}}_{i,j})$ can be a multi-objective function that weighs various mission objectives and $\boldsymbol{c}(\boldsymbol{\mathfrak{oe}}_{c,i}) \leq 0$ represents miscellaneous constellation constraints. As before, when $J(\delta\boldsymbol{\mathfrak{oe}}_{i,j}) = \|\delta\boldsymbol{\mathfrak{oe}}_{i,j}\|^2$, the spacecraft orbital element distances in $\mathcal{X}^{\boldsymbol{\mathfrak{oe}}}$ are minimized, which places them in orbits that are very close to each other. Solving this problem allows one to fit as many spacecraft as possible into a region of state-space, given the passive-safety constraints. When N_s is fixed, this problem is non-convex and nonlinear, and when it's variable, it is additionally a mixed-integer problem, which is computationally difficult to solve. Note again that $\mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)\big|_{\boldsymbol{\mathfrak{oe}}_{\mathrm{c}_j}}$ is itself a function of $\boldsymbol{\mathfrak{oe}}_{\mathrm{c}_j}$, and as such, reachable set computations are embedded into the optimization problem.

Constellations that are designed using (5.42) are inherently going to be safe for a time-horizon of $N\Delta T$. The problem above also serves as a primer to the space traffic management problem where inter-constellation safety is paramount. Generally speaking, the spacecraft considered need not belong to the same constellation.

5.7.2.1 Mean Elements: Matched period, Eccentricity, and Inclination

Here, we consider a special case where $\delta\bar{a} = \delta\bar{e} = \delta\bar{\imath} = 0$, that is, the mean semi-major axis, eccentricity, and inclination of the chief and deputy are the same. By considering slices along $\delta\bar{a} = \delta\bar{e} = \delta\bar{\imath} = 0$ of the perturbed BRS with J_2 using mean elements (5.29), i.e., using

$\delta\boldsymbol{\mathfrak{oe}}_{\mathrm{s}} = [0, 0, 0, \delta\bar{\Omega}, \delta\bar{\omega}, \delta\bar{M}]^{\mathsf{T}}$, one finds that for these design variables, the BRS collapse to slices of the terminal set again.

This yields a set a 3-dimensional set, which resides in $\mathbb{R}^6$

$$\mathcal{R}_b(N; \mathcal{S}_{k_{\mathrm{f}}}^{\bar{\mathfrak{oe}}})\big|_{\delta\bar{\boldsymbol{\mathfrak{oe}}}_s} = \{\delta\bar{\boldsymbol{\mathfrak{oe}}}_s \in \mathcal{X}^{\mathfrak{oe}} : H\delta\bar{\boldsymbol{\mathfrak{oe}}}_s \leq \boldsymbol{k}\} \tag{5.43}$$

and as a result of the slice, $\mathcal{R}_b(N; \mathcal{S}_{k_{\mathrm{f}}}^{\bar{\mathfrak{oe}}})\big|_{\delta\bar{\boldsymbol{\mathfrak{oe}}}_s} = \mathcal{S}_k^{\bar{\mathfrak{oe}}}\big|_{\delta\bar{\boldsymbol{\mathfrak{oe}}}_s}$, which holds for both the nonlinear and linearized equations of motion for the mean orbital elements with J_2 secular effects. Then, it becomes simple to design safe relative motion when matched mean period, eccentricity, and inclination by constraining

$$M\delta\bar{\boldsymbol{\mathfrak{oe}}}_{\mathrm{s}} \notin \bigcup_{k=0}^{N} \mathcal{S}_k^{\bar{\mathfrak{oe}}}\big|_{\delta\bar{\boldsymbol{\mathfrak{oe}}}_s}, \tag{5.44}$$

where M is a selection matrix, that isolates the last three components of $\delta\boldsymbol{\mathfrak{oe}}_{\mathrm{s}}$. This dimensionality reduction can be used to simplify (5.42), for example, and is leveraged for the purposes of constellation design later.

5.7.3 Orbital Slots

One of the main difficulties in space traffic management remains that of organizing constellations that already or will exist in such a way that passive safety is a strict requirement. To make the analysis and understanding of such problems more tractable, we introduce a new definition for an orbital slot that is based on the BRS.

Definition 5.7.3 (Orbital Slot)**.** *An orbital slot is a region in state-space, given by a convex set $\mathcal{S}$ around a spacecraft of interest whose state is given by $\boldsymbol{\mathfrak{oe}}_{\mathrm{c}}$, and its associated passively backwards reachable sets, i.e., $\mathcal{X}_{\mathrm{unsafe}}^{\mathrm{np}}(N)\big|_{\boldsymbol{\mathfrak{oe}}_{\mathrm{c}}}$.*

Defining a slot in terms of the BRS in $\mathcal{X}$ or $\mathcal{X}^{\mathfrak{oe}}$ guarantees then that no other spacecraft collide with this one for a certain number of time steps, i.e., at the very least short-term passive safety is guaranteed. A spacecraft may be designated a slot prior to launch or even

after, as these will have to be continuously updated due to perturbations and station-keeping requirements pertaining to the mission. As a consequence of the perturbing forces spacecraft are subjected to, orbital slots themselves have to be time-varying or dynamic.

Remark 13. *Embedding reachability analysis into the slot definition allows for the safe traffic management to be predictive or constructive rather than reactive, and as such, should be considered in future work.*

5.8 Results

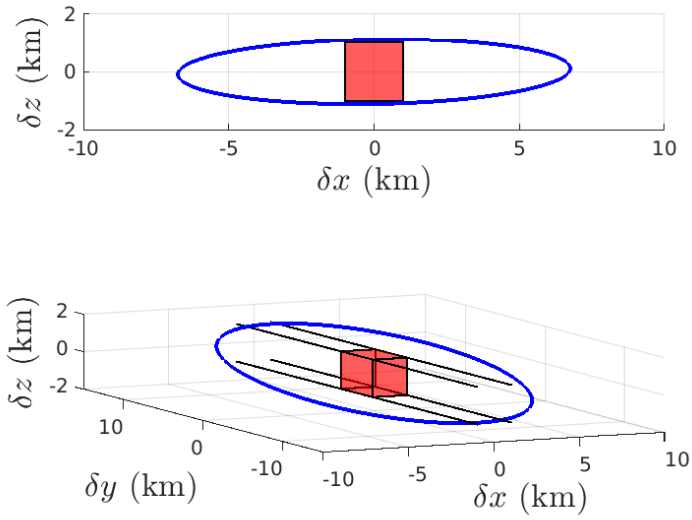
5.8.1 Formation Flying

Characterizing the BRS in terms of orbital element differences is mostly beneficial for the formation flying problem because **small** orbital element differences are considered. This in turn makes the usage of the linear mapping to express the set $\mathcal{S}$ in terms of $\delta\mathbf{oe}$ accurate to first order because high impact velocities, which need to be required in the constellation design problem, are not considered. The benefits of computing these sets in terms of $\delta\mathbf{oe}$ are that the linearization errors are smaller compared to the Cartesian Hill representation, making linearization domain larger. This has two interesting consequences, the first being that if one assumes additive white Gaussian process noise as in chapter 4, the true uncertainty of the relative states remains Gaussian for much longer, which ensures that both the stochastic unsafe sets and chance constraints are more accurate. Here, instead of repeating the work in chapter 4, we provide a few examples as to how these sets can be used for formation design.

Figure 5.7 demonstrates a relative orbit that is safe for an infinite amount of time under a Keplerian dynamics assumption. Here, $\delta a = 0$, which results in bounded and repeating relative orbits in the Keplerian case. If $\delta a \neq 0$, the safety ellipse in [68] is obtained, which is also safe for infinite time in an unperturbed environment. Similar observations are made in [24], where it is noted that having relative orbits that do not intersect the along-track axis

aid in maintaining passive safety. While such a relative orbit is not guaranteed to be safe for an infinite amount of time if perturbations are included, provided the shape properties of the deputy and chief are similar, such that non-conservative perturbations like differential drag or SRP are similar, the relative orbit may still be passively safe for a long time because as $\|\delta \boldsymbol{oe}\| \to 0$, then $\|\boldsymbol{a}_{\mathrm{d}} - \boldsymbol{a}_{\mathrm{c}}\| \to 0$, where $\boldsymbol{a}_{\mathrm{d}}$ and $\boldsymbol{a}_{\mathrm{c}}$ are the exogenous accelerations on the deputy and chief, respectively.

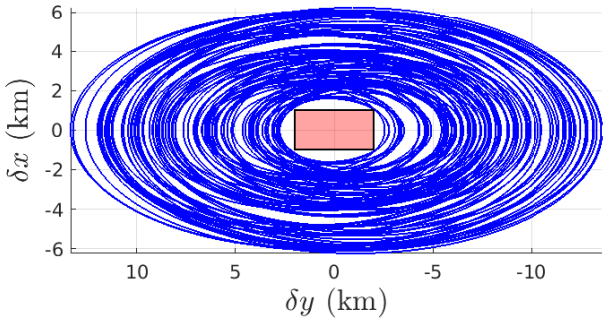
Figure 5.7: A safe relative orbit constrained by $\boldsymbol{x}(t_0) \notin \mathrm{proj}_{\mathcal{I}}(\bar{\mathcal{S}}^{\mathfrak{oe}})$, resulting in no intersections with the chief's orbit and along-track axis.



In Figure 5.8 we present various relative orbits that do not enter $\mathcal{S}$, shown in red, by considering slices $\delta\mathfrak{oe}_s = [0, \delta e, \delta i, \delta\Omega, \delta\omega, \delta M]^{\mathsf{T}}$ and constraining $\delta\mathfrak{oe}_{\mathrm{s}} \notin \bar{\mathcal{S}}^{\mathfrak{oe}}\big|_{\delta\mathfrak{oe}_{\mathrm{s}}}$. All of these relative orbits are generated by sampling in the safe region of the slices, which require sweeping $\mathcal{S}$ along the chief's orbit. Then, a single point solution in terms of $\delta\mathfrak{oe}$ results in a relative orbit that does not intersect $\mathcal{S}$ as shown in Figure 5.8. Such an approach is a promising way of tackling the formation packing problem (5.41).

Lastly, we consider a scenario using mean orbital element differences such that the deputy has a mean semi-major axis that is smaller than the chief's, resulting in a along-

Figure 5.8: Relative orbits with random initial states outside of the union matched-period sets, i.e., $\delta\bar{\mathbf{oe}}_{\mathrm{s}} \notin \bar{\mathcal{S}}^{\bar{\mathbf{oe}}_{\mathrm{s}}}\big|_{\delta\bar{\mathbf{oe}}_{\mathrm{s}}}$, resulting in no intersections of $\mathcal{S}$.



track flyby of the chief that does not enter $\mathcal{S}$. We select an initial condition such that $\delta\bar{\mathbf{oe}} \notin \mathcal{X}^{\mathrm{np}}_{\mathrm{unsafe}}(N)$, which is constructed with BRS using mean orbital element difference and J_2 secular effect, i.e., $\mathcal{R}_b(N; S_k^{\bar{\mathbf{oe}}})$. The initial condition is by design close to the unsafe region and as such, its trajectory barely misses the set $\mathcal{S}$, shown in 5.9. Here, the safety horizon N corresponds to two orbital periods, and as shown in Figure 5.9 the flyby is passively safe.

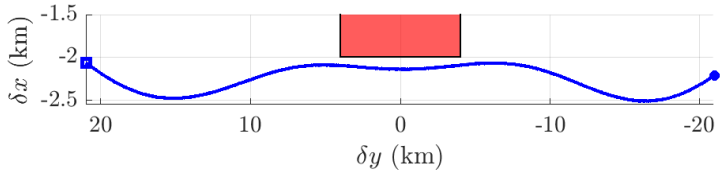
5.8.2 Constellation Design

While the BRS derived in this chapter are mostly applicable to formation flying scenarios, we consider a special case that allows us to utilize these sets for the sake of constellation design.

5.8.2.1 LEO Walker Constellation Design

Motivated by LEO Walker constellations such as SpaceX's Starlink constellation, we consider a case where the chief is in LEO with the orbital elements shown in Table 5.1. In this case, the deputy is a spacecraft on the same orbital plane as the chief or on an intersecting orbital plane. Both spacecraft have an orbital slot as defined in the prior section. The special case where $\delta\bar{a} = \delta\bar{e} = \delta\bar{\imath} = 0$, which is desired for many upcoming LEO constellations, results in the deputy's time-varying mean elements changing at the same rate as that of the chief,

Figure 5.9: A safe initial condition $\bar{\mathbf{oe}} \notin \mathcal{X}^{\mathrm{p}}_{\mathrm{unsafe}}(N)$, given by the mark on the right with respect to a near-circular chief $e_c = 0.05$. Here, $\delta\bar{a} < 0$ and in blue is the resulting trajectory after two orbital periods. The deputy passively drifts from right to left **underneath** the chief despite the effects of the J_2 perturbations.



i.e., $\dot{\bar{\Omega}}_{\mathrm{d}} = \dot{\bar{\Omega}}_{\mathrm{c}}$, $\dot{\bar{\omega}}_{\mathrm{d}} = \dot{\bar{\omega}}_{\mathrm{c}}$, and $\dot{\bar{M}}_{\mathrm{d}} = \dot{\bar{M}}_{\mathrm{c}}$. In this instance, the element drift rates are the same in both the nonlinear and linear (5.3) dynamic models. Because $\delta\dot{\bar{\Omega}} = \delta\dot{\bar{\omega}} = \delta\dot{\bar{M}} = 0$, we have time-invariant orbital element differences, i.e., $\delta\bar{\mathbf{oe}}_{k+1} = \delta\bar{\mathbf{oe}}_k$.

Table 5.1: Mean orbital elements of a near-circular chief in LEO

.

$\bar{a}_{\mathrm{c}}$ (km)	$\bar{e}_{\mathrm{c}}$	$\bar{\imath}_{\mathrm{c}}$ (°)	$\bar{\Omega}_{\mathrm{c}}$ (°)	$\bar{\omega}_{\mathrm{c}}$ (°)	$\bar{M}_{\mathrm{c}}$ (°)
6920.136	10^{-8}	53	0	0	0

Satisfaction of the constellation passive safety constraint (5.42b) is done via constraint (5.44), where the minimum safety horizon $N = k_{\mathrm{p}} - k_0$ corresponds to the number of time steps in the chief's osculating period. Now, because the deputy and chief have matching periods, letting $N \geq k_{\mathrm{p}} - k_0$ allows for the two craft to at least have two points of close approach.[1]

We perform the preliminary design of the constellation using mean elements with J_2 perturbations, which along with the two-body acceleration term, comprise the dominant forces acting on the spacecraft in the LEO regime of interest in Table 5.1. To this end, though in practice one uses $N \gg k_{\mathrm{p}} - k_0$ for multi-period safety, here, we simply enforce the constraints on the deputy to be safe for the following period, i.e., $N = k_{\mathrm{p}} - k_0$, which

[1] Due to the geometry of the deputy and chief here, the the union of slices in (5.44) contains many redundant constraints since in this constellation configuration, the deputy and the chief have two points of close approach.

limits the amount of sets used to characterize $\mathcal{X}^{\mathrm{p}}_{\mathrm{unsafe}}(N)$. Then, by virtue of the chosen orbital elements of the chief and deputy, to first order, the relative states are J_2-invariant [69]. The implication of this, in the safe constellation design case, is that the minimum distance between the craft is approximately the same for $t > t_0$, and thus, the deputy is passively safe for longer than the designed safety horizon N.

As seen in various LEO walker constellations, we let the deputy spacecraft have orbital elements such that $\delta\bar{a} = \delta\bar{e} = \delta\bar{i} = \delta\bar{\omega} = 0$. As such, $\delta\bar{\mathbf{oe}}_{\mathrm{s}} = [0, 0, 0, \delta\bar{\Omega}, 0, \delta\bar{M}]^{\mathsf{T}}$, which simplifies the structure of the non-convex constraints for safety to be maintained. For the constellation design scenario, we do not map the set $\mathcal{S}$ to the orbital element difference space because of the difficulties of the high impact velocities, which can occur at about 12 km/s in this LEO Walker example. However, we do note that if we had the non-convex set $\mathcal{S}^{\bar{\mathbf{oe}}}_k$ in this case, the slices along $\delta a = \delta e = \delta i = 0$ would still yield a BRS that is identically equal to slices of the terminal set $\mathcal{S}^{\bar{\mathbf{oe}}}_k$, by virtue of the dynamics model. This insight is then used to obtain a set of constraints that need to be satisfied to ensure passive safety of spacecraft within a constellation.

Recall that the set $\mathcal{S}$ is defined as $\mathcal{S} = \{\boldsymbol{x} \in \mathcal{X} : H\boldsymbol{x} \leq \boldsymbol{k}\}$. When one maps this set from Cartesian Hill frame relative states to mean orbital element differences is given by $\boldsymbol{h}(\boldsymbol{x}, t_k) : \mathcal{X} \mapsto \mathcal{X}^{\bar{\mathbf{oe}}}$, such that, $\delta\bar{\mathbf{oe}} = \boldsymbol{h}(\boldsymbol{x}, t_k)$. Then, using the inverse mapping, $\boldsymbol{h}^{-1}(\delta\bar{\mathbf{oe}}, t_k) : \mathcal{X}^{\bar{\mathbf{oe}}} \mapsto \mathcal{X}$, the non-convex set in terms of $\delta\bar{\mathbf{oe}}$ is obtained

$$\mathcal{S}^{\bar{\mathbf{oe}}}_{\mathrm{nl}} = \{\delta\bar{\mathbf{oe}} \in \mathcal{X}^{\bar{\mathbf{oe}}} : Hh^{-1}(\delta\bar{\mathbf{oe}}) \leq \boldsymbol{k}\}, \tag{5.45a}$$

which is not known analytically. This mapping is required for the general constellation passive safety scenario as the impact velocities are extremely high compared to formation flying scenarios. A constellation designer often selects a set of orbital planes via $\bar{\Omega}$ and $\bar{i}$ to satisfy mission, sensor or payload constraints, and as such, we assume such orbital planes have already been selected. Because five of the six mean orbital element differences are constrained, the passive safety between spacecraft in the constellation then depends on the

relative phase $\delta\bar{M}$, that is, the mean anomaly differences need to be chosen to avoid collisions between potentially intersecting orbits.

Instead of characterizing $\mathcal{S}_{\text{nl}}^{\bar{\text{oe}}}$ via samples or through approximations, in this work, the indicator function is used to determine the $\delta\bar{\text{oe}}$ that are contained in the Cartesian set $\mathcal{S}$. In this case,

$$\mathbb{1}_{\mathcal{S}}(\boldsymbol{x}) = \begin{cases} 1, \ \boldsymbol{x} = \boldsymbol{h}^{-1}(\delta\bar{\text{oe}}, t_k) \in \mathcal{S}, \\ \\ 0, \ \boldsymbol{x} = \boldsymbol{h}^{-1}(\delta\bar{\text{oe}}, t_k) \notin \mathcal{S}, \end{cases} \tag{5.46}$$

and if $\delta\bar{\text{oe}} = \delta\bar{\text{oe}}_s$ such that $\delta\bar{\text{oe}}_s = [0, 0, 0, \gamma, 0, \delta\bar{M}]^{\mathsf{T}}$, where γ is a selected mean ascending node difference, then $\delta\bar{\text{oe}}_s$ represents a 1-dimensional manifold in $\mathcal{X}^{\text{oe}}$ that depends only on $\delta\bar{M}$. Then, the set of unsafe $\delta\bar{M}$ is given by all $\delta\bar{\text{oe}}_s$ that satisfy

$$\mathbb{1}_{\mathcal{S}}(\boldsymbol{h}^{-1}(\delta\bar{\text{oe}}_{\text{s}}, t_k)) = 1, \ \exists k \in \{k_0, \ldots, k_{\text{p}}\}. \tag{5.47}$$

Consequently, the deputy's relative state $\delta\bar{\text{oe}}_{\text{s}}$ is said to be passively safe with respect to the chief if

$$\mathbb{1}_{\mathcal{S}}(\boldsymbol{h}^{-1}(\delta\bar{\text{oe}}_{\text{s}}, t_k)) = 0, \ \forall k = \{k_0, \ldots, k_{\text{p}}\}, \tag{5.48}$$

which is a $\delta\bar{M}$ phasing constraint.

5.8.2.2 Packing LEO Walker Constellations

In summary, instead of solving safe constellation design optimization (5.42) directly as a non-convex optimization problem, we consider a special scenario where the spacecraft in the constellation all have natched period, eccentricity, inclination, and argument of periapsis. This results in the passive safety constraint (5.48). We then pack the orbital planes under consideration as densely as possible using these phasing offets to obtain a Walker constellation that is passively safe for a long period of time. In this example, we have two intersecting orbital planes given by $\delta\bar{\Omega} = \pi$. This choice of the deputy's orbital elements results in the deputy and chief's inertial orbits approximately intersecting at two locations, at $M_{\text{c}} = 0$ and

$M_c = \pi$, shown in Figure 5.12.[2]

As noted in (5.48), a single deputy's relative phase $\delta\bar{M}$ must be sufficiently out of phase with the chief's mean anomaly to prevent it from entering $\mathcal{S}$. The unsafe $\delta\bar{M}$ for a deputy spacecraft on the same **mean** orbit as the chief, i.e., $\delta\bar{\Omega} = 0$, are shown in Figure 5.10, where $\boldsymbol{x}(\delta\bar{M})$ shows the explicit dependence of the states considered on the anomaly angle difference. In particular, Figure 5.10a - Figure 5.10b show the indicator function given variable $\delta\bar{M}$ and the corresponding relative states in the chief's Hill frame. The unsafe states clearly span the along-track direction of $\mathcal{S}$ as expected. The unsafe $\delta\bar{M}$ for a deputy spacecraft on a different orbit plane than the chief, i.e., $\delta\bar{\Omega} = \pi$, are shown in Figure 5.11. Figure 5.11a - Figure 5.11b show the indicator function given variable $\delta\bar{M}$ and the corresponding relative states in the chief's Hill frame. The unsafe states predominantly span the out of plane direction.

The minimum anomaly separation for the in-plane and out-of-plane cases are found using the analysis provided in Figures 5.10 - 5.11. From here, these phasing constraints can be used to pack satellites (deputies) in both orbital planes of the constellation, the results of which are shown in Figure 5.12. The phase differences allow us to pack the orbits with a total of 5804 spacecraft, maximizing the amount of spacecraft that fit in each orbit plane while respecting each others safety constraints. All of the spacecraft in this constellation are propagated forward in time and the minimum distance between spacecraft are monitored to check for safety, as shown in Figure 5.13. The minimum distance evolves over time but is predominantly around 4.5km and at times may be as high as 8km due to osculating effects. Figure 5.13 confirms that none of the spacecraft enter the avoidance regions $\mathcal{S}$ of other spacecraft in the constellation.

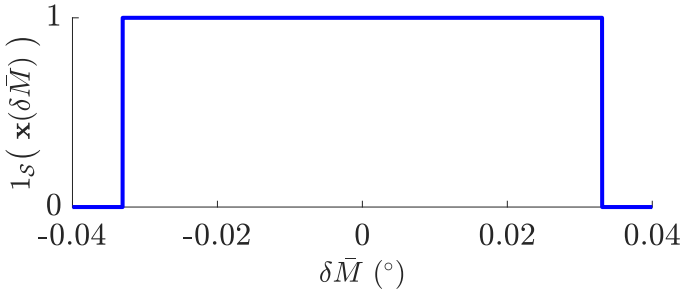
Such a solution can be interpreted as a feasible one for the constellation packing problem, given a specific set of orbital planes, and generalizes to more intersecting planes. The

[2] The orbits intersect exactly at two locations if they were circular and Keplerian dynamics are assumed, but in the near-circular and J_2 perturbed scenario, they have two points of close approach.

more planes there are, the larger the mean anomaly difference offsets have to be for the spacecraft in the constellation to be safe with respect to each other. From a traffic management point of view, as such orbit planes are increasingly packed, intersection of these planes becomes harder, which may not be desirable for launch services or for other missions that would need to be in similar areas of state-space. There is a clear trade-off between the density of a constellation and the "usability" of space for other spacecraft in the vicinity.

Figure 5.10: The unsafe $\delta\bar{M}$ given a deputy in the same mean orbit as the chief, i.e., $\delta\bar{\Omega} = 0$.

(a) The interval of $\delta\bar{M}$ that are contained in the set $\mathcal{S}$.



(b) The unsafe relative states, as a function of the mean anomaly difference $\boldsymbol{x}(\delta\bar{M})$, for a deputy in the same mean orbit as the chief is shown in blue in the chief's J_2-perturbed Hill frame.

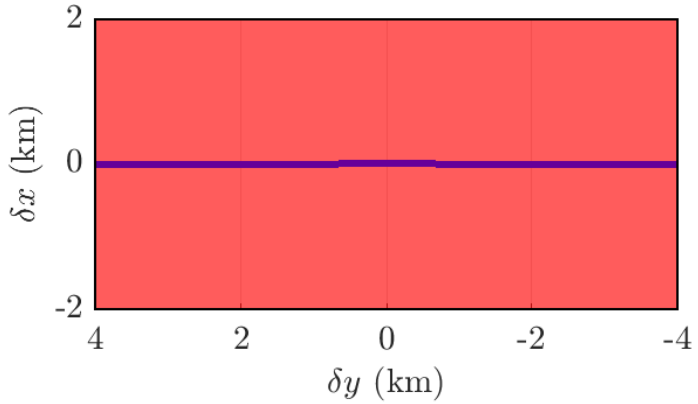
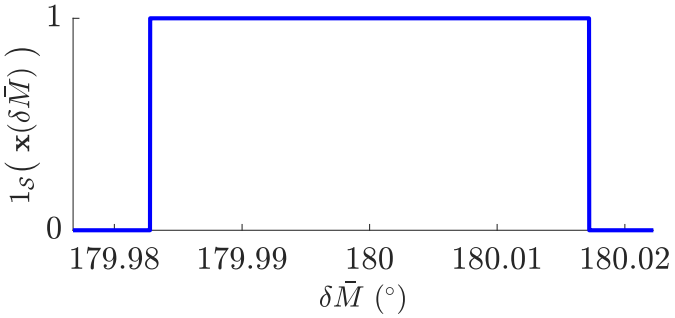


Figure 5.11: The unsafe $\delta\bar{M}$ given a deputy in a different mean orbit than chief, i.e., $\delta\bar{\Omega} = 0$.

(a) The interval of $\delta\bar{M}$ that are contained in the set $\mathcal{S}$.



(b) The unsafe relative states, as a function of the mean anomaly difference $\boldsymbol{x}(\delta\bar{M})$, for a deputy in a different mean orbit than the chief is shown in blue in the chief's J_2-perturbed Hill frame.

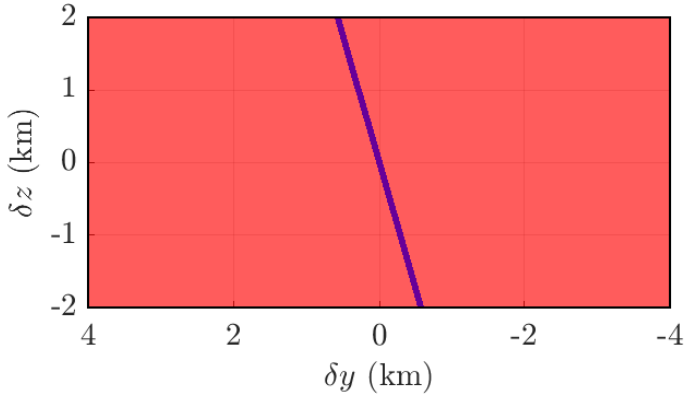


Figure 5.12: Initial states for a passively-safe constellation of 5804 spacecraft distributed along two intersecting orbital planes. In blue, the first orbit plane where each craft's orbital elements given by $\bar{\mathbf{oe}} = [6920.136\text{km}, 10^{-8}, 53°, 0°, 0°, M_i°]^\mathsf{T}$. The second orbit plane, in red, has $\bar{\mathbf{oe}} = [6920.136\text{km}, 10^{-8}, 53°, 180°, 0°, M_j°]^\mathsf{T}$. M_i and M_j depend on the spacecraft and satisfy the passive safety constraints.

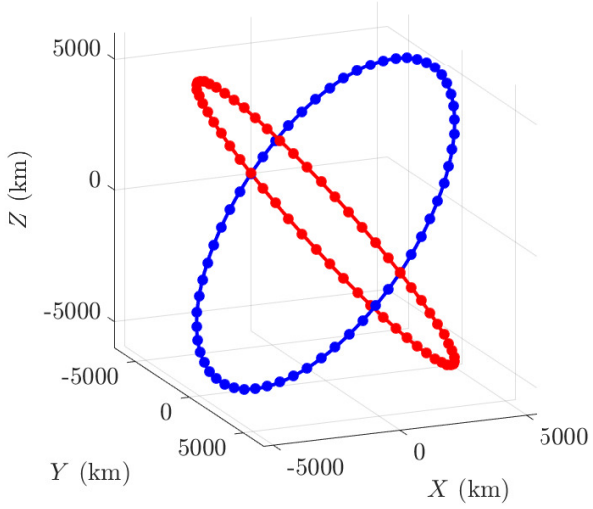
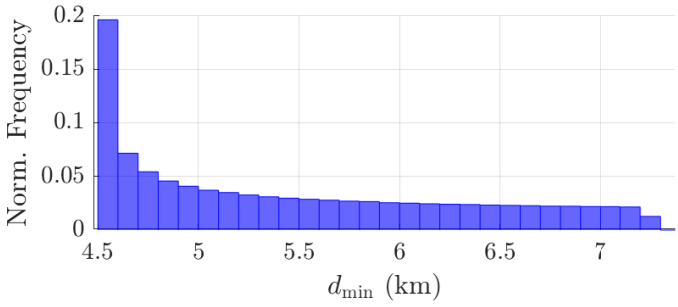


Figure 5.13: The minimum distances between spacecraft in the two orbit plane constellation when propagated with J_2 over a week. The minimum distance is always larger than 4.5 km by design, and as such the passive safety and slot constraints are satisfied.



Chapter 6

Conclusions

6.1 Passive and Active Abort-Safe Spacecraft Relative Motion

We develop an abort-safe control policy that is robust against hypothesized thruster failures in a spacecraft rendezvous mission for targets on generic elliptic orbits using robust backwards reachable sets and model predictive control. A fundamental contribution of this work is the demonstration of the existence of active or passive abort maneuvers outside of abort-unsafe sets, which is particularly novel in the active abort-safety scenario. Then, three convexification methods are presented, which are used to constrain the chaser to be outside of the unsafe region of state space. This guarantees, to the time-discretization used, that collisions with the target can be avoided through the use of a powered-abort or simply via natural motion. Several closed-loop simulations are presented for different failure scenarios, showing that the approach performs as predicted. Importantly, the algorithm works for generic LTV systems, resulting in its utility in other domains.

6.2 Fuel-Efficient Passive and Active Abort Safety

A safe rendezvous strategy that increasingly exploits the natural dynamics is presented. The work considers targets in near-Earth orbits as well as on NRHOs. A chaser spacecraft is steered into the constructed **coasting sets**, which contain the set of all states that have a high probability of naturally coasting into a specified goal set, while maintaining passive-safety. Stochastic passive backwards reachable sets are used to characterize the coasting

sets as well as the abort-unsafe state space; this contribution generalizes the prior one by incorporating random noise. The developed coasting arc approach reduces both the amount of propellant used and the required thruster on-time, important for thruster management and thruster fault mitigation during rendezvous and formation flying missions. In summary, a general and novel guidance and control algorithm is presented for future space missions, which is fuel-efficient, and is robust to disturbances.

6.3 Passive Abort-Safety using Orbital Element Differences

In the last chapter, the passively unsafe regions of state space with respect to a target set are obtained in terms of orbital element differences. This representation has smaller linearization errors making the derived PBRS more accurate and the linearizable domain larger. Such sets can be used with the methods in Chapters 3-4, to enhance the domain of the RPO algorithms developed. Moreover, by considering particular projections and slices of these sets, the dimensionality of the safe trajectory design problem is greatly reduced. Here, formation and constellation safety constraints are derived, which can inform how future constellations can best make use of certain regions of state space, and how these regions can be organized. A new orbital slot definition is also presented and illustrative design solutions are presented.

6.4 Broader Implications

While lots of work related to reachability theory has been done in the literature, the developed notions of abort-safety are novel and quite useful at large. How such sets can be used operationally is frequently not touched upon in the literature. In this thesis we developed algorithms that utilize and exploit such sets to guarantee, in discrete-time, the safety of the system under consideration. From an astrodynamics and astronautics perspective, the developed approaches can be used to verify future algorithm safety. By using convexification in the MPC, we further enable the algorithm's applications for on-board usage. The

solutions acquired can also be used as initial guesses to non-convex trajectory optimization solvers to improve the performance and safety of mission trajectory designs, with regards to RPOD, formations, and constellations.

The applications of abort-safety in general are not limited to spacecraft applications and could be of interest to general aerospace, robotics, automotive, maritime and potentially even biomedical industries. Naturally, motion-planning techniques at large can benefit from the safety constraints derived in this work. In such cases, abort-safety may guarantee collision avoidance between aerial or ground-based agents and can guarantee a boat's abort-safe entrance into a harbor. In the biomedical realm, an interesting application of such methods are in anaesthesia delivery and control, where we could guarantee the safety of the patient by ensuring that anaesthetic "aborts" exist so that dangerous regions of the pharmacological state space are avoided. In all of these cases, understanding where the abort-unsafe regions of state space are can result in improvements of system performance, and most importantly, safety. While control is often used as a feedback mechanism to optimally or correctly steer systems to exhibit desirable behaviors, it also makes sense that formal approaches are considered such that safe recovery of a system can be guaranteed with the control actions that one has.

6.5 Future Work

There are many potential future work directions that are directly related to this thesis. In the presented methods, stability of the safety constrained model predictive controller was not investigated. It would be interesting to consider approaches that incorporate reachability and stability constraints on the chaser to guarantee that the target is reachable under the available admissible control, despite the presence of the abort-safety constraints. While model predictive control was used as the algorithm of choice for the motion-planning and constrained feedback control in this thesis, alternative algorithms can be considered such as sampling-based methods. Such algorithms may be more effective in guiding the chaser

spacecraft into the coasting sets while avoiding the abort-unsafe regions of state space since the convexification approach used in this thesis can at times impedes the chaser from advancing towards the coasting sets. Moroever, the presented work could directly benefit RPOD mission planning by using the resulting trajectories from the MPC approach as an initial guess the full non-linear abort-safe optimal control problem, which would be particularly important in the passive abort-safety phase. Additionally, continuation methods could be used in conjunction with such approaches to obtain optimal solutions that tend from a quadratic cost function, as is used in this thesis, to an L1-norm cost function to optimize ΔV directly.

With respect to the final chapter, work needs to be done on describing the terminal sets $\mathcal{S}$ in terms of orbital element differences using the nonlinear mapping for cases with very high impact velocity, which are pertinent to the space traffic management and more general constellation design problem. This could for example be done by approximating the set $\mathcal{S}^{\text{oe}}$ using a union of convex sets, similar to how Gaussian mixtures are used to approximate multi-modal PDFs. From here, the PBRS could be computed which would yield a more accurate, albeit non-convex, PBRS. Such sets could be used to obtain optimal or sub-optimal solutions to the packing problems presented in the last chapter. Lastly, formal optimization or alternative heuristic-based solutions to the packing problems should be investigated to advance the state of the art in space traffic management.

Bibliography

[1] National Academies of Sciences, Engineering, and Medicine. "NASA Space Technology Roadmaps and Priorities Revisited". The National Academies Press, Washington, DC, 2016.

[2] Utku Eren, Anna Prach, Başaran Bahadır Koçer, Saša V Raković, Erdal Kayacan, and Behçet Açıkmeşe. Model predictive control in aerospace systems: Current state and opportunities. J. Guidance, Control, and Dynamics, 40(7):1541–1566, 2017.

[3] Emilio De Pasquale. Atv jules verne: a step by step approach for in- orbit demonstration of new rendezvous technologies. In SpaceOps Conference. 2012.

[4] Piero Miotto. Designing and validating proximity operations rendezvous and approach trajectories for the cygnus mission. In AIAA Guidance, Navigation, and Control Conference. 2010.

[5] Angel Flores-Abad, Ou Ma, Khanh Pham, and Steve Ulrich. A review of space robotics technologies for on-orbit servicing. Progress in Aerospace Sciences, 68:1–26, 2014.

[6] N. T. Redd. Bringing satellites back from the dead: Mission extension vehicles give defunct spacecraft a new lease on life - [news]. IEEE Spectrum, 57(8):6–7, 2020.

[7] Joseph A Starek, Behçet Açıkmeşe, Issa A Nesnas, and Marco Pavone. Spacecraft autonomy challenges for next-generation space missions. In Adv. in Control System Technology for Aerospace Applications, pages 1–48. Springer, 2016.

[8] Wigbert Fehse. Automated Rendezvous and Docking of Spacecraft. Cambridge Aerospace Series. Cambridge University Press, 2003.

[9] Louis S Breger and Jonathan P How. Safe trajectories for autonomous rendezvous of spacecraft. J. Guidance, Control, and Dynamics, 31(5):1478–1489, 2008.

[10] Matthias Althoff. Reachability analysis and its application to the safety assessment of autonomous cars. PhD thesis, Technische Universität München, 2010.

[11] Abraham P. Vinod. Scalable Stochastic Reachability: Theory, Computation, and Control. PhD thesis, The University of New Mexico, 2018.

[12] Marcus J Holzinger, Daniel J Scheeres, and John Hauser. Reachability using arbitrary performance indices. IEEE Transactions on Automatic Control, 60(4):1099–1103, 2015.

[13] Somil Bansal, Mo Chen, Sylvia Herbert, and Claire J Tomlin. Hamilton-jacobi reachability: A brief overview and recent advances. In IEEE Conf. Decision and Control, pages 2242–2253, 2017.

[14] Abraham P Vinod and Meeko MK Oishi. Optimal trade-off analysis for efficiency and safety in the spacecraft rendezvous and docking problem. IFAC-PapersOnLine, 51(12):136–141, 2018.

[15] Matthias Althoff. An introduction to cora 2015. In Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems, 2015.

[16] M. J. Holzinger and D. J. Scheeres. Reachability results for nonlinear systems with ellipsoidal initial sets. IEEE Trans. on Aerospace and Electronic Systems, 48(2):1583–1600, 2012.

[17] Marcus Holzinger and Daniel Scheeres. Applied reachability for space situational awareness and safety in spacecraft proximity operations. In AIAA Guidance, Navigation, and Control Conf., page 6096, 2009.

[18] John N. Maidens, Shahab Kaynama, Ian M. Mitchell, Meeko M.K. Oishi, and Guy A. Dumont. Lagrangian methods for approximating the viability kernel in high-dimensional systems. Automatica, 49(7):2017–2029, 2013.

[19] Alessandro Abate, Maria Prandini, John Lygeros, and Shankar Sastry. Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica, 44(11):2724–2734, 2008.

[20] Abraham P. Vinod and Meeko M. K. Oishi. Probabilistic occupancy via forward stochastic reachability for markov jump affine systems. IEEE Transactions on Automatic Control, 66(7):3068–3083, 2021.

[21] M. J. Holzinger and M. K. Jah. Challenges and potential in space domain awareness. Journal of Guidance, Control, and Dynamics, 41(1):15–18, 2018.

[22] Joseph W Gangestad. Orbital slots for everyone? Center for Space Policy & Strategy, The Aerospace Corporation, March, 2017.

[23] Adam W Koenig and Simone D'Amico. Robust and safe n-spacecraft swarming in perturbed near-circular orbits. J. Guidance, Control, and Dynamics, 41(8):1643–1662, 2018.

[24] Marcus Holzinger, Jeremiah DiMatteo, Jeremy Schwartz, and Mark Milam. Passively safe receding horizon control for satellite proximity operations. In IEEE Conf. Decision and Control, pages 3433–3440, 2008.

[25] Edward N Hartley, Paul A Trodden, Arthur G Richards, and Jan M Maciejowski. Model predictive control system design and implementation for spacecraft rendezvous. Control Eng. Practice, 20(7):695–713, 2012.

[26] M Saponara, V Barrena, Alberto Bemporad, EN Hartley, Jan M Maciejowski, A Richards, A Tramutola, and P Trodden. Model predictive control application to spacecraft rendezvous in mars sample return scenario. In Progress in Flight Dynamics, Guidance, Navigation, Control, Fault Detection, and Avionics, volume 6, pages 137–158. EDP Sciences, 2013.

[27] Greg Chavers, Nantel Suzuki, Marshall Smith, Lisa Watson-Morgan, Steven W Clarke, Walter C Engelund, Lindsay Aitchison, Shawn McEniry, Laura Means, Michael DeKlotz, et al. NASA's human lunar landing strategy. In 70th Int. Astronautical Congress, IAF Human Spaceflight Symposium, 2019.

[28] Joseph D Gleason. Software Design for Probabilistic Safety: Stochastic Reachability and Circadian Control. PhD thesis, 2019.

[29] Abraham P Vinod, Baisravan HomChaudhuri, and Meeko MK Oishi. Forward stochastic reachability analysis for uncontrolled linear systems using fourier transforms. In Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control, pages 35–44, 2017.

[30] Baisravan HomChaudhuri, Meeko Oishi, Matt Shubert, Morgan Baldwin, and R Scott Erwin. Computing reach-avoid sets for space vehicle docking under continuous thrust. In IEEE Conf. Decision and Control, pages 3312–3318, 2016.

[31] Abraham P Vinod, Joseph D Gleason, and Meeko MK Oishi. Sreachtools: A matlab stochastic reachability toolbox. In Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control, pages 33–38, 2019.

[32] Kendra Lesser, Meeko Oishi, and R Scott Erwin. Stochastic reachability for control of spacecraft relative motion. In IEEE Conf. Decision and Control, pages 4705–4712, 2013.

[33] Abraham P. Vinod and Meeko M.K. Oishi. Optimal trade-off analysis for efficiency and safety in the spacecraft rendezvous and docking problem. IFAC-PapersOnLine, 51(12):136–141, 2018. IFAC Workshop on Networked Autonomous Air Space Systems NAASS 2018.

[34] Nikolaos Kariotoglou, Kostas Margellos, and John Lygeros. On the computational complexity and generalization properties of multi-stage and stage-wise coupled scenario programs. Systems & Control Letters, 94:63–69, 2016.

[35] Hossein Sartipizadeh, Abraham P Vinod, Behçet Açikmeşe, and Meeko Oishi. Voronoi partition-based scenario reduction for fast sampling-based stochastic reachability computation of linear systems. In 2019 American Control Conference (ACC), pages 37–44. IEEE, 2019.

[36] Matt Shubert, Meeko Oishi, Morgan Baldwin, and R Scott Erwin. Under-approximating reach-avoid sets for space vehicle maneuvering in the presence of debris. IFAC, 51(12):142–147, 2018.

[37] Dimitri P Bertsekas et al. Dynamic programming and optimal control: Vol. 1. Athena scientific Belmont, 2000.

[38] Dimitri P Bertsekas and Steven E Shreve. Stochastic optimal control: the discrete-time case, volume 5. Athena Scientific, 1996.

[39] Joseph D. Gleason, Abraham P. Vinod, and Meeko M.K. Oishi. Lagrangian approximations for stochastic reachability of a target tube. Automatica, 128:109546, 2021.

[40] D.P. Bertsekas and I.B. Rhodes. On the minimax reachability of target sets and target tubes. Automatica, 7(2):233–247, 1971.

[41] Abraham P Vinod and Meeko MK Oishi. Stochastic reachability of a target tube: Theory and computation. Automatica, 125:109458, 2021.

[42] Sean Summers and John Lygeros. Verification of discrete time stochastic hybrid systems: A stochastic reach-avoid decision problem. Automatica, 46(12):1951–1961, 2010.

[43] Donald E Kirk. Optimal control theory: an introduction. Courier Corporation, 2004.

[44] James M Longuski, José J Guzmán, and John E Prussing. Optimal control with aerospace applications. Springer, 2014.

[45] Bruce A Conway. Spacecraft trajectory optimization, volume 29. Cambridge University Press, 2010.

[46] M. Mammarella, M. Lorenzen, E. Capello, H. Park, F. Dabbene, G. Guglieri, M. Romano, and F. Allgöwer. An offline-sampling smpc framework with application to autonomous space maneuvers. IEEE Trans. on Control Systems Technology, 28(2):388–402, 2020.

[47] Avishai Weiss, Morgan Baldwin, Richard Scott Erwin, and Ilya Kolmanovsky. Model predictive control for spacecraft rendezvous and docking: Strategies for handling constraints and case studies. IEEE Trans. Control Systems Technology, 23(4):1638–1647, 2015.

[48] B. P. Malladi, S. Di Cairano, and A. Weiss. Nonlinear model predictive control of coupled rotational-translational spacecraft relative motion. In Proc. American Control Conf., pages 3581–3586, 2019.

[49] Geoffrey T Huntington and Anil V Rao. Comparison of global and local collocation methods for optimal control. Journal of guidance, control, and dynamics, 31(2):432–436, 2008.

[50] Michael A Patterson and Anil V Rao. Gpops-ii: A matlab software for solving multiple-phase optimal control problems using hp-adaptive gaussian quadrature collocation methods and sparse nonlinear programming. ACM Transactions on Mathematical Software (TOMS), 41(1):1–37, 2014.

[51] John T Betts. Practical methods for optimal control and estimation using nonlinear programming. SIAM, 2010.

[52] Matthew W Harris and Behçet Açıkmeşe. Lossless convexification of non-convex optimal control problems for state constrained linear systems. Automatica, 50(9):2304–2311, 2014.

[53] Yuanqi Mao, Daniel Dueri, Michael Szmuk, and Behçet Açıkmeşe. Successive convexification of non-convex optimal control problems with state constraints. IFAC-PapersOnLine, 50(1):4063–4069, 2017.

[54] I. Michael Ross. Space trajectory optimization and L1-optimal control problems. Elsevier Astrodynamics Series, 1(1):1–14, 2006.

[55] Edward N Hartley, Marco Gallieri, and Jan M Maciejowski. Terminal spacecraft rendezvous and capture with lasso model predictive control. Int. J. Control, 86(11):2104–2113, 2013.

[56] Kyle Alfriend. Nonlinear Considerations In Satellite Formation Flying.

[57] John L Junkins, Maruthi R Akella, and Kyle T Alfrined. Non-gaussian error propagation in orbital mechanics. Guidance and control 1996, pages 283–298, 1996.

[58] Kyle Alfriend, Srinivas Rao Vadali, Pini Gurfil, Jonathan How, and Louis Breger. Spacecraft formation flying: Dynamics, control and navigation, volume 2. Elsevier, 2009.

[59] Glenn Peterson, Marlon Sorge, and William Ailor. Space traffic management in the age of new space. The Aerospace Corporation. Center for Space Policy and Strategy, 2018.

[60] Nathan Reiland, Aaron J. Rosengren, Renu Malhotra, and Claudio Bombardelli. Assessing and minimizing collisions in satellite mega-constellations. Advances in Space Research, 67(11):3755–3774, 2021. Satellite Constellations and Formation Flying.

[61] Claudio Bombardelli, Gabriele Falco, Davide Amato, and Aaron J. Rosengren. Space occupancy in low-earth orbit. Journal of Guidance, Control, and Dynamics, 44(4):684–700, 2021.

[62] Jeremy John Davis. Constellation reconfiguration: Tools and analysis. Texas A&M University, 2010.

[63] Sung Wook Paek, Luzius G Kronig, Anton B Ivanov, and Olivier L de Weck. Satellite constellation design algorithm for remote sensing of diurnal cycles phenomena. Advances in Space Research, 62(9):2529–2550, 2018.

[64] Yuri Ulybyshev. Satellite constellation design for complex coverage. Journal of Spacecraft and Rockets, 45(4):843–849, 2008.

[65] Adam W. Koenig and Simone D'Amico. Robust and safe N-spacecraft swarming in perturbed near-circular orbits. Journal of Guidance, Control, and Dynamics, 41(8):1643–1662, 2018.

[66] Adam W. Koenig and Simone D'Amico. Safe spacecraft swarm deployment and acquisition in perturbed near-circular orbits subject to operational constraints. Acta Astronautica, 153(January):297–310, 2018.

[67] Simone D'Amico and Oliver Montenbruck. Proximity operations of formation-flying spacecraft using an eccentricity/inclination vector separation. Journal of Guidance, Control, and Dynamics, 29(3):554–563, 2006.

[68] Christopher WT Roscoe, Jason J Westphal, Jacob D Griesbach, and Hanspeter Schaub. Formation establishment and reconfiguration using differential elements in j2-perturbed orbits. In 2014 IEEE Aerospace Conference, pages 1–19. IEEE, 2014.

[69] John L Junkins and Hanspeter Schaub. Analytical mechanics of space systems. American Institute of Aeronautics and Astronautics, 2009.

[70] M. Althoff, O. Stursberg, and M. Buss. Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization. In IEEE Conf. Decision and Control, pages 4042–4048, 2008.

[71] Matthias Althoff, Olaf Stursberg, and Martin Buss. Reachability analysis of nonlinear systems with uncertain parameters using conservative linearization. In 2008 47th IEEE Conference on Decision and Control, pages 4042–4048, 2008.

[72] Costantinos Zagaris and Marcello Romano. Reachability analysis of planar spacecraft docking with rotating body in close proximity. J. Guidance, Control, and Dynamics, 41(6):1416–1422, 2018.

[73] Colas Le Guernic and Antoine Girard. Reachability analysis of linear systems using support functions. Nonlinear Analysis: Hybrid Systems, 4(2):250–262, 2010. IFAC World Congress 2008.

[74] Matthias Althoff, Colas Le Guernic, and Bruce H Krogh. Reachable set computation for uncertain time-varying linear systems. In Proc. 14th int. conf. Hybrid systems: computation and control, pages 93–102, 2011.

[75] Elad Denenberg and Pini Gurfil. Debris avoidance maneuvers for spacecraft in a cluster. J. Guidance, Control, and Dynamics, 40(6):1428–1440, 2017.

[76] Arthur Richards, Tom Schouwenaars, Jonathan P How, and Eric Feron. Spacecraft trajectory planning with avoidance constraints using mixed-integer linear programming. J. Guidance, Control, and Dynamics, 25(4):755–764, 2002.

[77] Joseph A Starek, Edward Schmerling, Gabriel D Maher, Brent W Barbee, and Marco Pavone. Fast, safe, propellant-efficient spacecraft motion planning under clohessy–wiltshire–hill dynamics. J. Guidance, Control, and Dynamics, 40(2):418–438, 2016.

[78] Avishai Weiss, Christopher Petersen, Morgan Baldwin, R Scott Erwin, and Ilya Kolmanovsky. Safe positively invariant sets for spacecraft obstacle avoidance. J. Guidance, Control, and Dynamics, 38(4):720–732, 2015.

[79] Leonel Palacios, Matteo Ceriotti, and Gianmarco Radice. Close proximity formation flying via linear quadratic tracking controller and artificial potential function. Adv. in Space Research, 56(10):2167–2176, 2015.

[80] S. Di Cairano, H. Park, and I. Kolmanovsky. Model predictive control approach for guidance of spacecraft rendezvous and proximity maneuvering. Int. J. Robust and Nonlinear Control, 22(12):1398–1427, 2012.

[81] Francisco Gavilan, Rafael Vazquez, and Eduardo F. Camacho. Chance-constrained model predictive control for spacecraft rendezvous with disturbance estimation. Control Eng Practice, 20(2):111–122, 2012.

[82] M. Mammarella, E. Capello, H. Park, G. Guglieri, and M. Romano. Tube-based robust model predictive control for spacecraft proximity operations in the presence of persistent disturbance. Aerospace Science and Technology, 77:585–594, 2018.

[83] D. Aguilar Marsillach, S. Di Cairano, and A. Weiss. Fail-safe rendezvous control on elliptic orbits using reachable sets. In Proc. American Control Conf., pages 4920–4925, 2020.

[84] D. Aguilar Marsillach, S. Di Cairano, and A. Weiss. Abort-safe spacecraft rendezvous in case of partial thrust failure. In IEEE Conf. Decision and Control, pages 1490–1495, 2020.

[85] Howard D. Curtis. Chapter 7 - relative motion and rendezvous. In Howard D. Curtis, editor, Orbital Mechanics for Engineering Students (Third Edition), pages 367–404. Butterworth-Heinemann, Boston, third edition edition, 2014.

[86] Franco Blanchini and Stefano Miani. Set-Theoretic Methods in Control. Birkhäuser Basel, 1st edition, 2007.

[87] Stephen Boyd and Lieven Vandenberghe. Convex Optimization. Cambridge University Press, 2004.

[88] Michael Szmuk, Taylor P. Reynolds, and Behçet Açıkmeşe. Successive convexification for real-time six-degree-of-freedom powered descent guidance with state-triggered constraints. J. Guidance, Control, and Dynamics, 43(8):1399–1413, 2020.

[89] Francesco Borrelli, Alberto Bemporad, and Manfred Morari. Predictive Control for Linear and Hybrid Systems. Cambridge University Press, 2017.

[90] Jean-Pierre Aubin, Alexandre M Bayen, and Patrick Saint-Pierre. Viability theory: new directions. Springer Science & Business Media, 2011.

[91] Stefano Di Cairano and Ilya V Kolmanovsky. Real-time optimization and model predictive control for aerospace and automotive applications. In American control conference (ACC), pages 2392–2409, 2018.

[92] Danylo Malyuta, Taylor Reynolds, Michael Szmuk, Behcet Acikmese, and Mehran Mesbahi. Fast trajectory optimization via successive convexification for spacecraft rendezvous with integer constraints. In AIAA Scitech Forum, 2020.

[93] Ilya Kolmanovsky and Elmer G Gilbert. Theory and computation of disturbance invariant sets for discrete-time linear systems. Mathematical problems in engineering, 4, 1998.

[94] Giordana Bucchioni and Mario Innocenti. Open loop safe trajectory design for cislunar NRHO rendezvous. In American Control Conf., pages 4337–4342, 2020.

[95] Emmanuel Blazquez, Laurent Beauregard, Stéphanie Lizy-Destrez, Finn Ankersen, and Francesco Capolupo. Rendezvous design in a cislunar near rectilinear halo orbit. The Aeronautical Journal, 124(1276):821–837, 2020.

[96] Julio C Sanchez, Francisco Gavilan, and Rafael Vazquez. Chance-constrained model predictive control for near rectilinear halo orbit spacecraft rendezvous. Aerospace Science and Technology, 2020.

[97] Joseph D Gleason, Abraham P Vinod, and Meeko MK Oishi. Underapproximation of reach-avoid sets for discrete-time stochastic systems via lagrangian methods. In 2017 IEEE 56th Annual Conference on Decision and Control (CDC), pages 4283–4290. IEEE, 2017.

[98] Daniel Aguilar Marsillach, Stefano Di Cairano, Uroš Kalabić, and Avishai Weiss. Fail-safe spacecraft rendezvous on near-rectilinear halo orbits. In 2021 American Control Conference (ACC), pages 2980–2985. IEEE, 2021.

[99] Vivek Muralidharan, Avishai Weiss, and Uros V Kalabic. Control strategy for long-term station-keeping on near-rectilinear halo orbits. In AIAA Scitech Forum, 2020.

[100] C Davis, SA Bhatt, KC Howell, J Jang, R Whitley, FD Clark, D Guzzetti, EM Zimovan, and GH Barton. Orbit maintenance and navigation of human spacecraft at cislunar near rectilinear halo orbits, 27th aas. In AIAA Space Flight Mechanics Meet., 2017.

[101] RH Lyddane. Small eccentricities or inclinations in the brouwer theory of the artificial satellite. The Astronomical Journal, 68:555, 1963.

[102] Dirk Brouwer. Solution of the problem of artificial satellite theory without drag. , 64:378, November 1959. Provided by the SAO/NASA Astrophysics Data System.

[103] Louis Breger and Jonathan How. J2-modified gve-based mpc for formation flying spacecraft. In AIAA Guidance, Navigation, and Control Conference and Exhibit, page 5833, 2005.

[104] David A Vallado. Fundamentals of astrodynamics and applications, volume 12. Springer Science & Business Media, 2001.

[105] Donald T. Greenwood. Advanced Dynamics. Cambridge University Press, 2003.

Appendix A

Alternative Dynamical Models

A.1 Linearized relative equations of motion for perturbed chaser and target in target's Hill Frame

Perturbations can in general be added the nonlinear Cartesian equations of relative motion, as seen by the target. Recall that

$$\boldsymbol{r}_{\mathrm{c/b}} = \boldsymbol{r}_{\mathrm{t/b}} + \boldsymbol{\rho} \tag{A.1}$$

where $\boldsymbol{\rho} = \boldsymbol{r}_{\mathrm{c/t}}$ For now, we neglect attitude-dependent perturbations and consider conservative forces. The relative acceleration as seen by the target is then

$$\overset{t..}{\boldsymbol{\rho}} = \overset{I..}{\boldsymbol{r}}_{\mathrm{c/b}} + \boldsymbol{a}_{\mathrm{c}} + \boldsymbol{u}_{\mathrm{c}} - (\overset{I..}{\boldsymbol{r}}_{\mathrm{t/b}} + \boldsymbol{a}_{\mathrm{t}}) - \overset{I.}{\boldsymbol{\omega}}_{t/e} \times \boldsymbol{\rho} - 2\boldsymbol{\omega}_{t/e} \times \overset{t.}{\boldsymbol{\rho}} - \boldsymbol{\omega}_{\boldsymbol{t/e}} \times (\boldsymbol{\omega}_{t/e} \times \boldsymbol{\rho}) \tag{A.2}$$

$$\overset{t..}{\boldsymbol{\rho}} = -\frac{\mu \boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3} + \boldsymbol{a}_{\mathrm{c}} + \boldsymbol{u}_{\mathrm{c}} + \frac{\mu \boldsymbol{r}_{\mathrm{t/b}}}{\|\boldsymbol{r}_{\mathrm{t/b}}\|^3} - \boldsymbol{a}_{\mathrm{t}} - \overset{I.}{\boldsymbol{\omega}}_{t/e} \times \boldsymbol{\rho} - 2\boldsymbol{\omega}_{t/e} \times \overset{t.}{\boldsymbol{\rho}} - \boldsymbol{\omega}_{t/e} \times (\boldsymbol{\omega}_{t/e} \times \boldsymbol{\rho}) \tag{A.3}$$

$$\overset{t..}{\boldsymbol{\rho}} = -\frac{\mu \boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3} + \boldsymbol{a}_{\mathrm{c}} + \boldsymbol{u}_{\mathrm{c}} + \frac{\mu \boldsymbol{r}_{\mathrm{t/b}}}{\|\boldsymbol{r}_{\mathrm{t/b}}\|^3} - \boldsymbol{a}_{\mathrm{t}} - [\overset{I.}{\boldsymbol{\omega}}_{t/e}]_{\times} \boldsymbol{\rho} - [2\boldsymbol{\omega}_{t/e}]_{\times} \overset{t.}{\boldsymbol{\rho}} - [\boldsymbol{\omega}_{t/e}]_{\times} [\boldsymbol{\omega}_{t/e}]_{\times} \boldsymbol{\rho} \tag{A.4}$$

Note that since the target is no longer in a Keplerian orbit, its Hill frame angular velocity is

$$\boldsymbol{\omega}_{t/e} = \frac{\boldsymbol{h}_{\mathrm{t}}}{\|\boldsymbol{r}_{\mathrm{t/b}}\|^2} + \frac{\boldsymbol{r}_{\mathrm{t/b}}}{\|\boldsymbol{h}_{\mathrm{t}}\|} (\hat{\boldsymbol{h}}_{\mathrm{t}} \cdot \boldsymbol{a}_{\mathrm{t}}) \tag{A.5}$$

We need to take the inertial derivative of this quantity to derive the perturbed Cartesian relative equations of motion. In this thesis, we considered cases where the target and the

chaser are subjected have luni-solar and J2 perturbations, that is,

$$\boldsymbol{a}_{\mathrm{t}} = \boldsymbol{a}_{J2} + \boldsymbol{a}_{lunar} + \boldsymbol{a}_{solar}, \tag{A.6}$$

$$\boldsymbol{a}_{\mathrm{c}} = \boldsymbol{a}_{J2} + \boldsymbol{a}_{lunar} + \boldsymbol{a}_{solar}. \tag{A.7}$$

Note that the perturbing acceleration on the target is included in (A.5) such that the time-derivative of the perturbing accelerations (i.e. jerk) is required. That is, we also need

$$\overset{I.}{\boldsymbol{a}}_{\mathrm{t}} = \overset{I.}{\boldsymbol{a}}_{J2} + \overset{I.}{\boldsymbol{a}}_{lunar} + \overset{I.}{\boldsymbol{a}}_{solar} \ . \tag{A.8}$$

The linearized relative perturbed equations of motion are then obtained by taking the Jacobian of (A.2) with respect to variations in the relative state $\begin{bmatrix} \boldsymbol{\rho} & \overset{t.}{\boldsymbol{\rho}} \end{bmatrix}^{\mathsf{T}}$. Since the relative acceleration is given as

$$\overset{t..}{\boldsymbol{\rho}} = -\frac{\mu \boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3} + \boldsymbol{a}_{\mathrm{c}} + \boldsymbol{u}_{\mathrm{c}} + \frac{\mu \boldsymbol{r}_{\mathrm{t/b}}}{\|\boldsymbol{r}_{\mathrm{t/b}}\|^3} - \boldsymbol{a}_{\mathrm{t}} - [\overset{I.}{\boldsymbol{\omega}}_{t/e}]_{\times}\boldsymbol{\rho} - [2\boldsymbol{\omega}_{t/e}]_{\times}\overset{t.}{\boldsymbol{\rho}} - [\boldsymbol{\omega}_{t/e}]_{\times}[\boldsymbol{\omega}_{t/e}]_{\times}\boldsymbol{\rho}, \tag{A.9}$$

we take partial derivatives of this expression with respect to the relative position and velocity, yielding,

$$\frac{\partial \overset{t..}{\boldsymbol{\rho}}}{\partial \boldsymbol{\rho}} = -\frac{\partial}{\partial \boldsymbol{\rho}}\left(\frac{\mu \boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3}\right) + \frac{\partial \boldsymbol{a}_{\mathrm{c}}}{\partial \boldsymbol{\rho}} - [\overset{I.}{\boldsymbol{\omega}}_{t/e}]_{\times} - [\boldsymbol{\omega}_{t/e}]_{\times}[\boldsymbol{\omega}_{t/e}]_{\times} \in \mathbb{R}^{3\times 3} \tag{A.10}$$

$$\frac{\partial \overset{t..}{\boldsymbol{\rho}}}{\partial \overset{t.}{\boldsymbol{\rho}}} = -2[\boldsymbol{\omega}_{t/e}]_{\times} \in \mathbb{R}^{3\times 3} \tag{A.11}$$

Our perturbations are only chaser position-dependent. Since we linearize about the target's perturbed trajectory we obtain

$$\dot{\boldsymbol{x}}(t) = A(t)\boldsymbol{x}(t) + B(t)u(t) \tag{A.12}$$

where,

$$A(t) = \frac{\partial}{\partial \boldsymbol{x}} f(t, \boldsymbol{x}, \boldsymbol{p})\Big|_{\boldsymbol{x}=\boldsymbol{0}} = \begin{bmatrix} 0_{3\times 3} & I_3 \\ -\frac{\partial}{\partial \boldsymbol{\rho}}\left(\frac{\mu \boldsymbol{r}_{\mathrm{c/b}}}{\|\boldsymbol{r}_{\mathrm{c/b}}\|^3}\right) + \frac{\partial \boldsymbol{a}_{\mathrm{c}}}{\partial \boldsymbol{\rho}} - [\overset{I.}{\boldsymbol{\omega}}_{t/e}]_{\times} - [\boldsymbol{\omega}_{t/e}]_{\times}[\boldsymbol{\omega}_{t/e}]_{\times} & -2[\boldsymbol{\omega}_{t/e}]_{\times} \end{bmatrix}\Bigg|_{\boldsymbol{x}=\boldsymbol{0}} \tag{A.13}$$

$$B(t) = \begin{bmatrix} 0_{3\times 3} \\ I_3 \end{bmatrix} \tag{A.14}$$

A.2 J2-perturbed Mean Orbital Element Dynamics

The equations of motion for the mean orbital elements of a spacecraft under the effects of J2 and two-body accelerations:

$$\dot{\bar{a}} = 0 \tag{A.15a}$$

$$\dot{\bar{e}} = 0 \tag{A.15b}$$

$$\dot{\bar{i}} = 0 \tag{A.15c}$$

$$\dot{\bar{\Omega}} = -\frac{3}{2} J_2 \left(\frac{r_{\text{eq}}}{p} \right)^2 \bar{n} \cos i \tag{A.15d}$$

$$\dot{\bar{\omega}} = \frac{3}{4} J_2 \left(\frac{r_{\text{eq}}}{p} \right)^2 \bar{n} (5 \cos i^2 - 1) \tag{A.15e}$$

$$\dot{\bar{M}} = \bar{n} + \frac{3}{4} J_2 \left(\frac{r_{\text{eq}}}{p} \right)^2 \bar{\eta} \bar{n} (3 \cos i^2 - 1) \tag{A.15f}$$

where $\bar{n} = \sqrt{\frac{\mu}{\bar{a}^3}}$, $\bar{\eta} = \sqrt{1 - \bar{e}^2}$.

A.3 Cislunar Dynamics

Consider a target and a chaser in orbit around two primary bodies, e.g. Earth and the Moon, denoted e and m, respectively. The frame $\mathrm{F_I}$ is the Inertial frame, b is an unforced particle, assumed to be collocated with the Earth-Moon barycenter in the three-body problem. The Synodic frame is given by $\mathrm{F_s} = \{\hat{\boldsymbol{\imath}}_{\mathrm{s}}, \hat{\boldsymbol{\jmath}}_{\mathrm{S}}, \hat{\boldsymbol{k}}_{\mathrm{s}}\}$; $\hat{\boldsymbol{\imath}}_{\mathrm{s}}$ points from the primary to the secondary body, $\hat{\boldsymbol{k}}_{\mathrm{s}}$ is parallel to the system momentum, and $\hat{\boldsymbol{\jmath}}_{\mathrm{S}}$ completes the right-hand rule. The chaser and target's center of masses are denoted by c and t, respectively, and have spacecraft-fixed frames $\mathrm{F_c}$ and $\mathrm{F_t}$. In the two-body problem, the target's orbit frame $\mathrm{F_o} = \{\hat{\boldsymbol{\imath}}_r, \hat{\boldsymbol{\imath}}_\theta, \hat{\boldsymbol{\imath}}_h\}$ is Hill's frame with radial, along-track, and cross-track basis vectors. However, since no other angular velocity is of interest in this paper, the angular velocity of the orbital frame relative to the inertial frame will be denoted $\boldsymbol{\omega}$ for convenience. We assume the chaser is controlled and its fixed-frame is aligned with the Synodic frame, i.e., $\boldsymbol{\omega}_{\mathrm{c/s}} = \mathbf{0}$.

This is done for simplicity and since the attitude dynamics and control are faster than the corresponding translational dynamics and control. The spacecraft are assumed to be rigid bodies such that all exogenous forces act on their centers of mass and the target spacecraft is assumed to be uncontrolled.

Recall that the position of spacecraft i relative to a point j is given by $\boldsymbol{r}_{i/j} = \boldsymbol{r}_i - \boldsymbol{r}_j$. The relative position of the chaser spacecraft with respect to the target is denoted $\boldsymbol{r}_{\mathrm{c/t}} = \boldsymbol{r}_{\mathrm{c/b}} - \boldsymbol{r}_{\mathrm{t/b}}$ while $\overset{k.}{\boldsymbol{r}}_{\mathrm{c/t}} = \overset{I.}{\boldsymbol{r}}_{\mathrm{c/b}} - \overset{I.}{\boldsymbol{r}}_{\mathrm{t/b}} - \boldsymbol{\omega}_{\mathrm{K/I}} \times \boldsymbol{r}_{\mathrm{c/t}}$ is the relative velocity vector as seen by a frame $\mathrm{F_K}$, where b represents the barycenter of the inertial frame $\mathrm{F_I}$. Similar to before, the relative acceleration is given by

$$\overset{k..}{\boldsymbol{r}}_{\mathrm{c/t}} = \overset{I..}{\boldsymbol{r}}_{\mathrm{c/b}} - \overset{I..}{\boldsymbol{r}}_{\mathrm{t/b}} - \overset{I.}{\boldsymbol{\omega}}_{\mathrm{K/I}} \times \boldsymbol{r}_{\mathrm{c/t}} - \boldsymbol{\omega}_{\mathrm{K/I}} \times (\boldsymbol{\omega}_{\mathrm{K/I}} \times \boldsymbol{r}_{\mathrm{c/t}}) - 2\boldsymbol{\omega}_{\mathrm{K/I}} \times k.\boldsymbol{r}_{\mathrm{c/t}}, \tag{A.16}$$

where

$$\overset{I..}{\boldsymbol{r}}_{i/\mathrm{b}} = -\frac{\mu_{\mathrm{e}} \boldsymbol{r}_{i/\mathrm{e}}}{\|\boldsymbol{r}_{i/\mathrm{e}}\|_2^3} - \frac{\mu_{\mathrm{m}} \boldsymbol{r}_{i/\mathrm{m}}}{\|\boldsymbol{r}_{i/\mathrm{m}}\|_2^3} + \frac{\boldsymbol{f}_i}{m_i} \tag{A.17}$$

are the inertial accelerations on spacecraft $i \in \{\mathrm{c}, \mathrm{t}\}$. The vector $\boldsymbol{f}_i$ represents perturbing forces acting on spacecraft i, which include orbital perturbations as well as control. In this work, we choose to realize the relative equations of motion in the Synodic frame $\mathrm{F_S}$.

Note that if the lunar gravitational acceleration in (A.17) is neglected, $\mathrm{F_I} \triangleq \mathrm{F_e}$, $m_{\mathrm{i}} << m_{\mathrm{e}}$, and $\mathrm{F_k} \triangleq \mathrm{F_o}$, we obtain the nonlinear relative equations of motion about a target orbiting a single primary body, seen in the target's orbital frame.