Proceedings of the 17th World Congress
The International Federation of Automatic Control
Seoul, Korea, July 6-11, 2008

A Robust Model Predictive Control Algorithm with a Reactive Safety Mode

John M. Carson III [*,**] **Behçet Açıkmeşe** [**]
Richard M. Murray [*] **Douglas G. MacMynowski** [*]

[*] *California Institute of Technology, Pasadena, CA 91125 USA (e-mail: {carson,murray,macmardg}@cds.caltech.edu).*
[**] *California Institute of Technology, Jet Propulsion Laboratory, Pasadena, CA 91109 USA ({jmcarson, behcet}@jpl.nasa.gov).*

Abstract: A reactive safety mode is built into a robust model predictive control algorithm for uncertain nonlinear systems. The algorithm is designed to obey all state and control constraints and blend two operational modes: (I) *standard* mode guarantees re-solvability and asymptotic convergence to the origin in a robust receding-horizon manner; (II) *safety* mode, if activated, guarantees containment within an invariant set about a safety reference for all time. The research is motivated by vehicle control-algorithm design (e.g., spacecraft and hovercraft) in which operation mode changes must be considered. Incorporating the reactive *safety* mode provides robustness to unexpected state-constraint changes; e.g., other vehicles crossing/stopping in the feasible path, or unexpected ground proximity in landing scenarios. The *safety*-mode control is provided by an offline designed control policy that can be activated at any arbitrary time during *standard* mode. The *standard*-mode control consists of separate feedforward and feedback components; feedforward comes from online solution of a FHC (Finite-Horizon optimal Control problem), while feedback is designed offline to generate an invariant tube about the feedforward trajectory. The tube provides robustness (to uncertainties and disturbances in the dynamics) and guarantees FHC re-solvability. The algorithm design is demonstrated for a class of systems with uncertain nonlinear terms that have norm-bounded Jacobians.

1. INTRODUCTION

Control of physical systems requires algorithms that incorporate state and control constraints and that handle model uncertainty and disturbances. Further, the algorithms must often blend multiple operation modes. The research presented herein develops a control algorithm that handles two operation modes: I. *standard* mode to asymptotically drive the system toward a desired final target state; II. *safety* mode, if activated, to maintain the system within an invariant set about a desired reference for all time. The algorithm builds upon MPC (Model Predictive Control), which combines nonlinear optimal control with state and control constraints [e.g. Michalska and Mayne, 1993, Rawlings and Muske, 1993, Chen and Allgöwer, 1998, Mayne et al., 2000].

This work is motivated by vehicle control applications requiring safety from uncertainty in state-constraint knowledge (e.g., safety from other vehicles unexpectedly blocking the feasible path or unexpected ground proximity during landing). The SR-MPC (Safe and Robust MPC) Algorithm presented herein develops a *safety* mode, available at any time, that is reactive to changes in static state constraints outside the desired safety zone. From *safety* mode, higher-level algorithms (not part of this work) can search for a new feasible solution, if it exists, to the original target or to a new one. This work differs from prior research (e.g., Schouwenaars et al. [2004], Kuwata et al. [2005]) that guarantees safety only at the end of the MPC time horizon and assumes perfect state-constraint knowledge during the current horizon. The reactive *safety* mode herein allows for state-constraint uncertainty during the current horizon; the trade off is a more-conservative *standard* mode.

In traditional MPC, control is computed online by solving a FHC (Finite-Horizon optimal Control problem) subject to state and control constraints and with the current state of the system as the initial state. The control is then applied to the system in a feedforward (i.e. open-loop) manner over a specified time interval until the next re-computation provides an updated feedforward input, which is then applied to the system and the cycle repeats.

Since MPC feedforward computation relies on a nominal system model, robustness to system uncertainties and guarantees of re-solvability (i.e. continued FHC feasibility) are difficult to establish. Significant research has provided frameworks for robust MPC [e.g. Mayne et al., 2000, Magni et al., 2001, Kothare et al., 1996, Scokaert and Mayne, 1998, Bemporad et al., 2002a,b, Smith, 2004, W.Langson et al., 2004, Richards and How, 2006, Jalali and Nadimi, 2006]. The framework herein builds on the R-MPC (Robust and re-solvable MPC) Algorithm in Açıkmeşe and Carson [2006] for uncertain nonlinear systems.

For *standard* mode, separate feedforward and feedback components are used: feedforward comes from online solution of the FHC, implemented in a receding-horizon manner; feedback is generated offline and maintains the actual system states within a tube about the nominal feedforward trajectory. This tube provides robustness to uncertainty

978-1-1234-7890-2/08/$20.00 © 2008 IFAC

10.3182/20080706-5-KR-1001.3768

and disturbances and provides FHC re-solvability guarantees without bounding re-computation time intervals. For *safety* mode, the control policy comes from an offline design that maintains the actual state within an invariant set that includes the *standard*-mode state from any arbitrary safety-activation time.

The organization of the paper is as follows: Section 2 introduces the system and objectives; Section 3 develops the general control algorithm; Section 4 provides explicit design procedures for a class of systems with norm-bounded Jacobians and convex state and control constraints; and Section 5 provides an illustrative example.

2. SYSTEM AND CONTROL OBJECTIVE

Consider an uncertain, nonlinear dynamical system, referred to as the *actual* system:

$$\dot{x} = f(x, u, t), \quad x \in \mathbb{R}^n, u \in \mathbb{R}^m. \tag{1}$$

Let the *nominal* system model be of (1) be

$$\dot{z} = F(z, u_o, t), \quad z \in \mathbb{R}^n, u_o \in \mathbb{R}^m, \tag{2}$$

where $F(\cdot)$ is a known, approximate model of $f(\cdot)$ in (1).

The control objective is to obtain a control input $u(t)$ such that the closed-loop system in

(I) *standard* mode is asymptotically stable about the origin ($x = 0$), with region of attraction $\mathcal{R}_a \subseteq \mathbf{X}$, such that when $x(t_0) \in \mathcal{R}_a$,

$$x(t) \in \mathbf{X},\ u(t) \in \mathbf{U}\,,\ \forall t \geq t_0. \tag{3}$$

(II) *safety* mode is contained within an invariant set $\mathbf{X}_s$ about reference point r_s such that

$$\tilde{x}(t) \in \mathbf{X}_s, u(t) \in \mathbf{U}, x(t) \in \mathbf{X}, \forall t \geq t_s, \tag{4}$$

where $\tilde{x}(t) \triangleq x(t) - r_s$, and $t_s \geq t_0$.

Sets $\mathbf{X}$, $\mathbf{U}$, and $\mathbf{X}_s$ are given state and control constraints imposed on the control design, which utilizes the following relationships between constraint sets [1]:

$$\mathbf{U}_o + \mathbf{U}_f \subseteq \mathbf{U}, \quad \mathbf{Z}_n + \mathbf{X}_s \subseteq \mathbf{X}, \quad \mathbf{Z}_s + \mathbf{X}_f \subseteq \mathbf{X}_s. \tag{5}$$

In preview, the algorithm designs *standard*-mode control to maintain *nominal* states within constraint set $\mathbf{Z}_n$. Then, the algorithm establishes (i) invariant tube $\mathbf{X}_f$ about the *nominal* (guidance) trajectory to contain the *actual* states (providing robustness to dynamics uncertainty and disturbances), and (ii) invariant, tube-like set $\mathbf{X}_s$ for arbitrary-time switching into *safety* mode with $r_s \in \mathbf{Z}_n$ based on the *nominal* state at *safety* time (additionally providing robustness to unexpected state-constraint changes).

3. CONTROL ALGORITHM ARCHITECTURE

The control approach builds upon the R-MPC (Robust and re-solvable MPC) framework in Açıkmeşe and Carson [2006] where control u is composed of two components:

- Feedforward, $u_o \in \mathbf{U}_o$
- Feedback, $u_f \in \mathbf{U}_f$

such that

$$u(t) = u_o(t) + u_f(t). \tag{6}$$

This approach is utilized with *standard* mode, whereas *safety* mode utilizes an offline-design policy.

[1] All sets contain the origin. For sets A and B, $C = A + B$ implies that: If $a \in A$ and $b \in B$ then $a + b \in C$.

In *standard* mode, component u_o comes from online solution of a FHC (Finite Horizon optimal Control problem) that uses *nominal* system (2) to generate a feedforward (or guidance) policy. Component u_f is designed offline as a feedback policy to handle uncertainty and disturbances in *actual* system (1). The following Condition on the *actual* and *nominal* systems is used in the design of u_f:

Condition 1. There exists a feedback control law $u_f = \mathcal{K}_f(x, z) \in \mathbf{U}_f$ in (6) that renders set $\mathbf{X}_f$ invariant for $\eta(t) \triangleq x(t) - z(t) \in \mathbf{X}_f$, $\forall t \geq t_0$, and for all $u_o(t)$, with dynamics (1) for x and (2) for z. ◇

Set $\mathbf{X}_f$ forms a tube about the *nominal* states z: if $\eta(t_0) \in \mathbf{X}_f$ for some $t_0 \geq 0$, then $\eta(t) \in \mathbf{X}_f, u_f(t) \in \mathbf{U}_f, \forall t \geq t_0$ in *standard* or *safety* modes.

3.1 Standard-Mode Finite Horizon Optimal Control

Online solution of the FHC generates feedforward u_o for *standard* mode (control Objective I). This subsection augments the R-MPC approach from Açıkmeşe and Carson [2006] with an additional *safety* constraint.

The FHC uses *nominal* system (2), an objective function, and state and control constraints to generate $u_o \triangleq u_{\text{FHC}} \in \mathbf{U}_o$ and $z \triangleq z_{\text{FHC}} \in \mathbf{Z}_n$ for a finite time horizon.

FHC

$\min_{u_o} J(u_o; t_i, T, z(t_i))$ where

$$J = \int_{t_i}^{t_i+T} h(z(\tau), u_o(\tau))d\tau + V(z(t_i + T))$$

$$\text{subject to} \quad \left.\begin{array}{l} \dot{z} = F(z, u_o, t) \\ z(t) \in \mathbf{Z}_n \\ u_o(t) \in \mathbf{U}_o \\ z(t) - \mathcal{T}(z(t)) \in \mathbf{Z}_s \end{array}\right\} \forall\, t \in [t_i,\, t_i + T]$$

$$z(t_i + T) \in \mathbf{\Omega}_o$$

$$x(t_i) - z(t_i) \in \mathbf{X}_f$$

with $x(t_i)$ the state of *actual* system dynamics (1).

The region of attraction $\mathcal{R}_a$ for control objective I is defined in terms of the FHC:

$$\mathcal{R}_a = \{\xi \in \mathbf{Z}_n + \mathbf{X}_f\text{: FHC is feasible with } x(t_0) = \xi\}. \tag{7}$$

Set $\mathbf{Z}_n$ defines the *nominal* system constraints on state z_{FHC}, and $\mathbf{\Omega}_o$ defines constraints on the terminal state; both of these sets are part of the design process.

An innovation in FHC is the use of offline-designed feedback u_f from Condition 1 to generate invariant tube $\mathbf{X}_f$, which provides a relaxation on the FHC initial state:

$$x(t_i) - z(t_i) \in \mathbf{X}_f, \tag{8}$$

Aside from providing robustness (to the characterization of model uncertainty and disturbances), the relaxation provides a re-solvability guarantee, which leads to a robustly stabilizing controller (See Açıkmeşe and Carson [2006]).

The *safety*-mode availability at any arbitrary time is ensured by constraint

$$z(t) - \mathcal{T}(z(t)) \in \mathbf{Z}_s,\ \forall t \in [t_i,\, t_i + T], \tag{9}$$

where function $\mathcal{T} : \mathbf{Z}_n \mapsto \mathbf{Z}_n$ defines a mapping that will be used in the *safety* subsection to define the *safety* reference r_s.

The following conditions on the *actual* and *nominal* systems are useful in proving asymptotic stability of *standard* mode; the conditions are standard in proofs of MPC stability (e.g., Chen and Allgöwer [1998], Jadbabaie [2000]).

Condition 2. Function h in the FHC satisfies

$$h(z, u_o) \geq a||z||^p + b||u_o||^r, \quad \forall z, u, \tag{10}$$

with $p \geq 1$, $r \geq 0$, a and b both positive constants, and $h(0, 0) = 0$. ◇

Condition 3. Function V in the FHC is positive definite [Khalil, 1996] and there exists a feedback control law $u = \mathcal{L}(x)$ and $u_o = \mathcal{L}(z)$ such that V defines a *Control Lyapunov Function* for (1) and (2) satisfying

$$\nabla V(x) f(x, \mathcal{L}(x), t) + h(x, \mathcal{L}(x)) \leq 0\,, \ \forall\, x \in \mathbf{\Omega}_o, \tag{11}$$

$$\nabla V(z) F(z, \mathcal{L}(z), t) + h(z, \mathcal{L}(z)) \leq 0\,, \ \forall\, z \in \mathbf{\Omega}_o, \tag{12}$$

where $\mathbf{\Omega}_o \subset \mathbf{Z}_n$ contains the origin, $\mathcal{L}(x) \in \mathbf{U}_o, \forall\, x \in \mathbf{\Omega}_o$, and $\mathcal{L}(z) \in \mathbf{U}_o, \forall\, z \in \mathbf{\Omega}_o$. Additionally, feedback law $\mathcal{L}$ renders $\mathbf{\Omega}_o \subset \mathbb{R}^n$ invariant for dynamics (1) and (2), i.e., if $x(t_0) \in \mathbf{\Omega}_o (z(t_0) \in \mathbf{\Omega}_o)$ for some t_0, then $x(t) \in \mathbf{\Omega}_o\,,\ \forall\, t \geq t_0\ (z(t) \in \mathbf{\Omega}_o\,,\ \forall\, t \geq t_0)$. ◇

Condition 4. There exists closed balls [2] $\mathbf{B}_R$ and $\mathbf{B}_r$ in $\mathbb{R}^n$ around the origin such that set $\mathbf{\Omega}_o$ in the FHC satisfies

$$\mathbf{X}_f \subseteq \mathbf{B}_r \subset \mathbf{B}_R \subseteq \mathbf{\Omega}_o. \tag{13}$$

◇

3.2 Reactive Safety-Mode Control Policy

Control $u (\triangleq u_s)$ in *safety* mode (control Objective II) comes from an offline design that generates a second, invariant tube-like set $\mathbf{X}_s$ to maintain $x \in \mathbf{X}_s$ about reference r_s for all time after safety activation time t_s.

Reference r_s is defined with function $\mathcal{T}$ from the FHC that maps the *nominal* state $z_{\text{FHC}}(t_s)$ to a desired *safety* reference state,

Definition 1. (Safety Reference).

$$r_s = \mathcal{T}(z_{\text{FHC}}(t_s)) \in \mathbf{Z}_n \tag{14}$$

where $\mathcal{T} : \mathbf{Z}_n \mapsto \mathbf{Z}_n$. ◇

For example, a mechanical system with non-zero position and non-zero velocity at *safety* activation t_s may desire r_s to be rest (zero velocity) at the current non-zero position.

The following condition for the design of u_s is useful in proving satisfaction of *safety*-mode control objective II:

Condition 5. There exists control law $u_s = \mathcal{K}_s(t, x, r_s) \in \mathbf{U}$ that renders set $\mathbf{X}_s$ invariant for $\tilde{x}(t) \triangleq x(t) - r_s \in \mathbf{X}_s$, $\forall t \geq t_s$ with dynamics (1) for x and $r_s \in \mathbf{Z}_n$.

3.3 Safe and Robust Model Predictive Control Algorithm

The SR-MPC (Safe and Robust MPC) Algorithm builds upon R-MPC from Açıkmeşe and Carson [2006]:

[2] $\mathbf{B}_\rho \triangleq \{v : \|v\| \leq \rho, \rho > 0\}$.

Safe and Robust MPC Algorithm

Begin in *standard* mode ($x(t_0) \in \mathcal{R}_a$) with $k = 0$ and iterate the following steps over computation times t_k for $k \in \mathbb{Z}^+$:

standard mode

(1) Measure state $x(t_k)$ of *actual* system (1).
(2) Solve the FHC at time $t_i = t_k$ with $T = T_k$ to obtain $u^k_{\text{FHC}}(t)$ on $t \in [t_k, t_k + T_k]$.
(3) Monitor x and z, with $z_{\text{FHC}}(t) = z(t)$ on $t \in [t_k, t_{k+1}]$, while applying
   - $u = u_o + u_f$ to *actual* system (1)
   - u_o to *nominal* system (2)

   with $u_f = \mathcal{K}_f(x, z)$ and $u_o = u^k_{\text{FHC}}(t)$.
(4) Check the following over $t \in [t_k, t_{k+1}]$:
   - If *safety*-event detected at $t_s \geq t_k$, set $r_s = \mathcal{T}(z_{\text{FHC}}(t_s))$, and switch to *safety* mode.
   - If $z(\tilde{t}) \in \mathbf{\Omega}_o$ for some $\tilde{t} \geq t_0$, then $u_o = \mathcal{L}(z)$, for $t \geq \tilde{t}$.
   - If $x(\bar{t}) \in \mathbf{\Omega}_o$ for $\bar{t} \geq t_0$, then $u = \mathcal{L}(x)$, for $t \geq \bar{t}$.

safety mode

For $t \geq t_s$, apply $u = u_s = \mathcal{K}_s(t, x, r_s)$.

Lemma 1. (Re-solvability of the FHC). Suppose that the FHC is feasible at t_0 with T_0 and $x(t_0) \in \mathbf{Z}_n + \mathbf{X}_f$, and let t_k for $k \in \mathbb{Z}^+$ be the times that a solution of the FHC is computed. Then, the feasibility of the FHC is guaranteed at t_k with $T_k \geq T_{k-1} - \delta_k$, $\forall k \in \mathbb{Z}^+$, $\delta_k = t_k - t_{k-1}$, $0 \leq \delta_k < T_{k-1}$, provided conditions 1 and 3 hold. ◇

Proof. Açıkmeşe and Carson [2006] □

The following theorem builds upon Theorem 1 in Açıkmeşe and Carson [2006]:

Theorem 1. Consider system (1) with a control input described by the SR-MPC Algorithm. Suppose that conditions 1-5 are satisfied. Then, the resulting closed-loop system satisfies control objective I with a region of attraction $\mathcal{R}_a$ and control objective II. ◇

Proof. The proof is split into two pieces

(I) *standard* mode: The proof of asymptotic stability with region of attraction $\mathcal{R}_a$ is given in Açıkmeşe and Carson [2006], which also establishes FHC re-solvability guarantees in a receding-horizon implementation.
(II) *safety* mode: The control input in *standard* mode guarantees that $x(t_s) - z(t_s) \in \mathbf{X}_f$ (see Açıkmeşe and Carson [2006]). Further, the FHC is satisfied in *standard* mode, thus constraint (9) guarantees $z(t_s) - r_s = z(t_s) - \mathcal{T}(z(t_s)) \in \mathbf{Z}_s$ with r_s from (14). Thus, $x(t_s) - r_s = x(t_s) - z(t_s) + z(t_s) - r_s \in \mathbf{X}_f + \mathbf{Z}_s \subseteq \mathbf{X}_s$ as given in (5). Now by using Condition 5, we have $x(t) - r_s \in \mathbf{X}_s$ for all $t \geq t_s$ when the safety mode control input is applied. □

4. APPLICATION TO A CLASS OF SYSTEMS WITH DERIVATIVES CONTAINED IN CONVEX SETS

This section develops the SR-MPC (Safe and Robust MPC) Algorithm for a special class of systems with Jacobians contained in convex sets. The class of systems is defined first, followed by two subsections: one to review the *standard*-mode algorithm from Açıkmeşe and Carson [2006] that provides robust, re-solvable MPC for this class of these systems along with satisfaction of constraint (9) to ensure *safety*-mode availability; the second to describe two subclasses of systems for which constructive design method for Condition 5 ensure satisfaction of *safety*-mode.

The class of systems considered have *actual* dynamics of the following form:

$$\begin{aligned} \dot{x} &= Ax + Bu + E\phi(t,q) \\ q &= C_q x + D_q u\,, \end{aligned} \tag{15}$$

where $\phi : \mathbb{R} \times \mathbb{R}^{n_q} \to \mathbb{R}^{n_p}$ with $\phi(t,0) = 0, \forall t$, is a continuously differentiable function representing the uncertain nonlinear part of the dynamics. This form implies $f(x,u,t) = Ax + Bu + E\phi(t,q)$ in (1) with $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $E \in \mathbb{R}^{n\times n_p}$, $C_q \in \mathbb{R}^{n_q\times n}$, and $D_q \in \mathbb{R}^{n_q\times m}$.

The *nominal* system model for this class of systems is

$$\begin{aligned} \dot{z} &= Az + Bu_o + E\psi(t,q_o) \\ q_o &= C_q z + D_q u_o\,, \end{aligned} \tag{16}$$

where $\psi : \mathbb{R} \times \mathbb{R}^{n_q} \to \mathbb{R}^{n_p}$ with $\psi(t,0) = 0, \forall t$ is an approximation for ϕ in the *actual* system (15). Thus, $F(z,u_o,t) = Az + Bu_o + \psi(t,q_o)$ in (2).

Nonlinear functions ϕ and ψ are assumed to have Jacobians in convex sets, along with a bounded mismatch:

Condition 6. Functions ϕ and ψ are continuously differentiable and there exists a closed and convex set of matrices $\Theta \subseteq \mathbb{R}^{n_p\times n_q}$ such that

$$\frac{\partial\phi}{\partial q}(t,q) \in \Theta \quad \text{and} \quad \frac{\partial\psi}{\partial q}(q) \in \Theta\,, \qquad \forall\, q,\, t\,. \tag{17}$$

$\diamond$

Condition 7. There exists scalar $\gamma > 0$ such that

$$\|w(t,z,u_o)\| \le \gamma, \quad \forall t, z \in \mathbf{Z}_n + \mathbf{Z}_s, u_o \in \mathbf{U}_o, \tag{18}$$

where $w(t,z,u_o) = \phi(t,q_o) - \psi(t,q_o)$, with q_o from (16). $\diamond$

The *error* dynamics between *actual* and *nominal* states, $\eta \triangleq x - z$, are

$$\begin{aligned} \dot{\eta} &= A\eta + Bu_f + E\left[\phi(t,q) - \psi(t,q_o)\right] & (19)\\ &= A\eta + Bu_f + E[\pi(t,\eta,u_f) + w(t,z,u_o)]\,, & (20) \end{aligned}$$

where $u_f \triangleq u - u_o$ is the feedback policy, $w(t,z,u_o)$ is from Condition 7, and $\pi(t,\eta,u_f) = \phi(t,q) - \phi(t,q_o)$. The feedback u_f is designed to handle the uncertainty between the *nominal* model (16) and the *actual* system (15).

We obtain the following relationship for the *error* dynamics (20) by using Lemma 3 in Açıkmeşe and Carson [2006] with Condition 6

$$\pi(t,\eta,u_f) = \theta(t)(C_q\eta + D_q u_f), \text{ where } \theta(t) \in \Theta, \forall t. \tag{21}$$

This simplification aids in the generation of feedback laws that satisfy Condition 1 for this class of uncertain nonlinear systems.

The SR-MPC algorithm design herein makes use of a particular form of convex constraints; more general convex characterizations of the constraint sets (5) and Jacobians in Condition 6 are possible and can be integrated into the design framework (see Açıkmeşe and Carson [2006]). The following design specification prescribes bounds on the state and control constraint sets that are assumed to guarantee satisfaction of the set relationships in (5) for the closed-loop system.

Condition 8. (State and Control Constraints).

$$\begin{aligned} \mathbf{Z}_n &\supseteq \mathcal{Z}_\Omega \triangleq \{z \in \mathbb{R}^n :\ a_i^T z \le 1,\ i = 1,\ldots,m_o\}, \\ \mathbf{X}_f &\subseteq \mathcal{X}_f \triangleq \{\eta \in \mathbb{R}^n :\ b_i^T \eta \le 1,\ i = 1,\ldots,m_f\}, \\ \mathbf{Z}_s &\subseteq \mathcal{Z}_s \triangleq \{\tilde{z} : \tilde{z}^T C_s^T \Pi_s C_s \tilde{z} \le 1\}, \\ \mathbf{U}_o &\subseteq \{u_o \in \mathbb{R}^m :\ u_o^T \Pi_o u_o \le 1\}, \\ \mathbf{U}_f &\subseteq \{u_f \in \mathbb{R}^m :\ u_f^T \Pi_f u_f \le 1\}, \end{aligned}$$

where Π_o, Π_f, and Π_s are symmetric positive-definite matrices, and $\mathcal{X}_f$ and $\mathcal{Z}_s$ are such that $\mathcal{Z}_s + \mathcal{X}_f \subseteq \mathbf{X}_s$: thus, $\mathbf{X}_f \subseteq \mathcal{X}_f$ and $\mathbf{Z}_s \subseteq \mathcal{Z}_s$ provide additional conservatism. $\diamond$

Safety constraint $\mathbf{Z}_s$ uses C_s to constraint only portions of the state, which can be useful in practical applications (e.g., vehicles with relative-position sensors may only require safety in relative distance to other objects).

4.1 Standard-Mode FHC Algorithm

The following Corollary from Açıkmeşe and Carson [2006], for the *standard* mode, describes a design procedure for systems with norm-bounded Jacobians.

Corollary 1. Consider an uncertain nonlinear system (15) with a nominal model given by (16) satisfying conditions 6, 7, and 8 with

$$\Theta = \{\theta \in \mathbb{R}^{n_p\times n_q} :\ \|\theta\| \le 1\}\,. \tag{22}$$

Suppose there exist matrices $P = P^T > 0$, $Q = Q^T > 0$, L, Y and positive scalars λ, β, μ, c_1, and c_2 satisfying the following matrix inequalities,

$$\begin{bmatrix} \begin{pmatrix} PA^T + AP + BL + L^T B^T + P/\lambda \\ +(\beta + \lambda\gamma^2)EE^T \end{pmatrix} & PC_q^T + L^T D_q^T \\ C_q P + D_q L & -\beta I \end{bmatrix} \le 0$$

$$\begin{bmatrix} \begin{pmatrix} QA^T + AQ + BY + Y^T B^T \\ +\mu EE^T \end{pmatrix} & QC^T + Y^T D^T & QC_q^T + Y^T D_q^T \\ CQ + DY & -I & 0 \\ C_q Q + D_q Y & 0 & -\mu I \end{bmatrix} \le 0$$

$$\begin{bmatrix} P & L^T \\ L & \Pi_f^{-1} \end{bmatrix} \ge 0\,, \quad \begin{bmatrix} Q & Y^T \\ Y & \Pi_o^{-1} \end{bmatrix} \ge 0\,,$$

$$a_i^T Q a_i \le 1, i = \{1,\ldots,m_o\},\ b_j^T P b_j \le 1, j = \{1,\ldots,m_f\},$$
$$Q \ge c_1 I > c_2 I \ge P\,,$$

where C and D satisfy

$$C^T D = 0. \tag{23}$$

Then, ellipsoids

$$\begin{aligned} \mathbf{\Omega}_o &= \varepsilon_Q \triangleq \{x : x^T Q^{-1} x \le 1\} \ \Rightarrow\ \mathbf{\Omega}_o \subseteq \mathcal{Z}_\Omega \\ \mathbf{X}_f &= \varepsilon_P \triangleq \{\eta : \eta^T P^{-1} \eta \le 1\} \end{aligned}$$

and the SR-MPC algorithm with

$$h(z,u_o) = \|Cz\|^2 + \|Du_o\|^2\,, \quad V(z) = z^T Q^{-1} z\,,$$

$$\mathcal{L}(z) = Kz\,, \qquad K = YQ^{-1} \tag{24}$$

$$\mathcal{K}_f(x,z) = K_f(x - z)\,, \qquad K_f = LP^{-1} \tag{25}$$

result in an asymptotically stable closed-loop system for (15) with region of attraction $\mathcal{R}_a$ given in (7) and satisfaction of the constraints in Condition 8. $\diamond$

Proof. Açıkmeşe and Carson [2007] □

The satisfaction of Corollary 1 also ensures satisfaction of Conditions 1-4, which are sufficient to establish resolvability of the FHC and asymptotic stability and robustness of the *standard*-mode in Theorem 1. Further, the

Corollary is valid for any $\mathbf{Z}_n$ (including non-convex) with an initial feasible FHC solution. Note, a convex $\mathbf{Z}_n$ leads to a convex FHC, which can be solved online with finite-time convergence guarantees to a prescribed accuracy level. [Boyd and Vandenberghe, 2004, Nesterov and Nemirovsky, 1994].

4.2 Safety Mode for a Subclass of Systems

The special cases presented herein are motivated by practical application of the SR-MPC Algorithm. The following form for *nominal* system (16) in terms of *safety* state $\tilde{z}$ is used in the design of a nominal control policy u_{os} for *safety* mode:

$$\begin{aligned} \dot{\tilde{z}} &= A\tilde{z} + Ar_s + Bu_{os} + E\psi(t, q_o) \\ q_o &= C_q\tilde{z} + D_q u_{os} + C_q r_s \end{aligned} \tag{26}$$

Two special subclasses of system (26) will be discussed for which satisfaction of Condition 5 is assured.

Subclass I (contains velocity-dependent nonlinearity) The following Corollary provides the *safety*-mode component applicable to mechanical systems that can come to rest at arbitrary positions and have velocity-dependent nonlinearities (e.g., hovercraft/road vehicles with velocity-dependent drag).

Condition 9. Safety reference r_s satisfies

$$r_s \in \mathcal{N}(A) \cap \mathcal{N}(C_q), \tag{27}$$

where $\mathcal{N}(X)$ is the null-space of a matrix X. ◇

Corollary 2. Consider a class of systems modeled by (16) with r_s satisfying Condition 9. Suppose there exist matrices $S = S^T > 0$ and R and positive scalar β satisfying the following linear matrix inequalities:

$$\begin{bmatrix} SA^T + AS + BR + R^T B^T + \beta EE^T & SC_q^T + R^T D_q^T \\ C_q S + D_q R & -\beta I \end{bmatrix} \le 0 \tag{28}$$

$$\begin{bmatrix} S & SC_s^T \\ C_s S & \Pi_s^{-1} \end{bmatrix} \ge 0, \text{ and } \begin{bmatrix} S & R^T \\ R & \Pi_o^{-1} \end{bmatrix} \ge 0\,. \tag{29}$$

If *safety*-mode control $u_s = \mathcal{K}_s(t, x, r_s) \in \mathbf{U}$ is given by

$$\mathcal{K}_s(t, x, r_s) = K_s(z - r_s) + K_f(x - z), \quad K_s = RS^{-1}, \tag{30}$$

where $r_s = \mathcal{T}(z(t_s))$, and K_f and $\mathbf{X}_f$ obtained as described in Corollary 1, then $\mathbf{Z}_s = \{\tilde{z} : \tilde{z}^T S^{-1}\tilde{z} \le 1\}$ satisfies Condition 8, $\{r_s\} + \mathbf{Z}_s + \mathbf{X}_f$ is invariant for the *actual* dynamics, and $\mathbf{Z}_s + \mathbf{X}_f \subseteq \mathbf{X}_s$. Further, $u_s = \mathcal{K}_s(t, x, r_s) \in \mathbf{U}$ for all $x \in \mathbf{Z}_n + \mathbf{Z}_s + \mathbf{X}_f$ and $r_s \in \mathbf{Z}_n$. ◇

Proof. Omitted for brevity. Refer to Carson [2008]. ◇

Subclass II (contains position-dependent nonlinearity) The following Corollary provides the *safety*-mode component applicable to mechanical systems that have non-zero, position-dependent nonlinearities when the system comes to rest at arbitrary positions (e.g., spacecraft hovering in a gravity field).

Condition 10. Safety reference r_s satisfies

$$r_s \in \mathcal{N}(A), \tag{31}$$

where $\mathcal{N}(X)$ is the null-space of a matrix X. ◇

Condition 11. There exists scalar $\delta > 0$ such that

$$\|\psi(t, z, u_o)\| \le \delta, \quad \forall t, z \in \mathbf{Z}_n + \mathbf{Z}_s, u_o \in \mathbf{U}_o. \tag{32}$$

◇

Note, Condition 11, along with Condition 7, imply a bound on *actual* system nonlinearity ϕ.

Corollary 3. Consider a class of systems modeled by (16) with Condition 11 bounding the nonlinearity and r_s satisfying Condition 10. Suppose there exist matrices $S = S^T > 0$ and R and positive scalar α satisfying the following matrix inequalities:

$$\begin{bmatrix} SA^T + AS + BR + R^T B^T + \alpha S & E \\ E^T & -\frac{\alpha}{\delta^2} I \end{bmatrix} \le 0 \tag{33}$$

$$\begin{bmatrix} S & SC_s^T \\ C_s S & \Pi_s^{-1} \end{bmatrix} \ge 0, \text{ and } \begin{bmatrix} S & R^T \\ R & \Pi_o^{-1} \end{bmatrix} \ge 0\,. \tag{34}$$

If *safety*-mode control $u_s = \mathcal{K}_s(t, x, r_s) \in \mathbf{U}$ is given by

$$\mathcal{K}_s(t, x, r_s) = K_s(z - r_s) + K_f(x - z), \quad K_s = RS^{-1}, \tag{35}$$

where $r_s = \mathcal{T}(z(t_s))$, and K_f and $\mathbf{X}_f$ obtained as described in Corollary 1, then $\mathbf{Z}_s = \{\tilde{z} : \tilde{z}^T S^{-1}\tilde{z} \le 1\}$ satisfies Condition 8, $\{r_s\} + \mathbf{Z}_s + \mathbf{X}_f$ is invariant for the *actual* dynamics, and $\mathbf{Z}_s + \mathbf{X}_f \subseteq \mathbf{X}_s$. Further, $u_s = \mathcal{K}_s(t, x, r_s) \in \mathbf{U}$ for all $x \in \mathbf{Z}_n + \mathbf{Z}_s + \mathbf{X}_f$ and $r_s \in \mathbf{Z}_n$. ◇

Proof. Let positive-definite function $V_s(\tilde{z}) = \tilde{z}^T S^{-1}\tilde{z}$ be a Lyapunov function candidate. Pre- and post-multiply (33) by $\mathbf{diag}(S^{-1}, I)$, use $K_s = R\bar{S}$ from (35), and then pre- and post-multiply by ζ^T and ζ, respectively, where $\zeta = (\tilde{z}^T, \psi^T)^T$:

$$\tilde{z}^T(A^T S^{-1} + S^{-1}A)\tilde{z} + 2\tilde{z}^T S^{-1}(Bu_{os} + E\psi) + \alpha(\tilde{z}^T S^{-1}\tilde{z} - \tfrac{1}{\delta^2}\psi^T\psi) \le 0,$$

with $u_{os} = K_s\tilde{z}$. Condition 11 ensures

$$\tfrac{1}{\delta^2}\psi^T\psi \le \tilde{z}^T S^{-1}\tilde{z} \text{ when } \tilde{z}^T S^{-1}\tilde{z} \ge 1,$$

which implies that when $\tilde{z}^T S^{-1}\tilde{z} \ge 1$,

$$\tilde{z}^T(A^T S^{-1} + S^{-1}A)\tilde{z} + 2\tilde{z}^T S^{-1}(Bu_{os} + E\psi) \le 0,$$

and hence $\dot{V}_s(\tilde{z}) \le 0$ when $\tilde{z}^T S^{-1}\tilde{z} \ge 1$. Thus, $\mathbf{Z}_s$ is an invariant set for $\tilde{z}$ [Açıkmeşe and Corless, 2003].

Pre- and post-multiply the first LMI in (34) by matrix $\mathbf{diag}(S^{-1}, I)$, use a Schur complement, and pre- and post-multiply by $\tilde{z}^T$ and $\tilde{z}$, respectively:

$$\tilde{z}^T C_s^T \Pi_s C_s \tilde{z} \le \tilde{z}^T S^{-1}\tilde{z},$$

which implies $\mathbf{Z}_s \subseteq \mathcal{Z}_s$ from Condition 8.

Pre- and post-multiply the second LMI in (34) by $\mathbf{diag}(S^{-1}, I)$, use a Schur complement, and pre- and post-multiply by $\tilde{z}^T$ and $\tilde{z}$, respectively:

$$u_{os}^T \Pi_o u_{os} \le \tilde{z}^T S^{-1}\tilde{z}$$

where $u_{os} = K_s\tilde{z}$ and $K_s = RS^{-1}$. Thus, for $\tilde{z} \in \mathbf{Z}_s$, $u_{os}^T \Pi_o u_s \le 1$, so $u_{os} \in \mathbf{U}_o$, with $\mathbf{U}_o$ defined in Condition 8. Further, since $u_s = u_{os} + u_f$, where $u_f = K_f(x - z)$, and $u_f \in \mathbf{U}_f$ for all $x - z \in \mathbf{X}_f$ (as guaranteed by Corollary 1), the *safety*-mode control $u_s \in \mathbf{U}$, with $\mathbf{U}$ defined in (5).

From here, follow the proof of Theorem 1, part II. □

5. AN ILLUSTRATIVE EXAMPLE

The following example from Açıkmeşe and Carson [2006] illustrates the SR-MPC algorithm for a system satisfying Corollary 3. Simulations presented include (i) Original R-MPC without safety mode, (ii) SR-MPC where safety is not required, (iii) SR-MPC with safety mode initiated.

The *actual* and *nominal* system dynamics in (15) and (16), respectively, have the following properties:

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, E = \begin{bmatrix} 0 \\ -0.1 \end{bmatrix}$$

$$\phi(t,q) = \omega(t)\sin^2(C_q x), \quad C_q = [1 \ 0],$$
$$\psi(t,q_o) = \omega_0 \sin^2(C_q z), \quad D_q = 0,$$

where $\omega(t) \in [0, 0.5]$ and $\omega_0 = 0.2$; x is a vector with position and velocity components. Function ψ is the *nominal* model for *actual* system nonlinearity ϕ. The nonlinearities satisfy Condition 6 with Θ as in (22): $\|\frac{\partial \phi}{\partial q}\| \le 1$ and $\|\frac{\partial \psi}{\partial q}\| \le 1$. Further, Conditions 7 and 11 are satisfied with $\gamma = 0.3$ and $\delta = 0.2$, respectively. The FHC cost function $h(z, u_o)$ in Corollary 1 has matrices

$$C = \begin{bmatrix} 1 & 0 \\ 0 & 0.1 \\ 0 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix},$$

the FHC horizon is fixed at $T = 30$ seconds, and the initial condition is $x(0) = (4,\ 0.4)^T$

The *actual* state and control constraints for the example are $x_1 \in [-0.35, 5]$, $x_2 \in [-1, 1]$, and $\|u\| \le 1.4$. The safety requirement is $\tilde{x}_1 \in [-0.2, 0.2]$ with safety reference r_s being nominal rest ($z_2 = 0$) at the safety-activation nominal position $z_1(t_s)$. These constraints are partitioned into the definitions of Conditions 8 as follows:

$$\text{R-MPC: } a_i = \left\{ \begin{pmatrix} \frac{1}{4.95} \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{0.3} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{0.9} \end{pmatrix}, \begin{pmatrix} 0 \\ -\frac{1}{0.9} \end{pmatrix} \right\}$$

$$\text{SR-MPC: } a_i = \left\{ \begin{pmatrix} \frac{1}{4.8} \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{0.15} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \frac{1}{0.9} \end{pmatrix}, \begin{pmatrix} 0 \\ -\frac{1}{0.9} \end{pmatrix} \right\}$$

$$b_i = \left\{ \begin{pmatrix} 20 \\ 0 \end{pmatrix}, \begin{pmatrix} -20 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 10 \end{pmatrix}, \begin{pmatrix} 0 \\ -10 \end{pmatrix} \right\}$$

$$\Pi_o = \frac{1}{1.2^2}, \quad \Pi_f = \frac{1}{0.2^2}, \quad \Pi_s = \frac{1}{0.15^2}, \quad C_s = [1 \ 0]$$

where the a_i's define the full $\mathbf{Z}_n$ for the examples, and $i = \{1, 2, 3, 4\}$. Note, for the R-MPC simulations the a_i's define a larger $\mathbf{Z}_n$ (labeled $\mathbf{X}_o$ in the figures) than those for the SR-MPC simulations. The difference is due to R-MPC not needing to consider safety mode. Parameters Π_o and Π_f bound components $\|u_o\| \le 1.2$ and $\|u_f\| \le 0.2$, respectively, in control u. The safety reference from (14) is

$$r_s = \mathcal{T} z_{\text{FHC}}(t_s) = \begin{pmatrix} z_1^{\text{FHC}}(t_s) \\ 0 \end{pmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

where $\mathcal{T}(\cdot) = T$ and $z_1^{\text{FHC}}(t_s)$ is the first component of z_{FHC} at safety activation time t_s. Note, r_s satisfies Condition 10.

Figure 1 shows asymptotic convergence of the R-MPC Algorithm from Açıkmeşe and Carson [2006] and that invariant tube $\mathbf{X}_f$ contains the *error* state ($\eta(t) = x(t) - z(t)$). Set $\mathbf{X}_f$ guarantees FHC re-solvability due to relaxation (8), even when the actual trajectory leaves the nominal constraint set as seen in Figure 1.

The simulation in Figure 2 implements SR-MPC, which uses the smaller set $\mathbf{Z}_n$. Although safety mode is not activated here, SR-MPC reduces the maximum velocity ($z_2^{\text{FHC}}(t)$) to ensure that control object II for safety mode could be satisfied if needed. This result is intuitive: to ensure a desired vehicle stopping distance, the maximum allowable velocity must be bounded.

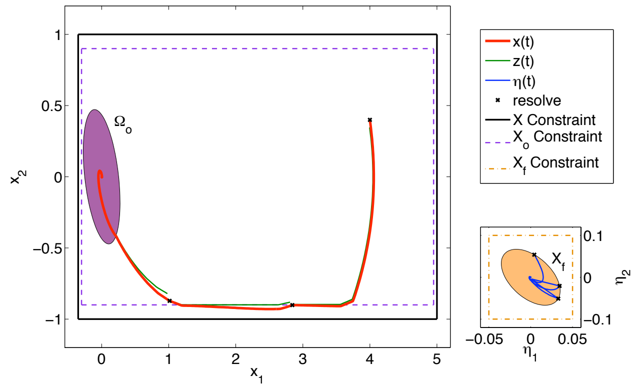

Fig. 1. Robust MPC without Safety

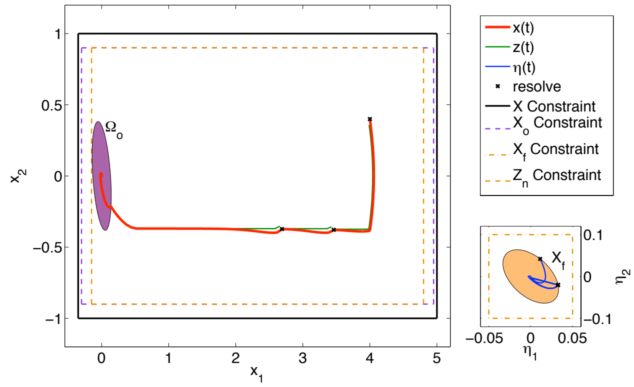

Fig. 2. Safe and Robust MPC without Safety Event

Figure 3 depicts a simulation where safety mode is entered, after approximately 7 seconds, due to a change in the original, actual constraints $\mathbf{X}$ (black line crossing the state constraints); the constraint change is excessive but demonstrates the algorithm ability to switch arbitrarily into safety mode. The nominal trajectory in safety mode remains inside $\mathbf{Z}_s$ (gray ellipse), and the actual trajectory remains inside $\mathbf{X}_s$, which is only slightly larger than $\mathbf{Z}_s$ due to the small size of $\mathbf{X}_f$ and appears as a cyan outline around the gray $\mathbf{Z}_s$. Again, perfect state knowledge (visibility) is assumed inside $\mathbf{X}_s$.

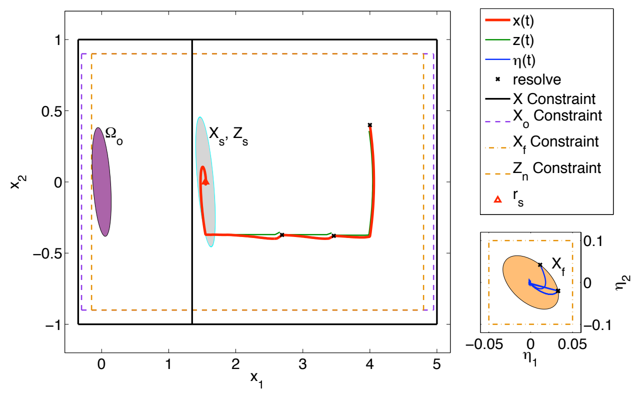

Fig. 3. Safe and Robust MPC with Safety Event

Figure 4 provides the control component time series to show that the control constraints are met along the entire simulation time span. The control components maintain a slight offset from 0 due to the nonlinearity not being zero at the safety reference location.

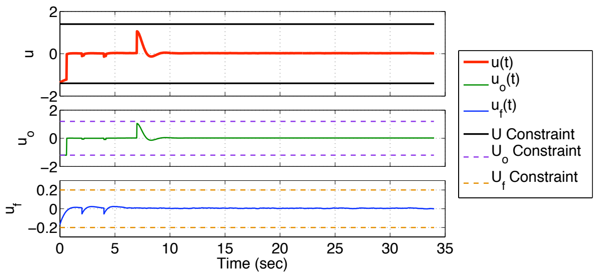

Fig. 4. Control Inputs for Figure 3

6. CONCLUSIONS

The SR-MPC Algorithm combines two operation modes while providing adherence to state and control constraints and robustness to uncertainty. In *standard* mode, the control algorithm provides asymptotic stability to the origin, along with re-solvability guarantees once an initial feasible solution is obtained. The reactive *safety* mode, if initiated, contains the closed-loop states within an invariant set about a desired safety reference for all time. The algorithm allows *safety*-mode activation at any arbitrary time, which is the major contribution of this research.

This algorithm is applicable to systems with state constraints that might change after initial feasibility is established in *standard* mode; e.g., another vehicle crossing/stopping in the feasible path, or unexpected proximity/altitude relative to the ground. If state constraints change, the guaranteed immediate availability of *safety* mode allows entry into an invariant safety state for all time. From this state, a higher-level, control-decision-making process (which is outside the scope of this paper) can search for a new feasible solution, if one exists, to continue toward the target or to define a new one.

ACKNOWLEDGEMENTS

This research was funded by AFOSR MURI grant FA9550-06-1-0303 and Caltech/NASA Jet Propulsion Laboratory internal R&TD (Research and Technology Development). Publication support was provided by the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

REFERENCES

A. B. Açıkmeşe and J. M. Carson. A nonlinear model predictive control algorithm with proven robustness and resolvability. In *Proceedings of the American Control Conference*, pages 887–893, June 2006.

A. B. Açıkmeşe and M. Corless. Robust tracking and disturbance rejection of bounded rate signals for uncertain/non-linear systems. *International Journal of Control*, 76(11):1129–1141, 2003.

B. Açıkmeşe and J. M. Carson. LMI-based generation of feedback laws for a robust model predictive control algorithm. JPL Document D-40295, Clearance #08-0025, Jet Propulsion Laboratory, California Institute of Technology, September 2007. Available from JPL Technical Report Server: "http://hdl.handle.net/2014/40622".

A. Bemporad, F. Borelli, and M. Morari. Model predictive control based on linear programming - the explicit solution. *IEEE Transactions on Automatic Control*, 47 (12):1974–1985, 2002a.

A. Bemporad, M. Morari, V. Dua, and E. N. Pistikopoulos. The explicit linear quadratic regulator for constrained systems. *Automatica*, 38(1):3–20, 2002b.

S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

J.M. Carson. *Robust Model Predictive Control with a Reactive Safety Mode*. PhD thesis, California Institute of Technology, 2008.

H. Chen and F. Allgöwer. A quasi-infinite horizon nonlinear model predictive control scheme with guaranteed stability. *Automatica*, 34(10):1205–1217, 1998.

A. Jadbabaie. *Receding Horizon Control of Nonlinear Systems: A Control Lyapunov Function Approach*. PhD thesis, California Institute of Technology, 2000.

A. A. Jalali and V. Nadimi. A survey on robust model predictive control from 1999-2006. In *Proceedings of the International Conference on CIMCA-IAWTIC*, pages 207–212, November 2006.

H. K. Khalil. *Nonlinear Systems, Second Edition*. Prentice Hall, 1996.

M. V. Kothare, V. Balakrishnan, and M. Morari. Robust constrained model predictive control using linear matrix inequalities. *Automatica*, 32(10):1361–1379, 1996.

Y. Kuwata, T. Schouwenaars, A. Richards, and J. How. Robust constrained receding horizon control for trajectory planning. In *Proceedings of the AIAA Guidance, Navigation, and Control Conference and Exhibit*, August 2005. AIAA-2005-6079.

M. Magni, H. Nijmeijer, and A. Van Der Schaft. A receding horizon approach to the nonlinear H_∞ control problem. *Automatica*, 37(3):429–435, 2001.

D.Q. Mayne, J. B. Rawlings, C.V. Rao, and P.O.M. Scokaert. Constrained model predictive control: Stability and optimality. *Automatica*, 36(6):789–814, 2000.

H. Michalska and D.Q. Mayne. Robust receding horizon control of constrained nonlinear systems. *IEEE Transactions on Automatic Control*, 38(11):1623–1633, 1993.

Y. Nesterov and A. Nemirovsky. *Interior-point Polynomial Methods in Convex Programming*. SIAM, 1994.

J. B. Rawlings and K. R. Muske. The stability of constrained receding horizon control. *IEEE Transactions on Automatic Control*, 38(10):1512–1516, 1993.

A. G. Richards and J.P. How. Robust stable model predictive control algorithm with constraint tightening. In *Proceedings of the American Control Conference*, pages 1557–1562, June 2006.

T. Schouwenaars, J. How, and E. Feron. Receding horizon path planning with implicit safety guarantees. In *Proceedings of the American Control Conference*, pages 5576–5581, June 2004.

P. O. M. Scokaert and D. Q. Mayne. Min-max feedback model predictive control for constrained linear sytems. *IEEE Transactions on Automatic Control*, 43(8):1136–1142, 1998.

R. S. Smith. Robust model predictive control of constrained linear systems. In *Proceedings of the American Control Conference*, pages 245–250, June 2004.

W.Langson, I. Chryssochoos, S.V. Raković, and D.Q. Mayne. Robust model predictive control using tubes. *Automatica*, 40(1):125–133, 2004.