Adversarial Model Predictive Control via Second-Order Cone Programming

James Guthrie and Enrique Mallada

***Abstract*— We study the problem of designing attacks to safety-critical systems in which the adversary seeks to maximize the overall system cost within a model predictive control framework. Although in general this problem is NP-hard, we characterize a family of problems that can be solved in polynomial time via a second-order cone programming relaxation. In particular, we show that positive systems fall under this family. We provide examples demonstrating the design of optimal attacks on an autonomous vehicle and a microgrid.**

I. INTRODUCTION

Safety-critical systems increasingly rely on distributed feedback for their underlying control algorithms. In these cyber-physical systems, the action of individual agents is impacted by the state of other agents which is either sensed directly or obtained over communication channels. Common examples include, for instance, power grids and vehicle platoons. Given the critical nature of these systems, it is essential to ensure that the control algorithms utilized are robust to adversarial attacks which can take many forms.

For example, in false data injection attacks, an adversary takes control over communication channels and corrupts the feedback data to compromise the system performance. Much recent work has focused on designing and detecting false data injection attacks within power systems [1]–[3]. Alternatively, instead of corrupting feedback channel information, an attacker could compromise existing agents or introduce new adversarial agents with the aim of degrading system performance. Examples include adding a rogue car to a vehicle platoon [4] or malicious demand response in power grids [5]. Lastly, instead of injecting false sensor data or introducing adversarial agents, the attacker might take over the whole system and control it with an antagonistic algorithm [6] that maximizes damage.

Performance of these cyber-physical systems is often measured with respect to a convex quadratic cost function. For example, consensus problems seek to minimize the disagreement between agents. Regulation problems seek to minimize the deviation from a desired equilibrium condition. In designing attacks on these systems, it is therefore natural to seek to maximize these same objectives. This leads to a non-convex problem which is NP-hard in general. Due to the computational complexity, suboptimal solutions are typically sought via convex-concave approximations [6], semidefinite relaxations [3], or general nonlinear programming methods. Alternatively, an attacker may avoid the non-convex problem by selecting a target state (which is different from the system's intended operational state) and minimizing deviations from it [7]. While the resulting problem is convex, the choice of target state is arbitrary and up to the attacker to determine. Thus the target state often acts as a surrogate for true adversarial intentions.

This paper seeks a different approach. Instead of looking for suboptimal or surrogate solutions, we focus on instances in which the non-convex problem can be solved to global optimality. By leveraging optimality guarantees for second-order cone program (SOCP) relaxations of non-convex quadratically-constrained quadratic programs (QCQPs), we provide a characterization of a family of systems that are highly susceptible to adversarial attacks. Surprisingly, the characterized family includes, as a special case, positive systems with non-positive quadratic objectives and constraints.

This has application to many cyber-physical systems, including micro-grids [8] and vehicle platoons [9] which often exhibit positive dynamics. Our results suggest that these systems are highly vulnerable to adversarial attacks and promotes the need of further research into the development of new methodologies that can make these systems less vulnerable to such attacks.

The rest of the paper is organized as follows. Section II introduces some preliminaries, including the formal definition of QCQP, an overview of the SOCP relaxation used in this paper, and the definition of positive systems. Section III formalizes the adversarial MPC problem to be used in this paper, as well some useful reformulations. Section IV establishes conditions under which a non-convex MPC problem has an exact SOCP relaxation. Section V provides a few numerical illustrations of our approach, and Section VI concludes the paper and discusses future directions.

A. Notation

Let $\mathbb{S}^n$ denote the set of $n \times n$ symmetric matrices, $\mathbb{N}$ denote the set of non-negative integers, $\mathbb{N}^+$ the set of positive integers, and A^T denote the transpose of a matrix A. Let a_j denote the element j of vector $a \in \mathbb{R}^n$ and $[A]_{jk}$ denote element (j,k) of matrix A. The inequalities $\leq$, $\geq$ are to be interpreted element-wise. I_n denotes the $n \times n$ identity matrix, $0_{m\times n}$ the $m \times n$ zero matrix, and $\mathbb{1}_n$ a vector in $\mathbb{R}^n$ with all entries equal to 1. We occasionally drop subscripts where dimensions can be inferred from context. For A, $B \in \mathbb{S}^n$, let $A \cdot B = \sum_{j=1}^n \sum_{k=1}^n [A]_{jk}[B]_{jk}$.

[1]James Guthrie and Enrique Mallada are with the Johns Hopkins University, Baltimore, Maryland, USA. jguthri6@jhu.edu, mallada@jhu.edu

The work was supported by ARO through contract W911NF-17-1-0092, US DoE EERE award DE-EE0008006, and NSF through grants CNS 1544771, EPCN 1711188, AMPS 1736448, and CAREER 1752362.

II. PRELIMINARIES

A. Exact Solutions of Some Non-Convex QCQPs

We first review the main result of [10] regarding the conditions under which non-convex QCQPs can be solved exactly via a SOCP relaxation. Consider the following QCQP

$$\begin{aligned} \min_{z} \quad & z^T Q_0 z + 2q_0^T z + \gamma_0 \\ \text{s.t.} \quad & z^T Q_i z + 2q_i^T z + \gamma_i \leq 0, \quad i = 1, \ldots, m \end{aligned} \tag{1}$$

where $z \in \mathbb{R}^n$, $Q_p \in \mathbb{S}^n$, $q_p \in \mathbb{R}^n$, $\gamma_p \in \mathbb{R}$ and $p \in \{0, 1, ..., m\}$. Define the following matrix:

$$P_p = \begin{bmatrix} \gamma_p & q_p^T \\ q_p & Q_p \end{bmatrix} \tag{2}$$

We rewrite the QCQP in homogeneous form as:

$$\begin{aligned} \min_{z} \quad & \begin{bmatrix} 1 \\ z \end{bmatrix}^T P_0 \begin{bmatrix} 1 \\ z \end{bmatrix} \\ \text{s.t.} \quad & \begin{bmatrix} 1 \\ z \end{bmatrix}^T P_i \begin{bmatrix} 1 \\ z \end{bmatrix} \leq 0, \quad i = 1, \ldots, m \end{aligned} \tag{3}$$

where $z \in \mathbb{R}^n$, and $P_p \in \mathbb{S}^{n+1}$ for $p \in \{0, 1, ..., m\}$.

Herein we make no assumptions about the sign definiteness of matrices P_p. When P_0 contains at least one negative eigenvalue, problem (3) is non-convex and NP-hard to solve [11]. In [10] it was shown that if the matrices collectively satisfy a specific sign property (defined below), the non-convex QCQP can be solved to global optimality via a second-order cone program. For convenience, we restate the relevant definitions and theorem of [10].

Definition 1 ([10])**.** A symmetric matrix $A \in \mathbb{S}^n$ is said to be *almost off-diagonal non-positive* if there exists a sign vector $\sigma \in \{-1, +1\}^n$ such that $[A]_{jk}\sigma_j\sigma_k \leq 0,\ (0 \leq j < k \leq n)$

Definition 2 ([10])**.** A family of symmetric matrices $A_p \in \mathbb{S}^n\ (0 \leq p \leq m)$ is said to be *uniformly almost off-diagonal non-positive* if there exists a sign vector $\sigma \in \{-1, +1\}^n$ such that $[A_p]_{jk}\sigma_j\sigma_k \leq 0,\ (1 \leq j < k \leq n,\ 0 \leq p \leq m)$

Theorem 1 ([10])**.** *Consider a QCQP of the form (3) in which the family of symmetric matrices $P_p \in \mathbb{S}^{n+1},\ (0 \leq p \leq m)$ is uniformly almost off-diagonal non-positive with respect to a sign vector $\sigma \in \{-1, +1\}^{n+1}$. Let $\Lambda = \{(j, k) : [P_p]_{jk} \neq 0$ for some $0 \leq p \leq m,\ 0 \leq j < k \leq n\}$. Then*

$$z = \begin{bmatrix} \sigma_0\sigma_1\sqrt{[X]_{11}} & \ldots & \sigma_0\sigma_n\sqrt{[X]_{nn}} \end{bmatrix}^T \tag{4}$$

is an optimal solution of (3) where X is the optimal solution of the following second-order cone program:

$$\begin{aligned} \min_{X} \quad & P_0 \cdot X \\ \text{s.t.} \quad & P_i \cdot X \leq 0, \quad i = 1, \ldots, m, \\ & [X]_{00} = 1, \\ & \left\| \begin{bmatrix} [X]_{jj} - [X]_{kk} \\ 2[X]_{jk} \end{bmatrix} \right\|_2 \leq [X]_{jj} + [X]_{kk}, (j, k) \in \Lambda \end{aligned} \tag{5}$$

B. Positive Systems

Consider a discrete-time linear system

$$x(k+1) = Ax(k) + Bu(k) \tag{6}$$

where $k \in \mathbb{N}, x(k) \in \mathbb{R}^{n_x}$ and $u(k) \in \mathbb{R}^{n_u}$. Let $x(0)$ denote the initial state of the system.

Definition 3. A discrete-time linear system is said to be *positive* if $A \geq 0$ and $B \geq 0$.

Lemma 1 ([12])**.** *Consider a positive system (A, B) with initial condition $x(0) \geq 0$. Given an input sequence $u(k) \geq 0,\ (0 \leq k \leq N-1)$, then $x(k) \geq 0,\ (1 \leq k \leq N)$.*

III. PROBLEM SETUP

A. Model Predictive Control

Consider a discrete-time, linear system model

$$x(k+1) = Ax(k) + Bu(k) \tag{7}$$

where $x(k) \in \mathbb{R}^{n_x}$ and $u(k) \in \mathbb{R}^{n_u}$. Let $x(0)$ denote the initial state of the system. To reduce notational clutter, we will write $x(0)$ as x_0 in the following. Standard linear MPC determines the optimal sequence of control actions over a prediction horizon $N \in \mathbb{N}^+$ to minimize a given quadratic cost function while respecting constraints on the system states and controls [13]. For convenience, define the following:

$$\begin{aligned} \mathcal{X} &= \begin{bmatrix} x(0) \\ x(1) \\ \vdots \\ x(N) \end{bmatrix} \mathcal{U} = \begin{bmatrix} u(0) \\ u(1) \\ \vdots \\ u(N-1) \end{bmatrix} S_x = \begin{bmatrix} I \\ A \\ \vdots \\ A^N \end{bmatrix} \\ S_u &= \begin{bmatrix} 0 & \ldots & \ldots & 0 \\ B & 0 & \ldots & 0 \\ AB & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ A^{N-1}B & \ldots & \ldots & B \end{bmatrix} \end{aligned} \tag{8}$$

The system dynamics over the horizon N then evolve according to

$$\mathcal{X} = S_x x_0 + S_u \mathcal{U} \tag{9}$$

The MPC cost and constraint functions will be represented by generic quadratic functions of the form

$$\begin{aligned} &F_i(\mathcal{X}, \mathcal{U}) = \\ &\quad \begin{bmatrix} \mathcal{X} \\ \mathcal{U} \end{bmatrix}^T \begin{bmatrix} Q_i & S_i \\ S_i^T & R_i \end{bmatrix} \begin{bmatrix} \mathcal{X} \\ \mathcal{U} \end{bmatrix} + 2 \begin{bmatrix} q_i \\ r_i \end{bmatrix}^T \begin{bmatrix} \mathcal{X} \\ \mathcal{U} \end{bmatrix} + \gamma_i \end{aligned} \tag{10}$$

where $Q_i \in \mathbb{S}^{(N+1)n_x}, R_i \in \mathbb{S}^{Nn_u}, S_i \in \mathbb{R}^{(N+1)n_x \times Nn_u}$, $q_i \in \mathbb{R}^{(N+1)n_x}, r_i \in \mathbb{R}^{Nn_u}, \gamma_i \in \mathbb{R}$.
The MPC problem can then be written compactly as:

$$\begin{aligned} \min_{\mathcal{X}, \mathcal{U}} \quad & F_0(\mathcal{X}, \mathcal{U}) \\ \text{s.t.} \quad & \mathcal{X} = S_x x_0 + S_u \mathcal{U}, \\ & F_i(\mathcal{X}, \mathcal{U}) \leq 0, \qquad i = 1, \ldots, m \end{aligned} \tag{11}$$

In this formulation, both the state $\mathcal{X}$ and control sequence $\mathcal{U}$ are decision variables.

B. Condensed MPC

We next project the quadratic cost and constraint functions $F_i(\mathcal{X},\mathcal{U})$ onto the dynamic equality constraint (9), eliminating the state vector $\mathcal{X}$ as a decision variable. This is often referred to as the condensed formulation as the resulting problem is of smaller dimension but with less sparsity in the matrices. We substitute (9) for $\mathcal{X}$ in (10) and define a new quadratic function of the form

$$G_i(x_0,\mathcal{U}) = \mathcal{U}^T M_i \mathcal{U} + 2(x_0^T N_i + d_i^T)\mathcal{U} + x_0^T T_i x_0 + 2v_i^T x_0 + \gamma_i \quad (12)$$

where

$$M_i = S_u^T Q_i S_u + S_u^T S_i + S_i^T S_u + R_i \quad (13)$$
$$N_i = S_x^T Q_i S_u + S_x^T S_i \quad (14)$$
$$d_i = S_u^T q_i + r_i \quad (15)$$
$$T_i = S_x^T Q_i S_x \quad (16)$$
$$v_i = S_x^T q_i \quad (17)$$

The condensed MPC formulation is then written as:

$$\begin{aligned} \min_{\mathcal{U}} \quad & G_0(x_0,\mathcal{U}) \\ \text{s.t.} \quad & G_i(x_0,\mathcal{U}) \leq 0, \quad i = 1,\dots,m \end{aligned} \quad (18)$$

Lastly, we rewrite the functions $G_i(x_0,\mathcal{U})$ in homogeneous form by defining the following matrix:

$$P_i(x_0) = \begin{bmatrix} x_0^T T_i x_0 + 2v_i^T x_0 + \gamma_i & (x_0^T N_i + d_i^T) \\ (N_i^T x_0 + d_i) & M_i \end{bmatrix} \quad (19)$$

We obtain the following equivalent homogeneous quadratic program:

$$\begin{aligned} \min_{\mathcal{U}} \quad & \begin{bmatrix} 1 \\ \mathcal{U} \end{bmatrix}^T P_0(x_0) \begin{bmatrix} 1 \\ \mathcal{U} \end{bmatrix} \\ \text{s.t.} \quad & \begin{bmatrix} 1 \\ \mathcal{U} \end{bmatrix}^T P_i(x_0) \begin{bmatrix} 1 \\ \mathcal{U} \end{bmatrix} \leq 0, \quad i = 1,\dots,m \end{aligned} \quad (20)$$

Remark. Although the homogeneous quadratic form is a less common MPC formulation, it will allow us to readily apply the proposed SOCP relaxation of Theorem 1.

IV. Adversarial MPC with Non-Convex Quadratic Functions

Provided the matrices P_i $(i = 0,\dots,m)$ of (20) satisfy the conditions of Theorem 1, the (possibly non-convex) QCQP can be solved exactly via its SOCP relaxation. However, a priori it is not easy to see what system properties and conditions of the MPC problem are necessary to ensure Theorem 1 applies. The following theorem identifies these system properties and conditions.

Theorem 2. *Consider the homogeneous MPC formulation (20) for controlling the discrete linear system (7) over a horizon length N. Define $n = Nn_u$ as the dimension of the decision variable $\mathcal{U}$. Let the system dynamics (A, B), cost and constraint matrices $(Q_i, R_i, S_i, i = 0,\dots,m)$ be such that the family of matrices $M_i \in \mathbb{S}^n (i = 0,\dots,m)$ defined by (13) is uniformly almost off-diagonal non-positive with respect to a given vector $\sigma \in \{-1,+1\}^n$. Then (20) can be solved exactly using the SOCP relaxation (5) and reconstructing $\mathcal{U}$ according to (4) with $\bar{\sigma}^+ = \begin{bmatrix} 1 & \sigma_1 & \dots & \sigma_n \end{bmatrix}^T$ when $x_0 \in \mathbb{X}^+$ and $\bar{\sigma}^- = \begin{bmatrix} 1 & -\sigma_1 & \dots & -\sigma_n \end{bmatrix}^T$ when $x_0 \in \mathbb{X}^-$ where $\mathbb{X}^+$ and $\mathbb{X}^-$ are given by:*

$$\mathbb{X}^+ = \{x \mid [x_0^T N_i + d_i^T]_{1k}\sigma_k \leq 0\}, \quad (21)$$
$$\mathbb{X}^- = \{x \mid [x_0^T N_i + d_i^T]_{1k}\sigma_k \geq 0\}, \quad (22)$$
$$0 \leq i \leq m, 1 \leq k \leq n$$

Proof. By Definition 2, the family of matrices $P_i(x_0), i = 0,\dots,m$, is uniformly almost off-diagonal non-positive with respect to $\bar{\sigma}^+$ if:

$$[P_i(x_0)]_{jk}\bar{\sigma}_j^+\bar{\sigma}_k^+ \leq 0 \quad (23)$$
$$0 \leq i \leq m, 1 \leq j < k \leq n+1$$

Given that $\bar{\sigma}_1^+ = 1$, it is straight-forward to see that this is equivalent to the conditions

$$[x_0^T N_i + d_i^T]_{1k}\sigma_k \leq 0 \quad (24)$$
$$[M_i]_{jk}\sigma_j\sigma_k \leq 0 \quad (25)$$
$$0 \leq i \leq m, 1 \leq j < k \leq n$$

Inequality (25) is satisfied by the stated assumption that M_i is uniformly almost off-diagonal non-positive with respect to σ. Thus we have (24) $\iff$ (23). Let $\mathbb{X}^+$ denote the set of vectors that satisfy (24). When $x_0 \in \mathbb{X}^+$, the family of matrices $P_i(x_0)$ is uniformly almost off-diagonal non-positive with respect to $\bar{\sigma}^+$ and Theorem 1 applies. A nearly identical proof establishes that $P_i(x_0)$ is uniformly almost off-diagonal non-positive with respect to $\bar{\sigma}^-$ for $x_0 \in \mathbb{X}^-$. □

Remark. Theorem 2 allows us to characterize a class of non-convex MPC problems that can be solved using the SOCP relaxation of Theorem 1. Notably, the solvability of the problem depends on the initial condition x_0 via the sets $\mathbb{X}^+$ and $\mathbb{X}^-$.

It is possible that, for different initial conditions, the conditions of Theorem 2 are satisfied for different σ. The follow lemma further illustrates the relationship between $P_i(x_0)$, σ and the corresponding sets $\mathbb{X}^+$ and $\mathbb{X}^-$.

Lemma 2. *Given a single matrix $P_i(x_0) \in \mathbb{S}^{n+1}, i \in \mathbb{N}$ that is almost off-diagonal non-positive with respect to some $\bar{\sigma} \in \{-1,+1\}^{n+1}$ then $-P_i(x_0)$ is also almost off-diagonal non-positive with respect to $\bar{\sigma}$ if and only if it is diagonal.*

Proof. Sufficient: $P_i(x_0)$ is diagonal implies $[P_i(x_0)]_{jk} = 0$ $(1 \leq j < k \leq n+1)$. Applying Definition 1, a matrix is almost off-diagonal non-positive with respect to $\bar{\sigma}$ if $[P_i(x_0)]_{jk}\bar{\sigma}_j\bar{\sigma}_k \leq 0$ $(1 \leq j < k \leq n+1)$. Given a diagonal matrix, this relationship is true for arbitrary $\bar{\sigma}$. If $P_i(x_0)$ is diagonal then $-P_i(x_0)$ is also diagonal and therefore almost off-diagonal non-positive with respect to any $\bar{\sigma}$. Necessary: Consider a matrix $P_i(x_0) \in \mathbb{S}^{n+1}$ with element $[P_i(x_0)]_{jk} \neq$

$0, (j < k)$ that is almost off-diagonal non-positive with respect to $\bar{\sigma}$. This implies $[P_i(x_0)]_{jk}\bar{\sigma}_j\bar{\sigma}_k < 0$ and thus $[-P_i(x_0)]_{jk}\bar{\sigma}_j\bar{\sigma}_k > 0$. Therefore $-P_i(x_0)$ cannot be almost off-diagonal non-positive with respect to $\bar{\sigma}$. □

Remark. Diagonal $P_i(x_0)$ includes the important case of norm bounds on the control vector as given by $l_b \leq \mathcal{U}^T R\mathcal{U} \leq u_b$ where R is diagonal with non-negative entries and $l_b, u_b \in \mathbb{R}$ are the lower and upper bounds respectively. When $l_b > 0$ and R contains more than one non-zero entry, the resulting constraint is non-convex. This can be rewritten as two constraints $-\mathcal{U}^T R\mathcal{U} \leq l_b$ and $\mathcal{U}^T R\mathcal{U} \leq u_b$ both of which give diagonal matrices when put in the form (19). We note that non-convex control constraints of this form arise in thrust vectoring problems [14].

Remark. Linear state weightings of the form $c^T\mathcal{X}$ with $c \in \mathbb{R}^{(N+1)n_x}$ translate to off-diagonal entries in (19). If a lower bound l_b and upper bound u_b is applied to a given state weighting, one obtains two equal and opposite matrices $P_i(x_0)$ and $-P_i(x_0)$ with off-diagonal terms. Applying Lemma 2, both of the matrices cannot be almost off-diagonal non-positive with respect to a given $\bar{\sigma}$. Thus Theorem 2 does not support MPC formulations with lower and upper bounds applied to a given state weighting. In adversarial control this is not a major limitation in practice as one is not attempting to keep the system state within some prescribed bounds.

A. Adversarial Control of Positive Systems

The previous section established state-dependent conditions under which the homogeneous adversarial MPC formulation (20) can be solved by applying Theorem 1. By restricting ourselves to positive systems, we establish conditions under which Theorem 1 holds for all $x_0 \geq 0$ (i.e. the positive orthant).

Theorem 3. *Consider the homogeneous MPC formulation (20) for controlling a discrete-time linear system (7) over a horizon length N. Let the system dynamics (A, B) be positive as described in Definition 3. Define $n = Nn_u$ as the dimension of the decision variable $\mathcal{U}$. Let the cost and constraint matrices be such that $Q_i \leq 0,\ [R_i]_{jk} \leq 0\ (j \neq k),\ S_i \leq 0,\ q_i \leq 0,\ r_i \leq 0$ for $i = 0, \ldots, m$. Then (20) can be solved using Theorem 1 with $\bar{\sigma}^+ = \mathbb{1}_{n+1}$ when $x_0 \geq 0$.*

Proof. The proof is simple but involves some tedious algebra. For clarity, we outline the main steps below:

1) Show that $[M_i]_{jk} \leq 0, \quad 1 \leq j < k \leq n,\ 0 \leq i \leq m$.
   Proof: See below
2) Show that $N_i \leq 0, d_i \leq 0, \quad 0 \leq i \leq m$
   Proof: See below
3) $N_i \leq 0, d_i \leq 0, x_0 \geq 0 \implies (x_0^T N_i + d_i^T) \leq 0$
4) Steps 1 and 3 imply $[P_i(x_0)]_{jk} \leq 0\ \forall\ (j \neq k, x_0 \geq 0)$. Therefore $P_i(x_0)$ is uniformly almost off-diagonal non-positive with respect to $\bar{\sigma}^+ = \mathbb{1}_{n+1}$ and (20) can be solved using Theorem 1.

Step 1) Recall that the product of two non-negative matrices is itself non-negative. We are given that $A \geq 0, B \geq 0$. By induction, the products $A^i \geq 0, A^iB \geq 0,\ \forall\ i \in \mathbb{N}$. This implies $S_x \geq 0$ and $S_u \geq 0$ as all the individual non-zero entries shown in (8) can be written in terms of A^i and A^iB for some $i \in \mathbb{N}$. Recall that the product of a non-negative matrix and non-positive matrix is non-positive. So $S_i \leq 0$, $S_u \geq 0, Q_i \leq 0 \implies S_u^T S_i \leq 0,\ S_u^T Q_i S_u \leq 0$ and therefore $S_u^T Q_i S_u + S_u^T S_i + S_i^T S_u \leq 0$. Lastly, we are given that $[R_i]_{jk} \leq 0\ (j \neq k)$. From (13), $M_i = S_u^T Q_i S_u + S_u^T S_i + S_i^T S_u + R_i$. Combining the previous results establishes that $[M_i]_{jk} \leq 0\ (1 \leq j < k \leq n, 0 \leq i \leq m)$.

Step 2) Given $S_x \geq 0,\ S_u \geq 0,\ Q_i \leq 0,\ S_i \leq 0,\ q_i \leq 0$, and $r_i \leq 0$, similar reasoning as Step 1 establishes that $N_i \leq 0$ and $d_i \leq 0$ as defined by (14) and (15) respectively. □

Remark. As $\bar{\sigma}^+ = \mathbb{1}_{n+1}$ determines the sign pattern of the solution, the resulting control sequence $\mathcal{U}$ is non-negative. A positive system will remain in the positive orthant under the action of this control sequence per Lemma 1.

Remark. Theorem 3 includes the practical case of an objective function with diagonal $Q_0 < 0$ and diagonal $R_0 > 0$. This represents a situation in which an adversary is attempting to push the system away from the origin while minimizing the energy expended to do so.

V. Numerical Examples

We demonstrate our results on some simple systems. To clearly point out sources of non-convexity, we write the examples in uncondensed form with state variables appearing in the cost function. However, the resulting problems are solved by converting the problem to the form of (20) and applying Theorem 1.

A. Indefinite Cost Function

Our first example applies an indefinite cost function to a two-state system. This allows us to show graphically the regions $\mathbb{X}^+$ and $\mathbb{X}^-$ where we can solve the problem exactly. Consider the following discrete state-space model:

$$A = \begin{bmatrix} 0.9 & -0.2 \\ 0 & 0.9 \end{bmatrix} \quad B = \begin{bmatrix} 0.2 & -0.05 \\ 0 & 2 \end{bmatrix}$$

We apply an indefinite quadratic objective of minimizing the product of the two states over a horizon N. The control at each step k is constrained to an annulus in $\mathbb{R}^2$. Additionally, the total control effort over the horizon N is constrained, reflecting energy constraints.

$$\begin{aligned} \min \quad & \sum_{k=0}^{N} x(k)^T \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} x(k) \\ \text{s.t.} \quad & \mathcal{X} = S_x x(0) + S_u \mathcal{U}, \\ & 0.2 \leq \|u(k)\|_2^2 \leq 0.5, \quad k = 0, \ldots, N-1, \\ & 0 \leq \|\mathcal{U}\|_2^2 \leq \frac{N}{3} \end{aligned}$$

We rewrite this in condensed form. Dropping constant terms, the resulting cost function becomes:

$$G_0(x(0), \mathcal{U}) = \mathcal{U}^T M_0 \mathcal{U} + 2(x(0)^T N_0)\mathcal{U}$$

Where for $N = 2$ we have:

$$M_0 = \begin{bmatrix} 0 & 0.0724 & 0 & 0.0360 \\ 0.0724 & -0.0506 & 0.0360 & -0.0260 \\ 0 & 0.0360 & 0 & 0.0400 \\ 0.0360 & -0.0260 & 0.0400 & -0.0200 \end{bmatrix}$$

$$N_0 = \begin{bmatrix} 0 & 0.3258 & 0 & 0.1620 \\ 0.3258 & -0.2187 & 0.1620 & -0.1125 \end{bmatrix}$$

Here there is no offset term d_0 as we have no linear terms (q_0, r_0) in our original, uncondensed cost. M_0 is off-diagonal non-positive with respect to $\sigma = \begin{bmatrix} 1 & -1 & 1 & -1 \end{bmatrix}$. From Theorem 2 the SOCP relaxation is exact for $x(0) \in \mathbb{X}^+ \cup \mathbb{X}^-$ where $\mathbb{X}^+ = \{x \mid x \in \mathbb{R}^2, [x(0)^T N_0]_{1k}\sigma_k \leq 0 \ (1 \leq k \leq 4)\}$ and $\mathbb{X}^-$ is similarly defined. Although $\mathbb{X}^+$ and $\mathbb{X}^-$ are described by the intersection of four hyperplanes which pass through the origin, we can limit ourselves to the two hyperplanes whose normal vector has the smallest inner product. This gives the following:

$$\mathbb{X}^+ = \{x \mid x \in \mathbb{R}^2, x_2 \leq 0, -0.32358x_1 + 0.2187x_2 \leq 0\}$$
$$\mathbb{X}^- = \{x \mid x \in \mathbb{R}^2, x_2 \geq 0, -0.32358x_1 + 0.2187x_2 \geq 0\}$$

Figure 1 shows the regions $\mathbb{X}^+$, $\mathbb{X}^-$ when $N = 2$. A sample trajectory is shown starting from $x(0) = [0 \ 0.1]^T$. With a horizon of $N = 2$ we only obtain control commands $u(0)$ and $u(1)$. As is standard in MPC, we apply the first command $u(0)$ which takes us to state $x(1)$. Redefining $x(1)$ as our new initial condition we then resolve the problem. We repeat this process 10 times to obtain the trajectory shown.

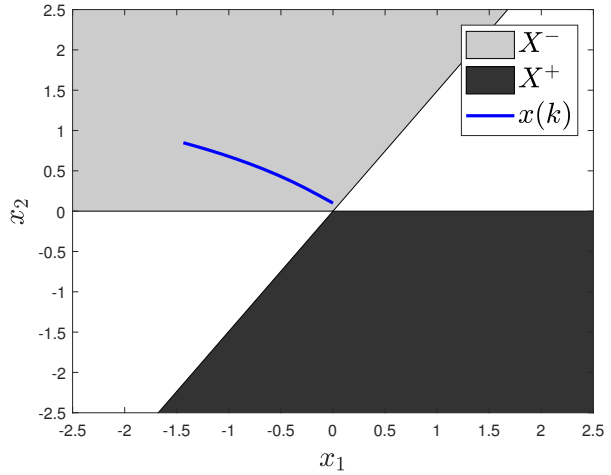

Fig. 1. Indefinite MPC example ($N = 2$) starting at $x(0) = [0 \ 0.1]^T$

Remark. $\mathbb{X}^+$ and $\mathbb{X}^-$ are described by the intersection of halfspaces formed from the columns of $N_0 \in \mathbb{R}^{n_x \times N n_u}$. Interestingly for this problem, as N is increased the sets $\mathbb{X}^+$, $\mathbb{X}^-$ cover a larger portion of $\mathbb{R}^2$. For example, Figure 2 shows $\mathbb{X}^+$, $\mathbb{X}^-$ for $N = 20$. With this horizon length we can solve a trajectory starting at $x(0) = [1 \ 0.5]^T$ which is outside the solvable regions when $N = 2$.

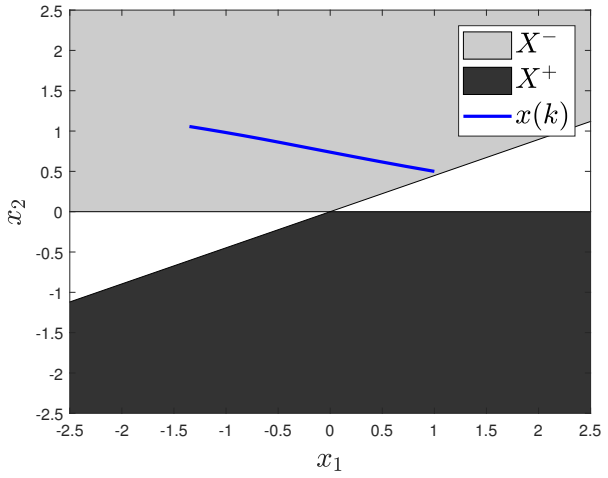

Fig. 2. Indefinite MPC example ($N = 20$) starting at $x(0) = [1 \ 0.5]^T$

Remark. Minimizing or maximizing the product of two states is frequently seen in economic MPC formulations. In some instances, an indefinite stage cost can still yield a convex problem if applied over a sufficiently long horizon [15]. That does not occur here. Instead the cost function remains indefinite with N positive eigenvalues and N negative eigenvalues for a given horizon length N.

B. Adversarial Control of Double Integrator

Consider a simple planar double integrator model of an autonomous vehicle with position states (p_x, p_y) and associated velocity states (v_x, v_y). State feedback damping terms regulate the system to the origin. An adversary is able to apply disturbance forces (u_1, u_2) to the system. The continuous dynamics are given by:

$$\frac{dp_x}{dt} = -0.1p_x + v_x \qquad \frac{dv_x}{dt} = -0.1v_x + u_1$$
$$\frac{dp_y}{dt} = -0.1p_y + v_y \qquad \frac{dv_y}{dt} = -0.1v_y + u_2$$

We discretize the continuous model using a zero-order-hold with 0.2s sample time obtaining matrices (A, B) with state vector $x = [p_x \ p_y \ v_x \ v_y]^T$ and control $u = [u_1 \ u_2]^T$. By inspection the discrete model is positive.

$$A = \begin{bmatrix} 0.9802 & 0 & 0.196 & 0 \\ 0 & 0.9802 & 0 & 0.196 \\ 0 & 0 & 0.9802 & 0 \\ 0 & 0 & 0 & 0.9802 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.01974 & 0 \\ 0 & 0.01974 \\ 0.198 & 0 \\ 0 & 0.198 \end{bmatrix}$$

We are given a safety envelope defined by the union of two ellipsoids centered at the origin. The adversaries objective is ensure the system's position is outside this safe operating envelope by the end of a horizon $N = 10$ while minimizing energy expenditure. This terminal position constraint is non-convex. The available control magnitude is bounded to be within an annulus representative of thrust vectoring constraints. The resulting adversarial MPC problem is:

$$\begin{aligned}
\min_{\mathcal{U}} \quad & \|\mathcal{U}\| \\
\text{s.t.} \quad & 1.0 \leq \left(\frac{p_x(k)}{1.0}\right)^2 + \left(\frac{p_y(k)}{0.5}\right)^2, \ k = N, \\
& 1.0 \leq \left(\frac{p_x(k)}{0.5}\right)^2 + \left(\frac{p_y(k)}{1.0}\right)^2, \ k = N, \\
& 0.04 \leq u_1^2(k) + u_2^2(k) \leq 0.25, \quad k = 0, \ldots, N-1
\end{aligned}$$

Written in the standard quadratic form of (10), the terminal position constraints have matrices $Q_i \leq 0$ while the control constraints consist of diagonal R_i. Thus Theorem 3 applies and we can solve this non-convex problem when $x_0 \geq 0$. Figure 3 plots the ellipse bounds in the positive orthant and shows sample trajectories with varying initial positions. Figure 4 shows the associated control command. The initial velocities are zero in each example. Starting at point $(0, 0)$ the adversarial control pushes the system towards the closest point on the border of the safety envelope, reaching this point only at the end in order to minimize the energy expended. Starting at $(0.5, 0)$ the damped dynamics of A are evident as the trajectory initially moves towards the origin. Finally, starting closer to the boundary at $(0.1, 0.7)$, the trajectory overshoots the boundary. This is due to the non-convex lower bound on the control magnitude which prevents us from turning off the control.

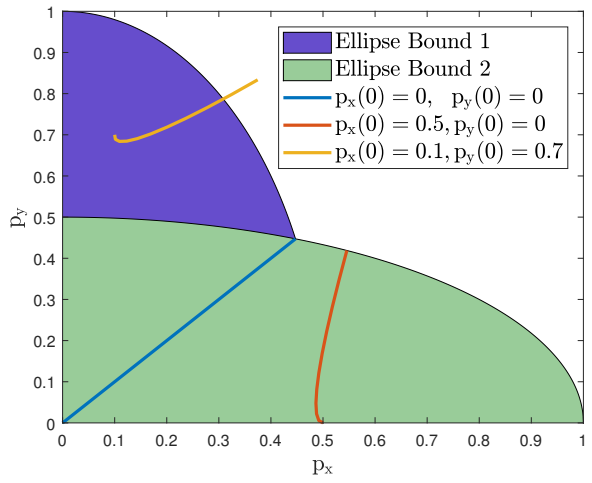

Fig. 3. Safety envelope violation with minimum energy expenditure

C. Maximizing Voltage Mismatch within a Microgrid

Finally we consider a simple microgrid model consisting of three buses. Without loss of generality, the origin is taken to be the equilibrium point. Each bus i is modeled as a capacitor c_i with voltage v_i. The buses are interconnected by resistive transmission lines r_2 and r_3. Collectively they supply power to a resistive load r_1 and a constant power load whose linearized dynamics can be represented by a negative resistance r_4. An adversary is able to inject current into the system through i_1 and i_2. Table I lists the parameters.

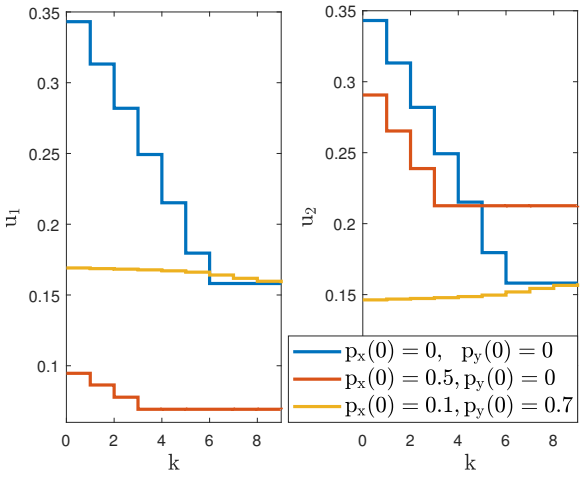

Fig. 4. Control history for safety envelope violation

TABLE I
MICROGRID PARAMETERS

c_1	c_2	c_3	r_1	r_2	r_3	r_4
0.2	0.2	0.2	8	1	0.5	-10

The continuous dynamics are given by:

$$\begin{aligned}
c_1 \frac{dv_1}{dt} &= -\frac{1}{r_1} v_1 - \frac{1}{r_2}(v_1 - v_2) + i_1 \\
c_2 \frac{dv_2}{dt} &= -\frac{1}{r_2}(v_2 - v_1) - \frac{1}{r_3}(v_2 - v_3) \\
c_3 \frac{dv_3}{dt} &= -\frac{1}{r_3}(v_3 - v_2) - \frac{1}{r_4} v_3 + i_2
\end{aligned}$$

The discrete model with time-step 0.1s is:

$$A = \begin{bmatrix} 0.6282 & 0.2221 & 0.1026 \\ 0.2221 & 0.4171 & 0.3646 \\ 0.1026 & 0.3646 & 0.5663 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.3941 & 0.0213 \\ 0.0716 & 0.1266 \\ 0.0213 & 0.3616 \end{bmatrix}$$

with state vector $x = [v_1 \ v_2 \ v_3]^T$ and control $u = [i_1 \ i_2]^T$. By inspection the discrete model is positive.

In traditional microgrid voltage regulation, the controls would attempt to achieve consensus on the voltages ($v_1 = v_2 = v_3$). Here we focus on maximizing disagreement by injecting currents i_1 and i_2. The voltage disagreement at time index k is defined as:

$$J(k) = (v_1(k) - v_2(k))^2 + (v_1(k) - v_3(k))^2 + (v_2(k) - v_3(k))^2$$

We use a horizon length of $N = 20$ and maximize disagreement at the end.

$$\begin{aligned} \min_{\mathcal{U}} \quad & -J(N) \\ \text{s.t.} \quad & i_1^2(k) + i_2^2(k) \leq 1, \qquad k = 0, \ldots, N-1 \end{aligned}$$

The resulting condensed MPC formulation has two negative eigenvalues, with the rest zero. Although the system is positive, the matrix of the quadratic cost function $-J(N)$ contains positive off-diagonal terms and thus we cannot apply Theorem 3. A simple numerical check reveals that the problem is uniformly almost off-diagonal non-positive with respect to $\sigma = \begin{bmatrix} 1 & -\mathbb{1}_{30}^T & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix}$.

Figure 5 shows the resulting state and control trajectory with all states initially zero. At the end, the disagreement in voltages is maximized. As σ contains both $+1$ and -1 entries the resulting control sequences $i_1(k)$ and $i_2(k)$ contain both positive and negative terms.

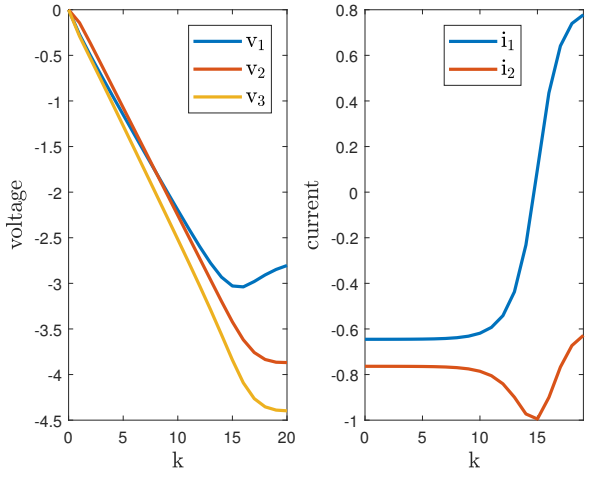

Fig. 5. Maximizing voltage disagreement in a microgrid

D. Implementation Details

All examples were solved using MOSEK [16] in conjunction with YALMIP [17]. For sufficiently small problems we also solved the original non-convex QCQP using the global optimization solver *BMIBNB* in YALMIP. This solver implements a simple branch-and-bound algorithm which can find global solutions to arbitrary optimization problems of modest size. In all instances, the solution obtained matched that provided by the SOCP formulation. Although our focus is not on solver efficiency, we note that for a problem with 20 decision variables the SOCP formulation was consistently solved in under $50ms$ while solving with *BMIBNB* took over 100 seconds. Larger problems were not validated with *BMIBNB* due to excessive runtimes.

VI. CONCLUSIONS

In this work we established conditions under which non-convex, adversarial model predictive control problems can be solved to global optimality via second-order cone programming. For general systems, the global solution can only be obtained in a subspace of the whole state-space. It was shown that many adversarial problems are readily solved for systems whose dynamics are invariant with respect to the positive orthant. Future work will examine whether similar conditions can be identified for systems which exhibit other forms of invariance. For cases in which the system does not admit an exact SOCP solution, we plan to combine our methods with heuristics for approximately solving the resulting indefinite QCQP [18].

REFERENCES

[1] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, CCS '09, (New York, NY, USA), pp. 21–32, ACM, 2009.

[2] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, pp. 2715–2729, Nov 2013.

[3] M. Jin, J. Lavaei, and K. Johansson, "A semidefinite programming relaxation under false data injection attacks against power grid ac state estimation," in *2017 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 236–243, Oct 2017.

[4] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: A study of misbehavior in vehicular platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, (New York, NY, USA), pp. 22:1–22:11, ACM, 2015.

[5] H. E. Brown and C. L. Demarco, "Risk of cyber-physical attack via load with emulated inertia control," *IEEE Transactions on Smart Grid*, vol. 9, pp. 5854–5866, Nov 2018.

[6] T. Lipp and S. Boyd, "Antagonistic control," *Systems & Control Letters*, vol. 98, pp. 44 – 48, 2016.

[7] Y. Chen, S. Kar, and J. M. F. Moura, "Cyber-physical attacks with control objectives," *IEEE Transactions on Automatic Control*, vol. 63, pp. 1418–1425, May 2018.

[8] A. Teixeira, K. Paridari, H. Sandberg, and K. H. Johansson, "Voltage control for interconnected microgrids under adversarial actions," in *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*, pp. 1–8, Sep. 2015.

[9] A. Rantzer, "Distributed control of positive systems," in *2011 50th IEEE Conference on Decision and Control and European Control Conference*, pp. 6608–6611, Dec 2011.

[10] S. Kim and M. Kojima, "Exact solutions of some nonconvex quadratic optimization problems via sdp and socp relaxations," *Computational Optimization and Applications*, vol. 26, pp. 143–154, Nov 2003.

[11] P. M. Pardalos and S. A. Vavasis, "Quadratic programming with one negative eigenvalue is np-hard," *Journal of Global Optimization*, vol. 1, pp. 15–22, Mar 1991.

[12] A. Rantzer and M. E. Valcher, "A tutorial on positive systems and large scale control," in *2018 IEEE Conference on Decision and Control (CDC)*, pp. 3686–3697, Dec 2018.

[13] F. Borrelli, A. Bemporad, and M. Morari, *Predictive Control for Linear and Hybrid Systems*. Cambridge University Press, 2017.

[14] B. Acikmese, J. M. Carson, and L. Blackmore, "Lossless convexification of nonconvex control bound and pointing constraints of the soft landing optimal control problem," *IEEE Transactions on Control Systems Technology*, vol. 21, pp. 2104–2113, Nov 2013.

[15] J. Berberich, J. Kohler, F. Allgower, and M. A. Muller, "Indefinite linear quadratic optimal control: Strict dissipativity and turnpike properties," *IEEE Control Systems Letters*, vol. 2, pp. 399–404, July 2018.

[16] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 8.1.*, 2017.

[17] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in matlab," in *In Proceedings of the CACSD Conference*, (Taipei, Taiwan), 2004.

[18] J. Park and S. Boyd, "General Heuristics for Nonconvex Quadratically Constrained Quadratic Programming," *arXiv e-prints*, p. arXiv:1703.07870, Mar 2017.