Parameter Sensitivity Analysis of Controlled Invariant Sets via Value Iteration

Liren Yang Denise Rizzo Matthew Castanier Necmiye Ozay

***Abstract*— In this paper we propose a value-iteration based algorithm to compute controlled invariant sets in cases where the range of certain parameters in the system model are not known a priori. By defining the value function in a way that is related to parameter ranges, the proposed computation allows us to analyze parameter sensitivity for the controlled invariant set. The convergence properties of the algorithm are analyzed for certain classes of systems. Finally, a vehicle team power management case study is used to illustrate the efficacy and scalability of the proposed algorithm.**

I. Introduction

This paper concerns safety control synthesis problem for dynamical systems. The term safety control synthesis refers to finding a controller that guarantees a system's state to stay in a specified set of safe states for all time [14]. While searching for this safety controller, we first need to ask what the set of all the initial states from where such a controller exists is, and this amounts to computing the maximal controlled invariant set that is contained in the safe set. The topic of controlled invariant sets is well studied by the control theory community both for discrete state and continuous state systems (see, for instance, [12] for the discrete case and [3] for the continuous case, and the references therein).

Often times, the system models we deal with are parametric, that is, the systems' dynamics, admissible control input sets and disturbance input sets may all vary with parameters, whose values are not known exactly. If a safety controller is synthesized for such a system, there will be a trade off between tolerating (being robust to) a large set of parameter values and having a large controlled invariant set. We will refer to the problem characterizing this trade off as "parameter sensitivity analysis of controlled invariant sets". In the context of temporal logic control synthesis, the problem is also known as parameter synthesis [5] or assumption mining [10], which asks the following question: given a state x, what is the maximal set $P(x)$ of parameter values under which the given specification (safety in our case) can be enforced when starting from x?

Answering the above question is useful for many reasons. First, from a control point of view, we may need different control laws to handle different set of parameter ranges [15]. In addition, for interconnected systems, one can design contracts by treating the output values of a subsystem as parameter values for another subsystem [7], [10] so that the controller of the overall system can be designed in a compositional manner. Second, from the point of view of analysis, finding $P(x)$ is useful to understand how sensitive the controlled invariant sets are against a change in parameter values. This is useful information at design time for instance for sizing or selecting components. Moreover, the set $P(x)$ can be used for system verification and testing. It is shown in [4] that controlled invariant sets can be used to generate non-trivial test cases to verify/falsify a system. In this context, one may want to run more test cases near a state x where $P(x)$ shrinks dramatically after a small perturbation to x.

In this paper, we propose a value iteration based approach in order to do parameter sensitivity analysis of controlled invariant sets. In fact, many fixed point algorithms computing controlled invariant sets that iterate over a set X_k of states, e.g., [1], [2], [13], can also be viewed as an iteration over a value function V_k, which is the indicator function of the set X_k. Such value iteration interpretation is powerful, especially when one wants to extend controlled invariance to more quantitative settings. For example, in recent works [6], [7], instead of iterating over an indicator function, the authors propose a more complicated fixed point algorithm that iterates a multi-valued function, so that a safety score is assigned to each state in the controlled invariant set. Similarly, yet in a probabilistic setting, the paper [8] uses value iteration to compute the probability of constraint violation of each initial state in a controlled invariant set.

We follow this line of work and propose a value iteration to perform parameter sensitivity analysis for a special class of parametric systems, whose admissible disturbance input set (relevant to sensitivity to model uncertainty) or control input set (relevant to actuator sizing) is parametrized by a non-negative scalar. We prove the convergence of the proposed iteration for certain classes of systems, and then, similar to [6], we obtain a characterization of the value function's level sets as a family of parametrized controlled-invariant sets. The main difference between our work and [6] is that the value function obtained by our approach has a direct physical meaning that arises from the disturbance or control input. More importantly, since the parameter value restricts the disturbance set or the control set, there is an extra player picking the parameter values in the max-min game defining the value iteration, which makes our value iteration different from that in [6]. In addition to this, we do not limit ourselves

This work is supported in part by NSF grant ECCS-1553873 and by US Army CCDC Ground Vehicle Systems Center under agreement W56HZV-14-2-0001. DISTRIBUTION A. Approved for public release; distribution unlimited. (OPSEC 3703). LY and NO are with the Dept. of Electrical Engineering and Computer Science, Univ. of Michigan, Ann Arbor, MI 48109 {yliren, necmiye}@umich.edu. DR and MC are with the US Army CCDC Ground Vehicle Systems Center, Warren, MI 48397 {denise.m.rizzo2, matthew.p.castanier}.civ@mail.mil.

$$V_0(x) = \begin{cases} \overline{p} & \text{if } x \in X_0 \\ -1 & \text{otherwise} \end{cases}, \tag{3}$$

$$V_{k+1}(x) = \max_{\substack{p \in [0,\overline{p}] \\ u \in U}} \min_{d \in D(p)} \min\Big\{p,\, V_k\big(f(x,u,d)\big),\, V_k(x)\Big\}. \tag{4}$$

to finite transition systems and link our results to the linear system case, for which the convergence of the value iteration is guaranteed. Finally, to illustrate the developed approach, we apply it to a finite transition system that arises from a vehicle team power management problem.

II. Preliminaries

In this section, we introduce necessary preliminaries on controlled invariant sets. Consider system

$$x(t+1) = f\big(x(t), u(t), d(t)\big) \tag{1}$$

where $x(t) \in X$ is the state, $u(t) \in U$ is the control input and $d(t) \in D$ is the disturbance. Let $K : X \to 2^U$ be a feedback control mapping, a trajectory generated by the system under K is an infinite sequence $x(0)x(1)x(2)\dots$ such that $x(t+1) = f\big(x(t), u(t), d(t)\big)$ for some $d(t) \in D$ and $u(t) \in K\big(x(t)\big)$.

Definition 1: (Robust Controlled Invariant Set) A set $C \subseteq X$ is robustly controlled invariant ("controlled invariant" for short in the rest of the paper) w.r.t. system in Eq. (1) if for all $x \in C$, there exists a feedback control law $K : C \to 2^U$ such that the all trajectories generated by the system starting from x under K stay in C for all time.

Remark 1: Clearly, given a set $X_0 \subseteq X$ of safe states, there exists a unique maximal controlled invariant set, denoted by $C_\infty(f, X_0, U, D)$, that is contained by X_0 because the union of any collection of controlled invariant sets in X_0 is also controlled invariant.

Proposition 1: (Proposition 1 in [1])A set C is controlled invariant if and only if $C \subseteq \mathbf{CPre}(C)$, where

$$\mathbf{CPre}(C) := \{x \in X \mid \exists u \in U : \forall d \in D : f(x,u,d) \in C\} \tag{2}$$

is the set of controllable predecessors of set C.

III. Problem Statement

In this paper, we are interested in performing parameter sensitivity analysis of the maximal controlled invariant set. The problem is formally stated in the sequel. Here, we will focus on the case where the disturbance input set is parametric. A similar problem can be defined for the case where the control input set is parametric, but we will not state the problem for the second case here.

Problem 1: (Parameter Sensitivity Analysis of the Maximal Controlled Invariant Set) Let the system dynamics be defined by Eq. (1) with state $x \in X$, control $u \in U$ and disturbance d from a parametric set $D(p)$, where p is a scalar parameter from the interval $[0, \overline{p}]$. Given a safe set X_0 and any state $x \in X$, our goal is to verify whether there exists $p \in [0, \overline{p}]$ such that $x \in C_\infty\big(f, X_0, U, D(p)\big)$, and if yes, find the maximal set of such p.

Assumption 1: We assume that $D(p)$ is monotone in the parameter p, that is, $p \le p'$ implies that $D(p) \subseteq D(p')$.

Assumption 1 holds, for instance, when the parameter p is used to describe the upper bound of the disturbance input, e.g., when $D(p) = \{d \in \mathbb{R}^{n_d} \mid \|d\|_\infty \le p\}$.

IV. Main Results for General Systems

We define a value iteration in Eqs. (3), (4) to solve Problem 1. The outcome of the value iteration is a function V_∞ defined on the state space such that $[0, V_\infty(x)]$ is the tolerable set of parameter values at state x. In this section, we do not make any further assumptions on the dynamics f.

To show V_∞ indeed solves Problem 1, we state and prove some properties of the proposed value iteration and its fixed points. In what follows, let us denote iteration (4) on value function V by $(V)^+$ to ease the notation.

First, we introduce two lemmas useful for later proofs.

Lemma 1: Iteration (4) is monotone in the sense that $V'(x) \ge V(x)$ for all x implies that $(V')^+(x) \ge (V)^+(x)$ for all x.

Proof: Let V' be no smaller than V pointwise, and let $x \in X$ be arbitrary. Define

$$L'_x(p,u,d) := \min\Big\{p, V'\big(f(x,u,d)\big), V'(x)\Big\}, \tag{5}$$

$$L_x(p,u,d) := \min\Big\{p, V\big(f(x,u,d)\big), V(x)\Big\}. \tag{6}$$

Clearly $L'_x(p,u,d) \ge L_x(p,u,d)$ for any p, u, d. Let p^*, u^*, d^* be the optimizers that solve the max min problem in Eq. (4) with objective function L_x, and let $p^\circ, u^\circ, d^\circ$ be the optimizers solving the max min problem with L'_x. Also define $d^\diamond = \arg\min_{d \in D(p^*)} L'_x(p^*, u^*, d)$, we have

$$\begin{aligned} (V)^+(x) &= L_x(p^*, u^*, d^*) \\ &\le L_x(p^*, u^*, d^\diamond) \\ &\le L'_x(p^*, u^*, d^\diamond) \\ &\le L'_x(p^\circ, u^\circ, d^\circ) = (V')^+(x). \end{aligned} \tag{7}$$

Since $x \in X$ is arbitrary, this finishes the proof. ∎

Lemma 2: Given a value function V and any positive number δ, let V^δ denote another value function such that $V^\delta(x) := V(x) + \delta$ for all $x \in X$. Then $(V^\delta)^+(x) \le (V)^+(x) + \delta$.

Proof: Let $x \in X$ be arbitrary, define

$$L^\delta_x(p,u,d) := \min\Big\{p, V^\delta\big(f(x,u,d)\big), V^\delta(x)\Big\}, \tag{8}$$

$$L_x(p,u,d) := \min\Big\{p, V\big(f(x,u,d)\big), V(x)\Big\}. \tag{9}$$

Clearly $L_x^\delta(p,u,d) \le L_x(p,u,d)+\delta$ for any p,u,d. Let p^*,u^*,d^* be the optimizers that solves the max min problem in Eq. (4) with objective function L_x, and let p°,u°,d° be the optimizers solving the max min problem with L_x^δ. Also define $d^\diamond = \arg\min_{d\in D(p^\circ)} L_x(p^\circ,u^\circ,d)$, we have

$$\begin{aligned}(V^\delta)^+(x) &= L_x^\delta(p^\circ,u^\circ,d^\circ)\\ &\le L_x^\delta(p^\circ,u^\circ,d^\diamond)\\ &\le L_x(p^\circ,u^\circ,d^\diamond)+\delta\\ &\le L_x(p^*,u^*,d^*)+\delta = (V)^+(x)+\delta. \end{aligned} \tag{10}$$

Since $x\in X$ is arbitrary, this finishes the proof. ∎

With Lemma 1 and 2, in the next theorem, we give some conditions under which V_k converges to a fixed point of iteration 4 that is maximal in certain sense.

Theorem 1: (Convergence of Value Iteration (4)) Let $\{V_k\}_{k=1}^\infty$ be the value function at the k^{th} iteration for $k=0,1,2,\dots$, the followings hold.

(i) V_k converges to a function V_∞ pointwise as $k\to\infty$.

(ii) If in addition to (i) we suppose that V_k uniformly converges to V_∞ on X, then V_∞ is a fixed point of iteration defined by Eq. (4), i.e., $(V_\infty)^+(x)=V_\infty(x)$ for all $x\in X$. Moreover, V_∞ is the maximal fixed point among all value functions from $\mathcal{V}:=\{V \mid V(x)\le V_0(x)\,\forall x\}$ in the sense that $V_\infty(x)\ge V(x)$ for all x given that $V\in\mathcal{V}$ also satisfies $V=(V)^+$ pointwise.

Proof: First, to prove bullet (i), let $x\in X$ be arbitrary. By (4), $V_k(x)$ is a monotonically nonincreasing sequence, i.e., $V_{k+1}(x)\le V_k(x)$. Also note that and $V_k(x)$ is lower bounded as $V_k(x)\ge -1$ for all k, hence $\lim_{k\to\infty}V_k(x)$ exists.

Let V_∞ be such that $V_\infty(x):=\lim_{k\to\infty}V_k(x)$, we now prove that V_∞ is a fixed point of iteration (4) given that V_k converges to V_∞ uniformly on X. Again let x be arbitrary, we have $(V_\infty)^+(x)\le V_\infty(x)$ by Eq. (4). In what follows, we show that $(V_\infty)^+(x)\ge V_\infty(x)$ also holds, which implies that $(V_\infty)^+(x)=V_\infty(x)$.

Since V_k converges to V_∞ uniformly on X, we have

$$\forall\delta>0:\exists k:\forall x\in X: V_k(x)\le V_\infty(x)+\delta \tag{11}$$

Now applying Lemma 2 yields

$$\begin{aligned}&\forall\delta>0:\exists k:\forall x\in X:\\ &V_\infty(x)\le V_{k+1}(x)\le (V_\infty(x))^+(x)+\delta,\end{aligned} \tag{12}$$

where $V_\infty(x)\le V_{k+1}(x)$ holds earlier. Since $\delta>0$ is arbitrary, this proves that $V_\infty(x)\le(V_\infty(x))^+(x)$ for any $x\in X$. Also recall that $V_\infty(x)\ge(V_\infty(x))^+(x)$ for $x\in X$, hence we have $V_\infty(x)=(V_\infty(x))^+(x)$ on X.

Finally, we show that V_∞ is the maximal fixed point. Let V be any function from $\mathcal{V}$ that also satisfies $V=(V)^+$ pointwise. Note that $V_0\ge V$ pointwise, hence by Lemma 1, we know that $V_1=(V_0)^+\ge(V)^+=V$ pointwise. It can be proved by induction that $V_k\ge V$ pointwise for all k, hence $V_\infty=\lim_{k\to\infty}V_k\ge V$ pointwise. ∎

Remark 2: Although V_k always converges to V_∞ pointwise, there is no guarantee in general that V_k converges to V_∞ uniformly. However, in case X is finite, the convergence occurs in finite time and therefore this reduces to a special case of uniformly convergence.

Next we state and prove the connection between the fixed points of iteration (4) and controlled invariant sets. This connection holds regardless of the fixed point and the controlled invariant set being maximal or not.

Theorem 2: (Connection between Fixed Points and Controlled Invariant Sets) If $V\in\mathcal{V}$ is a fixed point of iteration (4), then $C_{V,p}=\{x\in X \mid V(x)\ge p\}$ is a controlled invariant set under disturbance $d\in D(p)$; if set $C\subseteq X$ is a controlled invariant set for all disturbance $d\in D(p)$, then $V_{C,p}$ defined by

$$V_{C,p}(x):=\begin{cases}p & \text{if } x\in C\\ -1 & \text{otherwise}\end{cases} \tag{13}$$

is a fixed point of iteration (4).

Proof: First, let $V\in\mathcal{V}$ be a fixed point of iteration (4), and let $x\in C_{V,p}$, i.e., $V(x)=p'\ge p$. Then we know that

$$\begin{aligned}&\exists p''\in[0,\overline{p}],u\in U:\forall d\in D(p''):\\ &\min\Big\{p'',V\big(f(x,u,d)\big),V(x)\Big\}=p'=V(x).\end{aligned} \tag{14}$$

This implies that

(i) $p''\ge p'\ge p$ (hence $D(p'')\supseteq D(p)$ by Assumption 1) ,

(ii) $V\big(f(x,u,d)\big)\ge p'\ge p$.

Combining Eq. (14) and observation (ii) yields

$$\exists u\in U:\forall d\in D(p''):V\big(f(x,u,d)\big)\ge p, \tag{15}$$

which, together with observation (i) and the definition of $C_{V,p}$, implies that

$$\exists u\in U:\forall d\in D(p): f(x,u,d)\in C_{V,p}. \tag{16}$$

In other words $x\in\mathbf{CPre}_p(C_{V,p})$, where $\mathbf{CPre}_p(C):=\{x\in X \mid \exists u\in U:\forall d\in D(p): f(x,u,d)\in C\}$ consists of the controllable predecessors of set C under disturbance $d\in D(p)$. Since x is arbitrary from $C_{V,p}$, we know that $C_{V,p}\subseteq\mathbf{CPre}_p(C_{V,p})$, and this proves that $C_{V,p}$ is a controlled invariant set by Proposition 1.

Second, let C be a controlled invariant set under disturbance $d\in D(p)$ and $V_{C,p}$ be defined by Eq. (13), we show that $V_{C,p}$ is a fixed point of iteration 4. To this point, we consider the two cases where $x\notin C$ and $x\in C$ respectively.

(1) For $x\notin C$, $V_{C,p}(x)=-1$ by definition. Note that $(V_{C,p})^+(x)$ cannot take value smaller than -1 by iteration while $(V_{C,p})^+(x)\le V_{C,p}(x)$, thus $(V_{C,p})^+(x)=-1=V_{C,p}(x)$.

(2) For $x\in C$, $V_{C,p}(x)=p$ by definition. Since C is controlled invariant under $d\in D(p)$, this means

$$\begin{aligned}&\exists u\in U:\forall d\in D(p):f(x,u,d)\in C\\ \Rightarrow\ &\exists u\in U:\forall d\in D(p):V_{C,p}\big(f(x,u,d)\big)=p\\ \Rightarrow\ &\exists u\in U:\forall d\in D(p):\\ &\quad\min\Big\{p,V_{C,p}\big(f(x,u,d)\big),V_{C,p}(x)\Big\}=p\\ \Rightarrow\ &(V_{C,p})^+(x)\ge p.\end{aligned} \tag{17}$$

On the other hand, we also know that $(V_{C,p})^+(x) \leq V_{C,p}(x) = p$. Hence $(V_{C,p})^+(x) = V_{C,p}(x) = p$ in this case.

Now we have proved that $(V_{C,p})^+(x) = V_{C,p}(x)$ both for $x \notin C$ and $x \in C$, i.e., $V_{C,p}$ is a fixed point of iteration (4). ∎

With Theorem 1 and Theorem 2, we can characterize a family of parametrized controlled invariant sets by the level sets of V_∞. We formally state this result by following corollary.

Corollary 1: Suppose that V_k converges to V_∞ uniformly on X, then the p-suplevel set of V_∞ is the maximal controlled invariant set under disturbance $d \in D(p)$, i.e., $\{x \in X \mid V_\infty(x) \geq p\} = C_\infty\big(f, X_0, U, D(p)\big)$.

Proof: To ease notations, let $C^p_\infty := C_\infty\big(f, X_0, U, D(p)\big)$. Let $C_{V_\infty,p}$ denote the p-suplevel set of V_∞ and let $V_{C^p_\infty,p}$ be defined as in Theorem 2. We know that $V_{C^p_\infty,p}$ is a fixed point of iteration (4) by Theorem 2, while V_∞ is the maximal fixed point of iteration (4) by Theorem 1. Hence

$$\begin{aligned} C^p_\infty &= \{x \in X \mid V_{C^p_\infty,p}(x) \geq p\} \\ &\subseteq \{x \in X \mid V_\infty(x) \geq p\} = C_{V_\infty,p}. \end{aligned} \tag{18}$$

However, we know that $C_{V_\infty,p}$ is also a controlled invariant set under $d \in D(p)$ by Theorem 2, while C^p_∞ is the maximal controlled invariant set under $d \in D(p)$. Hence

$$C_{V_\infty,p} \subseteq C^p_\infty. \tag{19}$$

Eq. (18) and (19) implies that $C_{V_\infty,p} = C^p_\infty$, which is what we want to prove. ∎

Through the characterization in Corollary 1, it can be seen that Problem 1 is solved by the value iteration in the sense that, at a given state $x \in X_0$, the set of all parameters under which safety can be enforced is the interval $[0, V_\infty(x)]$. In other words, if $p \in [0, V_\infty(x)]$, we will have $x \in C^p_\infty$. This is true because $p \leq V_\infty(x)$ implies that $x \in \{x \mid V_\infty(x) \geq p\} = C_{V_\infty,p}$, which is equal to C^p_∞ by Corollary 1.

As promised in the introduction, we also consider the case where the control input set is parametric, i.e., the control set $U(q)$ varies with a parameter $q \in [0, \overline{q}]$. In this case, a similar sensitivity analysis can be done for the maximal controlled invariant set against parameter q. To this end, we define another value iteration by Eq. (20) and (21). Similar results can be obtained for this value iteration and we will not present them here.

V. Application to Certain System Classes

Although the proposed value iteration in Eq. (4) solves Problem 1, it is hard to compute in general. In addition, the uniform convergence of V_k, which guarantees that V_∞ is indeed a fixed point of the iteration, is not always easy to prove. In this section, we discuss two special classes of systems for which V_∞ is assured to be equal to the largest fixed point, and the proposed value iteration can be implemented in practice.

A. Finite Transition Systems

For a finite transition system, whose state set X, control set U and disturbance set D are finite, the proposed value iteration can be performed in practice. Such systems can be viewed as abstractions of continuous-state systems and are studied in similar work like [6]. In this case, V_k converges to V_∞ after finite round of iterations, and V_∞ indeed solves Problem 1 by Remark 2 and Corollary 1.

B. Linear Systems

In this part, we consider linear systems of the form:

$$x(t+1) = Ax(t) + Bu(t) + Ed(t), \tag{22}$$

where the safe set X_0, the control set U and the parametrized disturbance set $D(p)$ are polytopes in Euclidean spaces, and set $D(p)$ satisfies Assumption 1. Moreover, we assume that the vertex coordinates of the polytopic set $D(p)$ are linear in the parameter p. This is the case, for example, when $D(p) = \{d \in \mathbb{R}^{n_d} \mid \|\Lambda d\|_\infty \leq p\}$ where $\Lambda \in \mathbb{R}^{n_d \times n_d}$ is a diagonal positive semi-definite matrix.

For the systems described above, the value iteration in Eq. (4) can be done relatively efficiently.

Theorem 3: Define an iteration over a set $\mathcal{E}_k$ by Eq. (26), (28), $\mathcal{E}_k$ is a polytope that can be computed efficiently. Moreover, V_k defined by Eq. (4) can be recovered from $\mathcal{E}_k$ in the following sense:

$$X_k = \{x \mid \exists p : (x,p) \in \mathcal{E}_k\}, \tag{23}$$

$$V_k(x) = \begin{cases} \max\{p \mid (x,p) \in \mathcal{E}_k\} & \text{if } x \in X_k \\ -1 & \text{otherwise} \end{cases}. \tag{24}$$

The proof of Theorem 3 can be found in the appendix.

Essentially, Theorem 3 says that $\mathcal{E}_k$ is the region below the surface defined by function V_k and above the hyperplane $\{(x,p) \mid p = 0\}$. Also note that $V_k(x) \equiv -1$ whenever $V_k(x) < 0$, hence computing set $\mathcal{E}_k$ is equivalent to computing function V_k. In fact, Theorem 3 is not surprising because by Corollary 1, if V_∞ is the maximal fixed point, set $\mathcal{E} := \{(x,p) \mid p \in [0, \overline{p}], x \in C_{V_\infty,p}\}$ is the maximal controlled invariant set contained by $X \times [0, \overline{p}]$ of the following system:

$$\begin{aligned} x(t+1) &= Ax(t) + Bu(t) + Ed(t), \\ p(t+1) &= p(t) \end{aligned} \tag{25}$$

where $d(t) \in D\big(p(t)\big)$. Set iteration in Eq. (28) is exactly the same as that proposed by [1], which converges to the maximal controlled invariant set of the linear system with the above dynamics. Based on this interpretation with the augmented system in Eq. (25), it can be also seen that V_k does converge to the maximal fixed point of the iteration in Eq. (4) in the linear system case, because $\mathcal{E}_k$ is known to converge to $\mathcal{E}$ in this case [13]. Meanwhile it is difficult to prove such convergence directly using Theorem 1 by showing that V_k converges to its limit uniformly for arbitrary systems.

$$W_0(x) = \begin{cases} 0 & \text{if } x \in W_0 \\ \infty & \text{otherwise} \end{cases}, \tag{20}$$

$$W_{k+1}(x) = \min_{\substack{q \in [0,\overline{q}] \\ u \in U(q)}} \max_{d \in D} \max\Big\{q,\, W_k\big(f(x,u,d)\big),\, W_k(x)\Big\}. \tag{21}$$

$$\mathcal{E}_0 = X_0 \times [0, \overline{p}], \tag{26}$$

$$\begin{aligned} \mathcal{E}_{k+1} &= \mathcal{E}_k \cap \left\{ (x,p) \;\middle|\; \begin{array}{l} p \in [0,\overline{p}] \\ \exists u \in U : \forall d \in D(p) : (Ax + Bu + Ed, p) \in \mathcal{E}_k \end{array} \right\} \\ &= \mathcal{E}_k \cap \mathbf{Proj}_{(x,p)} \left(\left\{ (x,u,p) \;\middle|\; \begin{array}{l} u \in U, p \in [0,\overline{p}], \\ H_k^1(Ax + Bu + Ev) + H_k^2 p \le h_k,\, \forall v \in v_{D(p)} \end{array} \right\} \right). \end{aligned} \tag{27}$$

where $\mathcal{E}_k = \{(x,p) \mid H_k^1 x + H_k^2 p \le h_k\}$, $v_{D(p)}$ is the set of vertices of the polytopic set $D(p)$ (28)

VI. Case Studies

A. A Numerical Example

In this section, we first illustrate the value iteration presented in Section V-B using a simple 2D linear system:

$$x(t+1) = Ax(t) + B\big(u(t) + d(t)\big), \tag{29}$$

where

$$A = \begin{bmatrix} 0.9930 & 0.0358 \\ -0.2240 & 0.9930 \end{bmatrix}, \quad B = \begin{bmatrix} -0.0053 \\ 0.1205 \end{bmatrix}, \tag{30}$$

and $x \in X_0 = [-1, 5, 1.5] \times [-1, 1]$, $u \in U = [-1, 1]$, $d \in D(p) = [-p, p]$ and $p \in [0, \overline{p}] = [0, 0.3]$. We compute the value function V_k via computing set $\mathcal{E}_k$ in Eq. (28). Figure 1 shows the converged set after 51 iterations, i.e., $\mathcal{E}_{51}$, and the resulting $V_{51}(x)$ is defined by Eq. (24). As mentioned in Section V-B, the surface of polytope $\mathcal{E}_k$ can be interpreted as the graph of value function V_k, and $V_k(x)$ is the maximal parameter value that can be tolerated at state x. It can be seen from Figure 1 that there is a plateau in the middle of V_{51}'s graph, this means a larger parameter value (hence more disturbance) can be tolerated in the middle of the safe set X_0. The slope at the boundary of the graph (along x_1-dimension) corresponds to the fast drop of such tolerance while state x_1 approaching its limit. On the other hand, we can see that of the maximal controlled invariant set is not very sensitive to the parameter along x_2-dimension within the given safe set X_0.

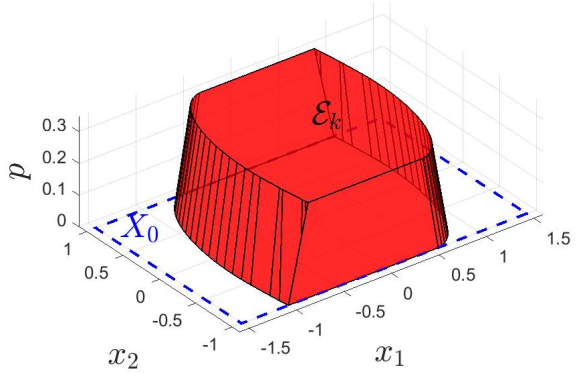

Fig. 1: Plot of set $\mathcal{E}_{51}$, obtained by applying iteration in Eq. (28) to a 2D linear system until convergence.

B. Vehicle Team Power Management

In the rest of this section, we consider a power management problem among a team of vehicles and multiple military camps. The problem is abstracted from [9]. Fig. 2 shows an illustration of the system. In this problem, we consider a network of military camps. Each camp is equipped with a static power generator, and has an uncertain time-varying power request to meet. At each camp, there is also an energy storage unit serving as a buffer against sudden peak power requests. If peak level power is kept being requested at a camp, we are allowed to send vehicles with smaller on-board power generators to that camp and support its power generation. The goal of the power management is to meet the power requests at all camps by dynamically allocating such a group of identical vehicles from one camp to another.

In this work, we model the system as a finite transition system $\mathcal{T} = (\mathcal{M}, X, U, D(p), f)$, where

- $\mathcal{M}$ is a map that captures the routing topology,
- X is the set of states,
- U is the set of control actions,
- $D(p)$ is the parametrized set of disturbance,
- $f : X \times U \times D(p) \to X$ is the nondeterministic transition relation parameterized by p.

Here we assume that all the sets are finite. In what follows, we will define each of the above components in details.

1) Map $\mathcal{M}$: A map $\mathcal{M} = (L, L_c, \sigma)$ is a directed graph consisting

- a finite set L of locations;
- a set $L_c \subseteq L$ of camp locations;
- a transition relation $\sigma \subseteq L \times L$ such that $(i,i) \in \sigma$ for all $i \in L_c$ (i.e., we assume that vehicles are always allowed to stay steady at a camp).

Map $\mathcal{M}$ describes the topology of the camp-network. The non-camp locations in $L \setminus L_c$ can be also used to capture

the distance between two camps. For example, we can insert intermediate non-camp nodes between two camps if they are far away from each other.

2) State Set X: The overall state set is defined by

$$X := \prod_{i \in L_c} S_i \times H. \tag{31}$$

In Eq. (31), S_i is a finite set of possible energy storage levels at the camp indexed by $i \in L_c$, and H contains all possible distributions of vehicles over the set L of locations. Let m be the total number of vehicles, H is defined to be the set $\{h = (h_1, h_2, \ldots, h_{|L|}) \mid \sum_{i \in L} h_i = m\}$, where h_i denotes the number of vehicles at location $i \in L$. In the sequel, a state will be denoted as (s, h) where s consists of the energy level $s_i \in S_i$ of each camp $i \in L_c$ and h describes the vehicle distribution. Since all the vehicles are assumed to be identical, the distribution h is sufficient to describe the location of the vehicles and using h as part of the state dramatically reduces the size of the state space [11].

3) Control Set U: The control action set $U \subseteq H \times H \times \{1, 2, \ldots, m\}^{|L_c|}$ is defined as follows. Let $h = (h_1, \ldots, h_{|L|}), h' = (h'_1, \ldots, h'_{|L|}) \in H$ and $v \in \{1, 2, \ldots, m\}^{|L_c|}$ consists of v_i for $i \in L_c$, $u = (h, h', v) \in U$ iff there exists a set $\{\phi_{(\ell,k)}\}_{(\ell,k)\in\sigma}$ such that

i) $\phi_{(\ell,k)}$ are non-negative integers;
ii) $\forall i \in L : \sum_{(i,k)\in\sigma} \phi_{(i,k)} = h_i$;
iii) $\forall i \in L : h'_i - h_i = \sum_{(\ell,i)\in\sigma} \phi_{(\ell,i)} - \sum_{(i,k)\in\sigma} \phi_{(i,k)}$;
iv) $\forall i \in L_c : v_i \leq \min\{h'_i, h_i\}$.

A control action $u = (h, h', v)$ is feasible iff it satisfies the above conditions. We now present some intuition in the following. Components h and h' captures the evolution of the distribution by moving the vehicles. The evolution must be consistent with the moves allowed by map $\mathcal{M}$. This amounts to finding a set of flows $\phi_{(\ell,k)}$ on each transition $(\ell, k) \in \sigma$, where σ is the transition relation of map $\mathcal{M}$, such that h' can be obtained from h under such flow. The v part of the control action captures how many vehicles are involved in power generation. Here v_i is the number of vehicles that are commanded to generate power at camp i. We assume that a vehicle can only generate power at camp i if it does not move. Note that the maximal number of steady vehicles at camp i is tightly bounded by $\min\{h'_i, h_i\}$, this hence leads to bullet iv).

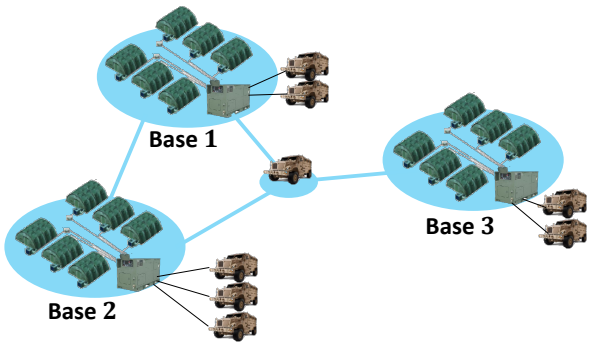

Fig. 2: Vehicle team power management problem [9]. The large circles are camp nodes, the small circle in the middle is a non-camp node, and the blue line segments correspond to the connection between two camps.

4) Disturbance Set $D(p)$: Let r_i be the power requested at camp $i \in L_c$, r is a tuple that contains r_i for all $i \in L_c$. The disturbance set $D(p)$ is then given by

$$D(p) := \{r \mid n_p \text{ of } r_i\text{'s take value from } [p_{\text{regular}}, p], \text{ and the rest } r_i = p_{\text{regular}}\}, \tag{32}$$

where p_{regular} is a given constant power level, and p is the upper bound of the peak power level, which is the parameter we are interested in. For example, in Fig. 3, the plots on the left illustrate a case where at most two of four camps may experience peak power request (upper bounded by $p = 5$) while the rest of the camps have regular power request ($p_{\text{regular}} = 2$ in this example).

5) Transition Mapping f: The transition mapping $f : X \times U \times D(p) \times X$ is a partial map that determines the next state of the transition system $\mathcal{T}$. Let $x := (s, h)$, $u := (h'', h', v)$, $d = r$, then $f(x, u, d)$ is well defined iff $h = h''$. Denote $f(x, u, r)$ by $x^+ := (s^+, h^+)$, s^+, h^+ are defined as follows:

- $h^+ = h'$;
- $\forall i \in L_c : s_i^+ = s_i + g_i + g_v v_i - r_i$.

where g_i is the power generated by the static generator at camp i, and g_v is the power generated by one vehicle. Both g_i and g_v are given constants.

6) Requirement: We wish to meet the power request at all camps, i.e., to provide exactly r_i unit of power as requested at camp i. This requirement can be actually treated as a safety requirement because we can always extract power from the storage unit and the only concern is to avoid overdischarging the energy storage unit. Hence we assume the extra power beyond the generation capability of a camp is always drawn from the storage, and pose the requirement as $s_i \geq 0$, where s_i is the energy storage level at camp i, for all time and all $i \in L_c$.

7) Results and Discussion: Given the above system model and requirement, we want to compute the largest peak power p that can be achieved without violating energy storage limit at each initial state. To this end, we applied the proposed value iteration to this vehicle team power management problem. TABLE I shows the results obtained for systems of different sizes. It can be seen from each row that the controlled invariant set's size reduces as we increase the parameter, which characterizes the disturbance level. It can also be seen that the size of the controlled invariant set increases with the total number of vehicles. Since we use the distribution of the vehicles, instead of the location of each vehicle, to describe the system's state, the system's size scales better w.r.t. the number of vehicles. For instance, thanks to this representation, the system in the last row of TABLE I has only 178750 states whereas naively taking the location of each vehicle to be a state would require approximately 6.5×10^8 states in total. On the other hand, the state space increases much faster with the number of the camps/locations in the map. Finally, the time consumed

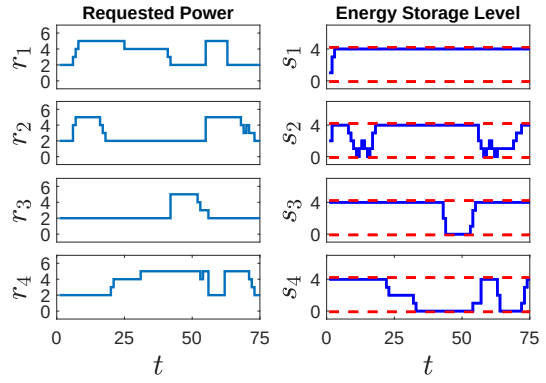

Fig. 3: Simulation of the closed loop system (corresponding to the last row of TABLE (I)) with four camps and the topology in Fig. 2. The dashed red lines in the plots on the right mark the safety bounds.

by the value iteration is usually much shorter than that of computing the transition system itself. Fig. 3 shows the closed-loop behavior of the system in the last row of TABLE I. The system is simulated with peak power level $p = 5$ in this case. It can be seen that the safety requirement is always satisfied.

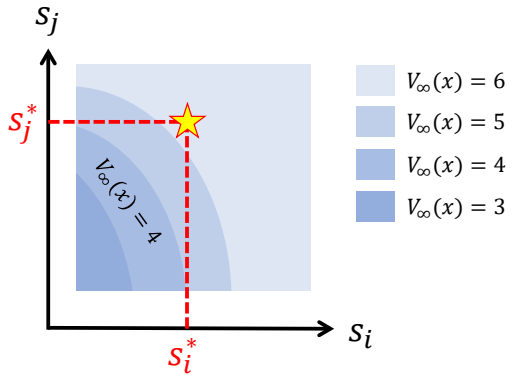

Fig. 4: Illustration: using the parameter analysis to determine the size of energy storage unit at design time. The yellow star s_i^*, s_j^* marks a size of the energy storage unit at camp i and j. Picking larger storage unit is unnecessary when $p = 5$ is the upper bound of the peak level of the requested power.

We would also like to point out that this parameter sensitivity analysis is useful at the design time of the system. For example, we can use the computed $V_\infty(x)$ to determine the necessary size of the energy storage unit at each camp when a prior knowledge on the parameter (peak level of the requested power) is assumed. Fig. 4 illustrates the idea. Assume that the parameter p takes integer values, and let $p = 5$ be the largest possible peak power. Then picking energy storage units with size larger than s_i^* and s_j^* does not gain us anything in terms of avoidance of over-charging/over-discharging the units, and hence is unnecessary. One key benefit of the proposed approach is that it allows us to do such analysis at design time in a systematical way for large systems.

VII. Conclusion

In this paper, we considered systems with parametric disturbance and control input sets, and studied the parameter sensitivity analysis problem of the maximal controlled invariant sets for such systems. A value iteration based algorithm was proposed. We analyzed the convergence properties of this value iteration and gave a useful interpretation of the level sets of its fixed points, which are shown to solve the parameter sensitivity analysis problem. The developed approach was then applied to a vehicle team power management case study. The algorithm was shown to scale well with respect to the number of vehicles and can be used to determine certain system parameters at design time. In the future, we will extend the framework to parameter sensitivity of winning sets for more complex specifications beyond safety (e.g., those given by temporal logic formulas).

Appendix: Proof of Theorem 3

Here, we will only discuss the case where d is a scalar and $d \in D(p) = [-p, p]$ for simplicity, but the results developed below easily extend to the general case.

The following property of set $\mathcal{E}_k$ is useful for later proofs.

Lemma 3: Let $\mathcal{E}_k$ be defined by Eq. (26), (28), and define

$$X_k = \{x \mid \exists p : (x, p) \in \mathcal{E}_k\}, \tag{33}$$

$$Y_k(x) = \begin{cases} \max\{p \mid (x, p) \in \mathcal{E}_k\} & \text{if } x \in X_k \\ -1 & \text{otherwise} \end{cases}. \tag{34}$$

Then, we have

$$\forall x, p \in [0, \overline{p}] : p \leq Y_k(x) \Leftrightarrow (x, p) \in \mathcal{E}_k. \tag{35}$$

Proof: "$\Leftarrow$" holds by definition of Y_k. To prove the other direction, let $p \leq Y_k(x)$. Given that U is a closed polytope, it can be easily seen from the definition that $\mathcal{E}_k$ is also a closed set. Hence there exists $p' \geq p$ such that $(x, p') \in \mathcal{E}_k$. Again, by the definition of $\mathcal{E}_k$, we can prove by induction that $(x, p') \in \mathcal{E}_k \Rightarrow (x, p) \in \mathcal{E}_k$ whenever $p' \geq p$. Hence $(x, p) \in \mathcal{E}_k$ holds. ■

Next, we prove Theorem 3. Since X_0 is assumed to be a polytope, $\mathcal{E}_0$ is also a polytope, and $\mathcal{E}_k$ can be then proved to be a polytope by induction. Hence what is left to verify is the following statement.

Proposition 2: Let V_k be defined by Eq. (3), (4) and Y_k be defined by Eq. (24), we have $Y_k = V_k$ for all k.

Proof: We prove this by induction. Clearly, $Y_0(x) = V_0(x)$. Now assume that $Y_k = V_k$, we will show that $Y_{k+1} = V_{k+1}$. To this end, we show that, for any x, $Y_{k+1}(x) \leq V_{k+1}(x)$ and $Y_{k+1}(x) \geq V_{k+1}(x)$ hold respectively.

We first show $Y_{k+1}(x) \leq V_{k+1}(x)$. Let $p^\circ := Y_{k+1}(x)$. By Lemma 3, we know that $(x, p^\circ) \in \mathcal{E}_{k+1}$. This means

$$(x, p^\circ) \in \mathcal{E}_k, \tag{36}$$

$$\exists u^\circ \in U : \forall d \in [-p^\circ, p^\circ] : (Ax + Bu^\circ + Ed, p^\circ) \in \mathcal{E}_k. \tag{37}$$

By Lemma 3 and the induction hypothesis, Eq. (36) yields

$$p^\circ \leq Y_k(x) = V_k(x), \tag{38}$$

TABLE I: Numerical results of systems with different sizes

CasesStatistics				total	size of controlled invariant set (# states)						cpu time (s)		# iterations
n_{p}	$\lvert L_{\mathrm{c}}\rvert$	$\lvert L\rvert$	m	# states	$p=2$	$p=3$	$p=4$	$p=5$	$p=6$	$p=7$	computing $\mathcal{T}$	value iteration	
1	2	2	3	100	100	90	62	0	0	0	0.28	0.02	4
1	2	2	4	125	125	115	95	0	0	0	0.49	0.06	6
1	2	2	6	175	175	165	145	115	0	0	1.06	0.09	6
1	2	2	8	225	225	215	195	165	125	0	1.78	0.18	6
2	3	3	6	3500	3500	2990	2135	0	0	0	54	4.28	6
2	3	3	7	4500	4500	3915	2910	0	0	0	84.64	7.37	6
2	3	3	8	5625	5625	4965	3810	2289	0	0	130.16	7.86	4
2	3	3	10	8250	8250	8250	7440	5985	1614	0	260.39	17.05	4
2	3	3	12	11375	11375	10415	8660	6365	3875	0	542.58	50.95	6
2	3	4	7	15000	15000	12379	8303	0	0	0	764.02	68.06	6
2	3	4	8	20625	20625	17344	12113	6261	0	0	1345.3	81.64	4
2	3	4	9	27500	27500	23484	16948	9799	0	0	2652.3	235.95	6
2	3	4	10	35750	35750	30924	22933	13939	0	0	4544.7	403.7	6
2	3	5	9	89375	89375	73458	59259	38309	22513	8573	20474	1042.1	3
2	4	4	9	137500	137500	110275	68100	0	0	0	11074	795.59	6
2	4	4	10	178750	178750	146075	94385	38729	0	0	18782	1013.6	4

while Eq. (37) yields

$$\exists u^\circ \in U : \forall d \in [-p^\circ, p^\circ] : p^\circ \leq Y_k(Ax + Bu^\circ + Ed) = V_k(Ax + Bu^\circ + Ed). \tag{39}$$

Also note that

$$V_{k+1}(x) \geq \min_{d \in [-p^\circ, p^\circ]} \min\{p^\circ, V_k(Ax + Bu^\circ + Ed), V_k(x)\}, \tag{40}$$

whereas the right hand side of Eq. (40) is nothing but p° by Eq. (38), (39). Hence $V_{k+1}(x) \geq p^\circ = Y_{k+1}(x)$.

Now we show $Y_{k+1}(x) \geq V_{k+1}(x)$. Let $p^\diamond := V_{k+1}(x)$. By definition of V_{k+1} in Eq. (4), we know that

$$p^\diamond \leq V_k(x), \tag{41}$$

$$\exists u^* \in U, p^* \in [0, \overline{p}] : \forall d \in [-p^*, p^*] : \min\{p^*, V_k(Ax + Bu^* + Ed), V_k(x)\} \geq p^\diamond. \tag{42}$$

Note that Eq. (42) further implies that

$$p^* \geq p^\diamond, \tag{43}$$

and hence

$$\exists u^* \in U : \forall d \in [-p^\diamond, p^\diamond] \subseteq [-p^*, p^*] : V_k(Ax + Bu^* + Ed) \geq p^\diamond. \tag{44}$$

Now applying the induction hypothesis, Eq. (41) becomes $p^\diamond \leq Y_k(x)$, which, by Lemma 3, implies that

$$(x, p^\diamond) \in \mathcal{E}_k. \tag{45}$$

Similarly, applying the induction hypothesis and Lemma 3 to Eq. (44) yields

$$\exists u^* \in U : \forall d \in [-p^\diamond, p^\diamond] : (Ax + Bu^* + Ed, p^\diamond) \in \mathcal{E}_k. \tag{46}$$

Finally combining Eq. (45), (46) gives $(x, p^\diamond) \in \mathcal{E}_{k+1}$, which implies that $Y_{k+1}(x) \geq p^\diamond$ by Lemma 3. Recall that $p^\diamond = V_{k+1}(x)$, hence $Y_{k+1}(x) \geq V_{K+1}(x)$ holds, which finishes the induction step and the proof. ■

REFERENCES

[1] D. Bertsekas. Infinite time reachability of state-space regions by using feedback control. *IEEE Transactions on Automatic Control*, 17(5):604–613, 1972.

[2] F. Blanchini. Ultimate boundedness control for uncertain discrete-time systems via set-induced lyapunov functions. *IEEE Transactions on automatic control*, 39(2):428–433, 1994.

[3] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[4] G. Chou, Y. E. Sahin, L. Yang, K. J. Rutledge, P. Nilsson, and N. Ozay. Using control synthesis to generate corner cases: A case study on autonomous driving. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(11):2906–2917, 2018.

[5] A. Donzé. Breach, a toolbox for verification and parameter synthesis of hybrid systems. In *International Conference on Computer Aided Verification*, pages 167–170. Springer, 2010.

[6] A. Eqtami and A. Girard. Safety control, a quantitative approach. *IFAC-PapersOnLine*, 51(16):187–192, 2018.

[7] A. Eqtami and A. Girard. A quantitative approach on assume-guarantee contracts for safety of interconnected systems. In *European Control Conference*, 2019.

[8] Y. Gao, K. H. Johansson, and L. Xie. Computing probabilistic controlled invariant sets. *arXiv preprint arXiv:1905.04117*, 2019.

[9] J. Hancock, S. Kolhoff, D. McGrew, M. Masrur, A. Skoweonska, J. Vandiver, J. Gatherer, J. Palmer, R. Wood, P. Curtiss, et al. Tactical vehicle to grid and vehicle to vehicle demonstration. In *Proc. NDIA Ground Vehicle Syst. Eng. Technol. Symp.(GVSETS)*, 2016.

[10] E. S. Kim, M. Arcak, and S. A. Seshia. Directed specifications and assumption mining for monotone dynamical systems. In *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*, pages 21–30. ACM, 2016.

[11] P. Nilsson and N. Ozay. Control synthesis for permutation-symmetric high-dimensional systems with counting constraints. *IEEE Transactions on Automatic Control*, 65(2):461–476, Feb 2020.

[12] P. J. Ramadge and W. Wonham. Modular feedback logic for discrete event systems. *SIAM Journal on Control and Optimization*, 25(5):1202–1218, 1987.

[13] M. Rungger and P. Tabuada. Computing robust controlled invariant sets of linear systems. *IEEE Transactions on Automatic Control*, 62(7):3665–3670, 2017.

[14] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[15] L. Yang and N. Ozay. Robustification and parametrization of switching controllers for a class of set invariance problems. *IFAC-PapersOnLine*, 50(1):1470–1477, 2017.