

Zonotope-based Controller Synthesis for LTL Specifications

Wei Ren, Julien Calbert and Raphaël Jungers

Abstract—This paper studies the controller synthesis problem for Linear Temporal Logic (LTL) specifications using (constrained) zonotope techniques. First, we implement (constrained) zonotope techniques to partition the state space and further to verify whether the LTL specification can be satisfied. Once the LTL specification can be satisfied, the next step is to design a controller to guarantee the satisfaction of the LTL specification for dynamic systems. Based on the verification of the LTL specification, an abstraction-based control design approach is proposed in this paper: a novel abstraction construction is developed first, then finite local abstract controllers are designed to achieve the LTL specification, and finally the designed abstract controllers are combined and refined as the controller for the original system. The proposed control strategy is illustrated via a numerical example from autonomous robots.

I. INTRODUCTION

In terms of high-level specifications like linear temporal logic (LTL) formulas [1], the control synthesis problem is generally not easy to be solved directly on continuous dynamics. One approach is based on discrete abstractions [2], [3], which allow to deal with controller synthesis problems efficiently via techniques developed in the fields of supervisory control [4] or game theory [5]. In this approach, a symbolic abstraction is first constructed for the continuous system such that certain behavioral relationship between them is satisfied, and then formal methods from the field of computer science are leveraged to synthesize a controller for the symbolic abstraction to satisfy the high-level specifications. This bottom-up control approach has been applied to study different systems and specifications [6]–[8].

Once the behavioral relation is guaranteed, the controller for the symbolic abstraction can be refined as the controller for the continuous dynamics [8]–[11]. Hence, the basis and essence of the abstraction-based control approach is the abstraction construction. Recently, many construction methods have been proposed. In terms of behavioral relations, (bi)simulation relation and its variants were applied in [6], [8], [12], and feedback refinement relation was proposed in [11]. In terms of the space partition, different partition approaches were proposed, like quantization techniques [8], [10], [11], [13], interval techniques [14], and reachability techniques [15]. These methods are based on the approximation of the whole state space, which may result in huge

complexity, and constrain system dynamics and the desired specifications; see e.g., [11], [15] for more details.

To deal with these limitations, we propose a novel control synthesis approach for nonlinear dynamic systems under LTL specifications. The proposed approach is based on the top-down design methodology [16], and thus is opposed to the bottom-up control approach in previous works. The approach consists of two steps: the specification verification and the controller design. The first step facilitates the second step by dividing the state space and allowing finite granular abstractions, whereas the second step leverages the first step in order to derive the corresponding controller. First, following the top-down design methodology and based on zonotope techniques, a novel approach is developed for the partition of the state space and the verification of the LTL specification. To be specific, the state space is divided via finite (constrained) zonotopes, which are allowed to intersect with each other, and the intersection relation among these (constrained) zonotopes results in an undirected graph. Given the initial state space, the satisfiability of the LTL specification can be verified based on the resulting graph. The specification verification leads to an ordered sequence of chosen (constrained) zonotopes to be applied in the controller synthesis, and a decomposition of the global specification into finite local specifications. Different from the existing partition approaches [13], [17] where all cells are disjoint, our approach allows different cells to be intersected, and this intersection relation plays an essential role in both the specification verification and the controller design.

The second step is to explore the controller for the LTL specification based on the abstraction-based control approach. To show this, we consider a chosen (constrained) zonotope. A local symbolic abstraction is first constructed for the current (constrained) zonotope such that certain equivalence relation between the original system and the constructed abstraction holds. Then, the intersection region between the current and previous (constrained) zonotopes is the initial region and the intersection region between the current and next (constrained) zonotopes is the target region. Finally, the local controller is designed via the local abstraction. In particular, the initial state set is the initial region for the first chosen (constrained) zonotope. Here, the applied approximation technique is based on the properties of zonotopes, which is different from the quantization technique [10], [12]. With the equivalence relation between the original system and the constructed abstraction, all designed local controllers are combined and refined as the controller for the original system with the LTL specification.

Preliminaries and problem formulation are introduced in

This work was supported by the European Research Council (ERC) Grant 864017–L2C, the CHIST-ERA 2018 project DRUID-NET, the Walloon Region and the Innoviris Foundation. J. Calbert is an FRIA fellow, and R. Jungers is an FNRS Research Associate.

W. Ren, J. Calbert and R. Jungers are with ICTEAM Institute, Université catholique de Louvain, 1348 Louvain-la-Neuve, Belgium. Email: {w.ren, julien.calbert, raphael.jungers}@uclouvain.be.

Section II. The zonotope-based partition is proposed in Section III and LTL specifications are verified in Section IV. The abstraction-based control design approach is proposed in Section V. A numerical example is given in Section VI. Conclusion and future work are presented in Section VII.

II. NOTATION AND PRELIMINARIES

$\mathbb{R} := (-\infty, +\infty)$; $\mathbb{R}_0^+ := [0, +\infty)$; $\mathbb{R}^+ := (0, +\infty)$; $\mathbb{N} := \{0, 1, \dots\}$; $\mathbb{N}^+ := \{1, 2, \dots\}$. Given $A, B \subset \mathbb{R}^n$, $B \setminus A := \{x : x \in B, x \notin A\}$. $A \subset \mathbb{R}^n$ is a connected region if it cannot be represented as the union of two or more disjoint non-empty open regions. Given a vector $x \in \mathbb{R}^n$, x_i is the i -th element of x , $|x|$ is the Euclidean norm of x , and $\|x\|$ is the infinite norm of x . The closed ball centered at $x \in \mathbb{R}^n$ with radius $\varepsilon \in \mathbb{R}^+$ is defined by $\mathbf{B}(x, \varepsilon) = \{y \in \mathbb{R}^n : \|x - y\| \leq \varepsilon\}$. Given a set $\Lambda \subset \mathbb{R}^n$, Λ° is the interior of Λ ; the ε -expansion of Λ is $\mathbf{E}_\varepsilon(\Lambda) := \{y \in \mathbb{R}^n : \exists x \in \Lambda, \|y - x\| \leq \varepsilon\}$. Given a measurable function $f : \mathbb{R}_0^+ \rightarrow \mathbb{R}^n$, the (essential) supremum of f is $\|f\| := \text{ess sup}\{\|f(t)\| : t \in \mathbb{R}_0^+\}$. Given $A, B \subset \mathbb{R}^n$, a relation $\mathcal{F} \subset A \times B$ is the map $\mathcal{F} : A \rightarrow 2^B$ defined by $b \in \mathcal{F}(a)$ if and only if $(a, b) \in \mathcal{F}$.

A set $Z \subset \mathbb{R}^n$ is a *zonotope*, if there exists $(\mathbf{c}, \mathbf{G}) \in \mathbb{R}^n \times \mathbb{R}^{n \times n_g}$ such that $Z = \{\mathbf{c} + \mathbf{G}\xi : \|\xi\| \leq 1\}$. A set $Z^c \subset \mathbb{R}^n$ is a *constrained zonotope*, if there exists $(\mathbf{c}, \mathbf{G}, \mathbf{A}, \mathbf{b}) \in \mathbb{R}^n \times \mathbb{R}^{n \times n_g} \times \mathbb{R}^{n_c \times n_g} \times \mathbb{R}^{n_c}$ such that $Z^c = \{\mathbf{c} + \mathbf{G}\xi : \|\xi\| \leq 1, \mathbf{A}\xi = \mathbf{b}\}$. $\mathbf{c}$ is the center, $\mathbf{G}$ is the generator matrix with each column being a generator, and $\mathbf{A}\xi = \mathbf{b}$ is the constraint. From [18], Z^c is a constrained zonotope if and only if it is a convex polytope, and a convex polytope is a zonotope if and only if every 2-face is centrally symmetric.

A. Transition Systems

Definition 1 ([12]): A *transition system* is a quadruple $T = (X, X^0, U, \Delta)$ with: (i) a state set X ; (ii) a set of initial states $X^0 \subseteq X$; (iii) an input set U ; (iv) a transition relation $\Delta \subseteq X \times U \times X$. T is *symbolic* if X and U are countable.

The transition $(x, u, x') \in \Delta$ is denoted by $x' \in \Delta(x, u)$, which means that the system can evolve from the state x to the state x' under the input u . An input $u \in U$ belongs to the *set of the enabled inputs* at the state x , denoted by $\text{enab}(x)$, if $\Delta(x, u) \neq \emptyset$. T is *deterministic* if for all $x \in X$ and all $u \in \text{enab}(x)$, $\Delta(x, u)$ has exactly one element. In this case, we write $x' = \Delta(x, u)$ with a slight abuse of notation.

Definition 2 ([11]): Let $T_i = (X_i, X_i^0, U_i, \Delta_i)$ with $i \in \{1, 2\}$ be two transition systems, and $U_2 \subseteq U_1$. A relation $\mathcal{F} \subseteq X_1 \times X_2$ is a *feedback refinement relation* from T_1 to T_2 , if for all $(x_1, x_2) \in \mathcal{F}$, (a) $U_2(x_2) \subseteq U_1(x_1)$; (b) $u \in U_2(x_2) \Rightarrow \mathcal{F}(\Delta_1(x_1, u)) \subseteq \Delta_2(x_2, u)$, where $U_i(x) := \{u \in U_i : u \in \text{enab}(x)\}$. Denote by $T_1 \preceq_{\mathcal{F}} T_2$ if $\mathcal{F} \subseteq X_1 \times X_2$ is a feedback refinement relation from T_1 to T_2 .

Definition 3 ([8]): A *control system* is a quadruple $\Sigma = (X, U, \mathcal{U}, f)$, where, (i) $X \subset \mathbb{R}^n$ is the state set; (ii) $U \subseteq \mathbb{R}^m$ is the input set; (iii) $\mathcal{U}$ is a subset of all piecewise continuous functions of time from the interval $[0, \infty) \subset \mathbb{R}$ to U ; (iv) $f : X \times U \rightarrow \mathbb{R}^n$ is a continuous map satisfying the Lipschitz assumption: there exists a constant $L \in \mathbb{R}^+$ such that for all

$x, y \in X$ and all $u \in U$, $\|f(x, u) - f(y, u)\| \leq L\|x - y\|$. Given any $b > a \geq 0$, a locally absolutely continuous curve $\xi : (a, b) \rightarrow \mathbb{R}^n$ is a *trajectory* of Σ , if there exists $\mathbf{u} \in \mathcal{U}$ such that $\dot{\xi}(t) = f(\xi(t), \mathbf{u}(t))$ for almost all $t \in (a, b)$.

The trajectory defined on $[0, \tau]$ with $\tau \in \mathbb{R}^+$ is denoted as $\mathbf{x} : [0, \tau] \rightarrow X$. The trajectory starting from the initial time t_0 is denoted by $x[t_0]$. Denote by $\mathbf{x}(t, x, u)$ the point reached at $t \in (a, b)$ under the input u from x . Such a point is determined uniquely from the assumptions on f .

B. Linear Temporal Logic Specifications

Let $\Pi := \{\pi_1, \dots, \pi_n\}$ be a finite set of atomic propositions with $n \in \mathbb{N}^+$, and Φ_Π be the set of all Boolean combinations of elements of Π . The denotation $\llbracket \cdot \rrbracket : \Pi \rightarrow \mathcal{P}(X)$ of each symbol in Π is a subset of X , i.e., $\llbracket \pi \rrbracket \subseteq X$ for any $\pi \in \Pi$. Here, $\mathcal{P}(\Gamma)$ denotes the powerset of a set Γ .

Based on atomic propositions, Boolean connectors like negation $\neg$ and conjunction $\wedge$, and two temporal operators $\bigcirc$ ('next') and $\bigcup$ ('until'), Linear Temporal Logic (LTL) is formed via the following syntax [1]: $\varphi ::= \top \mid \alpha \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 \bigcup \varphi_2$, where $\varphi, \varphi_1, \varphi_2$ are LTL formulas. The Boolean connector disjunction $\vee$, and temporal operators $\diamond$ ('eventually') and $\square$ ('always') can be derived below: $\varphi_1 \vee \varphi_2 := \neg(\neg\varphi_1 \wedge \neg\varphi_2)$, $\diamond\varphi := \top \bigcup \varphi$ and $\square\varphi := \neg\diamond\neg\varphi$. Formal definitions for the LTL semantics and model checking can be found in [1]. For the system Σ , if the LTL formula ϕ is satisfied over the trajectory $x[t_0]$ with respect to the atomic proposition mapping $\llbracket \cdot \rrbracket$, then we denote by $(x[t_0], \llbracket \cdot \rrbracket) \models \phi$, otherwise, $(x[t_0], \llbracket \cdot \rrbracket) \not\models \phi$. For the system Σ and the LTL formula ϕ , we aim to deal with the following two problems.

- 1 Given the system Σ and an LTL formula ϕ , verify whether the formula ϕ could be satisfied.
- 2 If the LTL formula ϕ is satisfied, design the controller C such that the LTL formula ϕ is satisfied for the system Σ .

By solving the first problem, we verify the satisfaction of the LTL specification in the given workspace in Section IV. If the verification is feasible, then the controller is designed for the system Σ to solve the second problem in Section V.

III. ZONOTOPES BASED PARTITION

To solve the above two problems, we first propose a novel method for the state-space partition. The partition strategy is presented in Algorithm 1. Line 1 is to generate finite zonotopes and constrained zonotopes to cover the state space. Since the generated zonotopes and constrained zonotopes are not necessarily overlapped, Line 2 is to expand all generated zonotopes and constrained zonotopes to ensure each (constrained) zonotope to overlap with its neighbour zonotopes and constrained zonotopes. In Line 2, the expansion operator is applied to all generated zonotopes and constrained zonotopes. We emphasize that Line 2 plays important roles in the controller synthesis, which will be explained in Section V in detail.

In the following, we establish Line 1 of Algorithm 1, which is formulated in Algorithm 2. To begin with, the number $N \in \mathbb{N}$ of zonotopes to be generated is set *a priori*, and then we choose $N \in \mathbb{N}$ points $\mathbf{c}_i \in X$ arbitrarily as the

Algorithm 1: State Space Partition

Input: the state space $X \subset \mathbb{R}^n$, the precision $\varepsilon > 0$

Output: the set of zonotopes $\mathbf{Z}$

- 1 Generate finite zonotopes Z_i and constrained zonotopes Z_j^c to cover the state space X
 - 2 Expand both Z_i and Z_j^c via the precision $\varepsilon > 0$
 - 3 **return** $\mathbf{Z} = (\cup_{i=1}^N \mathbf{E}_\varepsilon(Z_i)) \cup (\cup_{j=1}^M \mathbf{E}_\varepsilon(Z_j^c))$
-

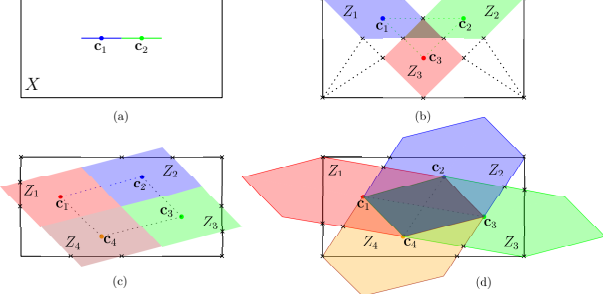


Fig. 1. Illustration of the zonotope generation. (a) $N = 2$: the generated zonotopes are 2 segments and thus not well-defined. (b) $N = 3$: 3 zonotopes are generated and overlapped. (c) $N = 4$ and each center connects with 2 neighbor centers: 4 zonotopes are not overlapped. (d) $N = 4$ and each center connects with 3 neighbor centers: 4 zonotopes are overlapped.

centers of zonotopes, where $i \in \mathcal{N}_1 := \{1, \dots, N\}$. Here, we assume that $N \in \mathbb{N}$ satisfies $N > n$ with $n \in \mathbb{N}^+$ being the dimension of the state space. These points are connected such that each point is connected with at least $n \in \mathbb{N}$ neighbour points. That is, these connections lead to at least $n \in \mathbb{N}$ vectors for each point, which is used as the generators for each zonotope. With these centers and generators, we can generate N zonotopes as in Line 3 in Algorithm 2.

In the zonotope generation, the constraints on the choice of the centers (i.e., $N > n$ and $\mathbf{G}_i$ is full-rank) are to guarantee the construction of zonotopes. To show this, we consider a two-dimensional space $X \subset \mathbb{R}^2$ as in Fig. 1. If we choose $N = 2$ as in Fig. 1(a), then the generated zonotopes are two segments. If $\mathbf{G}_i$ is not full-rank, then each center connects with only one neighbour center or some centers are in the same line, and the generated zonotopes are segments either. Therefore, the lower bound of $N \in \mathbb{N}$ and the full-rank condition on $\mathbf{G}_i$ are to ensure the well-definedness of the zonotope generation. Note that different $N \in \mathbb{N}$ and $\mathbf{G}_i$ have effects on the generated zonotopes; see Fig. 1.

If the union of all generated zonotopes covers the state space, then there is no need for the generation of constrained zonotopes; otherwise, constrained zonotopes are needed. The motivation of using constrained zonotopes is that constrained zonotopes are allowed to be asymmetric [18], [19] and thus can be used to cover asymmetric regions. The construction rule is based on intersection points among the generated zonotopes and the state space, and presented explicitly as follows: we first determine the intersection vertices among boundaries of the generated zonotopes and the state space, then rule out those in the interiors of at least one of the generated zonotopes and achieve the vertices to generate constrained zonotopes (see the crosses in Fig. 1), and finally connect these vertices to generate regions that do not

Algorithm 2: Zonotope Generation

Input: the state domain $X \subset \mathbb{R}^n$, the integer $N > n$

Output: finite zonotopes and constrained zonotopes

- 1 Choose N points in X randomly as the centers $\mathbf{c}_i \in \mathbb{R}^n$
- 2 Connect these points such that for each $\mathbf{c}_i \in \mathbb{R}^n$, there exists a full-rank matrix:

$$\mathbf{G}_i = (\mathbf{c}_{k_1} - \mathbf{c}_i, \dots, \mathbf{c}_{k_{k_i}} - \mathbf{c}_i), \quad k_i \geq n \quad (1)$$

- 3 With $\mathbf{c}_i \in \mathbb{R}^n$ and $0.5\mathbf{G}_i$, construct the zonotope

$$Z_i = \{\mathbf{c}_i + 0.5\mathbf{G}_i\xi : \|\xi\| \leq 1\} \quad (2)$$

- 4 **if** $X \setminus (\cup_{i=1}^N Z_i) = \emptyset$ **then**
 - 5 | No need to construct constrained zonotopes
 - 6 **else**
 - 7 | Determine the set $\mathbb{V}_1$ of intersection among $\partial Z_1, \dots, \partial Z_N, \partial X$
 - 8 | Refine $\mathbb{V}_1$ as $\mathbb{V}$ by excluding those in $\cup_{i=1}^N Z_i^\circ$
 - 9 | Generate the set $\mathbb{S}_1$ of regions by connecting vertices in $\mathbb{V}$
 - 10 | Refine $\mathbb{S}_1$ as $\mathbb{S}$ by excluding those intersecting with $\cup_{i=1}^N Z_i$
 - 11 | Construct M constrained zonotopes $\cup_{j=1}^M Z_j^c \supseteq \mathbb{S}$
 - 12 **return** $\mathbf{Z} = (\cup_{i=1}^N Z_i) \cup (\cup_{j=1}^M Z_j^c)$
-

intersect with the generated zonotopes. These regions are represented as constrained zonotopes.

The generation of constrained zonotopes relies on basic operations of zonotopes. For instance, the vertices of the generated zonotopes can be obtained via the transformation of zonotopes into the V-representation [20]. These vertices are connected to determine the intersection vertices, which form the set $\mathbb{V}_1$ in Line 7 of Algorithm 2. The set $\mathbb{V}_1$ is refined as the set $\mathbb{V}$ in Line 8 by excluding those in the generated zonotopes. Based on the vertices in $\mathbb{V}$ and using the transformation from V-representation into Z-representation [20], constrained zonotopes are generated in Lines 9-11 of Algorithm 2 to cover the region $X \setminus (\cup_{i=1}^N Z_i)$.

All generated zonotopes and constrained zonotopes are labeled via a symbol set $\Pi := \{\pi_1, \dots, \pi_N, \pi_{N+1}, \dots, \pi_{N+M}\}$, where $\llbracket \pi_i \rrbracket = \mathbf{E}_\varepsilon(Z_i)$ for all $i \in \mathcal{N}_1$, $\llbracket \pi_{N+j} \rrbracket = \mathbf{E}_\varepsilon(Z_j^c)$ for all $j \in \mathcal{N}_2 := \{1, \dots, M\}$. Let $\mathcal{N} := \{1, \dots, N + M\}$, and the partition of the state space X is $\mathbf{Z} := \{\mathbf{Z}_k : \mathbf{Z}_k = \llbracket \pi_k \rrbracket, k \in \mathcal{N}\}$.

IV. VERIFICATION OF LTL FORMULAS

With the partition of the state space, the LTL formula is verified in this section. For this purpose, we denote by $\mathcal{O} := \{\mathcal{O}_k : k \in \mathbb{J}\} \subset X$ all forbidden regions including obstacles and states that are not allowed to be visited, where $\mathbb{J} \subset \mathbb{N}$ is finite. A region $A \subset X$ is *admissible* if $A \setminus \mathcal{O}$ is a connected region. First, we verify whether all intersection regions are admissible and derive all admissible intersection regions, which further imply the relation among zonotopes and constrained zonotopes. Second, this relation can be transformed into an undirected graph via the adjacency matrix. This two-step mechanism is summarized as Algorithm 3.

Theorem 1: Algorithm 3 terminates in finite time. The obtained adjacency matrix Υ shows all admissible intersections

Algorithm 3: Adjacency Matrix

Input: the partition $\mathbf{Z}$, the forbidden region $\mathcal{O} \subset X$
Output: the matrix $\Upsilon = [a_{ij}]$ and the set $\mathbf{I} = \{\mathbf{I}_{ij}\}$

```

1 for  $i = 1 : 1 : N + M - 1$  do
2   if  $\mathbf{Z}_i \cap \mathcal{O} \neq \mathbf{Z}_i$  then
3     for  $j = 1 : 1 : N + M$  do
4       if  $\mathbf{Z}_j \cap \mathcal{O} \neq \mathbf{Z}_j$  then
5          $\Omega = \mathbf{Z}_i \cap \mathbf{Z}_j$ 
6         if  $\Omega = \emptyset$  then
7            $a_{ij} = 0$ 
8         else
9           if  $\Omega \setminus \mathcal{O}$  is a connected region then
10             $a_{ij} = 1$   $\mathbf{I}_{ij} = \Omega \setminus \mathcal{O}$ 
11          else
12             $a_{ij} = 0$ 
13        else
14           $a_{ij} = 0$ 
15      else
16         $a_{ij} = 0$  for  $j \in \mathcal{N}$ 
17 return  $\Upsilon = [a_{ij}], \mathbf{I} = \{\mathbf{I}_{ij}\}$ 

```

among all zonotopes and constrained zonotopes.

From the adjacency matrix Υ , we generate a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where the vertex set $\mathcal{V} = \Pi$, and the edge set is $\mathcal{E} \subseteq \Pi \times \Pi$ with $(\pi_i, \pi_j) \in \mathcal{E}$ if $a_{ij} = 1$. To include the initial state region and the LTL formula ϕ , the graph $\mathcal{G}$ is generalized. To be specific, the initial state region is contained in the constrained zonotope Z_0^c with the symbol π_0 . From the LTL formula ϕ , the regions of interest are obtained and denoted as finite constrained zonotopes $Z_{\phi, \ell}^c$ with the symbol $\pi_{\phi, \ell}$, where $\ell \in \mathbb{K} := \{1, \dots, K\}$ and $K \in \mathbb{N}$. Both Z_0^c and $Z_{\phi, \ell}^c$ may intersect with some elements of $\mathbf{Z}$, which can be verified easily. Hence, $\mathcal{G}$ is generalized as $\bar{\mathcal{G}} = (\bar{\mathcal{V}}, \bar{\mathcal{E}})$ with the vertex set $\bar{\mathcal{V}} = \Pi \cup \{\pi_0, \pi_{\phi, 1}, \dots, \pi_{\phi, K}\}$ and the edge set $\bar{\mathcal{E}} \subseteq \bar{\mathcal{V}} \times \bar{\mathcal{V}}$ extending $\mathcal{E}$ by adding the connections among $Z_0^c, Z_{\phi, \ell}^c$ and $\mathbf{Z}$. On the other hand, we can use any standard LTL model checker [1] to solve the LTL planning problem and to derive an accepting path $\bar{\pi} := \{\bar{\pi}_0, \bar{\pi}_1, \bar{\pi}_2, \dots\}$ with $\bar{\pi}_0 = \pi_0$ and $\bar{\pi}_k$ with $k \in \mathbb{N}^+$ from $\{\pi_{\phi, 1}, \dots, \pi_{\phi, K}\}$.

Theorem 2: Consider the state space $X \subseteq \mathbb{R}^n$, the initial state region $X_0 \subset Z_0^c$, the forbidden region $\mathcal{O}$, and the LTL formula ϕ . The following two statements are equivalent.

- 1) The LTL formula ϕ can be satisfied in $X \subseteq \mathbb{R}^n$.
- 2) In $\bar{\mathcal{G}}$ there exists a path $\mathbf{P}$ realizing the accepting path $\bar{\pi} := \{\bar{\pi}_0, \bar{\pi}_1, \bar{\pi}_2, \dots\}$. That is, there exists a sub-path in $\mathbf{P}$ for any pair $(\bar{\pi}_i, \bar{\pi}_{i+1})$ with $i \in \mathbb{N}$.

In terms of the state space, Theorem 2 shows how to verify the LTL formula ϕ via the graph theory, and thus solves Problem 1. In the graph $\bar{\mathcal{G}}$, each path $\mathbf{P}$ can be projected into a sequence of finite (constrained) zonotopes $\mathbf{Z}_p := \{\llbracket \pi \rrbracket \in \mathbf{Z} : \pi \in \mathbf{P}\}$. Note that the path $\mathbf{P}$ is not necessarily unique.

V. ABSTRACTION-BASED CONTROLLER SYNTHESIS

To solve Problem 2, the abstraction-based control techniques are applied, and the whole design process consists of four steps: the time discretization of the original system is

first derived; the state and input spaces are approximated; the symbolic abstraction is constructed; and finally the abstract controller is designed and refined into the controller for the original system for the LTL specification.

The time-discretization of the system Σ is established via the sampling technique. Let the sampling period be $\tau > 0$ as a design parameter, and the sampled-data system is written as a transition system $T_\tau(\Sigma) := (X_1, X_1^0, U_1, \Delta_1)$, where,

- the set of states is $X_1 = X$;
- the set of initial states is $X_1^0 = X$;
- the set of inputs is $U_1 = \{u \in \mathcal{U} : \mathbf{x}(\tau, x, u) \text{ is defined for all } x \in X\}$;
- the transition relation is as follows: for $x \in X_1$ and $u \in U_1$, $x' = \Delta_1(x, u)$ if and only if $x' = \mathbf{x}(\tau, x, u)$.

The system $T_\tau(\Sigma)$ is deterministic. Note that $T_\tau(\Sigma)$ can be treated as the time approximation of the system Σ .

A. Approximation of State and Input Spaces

With the time-discretization and the partition of the state domain, the next is to approximate state and input spaces. Without loss of generality, we focus on the approximation of any zonotope $Z \subset X_1$ and constrained zonotope $Z^c \subset X_1$.

1) *Approximation of Zonotopes:* Different from the quantization-based approximation technique in [12], the applied approximation technique is based on the properties of zonotopes. Let $Z = \{\mathbf{c} + \mathbf{G}\xi : \|\xi\| \leq 1\} \in \mathbf{Z}$ be a zonotope.

First, from the generator $\mathbf{G}$, let $\mathbf{G}_b := (g_1, \dots, g_L) = (g_1/N_1, \dots, g_L/N_L)$ be the basic generator, which plays the similar role of the state space discretization parameter as in [12]. The choice of $\{N_l : l \in \mathbb{L} = \{1, \dots, L\}\}$ determines the approximation of the state space, and is determined via the desired approximation precision. For instance, given the desired approximation precision $\varepsilon > 0$, $\max_{l \in \mathbb{L}} |g_l| \leq \varepsilon$ is imposed to constrain the choice of $\{N_1, \dots, N_L\}$. Based on the basic generator $\mathbf{G}_b$, we obtain the set $\mathbf{F} := \bigcup_{l \in \mathbb{L}} \mathbf{F}_l$ with $\mathbf{F}_l := \{\mathbf{c} \pm g_l, \dots, \mathbf{c} \pm (N_l - 1)g_l, \mathbf{c} \pm g_l\}$.

Second, based on the set $\mathbf{F}$, the zonotope Z is approximated as follows. Given $p_{lj} \in \mathbf{F}_l$, we generate other points in the following way: $p_{lj} \in \mathbf{F}_l$ is the basis; any vector in $\{g_1, \dots, g_{l-1}, g_{l+1}, \dots, g_L\}$ is the direction; and finally

$$\bar{\mathbf{F}}_l := \bigcup_{0 < j \leq N_l} \bigcup_{k \in \mathbb{L}, k \neq l} \{p_{lj} \pm g_k, \dots, p_{lj} \pm g_k\} \cap Z. \quad (3)$$

This generation mechanism is terminated until the generated point does not belong to Z . That is, $\bar{\mathbf{F}}_l \subset Z$. Since $\mathbf{F}_l$ is finite, this generation mechanism can be implemented recursively and terminated in finite time. Therefore, Z is approximated by the set $\mathcal{A}(Z) := \{\mathbf{c}\} \cup (\bigcup_{l \in \mathbb{L}} (\mathbf{F}_l \cup \bar{\mathbf{F}}_l))$.

2) *Approximation of Constrained Zonotopes:* Following the above approximation for zonotopes, the constrained zonotope Z^c can be approximated similarly. The only difference lies in $\mathbf{A}\xi = \mathbf{b}$. Hence, $\bar{\mathbf{F}}_l$ in (3) is changed to

$$\bar{\mathbf{F}}_l^c := \bigcup_{0 < j \leq N_l} \bigcup_{k \in \mathbb{L}, k \neq l} \{p_{lj} \pm g_k, \dots, p_{lj} \pm g_k\} \cap Z^c. \quad (4)$$

Following the same mechanism, we derive $\mathcal{A}(Z^c)$ to approximate Z^c . Based on the generator matrix $\mathbf{G}$, we introduce

the norm $\|\cdot\|_{\mathbf{G}}$ defined as $\|\mathbf{v}\|_{\mathbf{G}} := \max_{k \in \mathbb{L}} \{\mathbf{v} \cdot \mathbf{g}_k / \|\mathbf{g}_k\|\}$ for $\mathbf{v} \in \mathbb{R}^n$, where $\mathbf{v} \cdot \mathbf{g}_k / \|\mathbf{g}_k\|$ is the scalar projection of $\mathbf{v}$ onto $\mathbf{g}_k$. With the norm $\|\cdot\|_{\mathbf{G}}$, we can see that for any $x \in Z$ (or $x \in Z^c$), there exists $q \in \mathcal{A}(Z)$ (or $q \in \mathcal{A}(Z^c)$) such that $\|x - q\|_{\mathbf{G}} \leq 0.5 \max_{l \in \mathbb{L}} \{\|g_l\|\}$.

3) *Approximation of Input Space:* For the zonotope $Z \subset X_1$, its input set $U_1(Z) \subseteq U_1$ is defined as $\cup_{x \in Z} \text{enab}(x)$, and then approximated as follows. Given any $q \in \mathcal{A}(Z)$, the reachable set of $T_\tau(\Sigma)$ from q is denoted by $\mathbf{Reach}(\tau, q) := \{x' \in Z : \mathbf{x}(\tau, q, u) = x', u \in U_1(Z)\}$, which is well defined due to the input set $U_1(Z)$. The reachable set $\mathbf{Reach}(\tau, q)$ is approximated below. Given any $\eta \in \mathbb{R}^+$, consider the set $\mathcal{S}_\eta(\tau, q) := \{v \in \mathcal{A}(Z) : \exists z \in \mathbf{Reach}(\tau, q) \text{ such that } \|v - z\|_{\mathbf{G}} \leq \eta/2\}$, which is a countable set and where $\eta \in \mathbb{R}^+$ is constrained by the approximation precision. Define the function $\psi : \mathcal{S}_\eta(\tau, q) \rightarrow U_1(Z)$ such that for any $v \in \mathcal{S}_\eta(\tau, q)$, there exists an input $u_1 = \psi(v) \in U_1(Z)$ such that $\|v - \mathbf{x}(\tau, q, u_1)\|_{\mathbf{G}} \leq \eta/2$. We define the set $U_2(q) := \psi(\mathcal{S}_\eta(\tau, q))$, which captures the set of the inputs applied at the state $q \in \mathcal{A}(Z)$. The set $U_2(q)$ is countable since $U_2(q)$ is the image of the map ψ of the countable set $\mathcal{S}_\eta(\tau, q)$. Therefore, the input set $U_1(Z)$ is approximated by mean of the following countable set: $U_2(Z) := \cup_{q \in \mathcal{A}(Z)} U_2(q)$. That is, given any $q \in \mathcal{A}(Z)$, for any $u_1 \in U_1(Z)$, there exists $u_2 \in U_2(q)$ such that $\|\mathbf{x}(\tau, q, u_1) - \mathbf{x}(\tau, q, u_2)\|_{\mathbf{G}} \leq \eta$.

Finally, since all elements of $\mathbf{Z}$ are ε -expansion of (constrained) zonotopes and still are (constrained) zonotopes, the above approximation mechanism can be applied similarly.

B. Abstraction Construction

Now we construct the symbolic abstraction for $T_\tau(\Sigma)$ with the state space $Z \in \mathbf{Z}$, which is denoted as $T_\tau(\Sigma, Z)$. The symbolic abstraction of $T_\tau(\Sigma, Z)$ is described by the transition system $T_{\tau, \eta}(\Sigma, Z) = (X_2, X_2^0, U_2, \Delta_2)$, where,

- the set of states is $X_2 = \mathcal{A}(Z)$;
- the set of initial states is $X_2^0 = \mathcal{A}(Z_0)$ with $Z_0 \subseteq Z$;
- the set of inputs is $U_2 = U_2(Z)$;
- the transition relation is given by: for $q_1, q_2 \in X_2$ and $v \in U_2$, $q_2 \in \Delta_2(q_1, u)$ if and only if $q_2 \in \{\bar{q} \in X_2 : \|\mathbf{x}(\tau, q, v) - \bar{q}\|_{\mathbf{G}} \leq (0.5 + e^{L\tau})\varepsilon\}$.

From the transition relation, $T_{\tau, \eta}(\Sigma, Z)$ is nondeterministic.

Theorem 3: Consider the system $T_\tau(\Sigma, Z)$ and its abstraction $T_{\tau, \eta}(\Sigma, Z)$ with the time and input sampling parameters $\tau, \eta \in \mathbb{R}^+$. Given a desired precision $\varepsilon \in \mathbb{R}^+$, if the map $\mathcal{F} : Z \rightarrow \mathcal{A}(Z)$ is given by $\mathcal{F}(x) = \{q \in \mathcal{A}(Z) : \|x - q\|_{\mathbf{G}} \leq \varepsilon\}$, then $T_\tau(\Sigma, Z) \preceq_{\mathcal{F}} T_{\tau, \eta}(\Sigma, Z)$.

For each (constrained) zonotope, we can follow the similar mechanism to construct the symbolic abstraction. Hence, the symbolic abstraction is only for the system with the (constrained) zonotope in $\mathbf{Z}$ being the state space, which is different from the construction approach in [9], [10], [21].

C. Controller Design and Refinement

With the path $\mathbf{P}$ from Theorem 2 and the constructed symbolic abstraction, the controller is designed to achieve the LTL specification for the original system. For this purpose, we first denote by $\mathbf{Z}_p \subset \mathbf{Z}$ the (constrained) zonotope

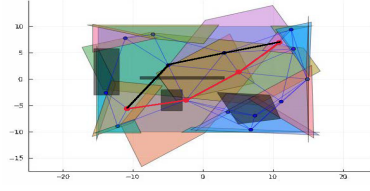


Fig. 2. Illustration of the partition of the state space and the graph generation. Both black and red lines are two paths for the LTL formula ϕ .

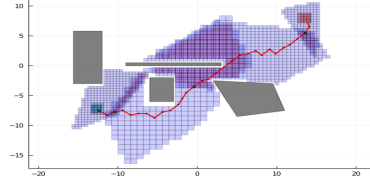


Fig. 3. State trajectory based on the abstract controller for the LTL formula ϕ . The grey regions are obstacles, the dark blue region is the initial state set, the orange region is the target region, the purple regions are intersection regions, and the state trajectory is shown in red line.

set from the path $\mathbf{P}$, then have the symbolic abstraction $T_{\tau, \eta}(\Sigma, \mathbf{Z}_p)$, and finally derive the following proposition.

Proposition 1: Given $T_\tau(\Sigma, \mathbf{Z}_p) \preceq_{\mathcal{F}} T_{\tau, \eta}(\Sigma, \mathbf{Z}_p)$, if there is an abstract controller $C_a : \mathbf{Z}_p \rightarrow U_2$ for $T_{\tau, \eta}(\Sigma, \mathbf{Z}_p)$ with the LTL formula ϕ , then there exists a controller $C(x) := C_a(\mathcal{F}(x))$ for $T_\tau(\Sigma, \mathbf{Z}_p)$ with the LTL formula ϕ .

With Proposition 1, the abstract controller can be refined as the controller for the system $T_\tau(\Sigma)$, and the next is the abstract controller design, which is presented in the following recursive steps. Let $\mathbf{Z}_p = \{\mathbf{Z}_{p1}, \dots, \mathbf{Z}_{pl}\}$ with $l \in \mathbb{N}^+$ be ordered (constrained) zonotopes from the path $\mathbf{P}$.

- 1) For $\mathbf{Z}_{p1}$, the initial set is $(\mathbf{Z}_{p1} \cap \mathbf{Z}_0^c) \setminus \mathcal{O}$ and the target set is $(\mathbf{Z}_{p1} \cap \mathbf{Z}_{p2}) \setminus \mathcal{O}$.
- 2) For $i \in \{2, \dots, l-1\}$, the initial set is $(\mathbf{Z}_{p(i-1)} \cap \mathbf{Z}_{pi}) \setminus \mathcal{O}$, and the target set is $(\mathbf{Z}_{pi} \cap \mathbf{Z}_{p(i+1)}) \setminus \mathcal{O}$. Note that the final target set is contained in $\mathbf{Z}_{pl}$.
- 3) Based on the classic fixed-point algorithm [4], the abstract controller C_i in $\mathbf{Z}_{pi}$ is designed such that the system can move from the initial set to the target set.
- 4) All designed abstract controllers C_i are combined sequentially as the overall abstract controller C_a for the system $T_{\tau, \eta}(\Sigma, \mathbf{Z}_p)$ with the LTL specification ϕ .

VI. NUMERICAL EXAMPLE

The derived results are illustrated in this section. The computation is executed using Julia on a laptop with a 16 GB RAM and an Intel i7-10610U processor (1.80GHz). Consider the autonomous vehicle [17] denoted by $\Sigma : (\dot{x}_1(t), \dot{x}_2(t)) = (u_1(t), u_2(t))$, where $x = (x_1, x_2) \in \mathbb{R}^2$ is the system state being the position of the autonomous vehicle, and $u = (u_1, u_2) \in \mathbb{R}^2$ is the control input being the velocities of the wheels. Let $x \in X := [-15, 15] \times [-10, 10]$ and $u \in U := [-2, 2] \times [-2, 2]$. Here, our objective is to design a controller such that the autonomous vehicle moves to a specific target region by avoiding four obstacles, where the target region is $\mathcal{O}_t = [12.7, 14.3] \times [7.2, 8.8]$, and the obstacles are denoted as the grey regions in Fig. 3. Therefore, the specification is formalized as the LTL formula: $\phi =$

TABLE I
COMPARISON OF TRANSITION NUMBERS AND RUN TIMES¹

	Classic approach ²	Our approach
transition number	662238	383252
t_{abs}	9.9094s	2.0905s
t_{con}	0.2514s	0.1520s

$\diamond \mathcal{O}_t \wedge \square \neg (\mathcal{O}_1 \vee \mathcal{O}_2 \vee \mathcal{O}_3 \vee \mathcal{O}_4)$. In this example, the vehicle is initialized in $X_0 = [-13.3, -12.1] \times [-7.8, -6.6]$.

We first apply Algorithms 1-2 to partition the state space, which is shown in Fig. 2. The partition results in $N = 4$ zonotopes and $M = 13$ constrained zonotopes. Based on intersection relation and Algorithm 3, these zonotopes and constrained zonotopes are labeled into 17 symbols (i.e., $\Pi = \{\pi_i : i = 1, \dots, 17\}$), and a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is generated (see Fig. 2). The graph $\mathcal{G}$ is generalized by including the initial state set X_0 and the target set $\mathcal{O}_t$, and further a path $\mathbf{P}$ can be found via graph techniques. In Fig. 2, both red and black lines are paths, and we choose the red one including 2 zonotopes and 2 constrained zonotopes, which are denoted as an ordered sequence $\mathbf{Z}_p := \{\mathbf{Z}_1^c, \mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_2^c\}$.

The second step is the controller design. Let $\tau = 0.5\text{s}$, and the set U is approximated as $U_2 := \{0.5i : i \in \{-4, -3, \dots, 3, 4\}\}^2$. Different (constrained) zonotopes can be approximated with different state space parameters, which are constrained by the desired precision $\varepsilon = 1$. The state space parameters are chosen as 0.4, 0.8, 0.5, 0.4 with the corresponding (constrained) zonotopes. Hence, the symbolic abstraction is constructed for each (constrained) zonotope, and the abstract controller is designed. For instance, in $\mathbf{Z}_2^c$, the target region is $\mathbf{Z}_2^c \cap \mathcal{O}_t$, and the initial region is $\mathbf{Z}_2^c \cap \mathbf{Z}_2$. It takes 0.1563s to construct the abstraction with 36729 transitions and 0.004425s to derive the abstract controller. The state trajectory is shown in Fig. 3.

Comparing with the existing works [8]–[11] where the whole state space is approximated, the partition-based specification verification results in finite (constrained) zonotopes, which are approximated only in this paper. In terms of the transition number and computation times, the comparison between our approach and the bottom-up approach (e.g., [11]) is shown in Table I.

VII. CONCLUSION

In this paper, we addressed the control design problem for nonlinear control systems with temporal logic specifications. We first proposed a novel method for the partition of the state space to verify whether the desired specification can be satisfied in the state space, and then applied abstraction-based techniques to explore the control design based on the specification verification. Finally, we presented a numerical example to demonstrate the proposed control strategy. Future

work will study the application of the proposed approach to complex specifications like spatio-temporal logic.

REFERENCES

- [1] C. Baier and J.-P. Katoen, *Principles of Model Checking*. MIT press, 2008.
- [2] R. Milner, *Communication and Concurrency*. Prentice Hall, 1989.
- [3] P. Tabuada and G. J. Pappas, “Linear time logic control of discrete-time linear systems,” *IEEE Trans. Autom. Control*, vol. 51, no. 12, 2006.
- [4] P. J. Ramadge and W. M. Wonham, “Supervisory control of a class of discrete event processes,” *SIAM J. Control Optim.*, vol. 25, no. 1, pp. 206–230, 1987.
- [5] —, “Modular feedback logic for discrete event systems,” *SIAM J. Control Optim.*, vol. 25, no. 5, pp. 1202–1218, 1987.
- [6] A. Girard, G. Pola, and P. Tabuada, “Approximately bisimilar symbolic models for incrementally stable switched systems,” *IEEE Trans. Autom. Control*, vol. 55, no. 1, pp. 116–126, 2010.
- [7] M. Zamani, G. Pola, M. Mazo, and P. Tabuada, “Symbolic models for nonlinear control systems without stability assumptions,” *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1804–1809, 2012.
- [8] G. Pola, A. Girard, and P. Tabuada, “Approximately bisimilar symbolic models for nonlinear control systems,” *Automatica*, vol. 44, no. 10, pp. 2508–2516, 2008.
- [9] A. Girard, “Controller synthesis for safety and reachability via approximate bisimulation,” *Automatica*, vol. 48, no. 5, pp. 947–953, 2012.
- [10] W. Ren and D. V. Dimarogonas, “Symbolic abstractions for nonlinear control systems via feedback refinement relation,” *Automatica*, vol. 114, p. 108828, 2020.
- [11] G. Reissig, A. Weber, and M. Rungger, “Feedback refinement relations for the synthesis of symbolic controllers,” *IEEE Trans. Autom. Control*, vol. 62, no. 4, pp. 1781–1796, 2017.
- [12] A. Girard and G. J. Pappas, “Approximation metrics for discrete and continuous systems,” *IEEE Trans. Autom. Control*, vol. 5, no. 52, pp. 782–798, 2007.
- [13] W. Ren and D. V. Dimarogonas, “Dynamic quantization based symbolic abstractions for nonlinear control systems,” in *IEEE Conference on Decision and Control*. IEEE, 2019, pp. 4343–4348.
- [14] Y. Li and J. Liu, “Invariance control synthesis for switched nonlinear systems: An interval analysis approach,” *IEEE Trans. Autom. Control*, vol. 63, no. 7, pp. 2206–2211, 2017.
- [15] P.-J. Meyer, A. Girard, and E. Witrant, “Compositional abstraction and safety synthesis using overlapping symbolic models,” *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1835–1841, 2017.
- [16] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach, Fourth Version*, 2020.
- [17] G. E. Fainekos, A. Girard, H. Kress-Gazit, and G. J. Pappas, “Temporal logic motion planning for dynamic robots,” *Automatica*, vol. 45, no. 2, pp. 343–352, 2009.
- [18] J. K. Scott, D. M. Raimondo, G. R. Marseglia, and R. D. Braatz, “Constrained zonotopes: A new tool for set-based estimation and fault detection,” *Automatica*, vol. 69, pp. 126–136, 2016.
- [19] B. S. Rego, G. V. Raffo, J. K. Scott, and D. M. Raimondo, “Guaranteed methods based on constrained zonotopes for set-valued state estimation of nonlinear discrete-time systems,” *Automatica*, vol. 111, 2020.
- [20] N. Kochdumper and M. Althoff, “Representation of polytopes as polynomial zonotopes,” *arXiv preprint arXiv:1910.07271*, 2019.
- [21] K. Hsu, R. Majumdar, K. Mallik, and A.-K. Schmuck, “Multi-layered abstraction-based controller synthesis for continuous-time systems,” in *Proceedings of International Conference on Hybrid Systems: Computation and Control*. ACM, 2018, pp. 120–129.

¹ t_{abs} and t_{con} denote the computation times of the abstraction construction and control synthesis, respectively.

²The classic approach is similar to the one in [11] and the related link is here: <https://github.com/dionysos-dev/Dionysos.jl>.