Synthesis of Maximally Permissive Strategies for $\text{LTL}_f$ Specifications

Shufang Zhu* and Giuseppe De Giacomo
Sapienza University of Rome, Rome, Italy
{zhu,degiacomo}@diag.uniroma1.it

Abstract
In this paper, we study synthesis of maximally permissive strategies for Linear Temporal Logic on finite traces ($\text{LTL}_f$) specifications. That is, instead of computing a single strategy (aka plan, or policy), we aim at computing the entire set of strategies at once and then choosing among them while in execution, without committing to a single one beforehand. Maximally permissive strategies have been introduced and investigated for safety properties, especially in the context of Discrete Event Control Theory. However, the available results for safety properties do not apply to reachability properties (eventually reach a given state of affair) nor to $\text{LTL}_f$ properties in general. In this paper, we show that maximally permissive strategies do exist also for reachability and general $\text{LTL}_f$ properties, and can in fact be computed with minimal overhead wrt the computation of a single strategy using state-of-the-art tools.

1 Introduction
One of the key problems of Artificial Intelligence is to equip intelligent agents with autonomous capability of deliberating the execution of complex courses of action to accomplish desired tasks [Reiter, 2001; Ghallab et al., 2016]. This problem is related to reactive synthesis in Formal Methods: we have an agent acting in an adversarial environment such that the agent controls certain variables (the agent actions) and the environment controls the others (the environment reactions); given a specification of the task, the agent has to find a strategy (plan/policy/controller/program) to choose its actions to fulfill the task in spite of all possible environment reactions [Pnueli and Rosner, 1989]. Specifically, reactive synthesis shares deep similarities with planning in fully observable nondeterministic domains (FOND, strong plans) [Cimatti et al., 2003; Geffner and Bonet, 2013].

In Formal Methods, the most common formalism for specifying tasks is Linear Temporal Logic ($\text{LTL}$) [Pnueli, 1977]. In AI, a finite trace variant of $\text{LTL}$ ($\text{LTL}_f$) is popular [Baier and McIraith, 2006; De Giacomo and Vardi, 2013; De Giacomo and Vardi, 2015; Zhu et al., 2017; De Giacomo and Rubin, 2018; Camacho et al., 2019]. The interest on finite traces is due to the observation that typically intelligent agents are not dedicated to a single task all their life, but are supposed to accomplish one task after another.

Deliberating courses of action (i.e., strategies) is also related to controller synthesis in Discrete Event Systems (DES) [Ehlers et al., 2017]. In DES we are primarily interested in a variant of the problem: suitably control an agent’s behavior to conform to a set of specifications while preserving its autonomy as much as possible. In other words, we want to synthesize a controller that embeds all possible allowed courses of action so that whatever actual course of action the agent chooses, the specifications are satisfied. Such a controller is said to be maximally permissive [Wonham and Ramadge, 1987; Cassandras and LaFortune, 2008; Wonham and Cai, 2019]. Maximally permissive controllers are indeed also of interest in AI, as discussed, e.g., in [De Giacomo et al., 2012; De Giacomo et al., 2013; Banihashemi et al., 2016; Banihashemi et al., 2018; De Giacomo et al., 2020].

In this paper, following this idea, instead of computing a classical (aka, deterministic) strategy for fulfilling a task, we aim at computing the maximally permissive strategy, i.e., the entire set of strategies that fulfill the task. This allows the agent to be able to choose among them while in execution, without committing to any specific one beforehand.

A classical strategy for a task, while already considers all possible environment reactions, prescribes in any circumstances exactly what action to do until the task is fulfilled. This leaves no freedom to the agent in choosing actions that would not harm fulfilling the original task, but would allow the agent to take additional opportunities, such as additional tasks. The maximally permissive strategy, i.e., the entire set of strategies fulfilling a task, instead, gives the maximal freedom of the agent in taking more opportunities, while guaranteeing that the original task is being accomplished.

To capture the notion of maximally permissive strategy, we rely on nondeterministic strategies. A classical (aka, deterministic) strategy is a function from the history so far to the next action the agent should perform. A nondeterministic strategy is a function from the history to a set of next actions such that by arbitrarily choosing among them, at each step, we get a deterministic strategy that accomplishes the task. In other words, a nondeterministic strategy represents a set of

*Corresponding Author
deterministic strategies. The foundational result of DES is that for the kind of specification of interest in DES, which are safety specifications, there exists a unique nondeterministic strategy that is able to represent the maximally permissive strategy, i.e., the entire set of deterministic strategies. Unfortunately, this powerful result applies only to safety properties [Bernet et al., 2002]. In particular, a nondeterministic strategy is that able to represent the entire set of deterministic strategies does not exist for reachability properties, or for LTL \( f \) specifications. Yet, the need for computing the maximally permissive strategies exists, and techniques to approximate it have been studied, e.g., in [Sakakibara and Ushio, 2020].

In this paper, we show that maximally permissive strategies for reachability and general LTL \( f \) properties are still representable via nondeterministic strategies. Specifically, the entire set of deterministic strategies to fulfill an LTL \( f \) task can be characterized by two (vs. one) nondeterministic strategies and a constraint that requires to eventually switch from the first one to the second one. Interestingly, these two nondeterministic strategies can be computed with minimal overhead w.r.t the computation of a single deterministic strategy using state-of-the-art tools.

2 Preliminaries

LTL \( f \) Basics. Linear-time Temporal Logic on finite traces (LTL \( f \)) is a specification language to express temporal properties on finite traces [De Giacomo and Vardi, 2013]. In particular, LTL \( f \) has the same syntax as LTL, which is instead interpreted over infinite traces [Pnueli, 1977]. Given a set of propositions \( \text{Prop} \), LTL \( f \) formulas are defined as follows:

\[
\varphi ::= a | (\varphi \land \varphi) | (!\varphi) | (\forall i \varphi) | (\varphi \land \varphi) | (\varphi \land \varphi)
\]

where \( a \in \text{Prop} \) is an atom, \( \varphi \) for Next, and \( \forall i \) for Until are temporal operators. We make use of standard Boolean abbreviations such as \( \lor \) (or) and \( \to \) (implies), \( \text{true} \) and \( \text{false} \). In addition, we define the following abbreviations Weak Next \( \varphi \equiv \neg \varphi \land \text{true} \), Eventually \( \varphi \equiv \varphi \land \text{true} \), and Always \( \varphi \equiv \varphi \land \text{false} \). We denote by \( R \) for Release.

A trace \( \pi = s_0 s_1 \ldots \) is a sequence of proposition interpretations (sets), where for every \( i \geq 0 \), \( \pi_i \in \text{Prop} \) is the \( i \)-th interpretation of \( \pi \). Intuitively, \( \pi_i \) is interpreted as the set of propositions that are \( \text{true} \) at instant \( i \). We denote the last instant (i.e., index) in a trace \( \pi \) by \( \text{lst}(\pi) \). A trace \( \pi \) is an infinite trace if \( \text{lst}(\pi) = \infty \), which is formally denoted as \( \pi \in (2^{\text{Prop}})\infty \): otherwise \( \pi \) is a finite trace, denoted as \( \pi \in (2^{\text{Prop}})^* \). Moreover, by \( \pi^k = \pi_0 \ldots \pi_k \) we denote the prefix of \( \pi \) up to the \( k \)-th iteration, and \( \pi^k = \epsilon \) denotes an empty trace if \( k < 0 \). LTL \( f \) formulas are interpreted over finite, nonempty traces. Given \( \pi \), we define when an LTL \( f \) formula \( \varphi \) holds at instant \( i \), \( 0 \leq i \leq \text{lst}(\pi) \), written as \( \pi, i \models \varphi \), inductively on the structure of \( \varphi \), as:

- \( \pi, i \models a \) iff \( a \in \pi_i \) (for \( a \in \text{Prop} \));
- \( \pi, i \not\models \neg \varphi \) iff \( \pi, i \models \varphi \);
- \( \pi, i \models \varphi_1 \land \varphi_2 \) iff \( \pi, i \models \varphi_1 \) and \( \pi, i \models \varphi_2 \);
- \( \pi, i \models \varphi \) iff \( i < \text{lst}(\pi) \) and \( \pi, i+1 \models \varphi \);
- \( \pi, i \models \varphi_1 \land \varphi_2 \) iff \( \exists j \) such that \( i \leq j \leq \text{lst}(\pi) \) and \( \pi, j \models \varphi_2 \), and \( \forall k, i \leq k < j \) we have that \( \pi, k \models \varphi_1 \).

We say \( \pi \) satisfies \( \varphi \), written as \( \pi \models \varphi \), if \( \pi, 0 \models \varphi \).

Reactive Synthesis. The problem of reactive synthesis can be viewed as a game of the environment and the agent. The goal of reactive synthesis is to synthesize an agent strategy such that no matter how the environment behaves, the combined behavior trace of both players satisfy desired properties [Pnueli and Rosner, 1989]. Formally, a reactive synthesis problem is described as a tuple \( \mathcal{P} = (X, Y, \varphi) \), where \( X \) and \( Y \) are disjoint sets of variables controlled by the environment and the agent, respectively, and \( \varphi \) is a logical specification formula over \( X \cup Y \) expressing desired properties. A deterministic agent strategy is a function \( \sigma_{ag}: (2^{X \cup Y})^* \times 2^X \to 2^Y \). A play is a sequence \( \pi = (X_0 \cup Y_0)(X_1 \cup Y_1) \ldots \in (2^{X \cup Y})^\omega \) over the alphabet \( 2^{X \cup Y} \). A play \( \pi \) is compatible with an agent strategy \( \sigma_{ag} \) if \( \sigma_{ag}(\pi^{i-1}, X_i) = Y_i \) for every \( i \geq 0 \). Analogously, finite prefix \( \pi^k \) is compatible with \( \sigma_{ag} \) if \( \sigma_{ag}(\pi^{i-1}, X_i) = Y_i \) for every \( 0 \leq i \leq k \). Given a synthesis problem \( \mathcal{P} = (X, Y, \varphi) \), an agent strategy \( \sigma_{ag} \) realizes \( \varphi \) with respect to the corresponding \( X \) and \( Y \), if every play \( \pi \) that is compatible with \( \sigma_{ag} \) satisfies \( \varphi \).

Definition 1 (LTL \( f \) synthesis). The problem of LTL \( f \) synthesis is described as a tuple \( \mathcal{P} = (X, Y, \varphi) \), where \( \varphi \) is an LTL \( f \) formula over \( X \cup Y \). Computing an agent strategy that realizes \( \varphi \) if one exists, is called the LTL \( f \) synthesis problem.

Solving LTL \( f \) synthesis is known to be 2EXPSPACE-complete [De Giacomo and Vardi, 2015].

Two-player Games. Classical solutions to LTL \( f \) synthesis relies on a reduction to two-player games. A two-player game is described as a tuple \( G = (A, W) \), where \( A \) is the game arena and \( W \) is the winning objective. For synthesis, we often take the corresponding deterministic automaton of the formula as the game arena, which is a tuple \( A = (2^{X \cup Y}, S, s_0, \delta) \), where \( \delta: S \times 2^{X \cup Y} \to S \) is the transition function. Given a play \( \pi = (X_0 \cup Y_0)(X_1 \cup Y_1) \ldots \in (2^{X \cup Y})^\omega \), running \( \pi \) on \( A \) gives us an infinite sequence \( s_0 = s_{i_1} \ldots s_{i_\omega} \) such that \( s_0 \) is the initial state and \( s_{i_{k+1}} = \delta(s_i, X_i \cup Y_i) \) for all \( i \geq 0 \). Since the transitions in \( A \) are all deterministic, we thus denote by \( \rho = \text{Run}(\pi, A) \) the unique sequence of running \( \pi \) on \( A \). Analogously, we denote by \( \rho^k = \text{Run}(\pi^k, A) \) the unique finite sequence of running \( \pi^k \) on \( A \), and \( \rho^k = \text{Run}(\pi^k, A) \). The winning objective \( W \) indicates a set of desired plays for the agent. A play \( \pi \) is a winning play with respect to winning objective \( W \) if \( \pi \in W \). In this paper, we only consider two-player games with Reachability objectives (Reachability games). More specifically, the winning objective \( W = \text{Reach}(F) \), and \( \text{Reach}(F) = \{ \pi \in (2^{X \cup Y})^\omega \mid \rho = \text{Run}(\pi, A) \land \exists \ell \geq 0: \rho\ell \in F \} \), where \( F \subseteq S \) is a set of goal states. Intuitively, reachability games require that a goal state in \( F \) is visited at least once.

An agent strategy \( \sigma_{ag} \) is winning in \( G = (A, \text{Reach}(F)) \) if every play \( \pi \) that is compatible with \( \sigma_{ag} \) is winning, i.e., \( \pi \in W \). In Reachability games, \( s \in S \) is a winning state for the agent (resp. environment) if the agent (resp. the environment) has a winning strategy in the game \( G = (A', \text{Reach}(F)) \), where \( A' = (2^{X \cup Y}, S, s, \delta) \), i.e., the same arena \( A \) but with the new initial state \( s \). By \( W_{ag}(G) \) (resp. \( W_{env}(G) \)) we denote the set of all agent (resp. environment) winning states.
Intuitively, $W_{ag}$ represents the “agent winning region”, from which the agent is able to win the game, no matter how the environment behaves.

**Symbolic LTL$_f$ Synthesis.** State-of-the-art LTL$_f$ synthesis tools [Bansal et al., 2020; De Giacomo and Favorito, 2021] leverage the symbolic synthesis framework presented in [Zhu et al., 2017; Tabajara and Vardi, 2019], which solves the synthesis problem via a symbolic reachability game computation. The game arena $A = (2^{X∪Y}, S, s_0, δ)$ is compactly represented symbolically, by encoding the state space using a logarithmic number of propositions. The symbolic representation of $A$ is a tuple $A_s = (X, Y, Z, I, η)$, where $Z$ is a set of variables such that $|Z| = ⌈\log |S|⌉$, and every state $s ∈ S$ corresponds to an interpretation $Z ∈ 2^Z$ over $Z$. $I$ is a Boolean formula satisfied only by the interpretation of the initial state $s_0$. Every induced strategy corresponds to an interpretation $Z ∈ 2^Z$ over $Z$. A Boolean formula mapping interpretations $X, Y$ and $Z$ of the propositions $X, Y$ and $Z$ to a new interpretation $Z'$ of the propositions of $Z$, such that if $Z$ corresponds to a state $s ∈ S$ then $Z'$ corresponds to the state $δ(s, X ∪ Y)$. The set of goal states is represented by a Boolean formula $g$ over $Z$ that is only satisfied by the interpretations of states in $F$. Accordingly, we denote the symbolic reachability game as $G_s = (A_s, Reach(g))$.

The game is solved by performing a least fixpoint computation over two Boolean formulas $w$ over $Z$ and $t$ over $Z ∪ X ∪ Y$, which represent the agent winning region $W_{ag}$ and tangles of winning states, environment actions with suitable agent actions, respectively. $w$ and $t$ are initialized as $w_0(Z) = g(Z)$ and $t_0(Z, X, Y) = g(Z)$, since every goal state is an agent winning state. Note that $t_0$ only depends on the propositions from $X ∪ Y$, since once the play reaches goal states, the agent can do whatever it wants. $t_{i+1}$ and $w_{i+1}$ are constructed as follows:

$$w_{i+1}(Z) = w_i(Z) ∨ ∀X∃Y.w_i(η(Z, X, Y))$$

$$t_{i+1}(Z, X, Y) = t_i(Z, X, Y) ∨ (∼w_i(Z)$$

$$\land w_{i+1}(Z) ∧ w_i(η(Z, X, Y)))$$

The computation reaches a fixpoint when $w_{i+1} ≡ w_i$. At this point, no more states will be added, and so all agent winning states have been collected. By evaluating $w_{i+1}$ on $I$ we can know if there exists a winning strategy. If that is the case, $t_{i+1}$ can be used to compute a winning strategy through the mechanism of Boolean synthesis [Fried et al., 2016].

**Non-deterministic Strategies.** An agent strategy can also be non-deterministic, which prescribes for each history $π^k ∈ (2^{X∪Y})^*$, and an environment action $X ∈ 2^X$, a set of agent actions to choose from nondeterministically. Formally, a non-deterministic agent strategy is a function $π_{ag} : (2^{X∪Y})^* × 2^X → 2^Y$. We denote the set of deterministic strategies induced by a non-deterministic strategy $π_{ag}$ as the set $[π_{ag}]$. Every deterministic strategy $σ_{ag} ∈ [π_{ag}]$ is obtained by a corresponding choice function $c : (2^{X∪Y})^* × 2^X → 2^Y$ such that for every $π^k ∈ (2^{X∪Y})^*$ that is compatible with $c$ and $X ∈ 2^X, c(π^k, X) ∈ π_{ag}(π^k, X)$ and $σ_{ag}(π^k, X) = c(π^k, X)$. Non-deterministic strategy $π_{ag}$ realizes $φ$ if every induced strategy $σ_{ag} ∈ [π_{ag}]$ realizes $φ$. Sometimes, for simplicity, we say $σ_{ag}$ (resp. $π_{ag}$) is a winning strategy of $φ$, instead of $σ_{ag}$ (resp. $π_{ag}$) realizes $φ$. A trace $π$ (finite or infinite) is compatible with a non-deterministic strategy $π_{ag}$ if $Y_i ∈ π_{ag}(π^{i−1}, X_i)$ for every $i ≥ 0$.

**Comparing Strategies.** Let $P = (X, Y, φ)$ be a synthesis problem, and $π_{ag}$ a winning strategy of $φ$. We consider the permissiveness of $π_{ag}$ with respect to the deterministic strategies that it induces.

**Definition 2.** Let $P = (X, Y, φ)$ be a synthesis problem, $π_{ag}$ and $π_{ag'}$ two winning strategies of $φ$. $π_{ag}$ is more permissive than $π_{ag'}$ if $[π_{ag'}] ⊆ [π_{ag}]$.

### 3 Maximally Permissive Strategy

We first introduce the notion of maximally permissive strategy for a task, denoted by MaxSet, which consists of the entire set of deterministic winning strategies for the task, from which to choose one during the execution. Then we show that for special cases, we can compute a single non-deterministic strategy to capture MaxSet. However, in general, this does not happen for LTL$_f$ specifications.

**Definition 3 (Maximally Permissive Strategy).** Let $P = (X, Y, φ)$ be a synthesis problem, the maximally permissive strategy of $φ$ is MaxSet($φ$) = $σ_{ag} | π_{ag}$ is a deterministic winning strategy of $φ$.

**Theorem 1.** Let $P = (X, Y, φ)$ be a synthesis problem. If there exists a nondeterministic winning strategy $π_{ag}$ that is more permissive than every other winning strategy, then $[π_{ag}] = \text{MaxSet}(φ)$.\(^1\)

**Proof.** Suppose there exists a non-deterministic winning strategy $π_{ag}$ that is more permissive than every other winning strategy $π_{ag'}$, such that $[π_{ag'}] ⊆ [π_{ag}]$. Note that every deterministic strategy $σ_{ag}$ can be considered as a special case of a non-deterministic strategy, in which case, $[σ_{ag}] = \{σ_{ag}\}$. Therefore, it holds that $σ_{ag} ∈ [π_{ag}]$ for every deterministic winning strategy of $φ$, and so $[π_{ag}] = \text{MaxSet}(φ)$. \(\square\)

Although it is practical to utilize a single non-deterministic strategy $π_{ag}$ to express the maximally permissive strategy $\text{MaxSet}(φ)$, this only applies to the cases where $φ$ specifies a safety property, meaning that every violating trace has a finite bad prefix that falsifies the specification $φ$. This is because the problem of synthesizing safety properties can be reduced to a safety game, which always has a non-deterministic winning strategy $π_{ag}$ that is more permissive than every other winning strategy [Bernet et al., 2002]. However, this result does not apply to properties that are not safety [Bernet et al., 2002]. In particular, we give here a direct proof for LTL$_f$ specifications.

**Theorem 2.** In general, LTL$_f$ specifications do not admit a non-deterministic winning strategy $π_{ag}$ that is more permissive than every other deterministic strategy.

**Proof.** We prove by showing that such a strategy does not even exist for a simple LTL$_f$ specification $φ = ◊b$. In particular, we have $b ∈ Y$ s.t. $b$ is under the control of the agent. It is trivial to see that no matter how the environment behaves on $X$, the satisfaction of $◊b$ only relies on the agent. Suppose $π_{ag}$ is a non-deterministic winning strategy of $◊b$ that is

\(^1\)It should be noted that the definition of maximally permissive strategy and Theorem 1 also applies to LTL synthesis.
more permissive than every other one. For every deterministic strategy \( \sigma_{ag} \in [\Pi_{ag}] \), its corresponding choice function \( c_h : \{2^k\}^* \rightarrow \{2^k\} \) satisfies that \( \exists k \geq 0 \) such that \( c_h \) emits \( b \) at time step \( k \) (where \( \mathcal{X} \) can be ignored here), and \( c_h \) keeps emitting \( \neg b \) for \( 0 \leq i < k \). Otherwise, \( \sigma_{ag} \) is indeed not a winning strategy. Therefore, we can label every choice function with its corresponding \( k \)-value. Now we take the choice function \( c_m \) that has the greatest \( k \)-value, comparing to other choice functions of \( \Pi_{ag} \). Then we can construct another choice function \( c' \) that keeps copying \( c_m \) but postponing the moment of outputting \( b \) for one timestep.

Indeed, \( c' \) leads to a deterministic winning strategy \( \sigma'_{ag} \), since \( \sigma'_{ag} \) outputs \( b \) at timestep \( m + 1 \) and thus the compatible play \( \pi \) (a unique sequence, where \( \mathcal{X} \) can be ignored in this example) is such that \( \pi^{n+1} = \emptyset b \) holds. Therefore, \( \sigma'_{ag} \in \text{MaxSet}(\emptyset b) \), but \( \sigma'_{ag} \notin [\Pi_{ag}] \) leading to a contradiction. Thus, in general, \( \text{LTL}_f \) specifications do not admit a nondeterministic winning strategy \( \Pi_{ag} \) that is more permissive than every other strategy.

\[ \square \]

4 \textbf{MaxSet of \textit{LTL\textsubscript{f}} Synthesis}

We now explain how to compute \( \text{MaxSet}(\varphi) \) of \( \text{LTL}_f \) synthesis problem \( P = (\mathcal{X}, \mathcal{Y}, \varphi) \), by reasoning on its corresponding reachability game. Recall that a winning strategy for safety games can be interpreted as a “staying in the winning region” strategy, since as long as the game stays in the winning region, the agent is able to force the game to move to another state that still belongs to the winning region [Bernet et al., 2002]. Nevertheless, for reachability games, such strategies do not necessarily lead to winning. This is because such a strategy can possibly generate a play that only stays in the winning region but never visits the goal states, which is indeed not a winning play. Therefore, apart from “staying in the winning region” such that the agent has the ability to win, no matter how the strategy keeps “deferring” the winning moment, a winning strategy also needs to start “non-deferring” such that eventually reaching goal states.

Here, we show how to capture the entire set of winning strategies of reachability games with two nondeterministic strategies. Intuitively, the first nondeterministic strategy keeps the agent in the winning region, where the agent is always able to win the game, which is called \textit{deferring} strategy. The second nondeterministic strategy aims to taking the agent to goal states without any hesitation such that aggressively winning the game, which is called \textit{non-deferring} strategy. Both strategies are defined with respect to the agent winning region, therefore, we assume that the agent winning region \( W_{ag} = \bigcup_{0 \leq i \leq n} W_i \) is computed apriori via a least fixpoint computation and \( s_0 \in W_{ag} \) such that there is at least one agent winning strategy of the reachability game [De Giacomo and Vardi, 2015].

4.1 \textbf{Deferring Strategy}

For reachability games \( G = (A, \text{Reach}(F)) \), a \textit{deferring} strategy should keep the play in the agent winning region \( W_{ag} \), if the reachability goal \( F \) is not visited yet, and so the agent is able to keep deferring the winning moment.

Definition 4 (Deferring strategy of reachability games). Let \( G = (A, \text{Reach}(F)) \) be a reachability game and \( W_{ag} \) be the set of agent winning states. \( \sigma_{ag} \) is a deferring strategy, if for every play that is compatible with \( \sigma_{ag} \), \( \rho = \text{Run}(\pi, A) \) such that \( \rho = s_0 s_1 \ldots \) satisfies \( s_0 \in W_{ag} \) and \( \forall \ell \geq 0, \exists i \leq \ell \text{ and } d(s_i) = d(s_j) - 1 \).

Lemma 1. Let \( G = (A, \text{Reach}(F)) \) be a reachability game, and \( W_{ag} \) be the agent winning region. Then \( s_0 \in W_{ag} \) iff there exists a deferring strategy.

In order to obtain a deferring strategy, we define a strategy generator based on the winning region \( W_{ag} \), represented as a nondeterministic transducer, where nondeterminism is of the kind “don’t-care”: all nondeterministic choices are equally good. The strategy generator \( T_{df}((X, s_0, \emptyset, \emptyset)) \) is constructed as follows:

- \( 2^{X \cup Y} \), \( s \) and \( s_0 \) are the same as in \( A \);
- \( \theta_{df} : S \times 2^X \rightarrow 2^Y \) is the transition function such that \( \theta_{df}(s, X) = \{ s' \mid s' = \delta(s, s_0 \cup Y) \} \) and \( s = \sigma_{ag} \leq 0 \).
- \( \tau_{df} : S \times 2^X \rightarrow 2^Y \) is the output function such that

\[
\forall X \in 2^X, \tau_{df}(s, X) = \{ Y \mid \delta(s, X \cup Y) \} \in W_{ag} \}
\]

This transducer represents a nondeterministic deferring strategy \( \Pi_{ag}((X, s, s_0, \emptyset)) \) in the following way, \( \forall \pi^k \in (2^{X \cup Y})^* \) that is compatible with \( \Pi_{ag} \), \( \delta(X, 0) \) and \( \forall \pi^k \in (2^{X \cup Y})^* \) that is compatible with \( \Pi_{ag} \) and \( \forall \pi^k \in (2^{X \cup Y})^* \) that is compatible with \( \Pi_{ag} \) and \( \delta(X, 0) \) and:

- \( \Pi_{ag}(\pi^k, X) \in \{ Y \in 2^Y \text{ if } \rho^k \text{ visits } F \}
- \tau_{df}(s_{k+1}, X) \text{ otherwise.}
\]

where \( \rho^k \text{ is } \text{Run}(\pi^k, A) \) such that \( \rho^k = s_0 s_1 \ldots s_{k+1} \).

Every deterministic deferring strategy \( \sigma_{ag} \) is generated from \( \Pi_{ag}((X, s_0, \emptyset, \emptyset)) \) by a corresponding choice function \( c_{df} : (2^{X \cup Y})^* \rightarrow 2^k \) such that \( \forall \pi^k \in (2^{X \cup Y})^* \) that is compatible with \( \Pi_{ag} \) and \( \forall X \in 2^X, \chi_{df}(\pi^k, X) \in \Pi_{ag}(\pi^k, X) \) and \( \delta(X, 0) \) and:

Theorem 3. Let \( G = (A, \text{Reach}(F)) \) be a reachability game, and \( W_{ag} \) be computed as above. Then deterministic strategy \( \sigma_{ag} \) is a deferring strategy iff \( \sigma_{ag} \in [\Pi_{ag}] \).

4.2 \textbf{Non-Deferring Strategy}

Different from a deferring strategy that keeps deferring the winning moment, a non-deferring strategy brings the play closer to goal states \( F \) at every timestep until reaching it. In order to represent the distance towards \( F \), for every state \( s \in W_{ag} \), where \( W_{ag} = \bigcup_{0 \leq i \leq n} W_i \) computed by a least fixpoint computation, we introduce a distance value \( d(s) \) that indicates the shortest distance from \( s \) to \( F \). Therefore, \( \forall s \in W_{ag} \) if \( s \in F \) (i.e., \( s \in W_0 \)) then \( d(s) = 0 \); otherwise, since \( s \in W_i \) for some \( 0 \leq i \leq n \), we have \( d(s) = i + 1 \). We now introduce non-deferring strategy.

Definition 5 (Non-deferring strategy of reachability games). Let \( G = (A, \text{Reach}(F)) \) be a reachability game and \( W_{ag} \) be the agent winning region. \( \sigma_{ag} \) is a non-deferring strategy, if for every play \( \pi \) that is compatible with \( \sigma_{ag} \), \( \rho = \text{Run}(A, F) \) such that \( \rho = s_0 s_1 \ldots \) satisfies \( s_0 \in W_{ag} \) and \( \forall \ell \geq 0, d(s_\ell) = a, j \leq \ell \text{ and } d(s_{\ell+1}) = d(s_{\ell}) - 1 \).
Lemma 2. Let $\mathcal{G} = (A, \text{Reach}(F))$ be a reachability game, and $W_{ag}$ be the agent winning region. Then $s_0 \in W_{ag}$ iff there exists a non-deferring strategy.

In order to obtain a non-deferring strategy, we also define a strategy generator based on the winning region $W_{ag} = \bigcup_{0 \leq i \leq n} W_i$, represented as a nondeterministic transducer $\tau_{\text{ndf}}, (2^{X \cup Y}, S, 0, \delta, \tau_{\text{ndf}})$, where:

- $2^{X \cup Y}$, $S$, and $0$ are the same as in $A$;
- $\delta_{\text{ndf}}(s, X) = \{s'|s' = \delta(s, X \cup Y) \text{ and } Y \in \tau_{\text{ndf}}(s)\}$;
- $\tau_{\text{ndf}}$, $S \times 2^X \to 2^S$ is the output function such that $\forall X \in 2^X, \tau_{\text{ndf}}(s, X) = \{Y|\delta(s, X \cup Y) \in W_i \}$ if $s \in W_{i+1} \setminus W_i$, otherwise $\tau_{\text{ndf}}(s, X) = 2^S$.

This transducer represents a nondeterministic non-deferring strategy $\Pi_{\text{ndf}}^\prime: (2^{X \cup Y})^* \times 2^X \to 2^{\mathbb{N}}$ in the following way: $\forall \pi^k \in (2^{X \cup Y})^*$ that is compatible with $\Pi_{\text{ndf}}^\prime$, and $\forall X \in 2^X$:

$$\Pi_{\text{ndf}}^\prime(\pi^k, X) = \begin{cases} Y \in 2^Y & \text{if } \rho^k \text{ visits } F, \\ \tau_{\text{ndf}}(s_{k+1}, X) & \text{otherwise.} \end{cases}$$

where $\rho^k = \text{Run}(\pi^k, A)$ such that $\rho^k = s_0s_1 \ldots s_{k+1}$. Every deterministic strategy $\sigma_{\text{ag}}$ is generated from $\Pi_{\text{ndf}}^\prime$ by a corresponding choice function $\text{ch}_{\text{ndf}}: (2^{X \cup Y})^* \times 2^X \to 2^Y$ such that $\forall \pi^k \in (2^{X \cup Y})^*$ that is compatible with $\Pi_{\text{ndf}}^\prime$, and $\forall X \in 2^X$, $\text{ch}_{\text{ndf}}(\pi^k, X) \in \Pi_{\text{ag}}(\pi^k, X)$ and $\sigma_{\text{ag}}(\pi^k, X) = \text{ch}_{\text{ndf}}(\pi^k, X)$.

Theorem 4. Let $\mathcal{G} = (A, \text{Reach}(F))$ be a reachability game, and $\Pi_{\text{ag}}$ be computed as above. Then deterministic strategy $\sigma_{\text{ag}}$ is a non-deferring strategy iff $\sigma_{\text{ag}} \in [[\Pi_{\text{ndf}}^\prime]]$.

Theorem 5. Let $\mathcal{G} = (A, \text{Reach}(F))$ be a reachability game, $\Pi_{\text{ag}}$ and $\Pi_{\text{ndf}}^\prime$ be computed as above, respectively. Then $[[\Pi_{\text{ndf}}^\prime]] \subseteq [[\Pi_{\text{ag}}]]$.

4.3 Maximally Permissive Strategy

We now explain how to obtain the maximally permissive strategy $\text{MaxSet}$ through nondeterministic strategies $\Pi_{\text{ag}}$ and $\Pi_{\text{ndf}}^\prime$. To do so, we start with showing how to induce deterministic strategies out of $\Pi_{\text{ag}}$ and $\Pi_{\text{ndf}}^\prime$. Every deterministic strategy $\sigma_{\text{ag}}$ is generated from nondeterministic strategies $\Pi_{\text{ag}}$ and $\Pi_{\text{ndf}}^\prime$ by a corresponding choice function $\text{ch}: (2^{X \cup Y})^* \times 2^X \to 2^Y$. Intuitively speaking, apart from restricting $\sigma_{\text{ag}}$ to be a deferring strategy such that being able to postpone the winning moment, $\text{ch}$ also restricts $\sigma_{\text{ag}}$ to change to a non-deferring strategy such that eventually reaching the goal states. Formally, we require $\text{ch}$ satisfying both of the following conditions:

1. for every $\pi^k \in (2^{X \cup Y})^*$ compatible with $\text{ch}$, and $\forall X \in 2^X$, $\text{ch}(\pi^k, X) \in \Pi_{\text{ag}}(\pi^k, X)$;
2. for every $\pi \in (2^{X \cup Y})^*$ compatible with $\text{ch}$, $\exists j \geq 0$ such that $\forall h \geq j$, $\text{ch}(\pi^{h-1}, X_h) \in \Pi_{\text{ag}}(\pi^{h-1}, X_h)$.

Every choice function $\text{ch}: (2^{X \cup Y})^* \times 2^X \to 2^Y$ that satisfies the above characteristic is able to induce a deterministic strategy out of nondeterministic strategies $\Pi_{\text{ag}}$ and $\Pi_{\text{ndf}}^\prime$. Note that choice functions are a general mathematical means to extract deterministic strategies from nondeterministic ones. Their role here is to prove soundness (every choice function with the above characteristic will create a deterministic winning strategy) and completeness (every deterministic winning strategy can be captured by one such choice function). We denote the set of all induced deterministic strategies by $[[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]]$. The following theorem shows that $[[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]]$ can capture the maximally permissive strategy.

Theorem 6. Let $\mathcal{P} = (X, Y, \phi)$ be an $\text{LTL}_f$ synthesis problem, and $\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime$ be computed as above. Then $[[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]] = \text{MaxSet}(\phi)$.

Proof. We prove $[[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]] = \text{MaxSet}(\phi)$ by showing that $\sigma_{\text{ag}} \in [[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]]$ iff $\sigma_{\text{ag}} \in \text{MaxSet}(\phi)$.

(\Rightarrow) We need to prove that every deterministic winning strategy $\sigma_{\text{ag}} \in [[\Pi_{\text{ag}}^\prime, \Pi_{\text{ndf}}^\prime]]$ is a winning strategy, such that $\sigma_{\text{ag}} \in \text{MaxSet}(\phi)$. Indeed, $\sigma_{\text{ag}}$ is generated by a corresponding choice function $\text{ch}: (2^{X \cup Y})^* \times 2^X \to 2^Y$ that follows our defined conditions. That is to say, $\forall \pi^k \in (2^{X \cup Y})^*$ that is compatible with $\sigma_{\text{ag}}$, and $\forall X \in 2^X$, $\sigma_{\text{ag}}(\pi^k, X) \in \Pi_{\text{ag}}(\pi^k, X)$. Moreover, $\forall \pi \in (2^{X \cup Y})^*$ that is compatible with $\sigma_{\text{ag}}$, $\exists j \geq 0$ such that $\forall h \geq j$, $\sigma_{\text{ag}}(\pi^{h-1}, X_h) \in \Pi_{\text{ag}}(\pi^{h-1}, X_h)$. Thus, for every play $\pi$ that is compatible with $\sigma_{\text{ag}}$, $\rho = \text{Run}(\pi, A)$ such that $\rho = s_0s_1 \ldots$ satisfies that $s_0 \in W_{ag}$ and $\forall \ell \geq 0$, if $s_{\ell+1} \notin W_{ag}$, then $\rho^\ell = s_0s_1 \ldots s_{\ell+1}$ definitively has visited $F$ already such that $\phi$ is satisfied already. This is because $\Pi_{\text{ag}}^\prime$ restricts $\pi$ to stay in $W_{ag}$ before reaching $F$. Otherwise, from $\ell = j$, $\sigma_{\text{ag}}$ switches to $\Pi_{\text{ndf}}$, which restricts $\rho$ to eventually reach $F$ such that $\phi$ is satisfied. Hence, $\sigma_{\text{ag}}$ is a winning strategy and so $\sigma_{\text{ag}} \in \text{MaxSet}(\phi)$.

5 Implementation and Empirical Evaluation

In this section, we first describe how to leverage synthesis framework being integrated in state-of-the-art $\text{LTL}_f$ synthesis
to compute the maximally permissive strategy. Then, by empirical evaluation, we show computing the maximally permissive strategy only brings a minimal overhead with respect to the computation of a single winning strategy.

5.1 Symbolic MaxSet Computation

Recall that the symbolic LTL$_f$ synthesis framework presented in [Zhu et al., 2017; Tabajara and Vardi, 2019] consists of computing two Boolean formulas $w$ and $t$, which represent the agent winning region $W_{ag}$ and tuples of winning states, environment actions with suitable agent actions, respectively. We observe that Boolean formula $t$ over $Z \cup X \cup Y$, in fact, is compatible with the non-deferring strategy generator $T_{ndf} = (2^{X \cup Y}, S, s_0, g_{ndf}, \tau_{ndf})$ introduced in Section 4.2. More specifically, $t$ is satisfied by interpretation $(Z \cup X \cup Y) \in 2^X \times 2^Y \times 2^Y$ if $Y \in \tau_{ndf}(s, X)$, where $s$ is the corresponding state of $Z$. This is because, during the fixpoint computation, an interpretation $(Z \cup X \cup Y) \in 2^X \times 2^Y \times 2^Y$ satisfies $t_{i+1}$ if: either $(Z \cup X \cup Y)$ satisfies $t_i$; or $Z$ was identified as a new winning state $(Z \models w_i \cup \neg w_i)$, and so for every environment action $X \in 2^X$ we can move from $Z$ to $w_i$ by setting agent action to some $Y \in 2^Y$ as long as following the transition function, expressed by $w_i(y(Z, X, Y))$. Note that the second case restricts the agent to be non-deferring such that the next transition will move closer to goal states. For nondeterministic deferring strategy $T_{df}$, we compute a boolean formula $t_{df}$ over $Z \cup X \cup Y$ as follows:

$$t_{df}(Z, X, Y) = t(Z, X, Y) \lor (w_{i+1}(Z) \land w_{i+1}(y(Z, X, Y))).$$

Note that $(Z \cup X \cup Y) \in 2^X \times 2^X \times 2^X$ satisfies $t_{df}$ if: either $(Z \cup X \cup Y)$ satisfies $t$; since every non-deferring strategy is a deferring strategy; or the agent can move back to the winning region $w_{i+1}(Z)$ with another $Y \in 2^Y$ as long as following the transition function, expressed by $w_{i+1}(y(Z, X, Y))$. In this case, $t_{df}$ is satisfied by interpretation $(Z \cup X \cup Y) \in 2^X \times 2^X \times 2^X$ iff they are compatible with the deferring strategy generator $T_{df} = (2^{X \cup Y}, S, s_0, g_{df}, \tau_{df})$ such that $Y \in \tau_{df}(s, X)$, where $s$ is the corresponding state of $Z$.

5.2 Empirical Evaluation

Implementation. We implemented the symbolic maximally permissive strategy computation technique for LTL$_f$ synthesis by extending the symbolic synthesis framework [Zhu et al., 2017; Tabajara and Vardi, 2019] integrated in state-of-the-art synthesis tools [Bansal et al., 2020; De Giacomo and Favorito, 2021]. In particular, we based on LTL$_f$ synthesis tool LYDIA 2, the overall best performing tool, and implemented our fixpoint-based computation presented in Section 5.1. More specifically, the computation consists of two steps. In the first step, we based on the code of LYDIA, to perform realizability checking, and the nondeterministic non-deferring strategy is also obtained as a side-effect, represented in Binary Decision Diagrams (BDDs). The second step makes use of Boolean operations provided by BDD library CUDD-3.0.0 [Somkenzi, 2016] to compute the nondeterministic deferring strategy.

3https://github.com/whitemech/lydia
4Source code at https://github.com/Shufang-Zhu/SyfMax

Experiment Setup. All tests were ran on a computer cluster. Each test took exclusive access to a node with Intel(R) Xeon(R) CPU E5-2650 v2 processors running at 2.60GHz. Time out was set to 300 seconds.

Benchmarks. We took the LTL$_f$ synthesis benchmarks from literature [Tabajara and Vardi, 2019; Bansal et al., 2020; De Giacomo and Favorito, 2021]. The goal of this experiment is to understand if maximally permissive strategies can be solved within the time limit, which are 391 in total.

Evaluation Results. We evaluated the overhead caused by maximally permissive strategy computation by comparing the time cost of computing a single strategy, which is represented by the time taken from receiving a synthesis instance to finishing realizability checking, by then Boolean formula $t_i$, i.e., the nondeterministic non-deferring strategy, is also obtained. The Boolean synthesis time for "choosing" a deterministic strategy out of $t$ is omitted, for a fair comparison, since the same procedure would also be required by "choosing" a deterministic strategy out of the maximally permissive strategy. Figure 1 displays a scatter plot (in log scale) comparing the time cost of two computations for each realizable instance. The gray line represents the points where the x-axis value is equal to the y-axis value. As shown in Figure 1, the points are closely above the gray line, this demonstrates that computing the maximally permissive strategy only brings minor overhead comparing to computing a single strategy.

6 Conclusions

Maximally permissive strategies are of interest when we want to allow for maximal freedom to the agent while still achieving the desired task. We have shown that we can naturally characterize maximally permissive strategies for LTL$_f$ specifications with two nondeterministic strategies and a constraint requiring to eventually switch from one to the other. Moreover, such a pair can be computed with minimal overhead. Given this nice computational result, it would be interesting to understand if maximally permissive strategies can be used to benefit LTL$_f$ synthesis itself. Indeed, state-of-the-art LTL$_f$ synthesis tools integrate techniques to compose specifications. Instead, one could compose the maximally permissive strategy of each specification piece, leading to an even smaller state space, and thus bring promising computational benefits. We leave this for future work.
Acknowledgments

This work is partially supported by the ERC Advanced Grant WhiteMech (No. 834228), the EU ICT-48 2020 project TAILOR (No. 952215), the PRIN project RIPER (No. 20203FFYLK), the JPMorgan AI Faculty Research Award “Resilience-based Generalized Planning and Strategic Reasoning”

References


[Cimatti et al., 2003] Alessandro Cimatti, Marco Pistore, Marco Roveri, and Paolo Traverso. Weak, strong, and strong cyclic planning via symbolic model checking. 1–2(147), 2003.


