Symbolic Approaches to LTL_f Best-Effort Synthesis

Giuseppe De Giacomo   Gianmarco Parretti   Shufang Zhu

ERC Advanced Grant
WhiteMech:
White-box Self Programming Mechanisms
SAPIENZA
UNIVERSITÀ DI ROMA

GenPlan@IJCAI-ECAI2022

July 23, 2022

SAPIENZA UNIVERSITÀ DI ROMA

- **Best-effort synthesis** is a **suitable form of planning**, finds a strategy that ensures the agent will do its best to achieve the goal, i.e., a best-effort strategy
- LTL_f **best-effort synthesis**, both the environment assumption and the agent goal are expressed as LTL_f formulas

- **Reactive synthesis**, a **general form of planning**, finds an agent strategy that achieves the given goal (temporal goal)
- An agent strategy is a function $\sigma_{ag} : (2^{\mathcal{X}})^{+} \rightarrow 2^{\mathcal{Y}}$

LTL$_f$ Reactive Synthesis Under Environment Assumptions

Given: Environment assumption $\mathcal{E}$, agent goal φ, LTL$_f$ formulas over $\mathcal{X} \cup \mathcal{Y}$

Obtain: An agent strategy σ_{ag} such that

$$\forall \sigma_{env} \triangleright \mathcal{E}, \pi(\sigma_{ag}, \sigma_{env}) \models \varphi$$

- **Best-effort synthesis** finds a **best-effort strategy**, i.e., a strategy that ensures the agent does its best to achieve the goal

Dominance

Let σ_1 and σ_2 be two agent strategies. σ_1 **dominates** σ_2 for goal φ under assumption $\mathcal{E}$, written $\geq_{\varphi|\mathcal{E}}$, if for every $\sigma_{env} \rhd \mathcal{E}, \pi(\sigma_2, \sigma_{env}) \models \varphi$ implies $\pi(\sigma_1, \sigma_{env}) \models \varphi$. σ_1 **strictly dominates** σ_2, written $\sigma_1 >_{\varphi|\mathcal{E}} \sigma_2$, if $\sigma_1 \geq_{\varphi|\mathcal{E}} \sigma_2$ and $\sigma_2 \not\geq_{\varphi|\mathcal{E}} \sigma_1$.

LTL$_f$ Best-Effort Synthesis Under Environment Assumptions

Given: Environment assumption $\mathcal{E}$, agent goal φ, LTL$_f$ formulas over $\mathcal{X} \cup \mathcal{Y}$

Obtain: An agent strategy σ such that there is no strategy σ' that strictly dominates σ

Contributions

SAPIENZA
UNIVERSITÀ DI ROMA

- Study of the relationship between reactive synthesis and best-effort synthesis for specifications in **Linear Temporal Logic on Finite Traces (LTL_f)**
- Three novel symbolic approaches to LTL_f best-effort synthesis:
  - Monolithic
  - Explicit-compositional
  - Symbolic-composiional
- Empirical evaluation

Contributions

SAPIENZA
UNIVERSITÀ DI ROMA

- Study of the relationship between reactive synthesis and best-effort synthesis for specifications in **Linear Temporal Logic on Finite Traces (LTL_f)**
- Three novel symbolic approaches to LTL_f best-effort synthesis:
  - Monolithic
  - Explicit-compositional
  - Symbolic-composiional
- Empirical evaluation

Contributions

SAPIENZA UNIVERSITÀ DI ROMA

- Study of the relationship between reactive synthesis and best-effort synthesis for specifications in **Linear Temporal Logic on Finite Traces (LTL$_f$)**
- Three novel symbolic approaches to LTL$_f$ best-effort synthesis:
  - Monolithic
  - Explicit-compositional
  - Symbolic-composiional
- Empirical evaluation

- The proposed approaches are based on a reduction to solving adversarial/cooperative reachability games on symbolic DFAs

Symbolic DFA [Zhu et al. 2017]

The symbolic representation of a DFA is a tuple $\mathcal{G}^s = (\mathcal{X}, \mathcal{Y}, \mathcal{Z}, Z_0, \eta, f)$ where:

- $\mathcal{X}$ and $\mathcal{Y}$ are environment and agent variables, respectively
- $\mathcal{Z}$ is the set of state variables
- Z_0 is the initial state
- $\eta: 2^{\mathcal{X}} \times 2^{\mathcal{Y}} \times 2^{\mathcal{Z}} \to 2^{\mathcal{Z}}$ represents the transitions of the DFA game
- f represents the final state of the DFA game

- **Winning strategy of an adversarial reachability game**. Least fixpoint computation on Boolean formulas w and t:

$$t_{i+1}(Z, Y, Y) = t_i(Z, X, Y) \vee (\neg w_i(Z) \wedge w_i(\eta(X, Y, Z)))$$
$$w_{i+1}(Z) = \forall X. \exists Y. t_{i+1}(Z, X, Y);$$

- **Winning strategy of a cooperative reachability game**. Least fixpoint computation on Boolean formulas $\hat{w}$ and $\hat{t}$:

$$\hat{t}_{i+1}(Z, Y, Y) = \hat{t}_i(Z, X, Y) \vee (\neg \hat{w}_i(Z) \wedge \hat{w}_i(\eta(X, Y, Z)))$$
$$\hat{w}_{i+1}(Z) = \exists X. \exists Y. \hat{t}_{i+1}(Z, X, Y);$$

- Fixpoint reached when $w_{i+1} \equiv w_i$ (resp. $\hat{w}_{i+1} = \hat{w}_i$)
- Computation of positional strategy by Boolean synthesis

Monolithic Approach

SAPIENZA UNIVERSITÀ DI ROMA

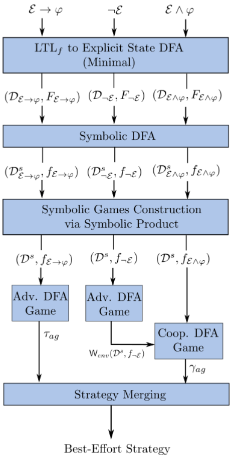


Figure: Monolithic

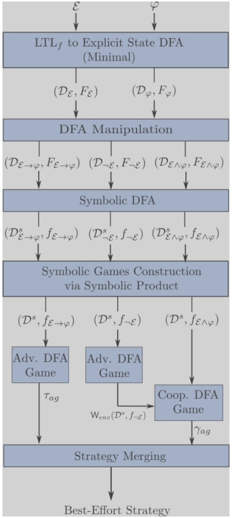


Figure: Explicit-Compositional

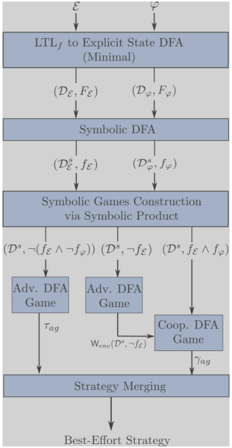


Figure: Symbolic-Compositional

Explicit-Compositional Approach

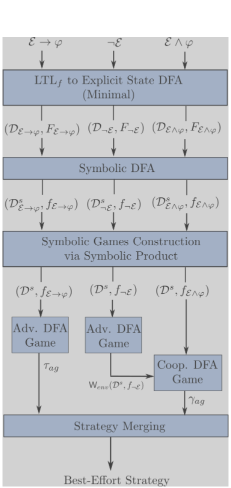
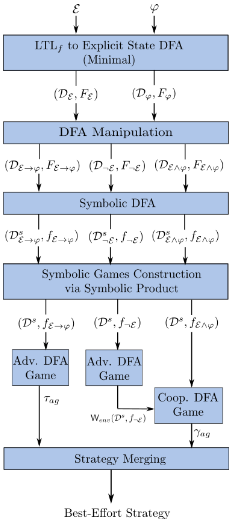


Figure: Monolithic



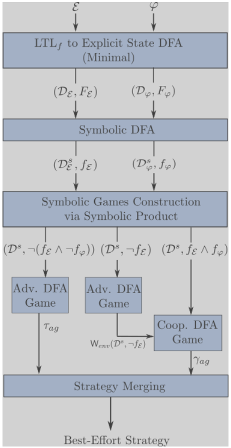


Figure: Symbolic-Compositional

Figure: Explicit-Compositional

Explicit-Compositional Approach

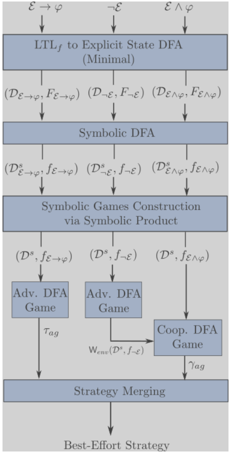


Figure: Monolithic

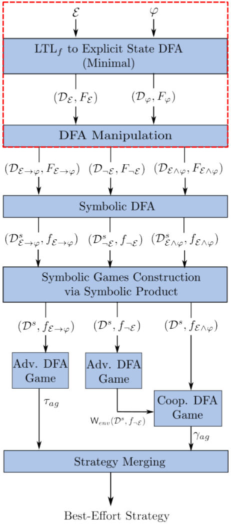


Figure: Explicit-Compositional

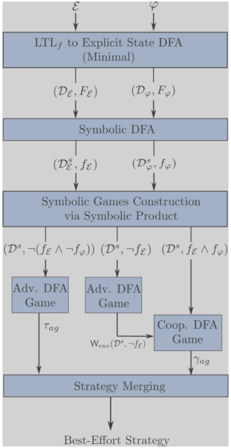


Figure: Symbolic-Compositional

Symbolic-Compositional Approach

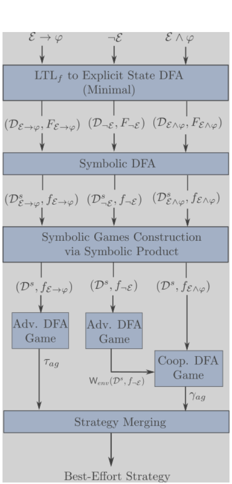


Figure: Monolithic

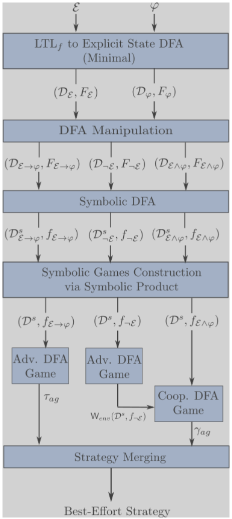


Figure: Explicit-Compositional

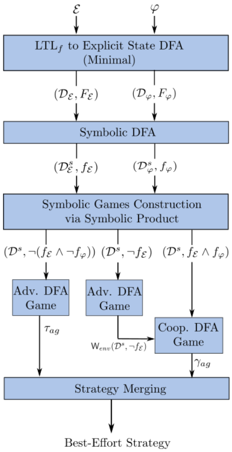
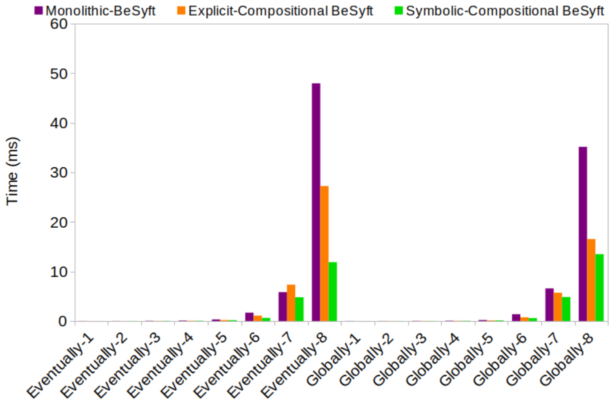


Figure: Symbolic-Compositional

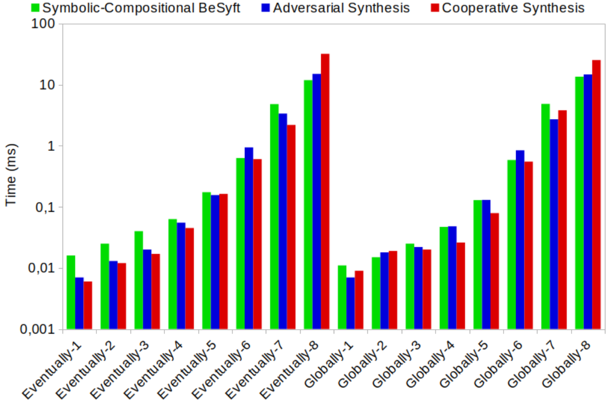
- **Implementation** of the symbolic approaches in a tool called ***BeSyft***:
  - Monolithic-*BeSyft*
  - Explicit-compositional-*BeSyft*
  - Symbolic-compositional-*BeSyft*

- **Experiments** performed on a scalable benchmark **counter games**:
  - Performance comparison of the three symbolic approaches
  - Performance comparison of best-effort and reactive synthesis
  - Evaluation of the bottleneck and impact of the cooperative phase

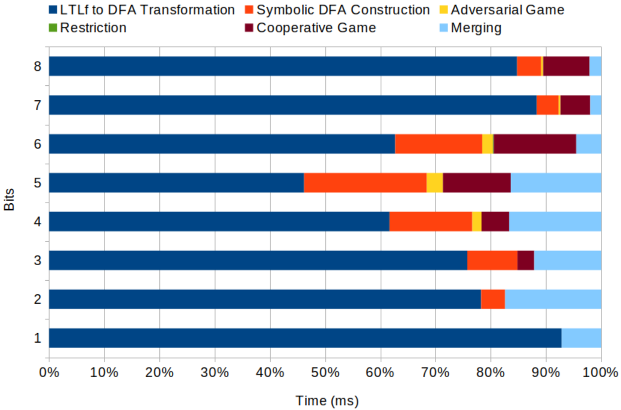
Experimental Results
Comparing Symbolic Approaches



Experimental Results
Comparing Best-Effort Synthesis and Reactive Synthesis



Experimental Results
Relative Time Cost Evaluation



SAPIENZA
UNIVERSITÀ DI ROMA

- Three symbolic approaches to LTL_f best-effort synthesis
- The symbolic-compositional approach has the best performance
- Automata minimization does not always lead to improvement
- LTL_f-to-DFA conversion is the bottleneck of LTL_f best-effort synthesis.
- Performing best-effort synthesis only brings minor overhead comparing with standard reactive synthesis

Future Directions

- LTL_f best-effort synthesis on planning domains
- LTL_f best-effort synthesis under multiple environment assumptions
- LTL best-effort synthesis