Studies in Systems, Decision and Control 89

Calin Belta
Boyan Yordanov
Ebru Aydin Gol

Formal Methods for Discrete-Time Dynamical Systems

Springer

Chapter 4
Largest Finite Satisfying Region

In Chap. 3, we introduced LTL model checking—a computational method for deciding automatically if a finite transition system T (Definition 1.1) satisfies an LTL formula ϕ (Sect. 2.1). This technique produces Yes/No answers (i.e., T satisfies ϕ or the specification is violated). In many applications, more quantitative results for the satisfaction of ϕ by T are required. For example, if the set of states was partitioned into satisfying and non-satisfying states, then the ratio of the cardinalities of the two sets would give us some indication on the degree of satisfaction. In this chapter, we focus on the problem of analyzing a finite transition system with the goal of partitioning its state space into satisfying and non-satisfying subsets of states. Since the focus is on analysis, as in Chap. 3, we consider transition systems with no inputs. In Chap. 5, we will present a control version of the same problem for finite transition systems. These techniques will then be extended in Chaps. 7 and 9 to infinite transition systems embedding discrete-time dynamical systems. The problem that we consider in this chapter can be formally stated as follows:

Problem 4.1 (*Largest satisfying region problem*) Given a finite transition system $T = (X, \delta, O, o)$ and an LTL formula ϕ over its set of observations O, find the largest subset of X from which ϕ is satisfied.

Before we begin developing our solution to Problem 4.1 in the following sections, we introduce several additional definitions necessary to formalize the problem and give an overview of our approach.

Definition 4.1 (*Largest satisfying region*) Given a transition system $T = (X, \delta, O, o)$ and an LTL formula ϕ over O,

$$X_T^\phi = \{x \in X \mid T(x) \vDash \phi\} \tag{4.1}$$

is the *largest satisfying region* of T—the set of all states of T where ϕ is satisfied.

C. Belta et al., *Formal Methods for Discrete-Time Dynamical Systems*,
Studies in Systems, Decision and Control 89, DOI 10.1007/978-3-319-50763-7_4

The set X_T^{ϕ} is the largest region of T satisfying ϕ since, for all states x of T where $x \notin X_T^{\phi}$, there exists a word in $\mathscr{L}_T(x)$ that violates ϕ. While any subset of X_T^{ϕ} contains only satisfying states and is therefore a "satisfying region" of T, the *largest satisfying region* X_T^{ϕ} is uniquely defined.

Definition 4.2 (*Largest violating region*) Given a transition system $T = (X, \delta, O, o)$ and an LTL formula ϕ over O, the set of all states of T where ϕ is not satisfied is the *largest violating region* of T

$$X \setminus X_T^{\phi} = \{x \in X \mid T(x) \nvDash \phi\} \tag{4.2}$$

Equivalently, there exists at least one run of T that violates ϕ originating in every state from the largest violating region.

Definition 4.3 (*Strictly violating region*) Given a transition system $T = (X, \delta, O, o)$ and an LTL formula ϕ over O,

$$X_T^{\neg\phi} = \{x \in X \mid T(x) \vDash \neg\phi\} \tag{4.3}$$

is the *strictly violating region* of T—the set of all states of T where the negation $\neg\phi$ is satisfied.

Relevant to analysis applications, no runs of T satisfying ϕ originate at any state $x \in X_T^{\neg\phi}$. Therefore, the strictly violating region is always a subset of the largest violating region. When T is deterministic, only a single run originates at each state $x \in X$ and satisfies either the formula ϕ or its negation $\neg\phi$ (i.e., $T(x) \vDash \phi$ or $T(x) \vDash \neg\phi$), allowing x to be included respectively in X_T^{ϕ} or $X_T^{\neg\phi}$ (see Example 4.1). As a result, X_T^{ϕ} and $X_T^{\neg\phi}$ partition the states of T (i.e., $X = X_T^{\phi} \cup X_T^{\neg\phi}$) for a deterministic T and the strictly violating region is also the largest violating region.

Example 4.1 Consider the finite, deterministic transition system T from Example 1.5 (Fig. 4.1) and specification $\phi = \bigcirc$ "on" requiring that, in the next time step, a state with the observation "on" is visited. The largest region of T satisfying ϕ is $X_T^{\phi} = \{x_3, \ldots, x_8\}$ and the strictly violating region for ϕ is $X_T^{\neg\phi} = \{x_1, x_2\}$ (both regions are shown in Fig. 4.1). Since transition system T is deterministic, the strictly violating region is also the largest region violating of T and the set of states $X = \{x_1, \ldots, x_8\}$ is partitioned into X_T^{ϕ} and $X_T^{\neg\phi}$, as shown in Fig. 4.1.

In general, when T is nondeterministic it is possible that both runs satisfying ϕ and runs satisfying $\neg\phi$ originate at a state $x \in X$ and therefore T does not satisfy either ϕ or $\neg\phi$ from x (i.e., $T(x) \nvDash \phi$ and $T(x) \nvDash \neg\phi$). Then, state x is an *uncertain* state of T with respect to the satisfaction of ϕ and is not included in either X_T^{ϕ} or $X_T^{\neg\phi}$ (see Example 4.2).

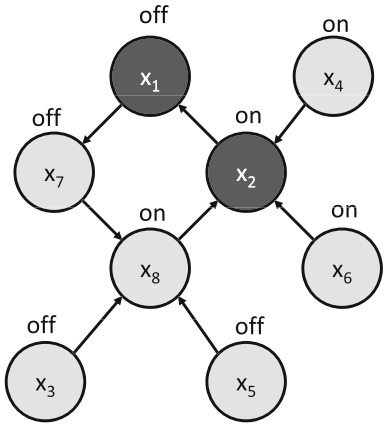


Fig. 4.1 Satisfying (*light gray*) and violating (*dark gray*) states of the deterministic system introduced in Example 1.5 (Fig. 1.5) for specification $\phi = \bigcirc$ "on" (for additional details, see Example 4.1)

Definition 4.4 (*Uncertain region*) Given a transition system $T = (X, \delta, O, o)$ and an LTL formula ϕ over O,

$$X_T^{\phi?} = \{x \in X \mid T(x) \not\models \phi \text{ and } T(x) \not\models \neg\phi\}. \tag{4.4}$$

is the *uncertain region* of T—the set of all states of T where neither ϕ nor $\neg\phi$ is satisfied.

The set $X_T^{\phi?}$ includes all uncertain states and, for a nondeterministic T where $X_T^{\phi?} \neq \emptyset$, the states of T is partitioned into the largest satisfying, strictly violating and uncertain regions $X = X_T^{\phi} \cup X_T^{\neg\phi} \cup X_T^{\phi?}$. As a result, the strictly violating region $X_T^{\neg\phi}$ is not necessarily the largest violating region (as for a deterministic T). Instead, the largest violating region is the union of the strictly violating and the uncertain regions, expressed equivalently as $X \setminus X_T^{\phi}$.

Example 4.2 Consider the finite, nondeterministic transition system T from Example 1.2 and specification $\phi = \bigcirc o_1$ requiring that, in the next time step, a state with the observation o_1 is visited. The largest region of T satisfying ϕ is $X_T^{\phi} = \{x_1\}$, while the strictly violating region for ϕ is $X_T^{\neg\phi} = \{x_2, x_4\}$. Runs satisfying both ϕ and $\neg\phi$ originate at state x_3, so $x_3 \notin X_T^{\phi}$ and $x_3 \notin X_T^{\neg\phi}$ and, therefore, state x_3 is uncertain (i.e., $x_3 \in X_T^{\phi?}$). The set of states $X = \{x_1, \ldots, x_4\}$ of T is partitioned into X_T^{ϕ}, $X_T^{\neg\phi}$ and $X_T^{\phi?}$, which are shown in Fig. 4.2.

While the solution to Problem 4.1 amounts to the computation of set X_T^{ϕ} only, sets $X_T^{\neg\phi}$ and $X_T^{\phi?}$ provide valuable information about system T and their explicit computation leads to significant optimizations of the overall analysis procedure, as it will become clear in the following sections. In the following, we refer to the computation

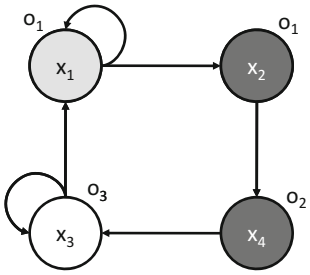


Fig. 4.2 Satisfying (*light gray*), violating (*dark gray*) and uncertain (*unshaded*) states of the nondeterministic system introduced in Example 1.2 (Fig. 1.2) for specification $\phi = \bigcirc o_1$ (for additional details, see Example 4.2)

of X_T^{ϕ}, $X_T^{\neg\phi}$ and $X_T^{\phi?}$ as the analysis of a transition system. For a finite T, which is the focus of this chapter, all three sets are computable through a direct application of model checking (as illustrated in Sect. 4.1), thus providing a solution to Problem 4.1. However, such analysis becomes computationally challenging when T is large. To address this issue, in the following sections we present alternative abstraction-based analysis strategies, generally leading to conservative solutions of Problem 4.1, where under-approximations of sets X_T^{ϕ} and $X_T^{\neg\phi}$ are computed. Specifically, we focus on approaches for the iterative refinement and analysis of quotients of T, allowing an approximate solution to be computed and improved incrementally. In addition, we derive conditions guaranteeing that an exact solution to Problem 4.1 is obtained. Besides providing a more feasible strategy for the analysis of large finite transition systems, these abstraction techniques are also applicable to infinite transition systems, which we will exploit in Chap. 7.

4.1 Model-Checking-Based Solution

Given a finite transition system T, the subset of states where an LTL formula ϕ is satisfied is computable by model-checking T against ϕ from individual states. We denote this procedure by ANALYZE() where, given a region $X_r \subseteq X$,

$$\text{ANALYZE}(T, X_r, \phi) = \{x \in X_r \mid T(x) \vDash \phi\} \tag{4.5}$$

is the subset of X_r satisfying the formula ϕ. For a finite transition system T, the largest satisfying region is computed as $X_T^{\phi} = \text{ANALYZE}(T, X, \phi)$, which provides a solution to Problem 4.1. Similarly, the strictly violating region is computed as $X_T^{\neg\phi} = \text{ANALYZE}(T, X, \neg\phi)$. Once X_T^{ϕ} and $X_T^{\neg\phi}$ have been computed, the uncertain region of T is computed as $X_T^{\phi?} = X \setminus (X_T^{\phi} \cup X_T^{\neg\phi})$.

An implementation of ANALYZE(), based on the function MODEL- CHECK() (Algorithm 2) from Chap. 3, is given in Algorithm 3. This implementation is applicable whenever model checking is feasible (i.e., when T is finite) but might require many model-checking steps. Therefore, if T has a large number of states, applying function ANALYZE() is computationally expensive. In the following sections we develop

analysis procedures suitable for larger systems, based on the construction and analysis of finite abstractions of T.

Example 4.3 In Example 3.1 we showed that the traffic light system described in Example 1.6 was unsafe with respect to specification $\phi_1 = \square\neg$ "green, walk". In other words, there existed runs of the system which led to an unsafe state, where both cars and pedestrians were allowed to cross the intersection simultaneously. In this example, we modify the system and use the analysis procedure described in Algorithm 3 to find initial states, guaranteeing the safe behavior of the traffic light.

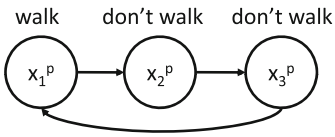
As before, we construct the overall system as the product $T^s = T_c \otimes T_p^s$ of the car and pedestrian traffic light components, where the car traffic light component T_c remains unchanged as in Example 3.1 (Fig. 1.6a). The pedestrian traffic light component T_p^s is modified from the one described in Example 1.6 and includes one additional state x_3^p with the observation "don't walk" (see Fig. 4.3a).

By analyzing the product T^s with specification $\phi_1 = \square\neg$ "green, walk", we compute the violating region $X_{T^s}^{\neg\phi_1} = \{(x_1^c, x_1^p), (x_2^c, x_2^p), (x_3^c, x_3^p)\}$, where all other states of the system are satisfying and belong to $X_{T^s}^{\phi_1}$ (see Fig. 4.3b). Therefore, we can guarantee that the safety specification ϕ_1 is satisfied, as long as the system is initialized in a state from the satisfying region $X_{T^s}^{\phi_1}$.

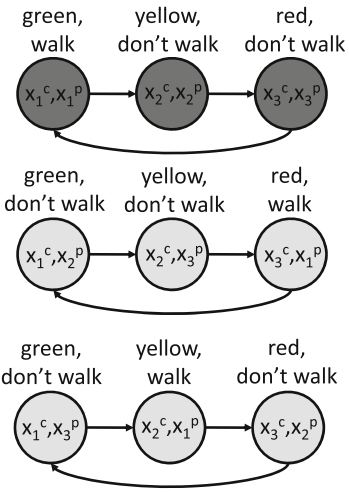
We can also analyze the system with the stronger safety specification $\phi_2 = \square\neg$ ("green, walk" $\vee$ "yellow, walk"), which requires that the potentially unsafe state of the system where pedestrians are allowed to cross but cars are not explicitly stopped by a red signal is also avoided. Analysis using Algorithm 3 reveals the satisfying region $X_{T^s}^{\phi_2} = \{(x_1^c, x_2^p), (x_2^c, x_3^p), (x_3^c, x_1^p)\}$ (Fig. 4.3c) and allows us to guarantee that the intersection is safe with respect to specification ϕ_2, provided that the system is initialized at a state from $X_{T^s}^{\phi_2}$.

Algorithm 3 ANALYZE(T, X_r, ϕ): Set of states of T in region X_r satisfying ϕ

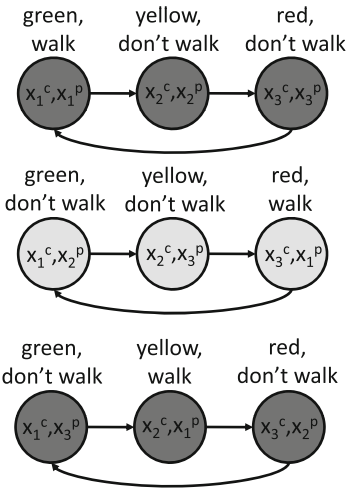
```
Initialize X_T^φ := ∅
for each state x ∈ X_r do
  if MODEL- CHECK(T, x, φ) then
    X_T^φ := X_T^φ ⋃{x}
  end if
end for
return X_T^φ
```



(a) Safe pedestrian traffic light (T_p^s).



(b) Satisfying and violating regions for specification $\phi_1 = \square\neg$ "green, walk".



(c) Satisfying and violating regions for specification $\phi_2 = \square\neg$ ("green, walk" $\vee$ "yellow, walk").

Fig. 4.3 Satisfying (*light gray*) and violating (*dark gray*) regions are computed by analyzing the safe pedestrian intersection traffic light described in Example 4.3

4.2 Abstraction-Based Solution

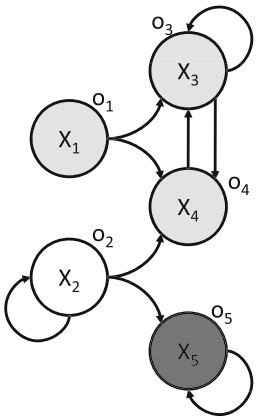
In Sect. 1.3 we introduced the notion of a quotient transition system $T/_\sim = (X/_\sim, \delta_\sim, O, o_\sim)$ as an abstraction of the concrete transition system $T = (X, \delta, O, o)$. The language inclusion property of Eq. (1.19) stated that, for all quotient states (equivalence classes of T) $X_i \in X/_\sim$, all words from the language of T originating from region $con(X_i)$ (representing the equivalent states of T from class X_i) are included in the language of the quotient $T/_\sim$ originating from state X_i (i.e., $\mathscr{L}_T(con(X_i)) \subseteq \mathscr{L}_{T/_\sim}(X_i)$). In other words, any behavior of T is reproduced by $T/_\sim$ (i.e., $T/_\sim$ simulates T), which guarantees that, for all quotient states $X_i \in X/_\sim$ and all LTL formulas ϕ, the concrete system T satisfies ϕ from region $con(X_i)$ only if the quotient $T/_\sim$ (usually much smaller than T) satisfies the formula from state X_i, i.e.,

$$T/_\sim(X_i) \vDash \phi \Rightarrow T(con(X_i)) \vDash \phi \tag{4.6}$$

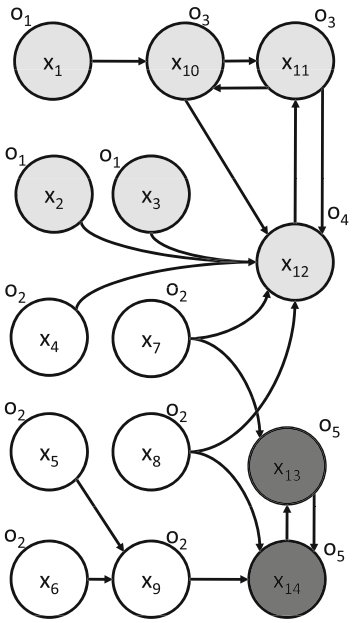
This property is relevant to model checking, since it allows us to extend results obtained for the quotient $T/_\sim$ to the concrete transition system T. Equation (4.6) also guarantees that when a state X_i of $T/_\sim$ satisfies the negation $\neg\phi$, all states $x \in con(X_i)$ of T satisfy $\neg\phi$ and, therefore, violate ϕ. Note that this strategy is conservative, since identifying states of $T/_\sim$ that do not satisfy ϕ or $\neg\phi$ does not lead directly to any guarantees for T.

Similar to the model checking approach described above, we apply Eq. (4.6) in order to extend analysis results obtained for the quotient $T/_\sim$ to the original, concrete system T. Given LTL formula ϕ, we use Algorithm 3 to compute the largest satisfying region $X^{\phi}_{T/_\sim}$ of $T/_\sim$ (i.e., $X^{\phi}_{T/_\sim}$ =ANALYZE($T/_\sim, X/_\sim, \phi$)). From Eq. (4.6) we guarantee that $con(X^{\phi}_{T/_\sim})$ is a satisfying region in T but, in general, it is not the largest satisfying region (i.e., $con(X^{\phi}_{T/_\sim}) \subseteq X^{\phi}_{T}$). However, this computation provides a strategy for obtaining satisfying regions of T when X^{ϕ}_{T} =ANALYZE(T, X, ϕ) cannot be computed directly (e.g., when T is large or infinite). The same approach is used to compute the strictly violating region $X^{\neg\phi}_{T/_\sim}$ =ANALYZE($T/_\sim, X/_\sim, \neg\phi$) in $T/_\sim$ with the guarantee that $con(X^{\neg\phi}_{T/_\sim})$ is a violating region of T but, in general, only a subset of its strictly violating region (i.e., $con(X^{\neg\phi}_{T/_\sim}) \subseteq X^{\neg\phi}_{T}$). While the computation of the uncertain region of $T/_\sim$ as $X^{\phi?}_{T/_\sim} = X/_\sim \setminus (X^{\phi}_{T/_\sim} \cup X^{\neg\phi}_{T/_\sim})$ is straightforward, in general, region $con(X^{\phi?}_{T/_\sim})$ is not the uncertainty region of T (i.e., it is possible that formula ϕ or its negation $\neg\phi$ is satisfied by all runs originating at a state $x \in con(X^{\phi?}_{T/_\sim})$). In fact, due to the under-approximation of the largest satisfying and strictly violating regions of T through the analysis of the quotient $T/_\sim$, region $con(X^{\phi?}_{T/_\sim})$ provides an over-approximation of the uncertain region of T (i.e., $X^{\phi?}_{T} \subseteq con(X^{\phi?}_{T/_\sim})$).

Example 4.4 We apply the analysis procedure based on quotient construction and Algorithm 3 to the transition system T from Example 1.10. We consider specification $\phi = \Box\Diamond o_3$, requiring that runs of the system keep visiting states with the observation o_3. The quotient $T/_\sim$ is constructed and, by applying the analysis procedure from Algorithm 3, the largest satisfying region $X^{\phi}_{T/_\sim} = \{X_1, X_3, X_4\}$ and the strictly violating region $X^{\neg\phi}_{T/_\sim} = \{X_5\}$ of $T/_\sim$ are identified (see Fig. 4.4a). This implies that the sets $con(X^{\phi}_{T/_\sim}) = \{x_1, x_2, x_3, x_{10}, x_{11}, x_{12}\}$ and $con(X^{\neg\phi}_{T/_\sim}) = \{x_{13}, x_{14}\}$ are respectively a satisfying and violating region of T (see Fig. 4.4b). However, these sets are only subsets of the largest satisfying and violating regions $X^{\phi}_{T} = \{x_1, x_2, x_3, x_4, x_{10}, x_{11}, x_{12}\}$ and $X^{\neg\phi}_{T} = \{x_5, x_6, x_9, x_{13}, x_{14}\}$ (Fig. 4.4c). We can also compute the uncertain region $X^{\phi?}_{T/_\sim} = \{X_2\}$ but region $con(X^{\phi?}_{T/_\sim}) = \{x_4, \ldots, x_9\}$ is an over-approximation of the uncertain region of T (i.e., only states x_7 and x_8 are uncertain in T).



(a) Satisfying (light gray) and violating (dark gray) states of $T/_{\sim}$.



(b) Satisfying (light gray) and violating (dark gray) states of T induced from the analysis of $T/_{\sim}$.

Fig. 4.4 Analysis of the finite quotient $T/_{\sim}$ with specification $\square\diamond o_3$ allows us to identify satisfying and violating states of T (see Example 4.4 for additional details)

The analysis approach discussed so far was conservative, due to the construction and analysis of a conservative simulation quotient of T—a limitation that is addressed through the construction of a bisimulation quotient. Equation (1.20) stated that the language of such a quotient is equivalent to the language of T (i.e., $\mathscr{L}_T(con(X_i)) = \mathscr{L}_{T/_{\approx}}(X_i)$), which allows us to guarantee that for all quotient states (equivalence classes of T) $X_i \in X/_{\approx}$ and all LTL formulas ϕ, we have

$$T/_{\approx}(X_i) \vDash \phi \Leftrightarrow T(con(X_i)) \vDash \phi. \tag{4.7}$$

Following from Eq. (4.7), we use the bisimulation quotient $T/_{\approx}$ equivalently instead of T for model checking (which was not true for the simulation quotient $T/_{\sim}$). In other words, by applying Algorithm 3 to the bisimulation quotient $T/_{\approx}$, we can compute the largest satisfying and violating regions of T through the computation of the largest satisfying and violating regions of $T/_{\approx}$ as

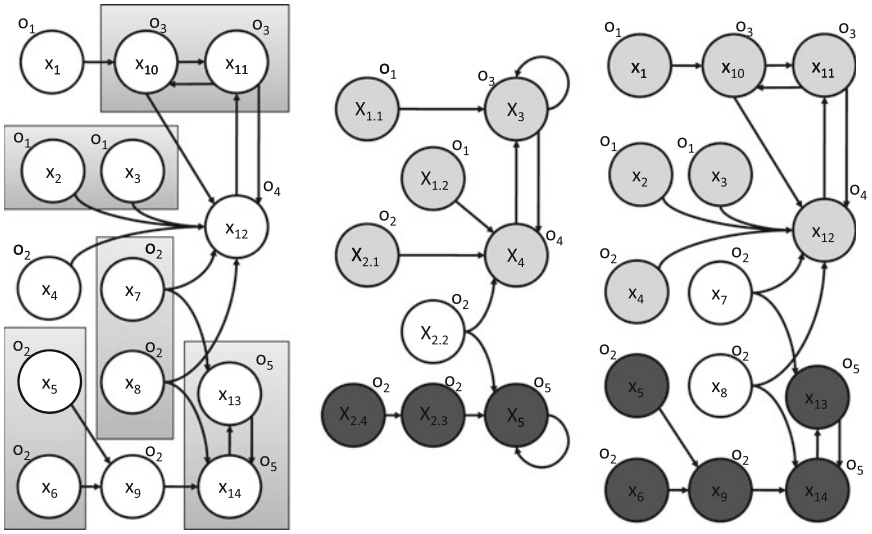
$$X_T^{\phi} = con(X_{T/\approx}^{\phi}) \text{ and } X_T^{\neg\phi} = con(X_{T/\approx}^{\neg\phi}) \tag{4.8}$$

As a consequence of Eq. (4.8), the set of uncertain states is computed as $X_T^{\phi?} = con(X_{T/\approx}^{\phi?})$, where $X_{T/\approx}^{\phi?} = X/\approx \setminus (X_{T/\approx}^{\phi} \cup X_{T/\approx}^{\neg\phi})$.

Using the results discussed so far, we obtain a solution to Problem 4.1, even when system T cannot be analyzed directly (e.g., when model checking is not feasible because T has too many or infinitely many states). The approach requires the computation of the quotient $T/\sim$ induced by the observational equivalence relation $\sim$. When $T/\sim$ simulates T, only an approximate solution to Problem 4.1 is obtained using this technique but the solution is exact when a bisimulation quotient $T/\approx$ can be constructed. A strategy for the computation of bisimulation quotients was already presented in Sect. 1.3 as Algorithm 1. Thus, the overall analysis procedure described in this section involves (i) computing the coarsest observation-preserving equivalence relation $\approx$=BISIMULATION(T) (Algorithm 1), (ii) constructing the bisimulation quotient $T/\approx$ and (iii) identifying the largest satisfying, strictly violating and uncertain regions of T through analysis of $T/\approx$ using Algorithm 3 (see Example 4.5).

Example 4.5 The analysis approach discussed in this section is applied to study transition system T from Fig. 1.11a with specification $\Box\Diamond o_3$. In Example 4.4, we showed that simply constructing the quotient $T/\sim$ under the observational equivalence relation $\sim$ and analyzing it using Algorithm 3 led to the identification of the satisfying region $\{x_1, x_2, x_3, x_{10}, x_{11}, x_{12}\}$ and violating region $\{x_{13}, x_{14}\}$ of T but the largest satisfying and strictly violating regions of T were not identified (i.e., the exact solution to Problem 4.1 was not obtained).

By applying the bisimulation algorithm to T we compute the bisimulation $\approx$ and construct the bisimulation quotient $T/\approx$ (Fig. 4.5b with equivalence classes shown in Fig. 4.5a). Using Algorithm 3, we identify the largest satisfying and strictly violating regions of $T/\approx$ as $X_{T/\approx}^{\phi} = \{X_{1.1}, X_{1.2}, X_{2.1}, X_3, X_4\}$ and $X_{T/\approx}^{\neg\phi} = \{X_{2.3}, X_{2.4}, X_5\}$, respectively. Following from the discussion from Sect. 1.3, we can guarantee that regions $con(X_{T/\approx}^{\phi}) = \{x_1, x_2, x_3, x_4, x_{10}, x_{11}, x_{12}\}$ and $con(X_{T/\approx}^{\neg\phi}) = \{x_5, x_6, x_9, x_{13}, x_{14}\}$ are respectively the largest satisfying and strictly violating region in T (see Fig. 4.5c). In addition, we can compute the region of uncertain states $X_{T/\approx}^{\phi?} = X/\sim \setminus (X_{T/\approx}^{\phi} \cup X_{T/\approx}^{\neg\phi}) = \{X_{2.2}\}$ of $T/\approx$ and guarantee that all states from the region $con(X_{T/\approx}^{\phi?}) = \{x_7, x_8\}$ are uncertain in T.



(a) Equivalence classes $X/_{\approx}$. (b) Satisfying and violating states of the bisimulation quotient $T/_{\approx}$. (c) Satisfying and violating states of T.

Fig. 4.5 The bisimulation $\approx$ (**a**) of system T from Fig. 1.11a is obtained using Algorithm 1 by refining the equivalence classes $X/_{\sim}$ highlighted in Fig. 1.11a (the quotient $T/_{\sim}$ was shown in Fig. 1.11b). This allows the construction of the bisimulation quotient $T/_{\approx}$ (**b**). The largest satisfying (*light gray*), strictly violating (*dark gray*) and uncertain (*white*) regions of $T/_{\approx}$ for specification $\square\diamond o_3$ can then be identified using Algorithm 3. This allows for the computation of the largest satisfying, strictly violating and uncertain regions of T (**c**). For additional details, see Example 4.5

4.3 Iterative Strategies

In Sect. 4.1, we presented a model-checking-based strategy (Algorithm 3), which could be applied directly on T to provide a complete solution to Problem 4.1. However, this approach was computationally expensive when T included a large number of states and could not be used directly when T was infinite as will be discussed in subsequent chapters. Algorithm 3 could also be applied to the quotient $T/_{\sim}$ (constructed with the observational equivalence relation $\sim$) but in general this led only to an approximate solution to Problem 4.1, which was too conservative as illustrated in Sect. 4.2. Finally, Algorithm 3 could also be applied to the bisimulation quotient $T/_{\approx}$, thus providing a complete solution to Problem 4.1 as discussed in the previous section. However, such an analysis strategy required that the bisimulation algorithm (Algorithm 1) has terminated before applying model-checking techniques. While this approach guarantees that the largest satisfying region of the system is identified, it is not practical for certain systems (e.g., when many refinement steps are required to compute a bisimulation quotient) and cannot be applied directly to infinite systems, which will be our focus in subsequent chapters. As a compromise, instead of relying