Checking Unwinding Conditions for Finite State Systems

Deepak D'Souza and Raghavendra K. R
Department of Computer Science and Automation
Indian Institute of Science, Bangalore 560012, India.
{deepakd, raghavendrakr}@csa.iisc.ernet.in.

Abstract. We consider the problem of checking the unwinding conditions of Mantel for Basic Security Predicates (BSP's) [7], for finite-state systems. We show how the unwinding conditions can be simplified to checking conditions on a maximal simulation relation. We conclude that the time complexity of verifying BSP's via the unwinding route compares favourably with the model-checking technique proposed in [2].

1 Introduction

Information flow properties are a way of specifying security properties of systems, that dates back to the work of Goguen and Meseguer [3] in the eighties. A system is viewed as generating traces containing "confidential" and "visible" events (only the latter being observable by a "low-level" user) and the information flow properties specify restrictions on the kind of traces the system may generate, so as to restrict the amount of information a low-level user can infer about confidential events having taken place in the system. For example, the "non-inference" [9, 8, 12] property states that for every trace produced by the system, its projection to visible events must also be a possible trace of the system. Thus if a system satisfies the non-inference information flow property, a low-level user cannot observe a trace of the system and be able to say whether certain confidential events must necessarily have taken place.

In [7] Mantel provides a framework for reasoning about the various information flow properties presented in the literature, in a modular way. He identifies a set of basic information flow properties which he calls "basic security predicates" or BSP's, which are shown to be the building blocks of most of the known trace-based properties in the literature. The framework is modular in that BSP's which are common to several properties of interest for the given system, need only be verified once for the system.

There have been two approaches to the problem of verifying information flow properties for a given system: a traditional one based on "unwinding" [4, 11, 7] and the more recent "model-checking" technique in [2]. The unwinding technique is based on identifying structural properties of the system model which ensure the satisfaction of the information flow property. The method is not complete in general, in that a system could satisfy the information flow property but fail the unwinding condition. In [7] Mantel gives unwinding conditions for most of the

BSP's he identifies. In the model-checking approach [2], BSP's are characterized in terms of regularity preserving language- theoretic operations. This leads to a sound and complete decision procedure for checking whether a finite state system satisfies a given BSP.

In this paper our aim is to investigate the problem of checking the unwinding conditions of [7] for finite-state systems, and compare the running time with that of the model-checking approach of [2], which is exponential in the number of states of the system.

The naive approach to checking the unwinding conditions the way they are stated in [7] – in terms of the existence of an unwinding relation that satisfies certain properties – would also be exponential in the size of the system. We first show that this is not necessary, as the unwinding conditions can be equivalently stated in terms of whether the *maximal* unwinding relation satisfies the required properties. Secondly, we show how this maximal unwinding relation can be viewed as a standard simulation relation on a edge-labelled transition system, thereby opening the door for the use of well-studied and efficient algorithms for computing simuluation relations in the literature [5, 10].

As a result we show that the unwinding conditions can be checked in polynomial time in the size of the system (except for the BSP's based on "admissibility", which require exponential time). Thus the unwinding conditions, though not complete, compare favourably with the model-checking approach in terms of the time required to check them on a given finite-state system. The unwinding condition based approach to verifying information flow properties can thus be useful for systems with large state spaces for which the model-checking approach runs out of memory.

2 Preliminaries

By an alphabet we will mean a finite set of symbols representing *events* or *actions* of a system. For an alphabet Σ we use Σ^* to denote the set of finite strings over Σ. The null or empty string is represented by the symbol ϵ. For two strings α and β in Σ^* we write $\alpha\beta$ for the concatenation of α followed by β. A *language* over Σ is just a subset of Σ^*.

For the rest of the paper we fix an alphabet of events Σ. We assume a partition of Σ into V, C, N, which in the framework of [6] correspond to events that are *visible*, *confidential*, and *neither* visible nor confidential, from a particular user's point of view.

Let $X \subseteq \Sigma$. The projection of a string $\tau \in \Sigma^*$ to X is written $\tau\restriction_X$ and is obtained from τ by deleting all events that are not elements of X. The projection of the language L to X, written $L\restriction_X$, is defined to be $\{\tau\restriction_X \mid \tau \in L\}$.

A *labelled transition system* (LTS) over an alphabet Σ is a structure of the form $\mathcal{T} = (Q, s, \longrightarrow)$, where Q is a set of states, $s \in Q$ is the start state, and $\longrightarrow \subseteq Q \times \Sigma \times Q$ is the transition relation. We write $p \xrightarrow{a} q$ to stand for $(p, a, q) \in \longrightarrow$, and use $p \xrightarrow{w}{}^* q$ to denote the fact that we have a path labelled

w from p to q in the underlying graph of the transition system $\mathcal{T}$. If some state q has an edge labelled a, then we say a is enabled at q.

The language generated by $\mathcal{T}$ is defined to be

$$L(\mathcal{T}) = \{\alpha \in \Sigma^* \mid \text{there exists a } t \in Q \text{ such that } s \xrightarrow{\alpha}{}^* t\}.$$

Let $X \subseteq \Sigma$. We say an event $e \in \Sigma$ is X-*enabled* at a state $p \in Q$ if there exists $\alpha, \gamma \in \Sigma^*$ and $q \in Q$ such that $s \xrightarrow{\alpha}{}^* p$, $s \xrightarrow{\gamma}{}^* q$, $\alpha\upharpoonright_X = \gamma\upharpoonright_X$, and e is enabled at q.

We say $\mathcal{T}$ is *deterministic* if there do not exist states p, q and r in Q, with $q \neq r$ and $a \in \Sigma$, such that $p \xrightarrow{a} q$ and $p \xrightarrow{a} r$.

We will asssume in the sequel that all states in an LTS are reachable from the start state.

3 Unwinding Conditions

We begin by recalling the *basic security predicates* (BSP's) of Mantel [7]. These definitions play no technical role in the paper, but we include these definitions for the reader to have an idea of the predicates associated with the unwinding conditions.

It will be convenient to use the notation $\alpha =_Y \beta$ where $\alpha, \beta \in \Sigma^*$ and $Y \subseteq \Sigma$, to mean α and β are the same "modulo a correction on Y-events". More precisely, $\alpha =_Y \beta$ iff $\alpha\upharpoonright_{\overline{Y}} = \beta\upharpoonright_{\overline{Y}}$, where $\overline{Y}$ denotes $\Sigma - Y$. By extension, for languages L and M over Σ, we say $L \subseteq_Y M$ iff $L\upharpoonright_{\overline{Y}} \subseteq M\upharpoonright_{\overline{Y}}$.

In the definitions below, we assume L to be a language over Σ.

1. L satisfies R *(Removal of events)* iff for all $\tau \in L$ there exists $\tau' \in L$ such that $\tau'\upharpoonright_C = \epsilon$ and $\tau'\upharpoonright_V = \tau\upharpoonright_V$.
2. L satisfies D *(stepwise Deletion of events)* iff for all $\alpha c \beta \in L$, such that $c \in C$ and $\beta\upharpoonright_C = \epsilon$, we have $\alpha'\beta' \in L$ with $\alpha' =_N \alpha$ and $\beta' =_N \beta$.
3. L satisfies I *(Insertion of events)* iff for all $\alpha\beta \in L$ such that $\beta\upharpoonright_C = \epsilon$, and for every $c \in C$, we have $\alpha' c \beta' \in L$, with $\beta' =_N \beta$ and $\alpha' =_N \alpha$.
4. Let $X \subseteq \Sigma$. Then L satisfies *IA (Insertion of Admissible events)* w.r.t X iff for all $\alpha\beta \in L$ such that $\beta\upharpoonright_C = \epsilon$ and for some $c \in C$, there exists $\gamma c \in L$ with $\gamma\upharpoonright_X = \alpha\upharpoonright_X$, we have $\alpha' c \beta' \in L$ with $\beta' =_N \beta$ and $\alpha' =_N \alpha$.
5. L satisfies *BSD (Backwards Strict Deletion)* iff for all $\alpha c \beta \in L$ such that $c \in C$ and $\beta\upharpoonright_C = \epsilon$, we have $\alpha\beta' \in L$ with $\beta' =_N \beta$.
6. L satisfies *BSI (Backwards Strict Insertion)* iff for all $\alpha\beta \in L$ such that $\beta\upharpoonright_C = \epsilon$, and for every $c \in C$, we have $\alpha c \beta' \in L$, with $\beta' =_N \beta$.
7. Let $X \subseteq \Sigma$. Then L satisfies *BSIA (Backwards Strict Insertion of Admissible events)* w.r.t X iff for all $\alpha\beta \in L$ such that $\beta\upharpoonright_C = \epsilon$ and there exists $\gamma c \in L$ with $c \in C$ and $\gamma\upharpoonright_X = \alpha\upharpoonright_X$, we have $\alpha c \beta' \in L$ with $\beta' =_N \beta$.
8. Let $X \subseteq \Sigma$, $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. Then L satisfies *FCD (Forward Correctable Deletion)* w.r.t V', C', N' iff for all $\alpha c v \beta \in L$ such that $c \in C'$, $v \in V'$ and $\beta\upharpoonright_C = \epsilon$, we have $\alpha\delta v \beta' \in L$ where $\delta \in (N')^*$ and $\beta' =_N \beta$.

9. Let, $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. Then L satisfies *FCI (Forward Correctable Insertion)* w.r.t C', V', N' iff for all $\alpha v \beta \in L$ such that $v \in V'$, $\beta \upharpoonright_C = \epsilon$, and for every $c \in C'$ we have $\alpha c \delta v \beta' \in L$, with $\delta \in (N')^*$ and $\beta' =_N \beta$.
10. Let $X \subseteq \Sigma$, $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. Then L satisfies *FCIA (Forward Correctable Insertion of admissible events)* w.r.t. X, V', C', N' iff for all $\alpha v \beta \in L$ such that: $v \in V'$, $\beta \upharpoonright_C = \epsilon$, and there exists $\gamma c \in L$, with $c \in C'$ and $\gamma \upharpoonright_X = \alpha \upharpoonright_X$; we have $\alpha c \delta v \beta' \in L$ with $\delta \in (N')^*$ and $\beta' =_N \beta$.
11. L satisfies *SR (Strict Removal)* iff for all $\tau \in L$ we have $\tau \upharpoonright_{\overline{C}} \in L$.
12. L satisfies *SD (Strict Deletion)* iff for all $\alpha c \beta \in L$ such that $c \in C$ and $\beta \upharpoonright_C = \epsilon$, we have $\alpha \beta \in L$.
13. L satisfies *SI (Strict Insertion)* iff for all $\alpha \beta \in L$ such that $\beta \upharpoonright_C = \epsilon$, and for every $c \in C$, we have $\alpha c \beta \in L$.
14. Let $X \subseteq \Sigma$. L satisfies *SIA (Strict Insertion of Admissible events)* w.r.t X iff for all $\alpha \beta \in L$ such that $\beta \upharpoonright_C = \epsilon$ and there exists $\gamma c \in L$ with $c \in C$ and $\gamma \upharpoonright_X = \alpha \upharpoonright_X$, we have $\alpha c \beta \in L$.

We say a Σ-labelled transition system $\mathcal{T}$ satisfies a BSP iff $L(\mathcal{T})$ satisfies the BSP. We now recall the "unwinding" conditions defined in [7], which are shown to be sufficient conditions for a transition system to satisfy the corresponding BSP's.

Let us fix a Σ-labelled transitions system $\mathcal{T} = (Q, s, \longrightarrow)$ for the rest of this section. We say a relation $\ltimes \subseteq Q \times Q$ is an *unwinding* relation for $\mathcal{T}$ if for all states $p, q, r \in Q$ and for all events $e \in \Sigma \setminus C$ if $p \xrightarrow{e} q$ and $p \ltimes r$, then there exists $t \in Q$ and $\delta \in (\Sigma \setminus C)^*$ such that $\delta \upharpoonright_V = e \upharpoonright_V$, $r \xrightarrow{\delta}{}^* t$, and $q \ltimes t$. In [7] the condition on $\ltimes$ above is refered to as *osc* for "output step consistency".

In the definitions below, let $\ltimes$ be an unwinding relation for $\mathcal{T}$.

1. We say $\mathcal{T}$ satisfies the unwinding condition *lrf* (*locally respects forwards*) w.r.t. the unwinding relation $\ltimes$ iff whenever we have $p \xrightarrow{c} q$ for some $c \in C$, we also have $q \ltimes p$.
2. We say $\mathcal{T}$ satisfies the unwinding condition *lrb* (*locally respects backwards*) w.r.t. $\ltimes$ iff for each $p \in Q$ and $c \in C$, there exists $q \in Q$ such that $p \xrightarrow{c} q$ and $p \ltimes q$.
3. Let $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. We say $\mathcal{T}$ satisfies the unwinding condition *fcrf* (*forward correctably respects forwards*) w.r.t. V', C', N' and $\ltimes$, iff for each $p, q \in Q$, $v \in V'$, and $c \in C'$, if $p \xrightarrow{cv}{}^* q$ then there exists $r \in Q$ and $\delta \in (N')*$, such that $p \xrightarrow{\delta v}{}^* r$ and $q \ltimes r$.
4. Let $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. We say $\mathcal{T}$ satisfies the unwinding condition *fcrb* (*forward correctably respects backwards*) w.r.t. V', C', N' and $\ltimes$, iff for each $p, q \in Q$, $v \in V'$, and $c \in C'$, if $p \xrightarrow{v} q$ then there exists $r \in Q$ and $\delta \in (N')^*$, such that $p \xrightarrow{c \delta v}{}^* r$ and $q \ltimes r$.
5. Let $X \subseteq \Sigma$. We say $\mathcal{T}$ satisfies the unwinding condition *lrbe* (*locally respects backwards for enabled events*) w.r.t. X and $\ltimes$, iff whenever c is X-enabled at p, then we have $p \xrightarrow{c} q$ with $p \ltimes q$.

6. Let $X \subseteq \Sigma$, $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. We say $\mathcal{T}$ satisfies the unwinding condition *fcrbe* (*forward correctably respects backwards for enabled events*) w.r.t. X, V', C', N' and $\ltimes$, iff for each $p, q \in Q$, $v \in V'$, and $c \in C'$ X-enabled at p, if $p \xrightarrow{v} q$ then there exists $r \in Q$ and $\delta \in (N')^*$, such that $p \xrightarrow{c\delta v}{}^{*} r$ and $q \ltimes r$.

Theorem 1 **([7]).** *Let $X \subseteq \Sigma$, $V' \subseteq V$, $C' \subseteq C$, and $N' \subseteq N$. The following implications are valid.*

1. *$\mathcal{T}$ satisfies BSD if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrf w.r.t. $\ltimes$.*
2. *$\mathcal{T}$ satisfies BSI if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrb w.r.t. $\ltimes$.*
3. *$\mathcal{T}$ satisfies BSIA w.r.t X if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrbe w.r.t. X and $\ltimes$.*
4. *$\mathcal{T}$ satisfies FCD w.r.t. V', C', N' if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies fcrf w.r.t. V', C', N' and $\ltimes$.*
5. *$\mathcal{T}$ satisfies FCI w.r.t. V', C', N' if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies fcrb w.r.t. V', C', N' and$\ltimes$.*
6. *$\mathcal{T}$ satisfies FCIA w.r.t X, V', C', N' if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies fcrbe w.r.t. X, V', C', N' and $\ltimes$.*
7. *$\mathcal{T}$ satisfies D if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrf w.r.t. $\ltimes$.*
8. *$\mathcal{T}$ satisfies I if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrb w.r.t. $\ltimes$.*
9. *$\mathcal{T}$ satisfies IA w.r.t X if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrbe w.r.t. X and $\ltimes$.*
10. *$\mathcal{T}$ satisfies R if there exists an unwinding relation $\ltimes$ for $\mathcal{T}$ such that $\mathcal{T}$ satisfies lrf w.r.t. $\ltimes$.*

□

We now show that there exists a *maximal* unwinding relation, and that it is sufficient to check the unwinding conditions on this maximal relation.

The following proposition states that unwinding relations are closed under union.

Proposition 2. *Let $\ltimes_1$ and $\ltimes_2$ be unwinding relations for $\mathcal{T}$. Then $\ltimes = \ltimes_1 \cup \ltimes_2$ is also an unwinding relation for $\mathcal{T}$.*

Proof. Let $p \xrightarrow{e} q$ for $e \in (\Sigma \setminus C)$ and $p \ltimes r$ in $\mathcal{T}$. Since $p \ltimes_1 r$ and $\ltimes_1$ is an unwinding relation for $\mathcal{T}$, there exists a $t \in Q$ such that $r \xrightarrow{\delta}{}^{*} t$ with $\delta \in (\Sigma \setminus C)^*$, $\delta \upharpoonright_V = e \upharpoonright_V$, and $q \ltimes_1 t$. Hence, $q \ltimes t$. Similarly, for the case of $\ltimes_2$. □

It now follows that if we take the union of the set of all unwinding relations for $\mathcal{T}$, we obtain an unwinding relation for $\mathcal{T}$, and it is *maximal* in the sense that every other unwinding relation for $\mathcal{T}$ is contained in it. We denote the maximal unwinding relation for $\mathcal{T}$ by $\ltimes_{\mathcal{T}}$.

Let us call an unwinding condition (of the type of *lrf* etc) *upward closed* if whenever $\mathcal{T}$ satisfies the condition w.r.t. an unwinding relation $\ltimes_1$, and $\ltimes_1 \subseteq \ltimes_2$, we also have that $\mathcal{T}$ satisfies the condition w.r.t. $\ltimes_2$. Then it is easy to check that:

Proposition 3. *The conditions lrf, lrb, fcrf, fcrb, lrbe and fcrbe are all upward closed.* □

The existence of the maximal unwinding relation $\ltimes_{\mathcal{T}}$ and Proposition 3 now gives us the following result:

Lemma 4. *There exists an unwinding relation* $\ltimes$ *such that* $\mathcal{T}$ *satisfies lrf (respectively lrb, fcrf, fcrb, lrbe, fcrbe) w.r.t.* $\ltimes$*, iff* $\mathcal{T}$ *satisfies lrf (respectively lrb, fcrf, fcrb, lrbe, fcrbe) w.r.t.* $\ltimes_{\mathcal{T}}$*.* □

Thus the conditions in the unwinding theorem 1 above can equivalently be checked on the maximal unwinding relation $\ltimes_{\mathcal{T}}$.

4 Unwinding and Simulation

In this section we recall the standard notion of a simulation relation and show how to express the maximal unwinding relation as a simulation relation on an appropriate transition system.

Let us fix a Σ-labelled transition system $\mathcal{T} = (Q, s, \longrightarrow)$ for the rest of this section. A relation $\prec \subseteq Q \times Q$ is called a *simulation* relation for $\mathcal{T}$ if for every $p, q, r \in Q$, and $e \in \Sigma$, whenever $p \xrightarrow{e} q$ and $p \prec r$, we have $t \in Q$ such that $r \xrightarrow{e} t$ and $q \prec t$.

Once again it is easy to see that simulation relations are closed under finite and infinite unions, and that hence there exists a maximal simulation relation for $\mathcal{T}$, which is the union of all simulation relations for $\mathcal{T}$. We denote this maximal simulation relation for $\mathcal{T}$ by $\prec_{\mathcal{T}}$.

Algorithm 1 shows a naive algorithm for computing the maximal simulation relation $\prec_{\mathcal{T}}$ for a finite state LTS $\mathcal{T}$, which runs in time $O(mn^4)$, where m and n are the number of edges and states in $\mathcal{T}$. We define $post_e(p)$ for a state p to be the set $\{q \mid p \xrightarrow{e} q\}$.

We now show how the maximal unwinding relation $\ltimes_{\mathcal{T}}$ coincides with the maximal simulation relation $\prec_{\mathcal{T}_V}$ for an appropriately defined transition system $\mathcal{T}_V$.

The transition system $\mathcal{T}_V$ is obtained from $\mathcal{T}$ by deleting all C-labelled transitions, and replacing all N-labelled transitions by ϵ transitions, and then computing the transitive closure of the resulting graph. Warshall's algorithm (see [1]), which runs in $O(n^3)$ time can be used to compute the transitive closure of the graph. Formally we define $\mathcal{T}_V = (Q, s, \longrightarrow_V)$ where for all $v \in V$, $p \xrightarrow{v}_V q$ iff there exists $\delta, \delta' \in N^*$ such that $p \xrightarrow{\delta v \delta'}{}^{*} q$

Theorem 5. *The maximal unwinding relation* $\ltimes_{\mathcal{T}}$ *for* $\mathcal{T}$ *coincides with the maximal simulation relation* $\prec_{\mathcal{T}_V}$ *for* $\mathcal{T}_V$*.*

Algorithm 1: Computing Maximal Simulation Relation

```
Input: $\mathcal{T}$, a finite state LTS
Output: $\prec_{\mathcal{T}}$, the maximal simulation relation for $\mathcal{T}$
for $p \in Q$ do
    $sim(p) = \{q \in Q \mid$ for all $e$ enabled at $p$, $e$ is also enabled at $q\}$
end
while there are states $p, q, r$ and $e \in \Sigma$ such that $r \in post_e(p)$, $q \in sim(p)$ and $post_e(q) \cap sim(r) = \phi$ do
    $sim(p) = sim(p) \setminus \{q\}$
end
$\prec_{\mathcal{T}} = \bigcup_{q \in Q} \{\{q\} \times sim(q)\}$
```

Proof. We first show that the maximal unwinding relation $\ltimes_{\mathcal{T}}$ for $\mathcal{T}$ is a simulation relation for $\mathcal{T}_V$. Let $p \xrightarrow{n_1} p_1 \xrightarrow{n_2} p_2 ... \xrightarrow{n_k} p_k \xrightarrow{v} p_{k+1} \xrightarrow{m_1} ... \xrightarrow{m_l} q$, with $v \in V$, $n_i, m_j \in N$, for $1 \leq i \leq k$, $1 \leq j \leq l$ and $p \ltimes_{\mathcal{T}} r$ in $\mathcal{T}$. This path will result in the transition $p \xrightarrow{v}_V q$ in $\mathcal{T}_V$, due to the construction of $\mathcal{T}_V$. From the definition of the unwinding relation, there exists $t, t_i \in Q$ with $1 \leq i \leq (k+m)$ such that $r \xrightarrow{\delta_1}^* t_1 \xrightarrow{\delta_2}^* ... \xrightarrow{\delta_k}^* t_k \xrightarrow{\delta}^* t_{k+1} \xrightarrow{\gamma_1}^* ... \xrightarrow{\gamma_l}^* t$ with $\delta_i, \gamma_j \in N^*$ for $1 \leq i \leq k$, $1 \leq j \leq l$, $\delta \in (\Sigma \setminus C)^*$ and $\delta \upharpoonright_V = v$, and $q \ltimes_{\mathcal{T}} t$. This path will result in the transition $r \xrightarrow{v}_V t$ in $\mathcal{T}_V$. This implies $\ltimes_{\mathcal{T}}$ is a simulation relation for $\mathcal{T}_V$. Recall that $\prec_{\mathcal{T}_V}$ is the union of all the simulation relations for $\mathcal{T}_V$. Hence $\ltimes_{\mathcal{T}} \subseteq \prec_{\mathcal{T}_V}$.

We show that the maximal simulation relation $\prec_{\mathcal{T}_V}$ for $\mathcal{T}_V$ is an unwinding relation for $\mathcal{T}$. Let $p \xrightarrow{e} q$ with $e \in (\Sigma \setminus C)$ in $\mathcal{T}$, $p \ltimes_{\mathcal{T}} r$ and $p \prec_{\mathcal{T}_V} r$ in $\mathcal{T}_V$. If $e \in V$, from the definition of the simulation relation, there exists a $t \in Q$ such that $r \xrightarrow{v}_V t$ in $\mathcal{T}_V$ and $q \prec_{\mathcal{T}_V} t$. This means that there exists a path labelled $\delta v \delta'$ with $\delta, \delta' \in N^*$ from r to t in $\mathcal{T}$. If $e \in N$, again from the definition of the simulation relation, for all paths labelled $n\delta v \delta'$ with $\delta, \delta' \in N^*$, $v \in V$ from p, we have a path labelled $\gamma v \gamma'$ with $\gamma, \gamma' \in N^*$ from r in $\mathcal{T}$. This implies for all $\delta v \delta'$ path from q, there is a path labelled $\gamma v \gamma'$ from r. So, $q \prec_{\mathcal{T}_V} r$. Hence for each $e \in (\Sigma \setminus C)$, $p, q, r \in Q$ with $p \xrightarrow{e} q$ in $\mathcal{T}$ and $p \prec_{\mathcal{T}_V} r$, we have $t \in Q$ such that $r \xrightarrow{\delta}^* t$ with $\delta \in N^*$ in $\mathcal{T}$ and $\delta \upharpoonright_V = e \upharpoonright_V$ and $q \prec_{\mathcal{T}_V} t$. Therefore $\prec_{\mathcal{T}_V}$ is an unwinding relation. Recall that $\ltimes_{\mathcal{T}}$ is the union of all the unwinding relations for $\mathcal{T}$. Hence $\prec_{\mathcal{T}_V} \subseteq \ltimes_{\mathcal{T}}$.

Hence, the maximal unwinding relation $\ltimes_{\mathcal{T}}$ for $\mathcal{T}$ coincides with the maximal simulation relation $\prec_{\mathcal{T}_V}$ for $\mathcal{T}_V$. □

5 Checking Unwinding Conditions

In this section, we make use of the Theorem 5 and check the unwinding conditions *lrf*, *lrb*, *fcrf*, *fcrb*, *lrbe* and *fcrbe* w.r.t. the maximal simulation relation $\prec_{\mathcal{T}_V}$ for a finite state LTS $\mathcal{T}$. The procedure to check the unwinding condition *lrf* is given below. The other unwinding conditions *lrb*, *fcrf*, *fcrb*, *lrbe* and *fcrbe* can also be checked in a similar way. Let m and n be the number of edges and states in $\mathcal{T}$. Let $X \subseteq \Sigma$, $V' \subseteq V$, $C' \subseteq C$ and $N' \subseteq N$.

1. Construct $\mathcal{T}_V$ using Warshall's algorithm [1] in $O(n^3)$ time.
2. Compute the maximal simulation relation $\prec_{\mathcal{T}_V}$ for $\mathcal{T}_V$ using the Algorithm 1.
3. Check the unwinding conditions *lrf* w.r.t. $\prec_{\mathcal{T}_V}$.

Now we describe the way to check all the unwinding conditions w.r.t. $\prec_{\mathcal{T}_V}$.

For every $p \xrightarrow{c} q$ with $c \in C$ in $\mathcal{T}$, if $q \prec_{\mathcal{T}_V} p$ then $\mathcal{T}$ satisfies *lrf* w.r.t. $\prec_{\mathcal{T}_V}$. For every $p \in Q$, $c \in C$, if there exists some $q \in Q$ with $p \xrightarrow{c} q$ in $\mathcal{T}$ and $p \prec_{\mathcal{T}_V} q$ then $\mathcal{T}$ satisfies *lrb* w.r.t. $\prec_{\mathcal{T}_V}$. The time complexity for checking *lrf* and *lrb* is $O(m)$ and $O(n|C|)$ respectively.

To check whether $\mathcal{T}$ satisfies *fcrf* w.r.t. $\prec_{\mathcal{T}_V}$, we construct adjacency matrices A_v and B_v for every $v \in V'$ such that $A_v[p,q] = 1$ iff there is a path labelled cv for some $c \in C'$ from state p to q, and $B_v[p,q] = 1$ iff there is a path of δv for some $\delta \in (N')^*$ from p to q. If for every $A_v[p,q] = 1$, there exists some $q' \in Q$ with $B_v[p,q'] = 1$ and $q \prec_{\mathcal{T}_V} q'$, then $\mathcal{T}$ satisfies *fcrf* w.r.t. $\prec_{\mathcal{T}_V}$. To check whether $\mathcal{T}$ satisfies *fcrb* w.r.t. $\prec_{\mathcal{T}_V}$, we construct adjacency matrices A_v and B_v for every $v \in V'$ such that $A_v[p,q] = 1$ iff there is a edge labelled v from state p to q, and $B_v[p,q] = 1$ iff there is a path labelled $c\delta v$ for some $\delta \in (N')^*$, $c \in C'$ from p to q. If for every $A_v[p,q] = 1$, there exists some $q' \in Q$ with $B_v[p,q'] = 1$ and $q \prec_{\mathcal{T}_V} q'$, then $\mathcal{T}$ satisfies *fcrb* w.r.t. $\prec_{\mathcal{T}_V}$. A_v and B_v can be computed in $O(n^3)$ time, since it involves computation of matrix product and transitive closure. The time complexity for checking *fcrf* and *fcrb* after the construction of A_v and B_v for every $v \in V'$ is $O(|V'|n^3)$.

To check whether some $c \in C$ is X-enabled at p, we construct $\mathcal{T}'$ with states containing two components: the first component keeps track of a state from $\mathcal{T}$, while the second keeps track of a set of states of $\mathcal{T}$ that are reachable by words that are X equivalent to the current word being read.

More precisely, let $\mathcal{M}$ be a transition system obtained by replacing non X-edges in $\mathcal{T}$ with ϵ edges. Then $\mathcal{T}' = (Q', s', \longrightarrow')$ where $Q' = (Q \times 2^Q) \cup Q$; $s' = (s, S)$ where $S = \{q \in Q \mid s \xrightarrow{\epsilon}{}^* q \text{ in } \mathcal{M}\}$; $\longrightarrow'$ is given below:

$$\begin{array}{lll}
(p,T) \overset{e}{\longrightarrow'} (q,T) & \text{if} & p \xrightarrow{e} q \text{ and } e \notin X \\
(p,T) \overset{e}{\longrightarrow'} (q,U) & \text{if} & p \xrightarrow{e} q, e \in X, \text{ and} \\
 & & U = \{r \mid \exists t \in T, t \xrightarrow{e}{}^* r \text{ in } \mathcal{M}\} \\
(p,T) \overset{c}{\longrightarrow'} p & \text{if} & \exists t \in T, q \in Q : t \xrightarrow{c} q \text{ and } c \in C; \\
p \overset{e}{\longrightarrow'} q & \text{if} & p \xrightarrow{e} q \text{ and } e \notin C.
\end{array}$$

A $c \in C$ is X-enabled at p iff for (p,T) in $\mathcal{T}'$, there exists a $t \in T$ and $r \in Q$ with $t \xrightarrow{c} r$. Some $c \in C$ can be idenfied as X-enabled at p in $2^{O(n)}$ time.

If for every $p \in Q$ and for every $c \in C, X$-enabled at p, there exists $q \in Q$ with $p \xrightarrow{c} q$ and $p \prec_{\mathcal{T}_V} q$, then $\mathcal{T}$ satisfies *lrbe* w.r.t. $\prec_{\mathcal{T}_V}$. If for every $p \xrightarrow{v} q$ with $v \in V'$ and for every $c \in C', X$- enabled at $p \in Q$, there exists $q' \in Q$ with

$p \xrightarrow{c\delta v}{}^{*} q'$ for some $\delta \in (N')^*$ and $q \prec_{\mathcal{T}_V} q'$, then $\mathcal{T}$ satisfies *fcrbe* w.r.t $\prec_{\mathcal{T}_V}$. The time complexity to check for *lrbe* and *fcrbe* is $|\Sigma|2^{O(n)}$.

6 Complexity Analysis

The following table gives the comparision for checking BSP's using the model checking approach described in [2] and the unwinding conditions approach given in this paper. Here m and n are the number of edges and number of states in the given transition system $\mathcal{T}$ respectively. The time complexities given under the unwinding conditions heading are when used with the naive Algorithm 1 for computing the maximal simulation relation.

BSP's	Unwinding Conditions	Model Checking
R	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
D	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
I	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
IA	$\|\Sigma\|2^{O(n)}$	$2^{O(n^2\|\Sigma\|)}$
BSD	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
BSI	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
$BSIA$	$\|\Sigma\|2^{O(n)}$	$2^{O(n^2\|\Sigma\|)}$
FCD	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
FCI	$O(\|\Sigma\|n^6)$	$2^{O(n^2\|\Sigma\|)}$
$FCIA$	$\|\Sigma\|2^{O(n)}$	$2^{O(n^2\|\Sigma\|)}$
SR	-	$O(mn^2\|\Sigma\|)$
SD	-	$O(mn^2\|\Sigma\|)$
SI	-	$O(mn^2\|\Sigma\|)$
SIA	-	$\|\Sigma\|^2 2^{O(n)}$

Thus, the unwinding techniques provide a more efficient way for checking BSP's. Though the unwinding techniques are incomplete in general, it will be useful for checking large systems. The running time of the unwinding techniques can be improved by using the ideas of [5, 10].

References

1. Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms.* McGraw-Hill Higher Education, 2001.
2. Deepak D'Souza, Raghavendra K R, and Barbara Sprick. An automata based approach for verifying information flow properties. In *Proceedings of the second workshop on Automated Reasoning for Security Protocol Analysis (ARSPA 2005)*, volume 135, pages 39–58, 2005.
3. J. A. Goguen and J. Meseguer. Security policies and security models. In *Proc. IEEE Symp. on Security and Privacy*, pages 11–20, April 1982.
4. Joseph A. Goguen and José Meseguer. Unwinding and inference control. In *IEEE Symposium on Security and Privacy*, pages 75–87, 1984.

5. Monika Rauch Henzinger, Thomas A. Henzinger, and Peter W. Kopke. Computing simulations on finite and infinite graphs. In *IEEE Symposium on Foundations of Computer Science*, pages 453–462, 1995.
6. Heiko Mantel. Possibilistic Definitions of Security – An Assembly Kit. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop*, pages 185–199, Cambridge, UK, July 3–5 2000. IEEE Computer Society.
7. Heiko Mantel. *A Uniform Framework for the Formal Specification and Verification of Information Flow Security.* PhD thesis, Universität des Saarlandes, 2003.
8. John McLean. A general theory of composition for trace sets closed under selective interleaving functions. In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 79 – 93. IEEE Computer Society Press, 1994.
9. Colin O'Halloran. A calculus of information flow. In *Proceedings of the European Symposium on Research in Computer Security, ESORICS 90*, 1990.
10. Robert Paige and Robert E. Tarjan. Three partition refinement algorithms. *SIAM J. Comput.*, 16(6):973–989, 1987.
11. John Rushby. Noninterference, transitivity, and channel-control security policies. Technical report, dec 1992.
12. A. Zakinthinos and E. S. Lee. A general theory of security properties. In *SP '97: Proceedings of the 1997 IEEE Symposium on Security and Privacy*, page 94, Washington, DC, USA, 1997. IEEE Computer Society.