SIGALI User’s manual

Hervé Marchand, Éric Rutten & Michel Le Borgne

March 30, 2004

Abstract

SIGALI is a model-checking tool-based which manipulates Polynomial Dynamical Systems (PDS) (that can be seen as an implicit representation of an automaton) as intermediate models for discrete event systems. It offers functionalities for verification of reactive systems and discrete controller synthesis. It is developed jointly by Espresso1 and Vertecs2.

The techniques used consist in manipulating the system of equations instead of the sets of solution, which avoids the enumeration of the state space. Each set of states is uniquely characterized by a polynomial and the operations on sets can be equivalently performed on the associated polynomials. Therefore, a wide spectre of properties, such as liveness, invariance, reachability and attractivity can be checked. Many algorithms for computing predicates states are also available.

1 The model checker SIGALI

1.1 Basic facts about SIGALI

The theory of Polynomial Dynamical Systems uses classical tools in algebraic geometry, such as ideals, varieties and comorphisms [?]. The techniques consist in manipulating the system of equations instead of the sets of solutions, which avoids enumerating the state space.

1.1.1 The mathematical framework : an Overview

Let \( Z = \{Z_1, Z_2, \ldots, Z_p\} \) be a set of \( p \) variables and \( \mathbb{Z}/3\mathbb{Z}[Z] \) be the ring of polynomials with variables \( Z \). Thus \( \mathbb{Z}/3\mathbb{Z}[Z] \) is the set of all polynomials of \( p \) variables. Given an element of \( \mathbb{Z}/3\mathbb{Z}[Z] \), \( P(Z_1, Z_2, \ldots, Z_p) \) (shortly \( P(Z) \)), we associate its set of solutions \( \text{Sol}(P(Z)) \) as follows:

\[
\text{Sol}(P) \overset{\text{def}}{=} \{(z_1, \ldots, z_k) \in (\mathbb{Z}/3\mathbb{Z})^k | P(z_1, \ldots, z_k) = 0\}
\] (1)

It is worthwhile noting that in \( \mathbb{Z}/3\mathbb{Z}[Z] \), \( Z_1^n - Z_1, \ldots, Z_k^n - Z_k \) evaluate to zero. Then for any \( P(Z) \in \mathbb{Z}/3\mathbb{Z}[Z] \), one has \( \text{Sol}(P) = \text{Sol}(P + (Z_1^n - Z_1)) \). We then introduce the quotient ring of polynomial functions \( A[Z] = \mathbb{Z}/3\mathbb{Z}[Z]/\langle Z_1^n - Z_1 \rangle \), where all polynomials \( Z_1^n - Z_1 \) are identified to zero, written for short \( Z_1^n = Z_1 \). A[Z] can be regarded as the set of polynomial functions with coefficients in \( \mathbb{Z}/3\mathbb{Z} \), for which the degree in each variable is lower than 2. [?] showed how to define a representative of \( \text{Sol}(P) \) called the canonical generator. Our techniques will rely on the following: For all polynomials \( P_1, P_2, P \in \mathbb{Z}/3\mathbb{Z}[Z] \):

- \( \text{Sol}(P_1) \subseteq \text{Sol}(P_2) \) whenever \( (1 - P_1^2) * P_2 \equiv 0 \). (inclusion)
- \( \text{Sol}(P_1) \cap \text{Sol}(P_2) = \text{Sol}(P_1 \oplus P_2) \) (intersection), where
  \[
P_1 \oplus P_2 \overset{\text{def}}{=} (P_1^2 + P_2^2)^2
\] (2)
- \( \text{Sol}(P_1) \cup \text{Sol}(P_2) = \text{Sol}(P_1 \ast P_2) \) (union) and \((\mathbb{Z}/3\mathbb{Z})^m \setminus \text{Sol}(P) = \text{Sol}(1 - P^2) \) (complementary).

\[\text{Espresso Web Site: \url{http://www.irisa.fr/espresso}}\]
\[\text{Vertecs Web Site: \url{http://www.irisa.fr/vertecs}}\]
1.1.2 Dynamical systems: Basics

A dynamical system can be mathematically modelled as a system of polynomial equations over \( \mathbb{Z}/3\mathbb{Z} \) (the Galois field of integers modulo 3) of the form:

\[
\begin{align*}
Q(X, Y) &= 0 \\
X' &= P(X, Y) \\
Q_0(X) &= 0
\end{align*}
\]  

(3)

where,

- \( X \) is the set of \( n \) state variables, represented by a vector in \( (\mathbb{Z}/3\mathbb{Z})^n \);
- \( Y \) is the set of \( m \) event variables, represented by a vector in \( (\mathbb{Z}/3\mathbb{Z})^m \);
- \( Q(X, Y) = 0 \) is the constraint equation;
- \( X' = P(X, Y) \) is the evolution equation. It can be considered as a vectorial function from \( (\mathbb{Z}/3\mathbb{Z})^{n+m} \) to \( (\mathbb{Z}/3\mathbb{Z})^n \); and,
- \( Q_0(X) = 0 \) is the initialization equation.

We now explain how one can use the model-checker Sigali, in order to analyze the obtained polynomial dynamical system.

1.2 The Sigali commands & Operations

1.2.1 General Commands

Starting and exiting  The Sigali environment can be started by the \texttt{sigali} command. A prompt \texttt{Sigali:} appears. To quit, one can use the Sigali command \texttt{quit();}

\texttt{quit();}

Loading the file of a model  The \texttt{.z3z} (.lib) file which contains the model of the system (or any other Sigali files, can be loaded by using the \texttt{load} or the \texttt{read} command. For example, in case of a file \texttt{filename.z3z} the command is:

\texttt{read("filename");}

Trace  By the \texttt{trace} command it is possible to save in a file all the commands executed and results obtained in the Sigali environment:

\texttt{trace("filename"); opens the file for trace.}

\texttt{fintrace();} closes the current trace file.

All commands executed (and the corresponding responses) in between are saved in the trace file.

Execution time  Sigali allows the measurement of the time taken for each computation.

\texttt{chrono(true);} starts the clock. After each subsequent command, the time taken for the computation is displayed.

\texttt{chrono(false);} stops the clock.

1.2.2 Symbols and declarations

A symbol or an identifier can be assigned to an expression in the following format:

\texttt{symbol : <expression>;}  

For example:

\texttt{p : a^2 * b + c^2;}  

assigns the identifier \( p \) to the expression \( a^2b + c^2 \).

Variables can be declared by the command: \texttt{declare} or \texttt{ldeclare}. For example:

\texttt{declare(a,b,c,d);} takes one or more parameters.
- `declare([a,b,c,d]);` takes only one parameter (as a list).

The order of the variables corresponds to the order of declaration. For example, in the previous example, the order is $a < b < c < d$.

The command `indeter();` lists all the indeterminate symbols.

In order to declare variables in a given order, one can use the commands `declare_after`, `declare_first` or `declare_suff`. For example, if the variables $x < y < z$ are already declared, the command

- `declare_after(a,b,c)` will declare the variables according to the following order: $x < y < z < a < b < c$
- $a < b < c < x < y < z$ if you use `declare_first(a,b,c)`.
- `declare_suff([a,b,c])` will declare the variables $a_1, b_1, c_1$, in the following order: $a < a_1 < b < b_1 < c < c_1$.

We can manipulate list of variables as follows: If $L_1$ and $L_2$ are two lists of variables, then
- $L : union_lvar(L_1,L_2)$ is the list of variables which contains the variables of $L_1$ and $L_2$.
- $L : inter_lvar(L_1,L_2)$ performs the intersection of the two lists.
- $L : comp_lvar(L_1)$ is the complementary list according to all the declared variable.
- $L : diff_lvar(L_1,L_2)$ is equal to $L_1 \setminus L_2$
- given a list of variables $L$ and a variable $a$, `belong_lvar(a,L);` is true whenever $a \in L$

### 1.2.3 Polynomials and equations

#### Polynomials

We can write polynomial expressions, lists of polynomials, etc. All the usual polynomial operations are also available (+, -, *, ....). For example, the polynomial $a^2(-b-b^2)$ is written as $P : a^2*(-b-b^2)$.

A symbol can be assigned to a polynomial:

- $P : a^2*(-b-b^2);$  

Note that the variables $a, b$ have to be declared first in order to specify this polynomial.

Now, given a polynomial $P$ over the variables $L$,

- `varof(P)` gives access to the variable set of $P$
- `nbvar(P)` gives the number of variables of $P$
- `nb_solution(P,X)` gives the number of solution of the equation $P(X) = 0$, where $X$ is a set of variables that must contains `varof(P)`.

#### Representation of polynomials

A variable or polynomial can only take values belonging to $\mathcal{F}_3 = \{-1, 0, 1\}$. In Sigali, a polynomial is represented by means of a Ternary Decision Diagram (TDD) which is an extension of a Binary Decision Diagram (BDD). In a TDD, each non-leaf node represents a variable and each leaf node is a value of the polynomial. An arbitrary ordering of the variables must be done to facilitate the assignment of a node to a variable. Further, each non-leaf node has 3 edges emanating from it, labelled by the 3 possible values: $\{-1, 2\}$, $0$, $1$ that the corresponding variable may take. So, each path from the root to a leaf assigns a unique sequence of values to the variables and the value of the leaf gives the value of the polynomial for that particular assignment. For example, if $p$ is the polynomial $a^2b + c^2$, and the ordering is $a < b < c$, then $p$ is represented by Sigali as follows (The TDD representation of $p$ is shown in Fig. 6):
Figure 1: TDD representation of the polynomial $a^2b + c^2$.

In order to avoid repetitions in listing, portions occurring more than once are labelled as $\#n\#$ ($n = 0, 1, 2, ...$). These repetitions tend to occur when two or more edges enter a non-leaf node in the TDD. While reading the TDD, the label subformula $n$, wherever it occurs, is to be replaced by the portion labelled $\#n\#$.

The command size($P$); gives the number of nodes of the TDD that encodes the polynomial $P$.

Lists
The list of polynomials, equations, etc. are written as follows: [$a+b, c+d$] is a list of polynomials and [$a+b=x, a^2=b^2$] is an equation system. Of course, a symbol can be assigned to a list or an equation system as well. For example:

- list : [a + b, a, b, 0, 1];
- equations : [a ^2 = b ^2, c = a and b];
If \( p \) is a polynomial, \( lp1 \) and \( lp2 \) are two lists of polynomials, \( lvar1 \) and \( lvar2 \) are two lists of variables, and \( lconst \) is a list of constants (with values 0, 1 or -1), then:

- eval\( (p, [a, b, c], [0, 1, -1]) \):
  evaluates the polynomial \( p \) after substituting 0, 1 and -1 for \( a \), \( b \) and \( c \) respectively. Of course these variables must occur in \( p \).
  
  Note that we can use the command init\( lconst \) to declare the list of constants, e.g.
  
  \[ lconst : \text{init}\_lconst(3, 0) \]
  is a list of 3 elements that are equal to 0, i.e. \( lconst = [0, 0, 0] \).

- rename\( (p, lvar1, lvar2) \):
  replaces in \( p \), the \( i \)th variable of \( lvar1 \) by the \( i \)th variable of \( lvar2 \).

- subst\( (p, lvar1, lp1) \):
  replaces in \( p \), the \( i \)th variable of \( lvar1 \) by the \( i \)th polynomial of \( lp1 \).

In case of the functions:

- \_eval\( (lp1, lvar1, lconst) \);
- \_rename\( (lp1, lvar1, lvar2) \);
- \_subst\( (lp1, lvar1, lp2) \);

the first argument is a list of polynomials instead of one polynomial and they perform the same function as their counterparts for each polynomial of the list.

### 1.2.4 (System of) Polynomials manipulation

The canonical generator of a polynomial system given by a list of polynomials can be computed by the function \( \text{gen} \). The command is \( \text{gen}(lpoly) \) where \( lpoly \) is a list of polynomials. For example:

- \( \text{gen}([a + b - c, a^2 - 1]) \);

  gives the canonical generator of the polynomial system given by the two polynomials \( a + b - c \) and \( a^2 - 1 \). The previous command can also be given as:

- \( \text{gen}([a + b = c, a^2 = 1]) \);

  If \( P_1 = a+b-c \) and \( P_2 = a^2 - 1 \), then the previous command will compute the polynomial \( P = P_1 \oplus P_2 = (P_1^2 + P_2^2)^2 \), which entails that the solution of \( P \) will be the solution that are common to \( P_1 \) and \( P_2 \).

- equal\( (p1, p2) \) compares two polynomials \( p1 \) and \( p2 \) and test whether they are equal or not.

**Complementation.** Let \( g \) be a polynomial and \( V \) its set of solutions, then the generator of the complement of \( V \) is obtained by:

- \( \text{complementary}(g) \);

**Intersection.** Let \( p1 \) and \( p2 \) be two polynomials and \( V1 \) and \( V2 \) be the corresponding set of solutions, then:

- \( \text{intersection}(p1, p2) \);

  is the canonical generator of \( V1 \cap V2 \). The number of arguments can be greater than 2. For example one can write \( \text{intersection}(p1, p2, p3, p4) \);

**Union.** Let \( p1 \) and \( p2 \) be two polynomials and \( V1 \) and \( V2 \) be the corresponding set of solutions, then:

- \( \text{union}(p1, p2) \);

  is the canonical generator of \( V1 \cup V2 \). As in case of \( \text{intersection} \), the number of arguments can be greater than 2.

**Tests of inclusion** Let \( p1 \) and \( p2 \) be two polynomials and \( V1 \) and \( V2 \) be the corresponding set of solutions, then:

- \( \text{subset}(g1, g2) \);

  is True if and only if \( V1 \subseteq V2 \).
1.2.5 Existential/universal variable elimination

Given a polynomial $P$ over the variables $X, Y$, then we define the Existential/universal variable elimination as follows

- $P' : \exists(Y, P)$ is a polynomial such that $\text{Sol}(P') = \{x| \exists y, P(x, y) = 0\}$
- $P' : \forall(X, P)$ is a polynomial such that $\text{Sol}(P') = \{x| \forall y, P(x, y) = 0\}$

1.2.6 Automatic reordering

The `set_reorder(1)` (exists also with the parameter 2) performs an automatic variable reordering using heuristics. This is very useful to decrease the size of the TDD. `set_reorder(0)` stops the automatic reordering.

1.3 Systems and Processes

SIGALI distinguishes between two categories of dynamical systems: systems and processes. Systems are general dynamical systems in which null transitions (basically self loops) are taken into account even when all the signals are absent, whereas in a process, null transitions are excluded i.e. No transition can take place in the absence all the signals. Dynamical systems can be automatically derived from either SIGNAL programs or Matou programs thus allowing to allowing the modeling of reactive systems by means of Mode Automata.

From a Signal/Matou programs, a file is automatically generated. it contains the following data:

- `events` is a list of variables encoding the event variables
- `states` is a list of variables which encodes the states variables
- `controllables` is a subset of `events` and corresponds to the controllable event variables (See section 3 for more details).
- `evolutions` is a list of polynomials (one for each state variables) which corresponds to the evolution of each state variables.
- `initialisations` is a list of polynomials (the solutions of this polynomial systems correspond to the initial states of the system).
- `constraints` is also a list of polynomial encoding the constraints part of the polynomial dynamical system (i.e. $Q(X, Y) = 0$).

If one want to construct from these sets a process (respectively a system), the following command has to be used.

- `syst : processus(events, states, evolutions, initialisations, constraints, controllables);`

Conversely, if `syst` is a dynamical system, as described by (3), constructed by the command `system` or `process`, then the 6 components of `syst` can be accessed by:

- `event_var(syst);` : returns the event variable set of a system, i.e. the vector $Y$
- `state_var(syst);` : returns the state variable set of a system, i.e. the vector $X$
- `evolution(syst);` : returns the vector of polynomials encoding the evolution equations, i.e. $[P_1(X, Y), \ldots, P_n(X, Y)]$
- `initial(syst);` : returns the polynomial encoding the initial states of the systems
- `constraint(syst);` : returns the constrains polynomial $Q(X, Y)$
- `controllable_var(syst);` : returns the controllable variable set of a system, i.e. the vector $U$ with $U \subseteq Y$ (See section 3 for more details).

1.3.1 Some special sets

If $g$ is the canonical generator of a set of states $E$, then:

- `pred(syst, g);` is the canonical generator of the set of predecessors of $E$.
- `all_succ(syst, g);` is the canonical generator of the set of states, such that all successors belong to $E$. 

6
• adm_events(syst, g); is the canonical generator of the set of events admissible in $E$.

If $g$ is the canonical generator of a set of events $F$, then:
• adm_states(syst, g);
  is the canonical generator of the set of states compatible with at least one of the events in $F$.

1.3.2 Implicit System

Starting from a system modeled as a PDS $S$ as described in Equation System (3), for some particular analysis, it is important to have access to the implicit corresponding implicit PDS of the form

\[
\begin{align*}
R(X, Y, X') &= 0 \\
Q_0(X_0) &= 0
\end{align*}
\] (4)

The Sigali function that gives access to this new system is implicit_sys(syst). The result is an I-PDS (for implicit PDS). From a structure point of view, it is a 5-tuple $(X, X', Y, R, Q_0)$ and the functions that gives access to the components of this I-PDS are respectively state_var_I(), state_var_next_I(), event_var_I(), trans_rel_I(), initial_I(), "controllable_var_I()".

y loading the library Orbite.lib, you have access to the two following commands:

• P : Orbite(S_Imp); returns the set of reachable states of the implicit system $S_{Imp}$

• S_I : Pruned((S_Imp, Orbite); is an implicit Dynamical system, where all the states are reachable.

1.4 Fix-point Computation & Function definition

Fix point computation can also be performed. For example, given :

\[
\begin{align*}
p_0 &= 0 \\
p_{i+1} &= p^2 + 1
\end{align*}
\]

the corresponding expression in Sigali is

\[
\text{loop x=x^2+1 init 0;}
\]

Of course, such sequences do not always converge. This is not checked by the system.

New function construction. Starting from the existing functions, it is also possible to define new functions. The syntax is the following:

\[
def f(x, y, z):
\]

\[
\text{with}
\]

\[
\text{intern}_1 = \text{sigali expression},
\text{intern}_2 = \text{sigali expression}
\]

\[
\text{Sigali body of the function ;}
\]

For example, assume we want to compute the set of reachable states from Sol(P) in one step of an implicit system $S_I$. The corresponding function succ(P) is the following:

\[
def \text{succ}(P):
\]

\[
\text{with}
\]

\[
X = \text{state_var_I}(S_I),
X_{\text{Next}} = \text{state_var_next_I}(S_I),
Y = \text{event_var_I}(Y),
Rel = \text{trans_rel_I}(S_I)
\]

\[
\text{do}
\]

\[
\text{rename(exist}(X, \text{intersection}(P, \text{exist}(Y, Rel)), X_{\text{Next}}, X));
\]
1.5 Cost functions

**Sigali** also offers the possibility to manipulate integers. Let \( X = (x_1, \ldots, X_n) \) be declared variables of the system. Then, a cost function is a map from \((\mathbb{Z}/3\mathbb{Z})^n\) to \( \mathbb{N} \), which associates to each \( x = (x_1, \cdots, x_n) \) of \((\mathbb{Z}/3\mathbb{Z})^n\) some integer \( k \). When \( f(x) \) is not defined then we assume that \( f(x) = \infty \). To encode these functions, we make the use of the ADD (Arithmetic decision diagrams). The ADD are similar to the TDD expect that we attach integers to the leaves of the ADD. For example, let \( X < Y \) be two variables in \( \mathbb{Z}/3\mathbb{Z} \) and \( f \) a cost function such that

<table>
<thead>
<tr>
<th>X</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>-1</th>
<th>-1</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>f</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>6</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>8</td>
<td>3</td>
</tr>
</tbody>
</table>

Then the ADD that represents the function \( f \) is given by the graph of Figure 2:

![Figure 2: Exemple d’un ADD](image)

In order to build and manipulate cost functions, the following **Sigali** operations are available.

- \( \text{a\_const}(n) \) build the constant function equal to the integer \( n \)
- \( \text{a\_var}(X,n1,n2,n3) \): given a declared variable \( X \) and 3 integers, \( f\text{-a\_var}(X,n1,n2,n3) \) build the cost function such that
  
  \[
  \begin{align*}
  X = 1 & \rightarrow c_i(X) = a \\
  X = -1 & \rightarrow c_i(X) = b \\
  X = 0 & \rightarrow c_i(X) = c
  \end{align*}
  \]

- Given two cost functions \( f_1 \) and \( f_2 \), one can perform the sum and the product of \( f_1 \) and \( f_2 \) by simply using the classical operators + and *.
- \( \text{a\_min}(f_1,f_2) \) is such that \( \forall x \in \mathbb{Z}/3\mathbb{Z}^n, \text{a\_min}(f_1(x),f_2(x)) = \min(f_1(x),f_2(x)) \)
- \( \text{a\_max}(f_1,f_2) \) is such that \( \forall x \in \mathbb{Z}/3\mathbb{Z}^n, \text{a\_max}(f_1(x),f_2(x)) = \max(f_1(x),f_2(x)) \)
- \( \text{a\_part}(P,f1,f2,f3) \) build a cost function such that \( \text{a\_part}(P,f1,f2,f3)(x) = f1 \) if \( P(x)=0 \), \( f2 \) if \( P(x)=1 \) and \( f3 \) if \( P(x)=-1 \)
- \( \text{a\_margmin}(f,Y) \), given a cost function \( f \) defined over \( X \cup Y \), \( \text{a\_margmin}(f,Y) \) is a function, say \( f' \) over the variables \( X \) such that \( f'(X) = \min_Y(f(X,Y)) \), i.e. \( \forall y, f'(x) < f(x,y) \)
- \( \text{a\_margmax} \) (same as \( \text{a\_margmin} \) but with the max)
- \( \text{P: a\_min\text{\_}inv}(f,n) \) is a polynomial such that \( P(x) = 0 \Leftrightarrow f(x) = n \)
- \( \text{P: a\_max\text{\_}inv}(f) \) is the minimum value taken by \( f \) and \( \text{a\_min\text{\_}inv} \) is the maximum value taken by \( f \)
- \( \text{P: a\_inf}(f,n) \) is a polynomial such that \( P(x) = 0 \Leftrightarrow f(x) \leq n \) (\( \text{a\_sup} \) is also defined)
- \( \text{R: a\_cost2rel}(f1,f2) \). Given two cost functions over \( X1 \) and \( X2 \) (with the same cardinality) \( \text{a\_cost2rel}(f1,f2) \) is a polynomial \( R(X1,X2) \) such that \( R(x1,x2) = 0 \Leftrightarrow f1(x1) \leq f2(x) \).

2 Verification of systems using **Sigali**

**Sigali** provides certain functionalities for the verification of the properties of a dynamical system.
2.1 Liveness

Definition: A dynamical system is **alive** if \( \forall x, y \) such that \( Q(x, y) = 0, \exists y' \) such that \( Q(P(x, y), y') = 0 \).

In other words, a system is **alive** if it contains no sink states.

If \( \text{syst} \) is a system or a process, then:

- \( \text{alive}(\text{syst}) \);

is True if and only if \( \text{syst} \) is **alive**.

2.2 Safety Properties

2.2.1 Invariance

Definition: A set of states \( E \) is invariant for a dynamical system if \( \forall x \) in \( E \) and \( \forall y \) admissible in \( x \), the successor state \( x' = P(x, y) \) is also in \( E \).

If \( \text{syst} \) is a dynamical system and \( g \) is the canonical generator polynomial of a set of states \( E \),

- \( \text{invariant}(\text{syst}, g) \);

is True if and only if \( E \) is invariant for \( \text{syst} \).

For example, in case of the process `double.m`, one can specify a property \( \text{pr_eq}: [\text{etat}_1 = \text{etat}_2] \); The invariance of this property can then be tested by the command:

- \( \text{invariant}(\text{pf}, \text{gen}(\text{pr_eq})) \);

where \( \text{pf} \) is the process constructed by the command `system`.

2.2.2 Invariance under control

Definition: A set of states \( E \) is control-invariant for a dynamical system if \( \forall x \) in \( E \), there exists an event \( y \) such that \( Q(x, y) = 0 \) and the successor state \( x' = P(x, y) \) is also in \( E \).

If \( \text{syst} \) is a dynamical system and \( g \) is the canonical generator polynomial of a set of states \( E \),

- \( \text{Invariant\_under\_control}(\text{syst}, g) \);

is True if and only if \( E \) is control-invariant for \( \text{syst} \).

2.2.3 Greatest (control-)invariant subset

Given a set of states \( E \), there exists a set \( F' \) which is the greatest (control-)invariant subset of \( E \). If \( \text{syst} \) is a dynamical system and \( g \) is the canonical generator polynomial of \( E \), then:

- \( \text{greatest\_inv}(\text{syst}, g) \);
- \( \text{greatest\_c\_inv}(\text{syst}, g) \);

gives the canonical generator of \( F' \).

2.3 Reachability Properties

2.3.1 Reachability

Definition: A set of states \( E \) is reachable if \( \forall x \in E \) there exists a trajectory starting from the initial states that reaches \( x \).

If \( \text{syst} \) is a dynamical system and \( g \) is the canonical generator polynomial of a set of states \( E \),

- \( \text{Reachable}(\text{syst}, g) \);

is True if and only if \( E \) is reachable from the initial states of \( \text{syst} \).

2.3.2 Attractivity

Definition: A set of states \( F \) is attractive for a set of states \( E \) if \( \forall y \) trajectory initialized on \( E \) reaches \( F \). If \( \text{syst} \) is a dynamical system and \( g \) is the canonical generator polynomial of a set of states \( E \),

- \( \text{Attractivity}(\text{syst}, g) \);

is True if and only if \( E \) is Attractive from the initial states of \( \text{syst} \).
3 Synthesis of controllers using Sigali

3.1 Essentials of the control synthesis problem

For controllable polynomial dynamic systems, the set of events $Y$ can be partitioned into two sets $Y$ and $U$, where,

- $Y$ is the set of uncontrollable events,
- $U$ is the set of controllable events.

The PDS can now be written as:

\[
\begin{align*}
Q(X,Y,U) & = 0 \\
X' & = P(X,Y,U) \\
Q_0(X) & = 0
\end{align*}
\]

Let $n$, $m$, and $p$ be the respective dimensions of $X$, $Y$, and $U$. The trajectories of a controlled system are sequences $(x_t, y_t, u_t)$ in $(\mathbb{Z}/\mathbb{Z})^{n+m+p}$ such that $Q_0(x_0) = 0$ and, for all $t$, $Q(x_t, y_t, u_t) = 0$ and $x_{t+1} = P(x_t, y_t, u_t)$. The events $(y_t, u_t)$ include an uncontrollable component $y_t$ and a controllable component $u_t$.

**The controller**: The PDS can be controlled by first selecting a particular initial state $x_0$ and then by choosing suitable values for $u_1, u_2, \ldots$. Here, we only consider static control policies where the value of the control $u_t$ is instantaneously computed from the value of $x_t$ and $y_t$. Such a controller is called a static controller. Formally, it is a system of two equations:

\[
\begin{align*}
C(X,Y,U) & = 0 \\
C_0(X) & = 0
\end{align*}
\]

where the latter equation determines the initial states satisfying the control objectives and the former describes how to choose instantaneous controls. When the controlled system is in state $x$, an event $y$ occurs, any value $u$ such that $Q(x, y, u) = 0$ and $C(x, y, u) = 0$ can be chosen. The behavior of the system composed with the controller is then modeled as:

\[
\begin{align*}
Q(X,Y,U) & = 0 \\
C(X,Y,U) & = 0 \\
X' & = P(X,Y,U) \\
Q_0(X) & = 0 \\
C_0(X) & = 0
\end{align*}
\]

Control objectives ensuring properties like invariance, reachability, attractivity, etc are called traditional control objectives. There are also other kinds of control objectives which can be expressed as partial order relations over the states of the PDS. These are called optimization control objectives. Sigali provides functionalities for synthesis of controllers ensuring traditional as well as optimization control objectives. There does not exist pre-existing Sigali functionalities. Instead, one have to load different libraries in which Sigali functions are written.

3.2 Loading of the necessary libraries

For controller synthesis ensuring traditional control objectives, the `Synthesis.lib` file must be loaded.

- `S_c : S_Invariance(S,prop);` (or equivalently `S_Security(S,prop)`); If prop encodes a set of states $E$, `S_Invariance(S,prop)` computes a controller that ensures the invariance of $E$ with respect to the system $S$. The controlled system is the output of this function.
- `S_c : S_Reachbale(S,prop);` If prop encodes a set of states $E$, `S_Reachbale(S,prop)` computes a controller that ensures the reachability of $E$ from the initial states. The controlled system is the output of this function. To ensure the attractivity, one have to use the `S_Attractivity(S,prop);` command.

For dealing with optimization control objectives, two additional files: `Synthesis_Partial_order.bib` and `Synthesis_Optimal_Control.bib` must also be loaded.
The file `Synthesis_Partial_Order.lib` contains the definition of a function called `S_Free_Max` which helps in choosing a control such that the system evolves, in the next instant, into a state where the maximum number of uncontrollable events are admissible.

The file `Synthesis_Partial_Order_Relation.lib` contains function definitions for the synthesis of optimal controllers. The goal is to synthesize a controller that will choose a control from amongst all the admissible controls in such a way that the system evolves into a state according to a given choice criterion. This criterion is expressed as a cost function relation on the set of states. Intuitively speaking, the cost function is used to express priority between the different states that a system can reach in one transition.

**Technical Restriction**

Input: C(X) is the cost function used for the control C_Dup(X_1) is the duplicated cost function of C(X) where X_1 is, for example obtained as follows:

```sigal
> duplicate_states : declare_suff(state_var(S));
```

next, one have to declare C_Dup (i.e. same as for C but with the variables of the set `duplicate_states`

Nb. No automatic reordering -> set reorder(0) the variable order must be as follows: X1>X1_1>X2>X2_1... So, if you plan to use the functions of this library then never use the reordering after the use of declare_suff(state_var(S)) Once you plan not to use these functions anymore, then you activate again the automatic reordering.

The different functions of the `Synthesis_Partial_Order_Relation.lib` are:

- Supervisor_Lower_than(S,C,C_Dup,duplicate_states) gives access to a controlled system such that whatever the current position of the system S under control, the supervisor will make the system evolve into the state x such that forall x' reachable from the current position C(x) ≤ C_Dup(x'). `Lower_than(S,C,C_Dup,duplicate_states)` build the controlled system.
- idem for Supervisor_Greater_than(S,C,C_Dup,duplicate_states) and `Greater_than(S,C,C_Dup,duplicate_states)` (i.e. C(x) ≥ C_Dup(x')).
- idem for Supervisor_Strictly_Lower_than(S,C,C_Dup,duplicate_states) and `Strictly_Lower_than(S,C,C_Dup,duplicate_states)` (i.e. C(x) < C_Dup(x')).
- idem for Supervisor_Strictly_Greater_than(S,C,C_Dup,duplicate_states) and `Strictly_Greater_than(S,C,C_Dup,duplicate_states)` (i.e. C(x) > C_Dup(x')).