Lectures Outline

- Overview of System Synthesis.
- Fair Discrete Systems and their Computations.
- Model Checking Invariance and feasibility.
- Temporal Testers and general LTL Model Checking.
- Controller Synthesis via Games.
- Synthesis from Recurrence Specifications.
- Synthesis from Reactivity Specifications. – The general case.

The Control Framework

Classical (Continuous Time) Control

Required: A design for a controller which will cause the plant to behave correctly under all possible (appropriately constrained) environments.

Discrete Event Systems Controller: [Ramadge and Wonham 89]. Given a Plant which describes the possible events and actions. Some of the actions are controllable while the others are not.

Required: Find a strategy for the controllable actions which will maintain a correct behavior against all possible adversary moves. The strategy is obtained by pruning some controllable transitions.

Application to Reactive Module Synthesis: [PR88], [ALW89] — The Plant represents all possible actions. Module actions are controllable. Environment actions are uncontrollable.

Required: Find a strategy for the controllable actions which will maintain a temporal specification against all possible adversary moves. Derive a program from this strategy. View as a two-persons game.

The Runner Blocker System

The runner R tries to reach the goal. The blocker B tries to intercept and stop the runner.
Lecture 6: Controller Synthesis  

A. Pnueli

State Transitions Diagram

Verification and Synthesis of Reactive Programs, Rome, June, 2006

All of our algorithms will be computing sets of states out of the state-transition diagram. Let $\|win\|$ denote the set of states labeled by the $win$ proposition. Let $\rho$ be the transition relation, such that $\rho(s_1, s_2)$ holds whenever $s_2$ is a direct successor of the state $s_1$ in the state-transition diagram.

For a state-set $S$, we introduce the predecessor operator $Pre_\exists$ which computes the set of all one-step predecessors of the states in $S$. That is,

$$Pre_\exists(S) = \{s \mid s \text{ has a } \rho\text{-successor in } S\}$$

Recursively, we define a state $s$ to be goal reaching if either $s \in \|win\|$ or $s$ has a goal reaching successor. That is,

$$R = \|win\| \cup Pre_\exists(R)$$

We may expect that the solution to this fix-point equation, will give us the set of all states from which $\|win\|$ is reachable.

Problem: Not Every Solution is Satisfactory

Consider the diagram:

Both $R_{0,1} = \{s_0, s_1\}$ and $R_{0,2} = \{s_0, s_1, s_2\}$ satisfy the equation

$$R = \|win\| \cup Pre_\exists(R)$$

but only $R_{0,1} = \{s_0, s_1\}$ captures the set of states from which $\|win\|$ is reachable.

Conclusion: We should take the minimal solution of the fix-point equation $R = \|win\| \cup Pre_\exists(R)$ which we denote by

$$\mu R. (\|win\| \cup Pre_\exists R)$$

This minimal solution can be effectively computed by the iteration sequence:

$$R_0 = \emptyset$$
$$R_1 = \|win\|$$
$$R_2 = R_0 \cup Pre_\exists R_0$$
$$R_3 = R_1 \cup Pre_\exists R_1$$

... 

Consequently, the goal is reachable from an initial state $s_0$ iff $s_0 \in \mu R. (\|win\| \cup Pre_\exists R)$. 

Computing $\mu R. \|win\| \cup Pre_\exists R$
Controller Synthesis

Distinguishing between the two players, we define

\[
\text{Pre}_\exists(S) = \{s \mid \text{Some red successor of } s \text{ is in } C\}
\]

\[
\text{Pre}_\forall(S) = \{s \mid \text{All black successors of } s \text{ are in } C\}
\]

The two operators can be combined, and the expression

\[
\text{Pre}_\exists(S) \cup \text{Pre}_\forall(S)
\]

denotes the set of states \(s\) which have at least one red successor \(s_1\) all of whose black successors belong to \(C\). If we think about the moves as taken in turn by two players, then \(\text{Pre}_\exists(S)\) denotes the states from which the red player can force the game after a complete round (each player making one move) into a \(C\)-state.

The expression \(\text{control}(\text{win}) = \mu C. \parallel \text{win} \parallel \cup \text{Pre}_\forall(S)\) characterizes all the states from which the red player can force a visit to a win state in a finite number of moves.

Conclusions

The runner and the blocker can cooperate to reach a winning state for \(R\).

However, \(R\) cannot force a win.

The Modified Runner Blocker System

Additional transitions have been added to the runner.
Game Tree for the Modified System

Computing $\mu R. \parallel \text{win} \parallel \cup \text{Pre}_R(R)$

A Winning Strategy
Apply to Programs

Let us apply the controller synthesis paradigm to synthesis of programs (or designs, in general).

Example Design: Arbiter

Consider a specification for an arbiter.

The protocol for each client:

Required to satisfy

\[ \bigwedge_{i \neq j} \neg (g_i \land g_j) \land \bigwedge_i \Box (g_i = r_i) \]

Start by Controller Synthesis

Assume a given platform (plant), identifying controllable (system) and uncontrollable (environment) transitions:

By default every node is connected to itself by both green and red transitions. A complete move consists of a red edge followed by a green edge, visiting at most two different states. Also given is an LTL specification (winning condition):

\[ \varphi : \Box \neg (g_1 \land g_2) \land \Box (g_1 = r_1) \land \Box (g_2 = r_2) \]

Synthesis Via Game Playing

A game is given by \( G : \langle V = X \cup Y, \Theta, \rho_1, \rho_2, \varphi \rangle \), where

- \( V = X \cup Y \) are the state variables, with \( X \) being the environment's (player 1) variables, and \( Y \) being the system's (player 2) variables. A state of the game is an interpretation of \( V \). Let \( \Sigma \) denote the set of all states.
- \( \Theta \) — the initial condition. An assertion characterizing the initial states.
- \( \rho_1(X, Y, X') \) — Transition relation for player 1 (Environment).
- \( \rho_2(X, Y, X', Y') \) — Transition relation for player 2 (system).
- \( \varphi \) — The winning condition. An LTL formula characterizing the plays which are winning for player 2.

A state \( s_2 \) is said to be a \( G \)-successor of state \( s_1 \), if both \( \rho_1(s_1[V], s_2[X]) \) and \( \rho_2(s_1[V], s_2[V]) \) are true.

We denote by \( D_X \) and \( D_Y \) the domains of variables \( X \) and \( Y \), respectively.
Plays and Strategies

Let $G = (V, \Theta, \rho_1, \rho_2, \varphi)$ be a game. A play of $G$ is an infinite sequence of states

$$\pi: s_0, s_1, s_2, \ldots,$$

satisfying:

- Initiality: $s_0 \models \Theta$.
- Consecution: For each $j \geq 0$, the state $s_{j+1}$ is a $G$-successor of the state $s_j$.

A play $\pi$ is said to be winning for player 2 if $\pi \models \varphi$. Otherwise, it is said to be winning for player 1.

A strategy for player 1 is a function $\sigma_1: \Sigma^+ \mapsto D_X$, which determines the next set of values for $X$ following any history $h \in \Sigma^+$. A play $\pi: s_0, s_1, \ldots$ is said to be compatible with strategy $\sigma_1$ if, for every $j \geq 0$, $s_{j+1}[X] = \sigma_1(s_0, \ldots, s_j)$.

Strategy $\sigma_1$ is winning for player 1 from state $s$ if all $s$-originated plays compatible with $\sigma_1$ are winning for player 1. If such a winning strategy exists, we call $s$ a winning state for player 1.

Similar definitions hold for player 2 with strategies of the form $\sigma_2: \Sigma^+ \times D_X \mapsto D_Y$.

From Winning Games to Programs

A game $G$ is said to be winning for player 2 (player 1, respectively) if all (some) initial states are winning for 2 (1, respectively).

We solve the game, attempting to decide whether the game is winning for player 1 or 2. If it is winning for player 1 the specification is unrealizable. If it is winning for player 2, we can extract a winning strategy which is a working implementation.

When applying controller synthesis, the platform provides the transition relations $\rho_1$ and $\rho_2$, as well as the initial condition.

Thus, the essence of synthesis under the controller framework is an algorithm for computing the set of winning states for a given platform and specification $\varphi$.

The Controlled Predecessor

As in symbolic model checking, computing the winning states involves fix-point computations over a basic predecessor operator. For model checking the operator is $\Diamond p$ satisfied by all states which have a $p$-state as a successor.

For synthesis, we use the controlled predecessor operator $\Box p$. Its semantics can be defined by

$$\Box p : \forall X' : \rho_1(V, X') \rightarrow \exists Y' : \rho_2(V, Y') \land p(Y')$$

where $\rho_1$ and $\rho_2$ are the transition relations of the environment and system, respectively.

In our graphic notation, $s \models \Box p$ iff $s$ has at least one green $p$-successor, and all red successors different from $s$ satisfy $p$.

Solving $\square p$ Games, Iteration 0

The set of winning states for a specification $\square p$ can be computed by the fix-point expression:

$$\nu Y \cdot p \land \Box Y = p \land \Box p \land \Box p \land \ldots$$

We illustrate this on the specification $\neg(g_1 \land g_2)$. 

![Diagram](image-url)
Solving □ p Games, Iteration 1
The set of winning states for a specification □ p can be computed by the fix-point expression:
\[ \nu Y. p \land Y = p \land \Box \Box p \land \cdots \]
We illustrate this on the specification □(g_1 \land g_2).

Solving ◊ q Games, Iteration 1
The set of winning states for a specification ◊ q can be computed by the fix-point expression:
\[ \mu Y. q \lor Y = q \lor \Box \Box \Box q \lor \cdots \]
We illustrate this on the specification ◊(g_1 = r_1).

Solving ◊ q Games, Iteration 2
The set of winning states for a specification ◊ q can be computed by the fix-point expression:
\[ \mu Y. q \lor Y = q \lor \Box \Box \Box q \lor \cdots \]
We illustrate this on the specification ◊(g_1 = r_1).

Solving ◊ q Games, Iteration 3
The set of winning states for a specification ◊ q can be computed by the fix-point expression:
\[ \mu Y. q \lor Y = q \lor \Box \Box \Box q \lor \cdots \]
We illustrate this on the specification ◊(g_1 = r_1).
Lecture 7: Application to Program Synthesis

Solving $\Diamond q$ Games, Iteration 4 (Final)

The set of winning states for a specification $\Diamond q$ can be computed by the fix-point expression:

$$\mu Y. q \lor \Box Y = q \lor \Box Y \lor q \lor \Box Y \lor \cdots$$

We illustrate this on the specification $\Diamond (g_1 = r_1)$.

Solving $\Box q$ Games

A game for a winning condition of the form $\Box q$ can be solved by the fix-point expression:

$$\nu Z. \mu Y. q \land \Box Z \lor \Box Y$$

This is based on the maximal fix-point solution of the equation

$$Z = \mu Y. (q \land \Box Z) \lor \Box Y$$

This nested fix-point computation can be computed iteratively by the program:

$$Z := 1$$
$$\text{Fix } (Z)$$

Generalized Response (Büchi)

Solving the game for $\Box q_1 \land \cdots \land \Box q_n$.

$$\varphi = \nu$$

Iteratively:

For $i \in 1..n$ do $[Z[i] := 1]$
$$\text{Fix } (Z[1])$$

For $i \in 1..n$ do

$$\begin{cases} 
Z_1 & \mu Y \left( (q_1 \land \Box Z_2) \lor \Box Y \right) \\
Z_2 & \mu Y \left( (q_2 \land \Box Z_3) \lor \Box Y \right) \\
\vdots & \vdots \\
Z_n & \mu Y \left( (q_n \land \Box Z) \lor \Box Y \right)
\end{cases}$$

Return $Z[1]$
Specification is Unrealizable

Applying the above algorithm to the specification
\[ \square \diamond (g_1 = r_1) \land \square \diamond (g_2 = r_2) \]
we find that it fails. Conclusion:

The considered specification is unrealizable

Indeed, without an environment obligation of releasing the resource once it has been granted, the arbiter cannot satisfy any other client.

Property-Based System Design

While the rest of the world seems to be moving in the direction of model-based design (see System-C, UML), some of us persist with the vision of property-based approach.

Specification is stated declaratively as a set of properties, from which a design can be extracted.

This is currently studied in the project PROSYD.

Design synthesis is needed in two places in the development flow:

- Automatic synthesis of small blocks whose time and space efficiency are not critical.
- As part of the specification analysis phase, ascertaining that the specification is realizable.

Program Synthesis from LTL Specification

Assume we are given a set of LTL specifications. We construct a game as follows:

- As \( \Theta \) we take all the non-temporal specification parts which relate to the initial state.
- As \( \rho_1 \) and \( \rho_2 \), we can take True. A more efficient choice is to include in \( \rho_1 \) (similarly \( \rho_2 \)) all local limitations on the next values of \( X \) (resp. \( Y \)), such as
  \[ r_i \land \neg g_i \rightarrow r'_i \]

We place in \( \varphi \) all the remaining properties that have not already been included in \( \Theta \), \( \rho_1 \), and \( \rho_2 \).

We solve the game, attempting to decide whether the game is winning for player 1 or 2. If it is winning for player 1, the specification is unrealizable. If it is winning for player 2, we can extract a working strategy which is a working implementation.
The Game for the Sample Specification

For the specification
\[ \bigwedge_i (r_i \neq g_i) \Rightarrow (\bigcirc r_i = r_i) \land r_i \land g_i \Rightarrow \Box r_i \Rightarrow \bigcirc g_i = g_i \land \bigwedge_i \biggl( r_i = g_i \Rightarrow \bigcirc g_i = g_i \land \Box r_i \land g_i \Rightarrow \Box g_i = g_i \biggr) \]

We take the following game components:

- \( X \cup Y = \{ r_i \mid i = 1, \ldots, n \} \cup \{ g_i \mid i = 1, \ldots, n \} \)
- \( \Theta = \bigwedge_i (r_i \land g_i) \)
- \( \rho_1 = \bigwedge_i \bigl( (r_i \neq g_i) \rightarrow (r_i' = r_i) \bigr) \)
- \( \rho_2 = \bigwedge_{i \neq j} (g_i' \land g_j') \land \bigwedge_i \bigl( (r_i = g_i) \rightarrow (g_i' = g_i) \bigr) \)
- \( \varphi = \bigwedge_i (r_i \land g_i \Rightarrow \Box r_i) \Rightarrow \bigwedge_i ((r_i \land g_i) \Rightarrow \Box g_i) \land (\Box r_i \land g_i \Rightarrow \Box g_i) \)

Solving Games for Generalized Reactivity[1] (Streett[1])

Following [KPP03], we present an \( n^3 \) algorithm for solving games whose winning condition is given by the (generalized) Reactivity[1] condition

\[ (\Box p_1 \land \Box p_2 \land \cdots \land \Box q_m) \rightarrow \Box q_1 \land \Box q_2 \land \cdots \land \Box q_n \]

This class of properties is bigger than the properties specifiable by deterministic Büchi automata. It covers a great majority of the properties we have seen so far.

For example, it covers the realizable version of the specification for the Arbiter design.
The Solution

The winning states in a Streett[1] game can be computed by

\[
\varphi = \nu \begin{bmatrix}
Z_1 \\
Z_2 \\
\vdots \\
Z_n \\
\end{bmatrix}
\begin{bmatrix}
\mu Y \left( \bigvee_{j=1}^{m} \nu X (q_1 \land \Box Z_2 \lor \Box Y \lor \neg p_j \land \Box X) \right) \\
\mu Y \left( \bigvee_{j=1}^{m} \nu X (q_2 \land \Box Z_3 \lor \Box Y \lor \neg p_j \land \Box X) \right) \\
\vdots \\
\mu Y \left( \bigvee_{j=1}^{m} \nu X (q_n \land \Box Z_1 \lor \Box Y \lor \neg p_j \land \Box X) \right)
\end{bmatrix}
\]

where

\[\varphi : \forall X' : \rho_1(V,X') \rightarrow \exists V' : \rho_2(V,V') \land \varphi(V')\]

Results of Synthesis

The design realizing the specification can be extracted as the winning strategy for Player 2. Applying this to the Arbiter specification, we obtain the following design:

There exists a symbolic algorithm for extracting the implementing design/winning strategy.

Conclusions

- It is possible to perform design synthesis for restricted fragments of LTL in acceptable time.
- The tractable fragment (React(1)) covers most of the properties that appear in standard specifications.
- It is worthwhile to invest an effort in locating the formula within the temporal hierarchy. Solving a game in React(k) has complexity \(N^{(2^k+1)}\).
The Semantics of Game Analysis

We can always construct the **game tree**

<table>
<thead>
<tr>
<th><img src="image" alt="Game Tree Diagram" /></th>
</tr>
</thead>
</table>

**Strategies**

All strategies can be represented as pruning of the tree at the controllable levels. For example, a strategy for the specification

\[(r \Rightarrow \Box g) \land (\Box \Rightarrow \Box g)\]

<table>
<thead>
<tr>
<th><img src="image" alt="Strategy Diagram" /></th>
</tr>
</thead>
</table>

Folding the Tree Into a Finite Graph

In order to be algorithmically tractable, we need to perform the pruning process over the finite graph which generated the game tree. In many cases, this is possible (and leads to memory-less strategy).

<table>
<thead>
<tr>
<th><img src="image" alt="Folding Diagram" /></th>
</tr>
</thead>
</table>

Folding not Immediate

There are cases in which the pruning must depend on the path leading to the current state. Folding is still possible but may need a longer period.

| ![Folding Not Immediate Diagram](image) |
Controller (Design) Extraction

It remains to show how to extract a winning strategy for the case that a game is winning for player 2.

Let $G : (V = X \cup Y, \Theta, \rho_1, \rho_2, \varphi)$ be a given game. A controller for $G$ is an FDS $G_c : (V_c, \Theta_c, \rho_c, \emptyset, \emptyset)$, such that:

- $V_c \supseteq V$. That is, $V_c$ extends the set of variables of $G$.
- $\Theta_c \downarrow V = \Theta$. That is, when projecting the initial states of $G_c$ on the variables of $G$, we obtain precisely the initial states of $G$.
- $\rho_c \rightarrow \rho$, where $\rho = \rho_1 \land \rho_2$. That is, if $s_2$ is a $\rho_c$ successor of $s_1$, then $s_2$ is also a $\rho_c$ successor of $s_1$.
- Player-1 Completeness — $\rho_c \downarrow V X \rho = \rho_1$. That is, a state $s_1 \in \Sigma_c$ has a $\rho_1$-successor $s_2$ iff $s_1$ has a $\rho_c$-successor which agrees with $s_2$ on the valuation of $X$.
- Every infinite run of $G_c$ satisfies the winning condition $\varphi$.

Example: Extracted Controller for Arbiter

Following is the controller extracted for the Arbiter example:

Interpreting a Controller as a Program

A program (equivalently, a circuit) implementing the extracted controller follows the states that are contained in $G_c$. It has a program counter which ranges over the states of $G_c$.

Assume that control is currently at state $S$ of $G_c$. Let the next values of the input variables be $X = \xi$. Choose a state $S'$ which is a $\rho_c$-successor of $S$, and such that $S'[X] = \xi$. By the requirement of Player-1 Completeness, there always exists such a successor.

The actions of the program is to output the values $\eta$ such that $S'[Y] = \eta$, and to move to state $S'$.

Computing a Controller for the Winning Condition $\Box p$

The winning states in a game with a winning condition $\Box p$ are given by:

$$\text{win} = \nu Z. p \land \Box Z$$

The full controller extraction algorithm can be given by the following program:

$$Z := 1$$
$$\text{Fix (} Z \text{)}$$
$$\begin{cases} Z := p \land \Box Z \\ \text{if } (\Theta \land \neg Z) \neq 0 \text{ then} \\ \text{Print "Specification is unrealizable"} \\ \text{else} \\ \Theta_c := \Theta \\ \rho_c := Z \land p \land Z' \end{cases}$$

Claim 10. If $s$ is a winning state of a $(\Box p)$-game, then $s \models p$, and player 2 can force the game to move from $s$ to a successor which is also a winning state.
Computing A Controller for the Winning Condition $\Diamond q$

The winning states in a game with a winning condition $\Diamond p$ are given by:

$$\text{win} = \mu Y. q \lor \Box Y$$

The full controller extraction algorithm can be given by the following program:

$$Y := q; \quad r := 0; \quad U[0] := q$$

Fix (Y)

$$\begin{cases} Y := q \lor \Box Y; & r := r + 1; \quad U[r] := Y \\ \text{if } (\Theta \land \neg Y) \neq 0 \text{ then} \\ \text{Print "Specification is unrealizable"} \\ \text{else} \\ \Theta_c := \Theta \\ \rho_c := 0; \quad \text{prev} := U[0] \\ \text{for } i \in 1 \ldots r \text{ do} \\ \quad \rho_c := \rho_c \lor (U[i] \land \neg \text{prev}) \land \rho \land \text{prev}'; \quad \text{prev} := \text{prev} \lor U[i] \end{cases}$$

Claim 11. Every winning state $s$ in a $(\Diamond q)$-game is associated with a natural rank $r(s) \geq 0$, such that if $r(s) = 0$ then $s \models q$, and if $r(s) > 0$, then player 2 can force the game to move from $s$ to a winning successor with a lower rank.

Computing A Controller for the Winning Condition $\Box \Diamond q$

The winning states in a game with a winning condition $\Box \Diamond p$ are given by:

$$\text{win} = \nu Z \mu Y. (q \land \Box Z) \lor \Box Y$$

The full controller extraction algorithm can be given by the following program:

$$Z := 1$$

Fix (Z)

$$\begin{cases} Y := q \land \Box Z; & r := 0; \quad U[0] := Y \\ \text{Fix (Y)} \\ \quad \begin{cases} Y := q \lor \Box Y; & r := r + 1; \quad U[r] := Y \\ \text{if } (\Theta \land \neg Z) \neq 0 \text{ then} \\ \text{Print "Specification is unrealizable"} \\ \text{else} \\ \Theta_c := \Theta \\ \rho_c := U[0] \land \rho \land Z'; \quad \text{prev} := U[0] \\ \text{for } i \in 1 \ldots r \text{ do} \\ \quad \rho_c := \rho_c \lor (U[i] \land \neg \text{prev}) \land \rho \land \text{prev}'; \quad \text{prev} := \text{prev} \lor U[i] \end{cases} \end{cases}$$

Claim 12. Every winning state $s$ in a $(\Box \Diamond q)$-game is associated with a natural rank $r(s)$, such that player 2 can force the game to move from $s$ to a winning successor $s'$, where either $r(s) = 0$ and $s \models q$, or $r(s) > r(s')$. 