From verification to synthesis

Verification:
  first write program (or model of a system), then specify formal properties, then check correctness.

Synthesis:
  first specify formal properties, then let synthesizer automatically generate a correct program.

Put another way:
  from imperative (how) to declarative (what) design; “raising the level of abstraction”.
What is synthesis?

Roughly:

\[ \exists P : \forall x: \varphi(x, P(x)) \]

Many different variants, depending on what is P, \( \varphi \), and how search is done.

Very old topic (Church, 1960s) recently rejuvenated.

Dimensions in Synthesis (Gulwani)

Concept Language (Application)
- Programs
  - Straight-line programs
- Automata
- Queries
- Sequences

User Intent (Ambiguity)
- Logic, Natural Language
- Examples, Demonstrations/Traces

Search Technique (Algorithm)
- SAT/SMT solvers (Formal Methods)
- A*-style goal-directed search (AI)
- Version space algebras (Machine Learning)

Also: logic synthesis

Compilers vs. Synthesizers (Gulwani)

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Compilers</th>
<th>Synthesizers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept Language</td>
<td>Executable Program</td>
<td>Variety of concepts: Program, Automata, Query, Sequence</td>
</tr>
<tr>
<td>User Intent</td>
<td>Structured language</td>
<td>Variety/mixed form of constraints: logic, examples, traces</td>
</tr>
<tr>
<td>Search Technique</td>
<td>Syntax-directed translation (No new algorithmic insights)</td>
<td>Uses some kind of search (Discovers new algorithmic insights)</td>
</tr>
</tbody>
</table>

Program synthesis and proofs

From 2nd order formula

\[ \exists P: \forall x: \varphi(x, P(x)) \]

to 1st order formula

\[ \forall x: \exists y: \varphi(x, y) \]

Synthesizing program P can be done by proving constructively that the above formula is valid.
Designing controllers can be tricky and time consuming

Example: Electrical Power Generation and Distribution System (EPS) of a modern aircraft

Thanks to:
Pierluigi Nuzzo
Antonio Iannopollo
Designing controllers can be tricky and time consuming

Example: EPS requirements (in English)

A2) At least one power source is always “healthy” (i.e. it is operational and can be inserted into the network to deliver power);

A3) Failures can only affect the power sources; once a power source becomes “unhealthy” (i.e. it is not operational and cannot be inserted into the network to deliver power), it will never return to be “healthy” (e.g., turned back on) during the cruising phase of the mission;

A4) An AC bus is correctly powered if the root-mean-square (RMS) voltage at its loads is between 110 V and 120 V and the frequency is 400 Hz.

Under the above assumptions, the BPCU offers the following guarantees:

G1) At start-up all the power source contactors are “open”;

G2) In normal conditions (i.e. no faults or failures in the system) $G_7$ and $G_8$ are “on” and provide power for the left side and the right side of the system, respectively; auxiliary power units are “off”; $G_9$ and $G_{10}$ are open (“off”);

G3) No AC bus is powered by more than one power source at the same time, i.e. AC power sources can never be paralleled;

G4) It never happens that both the APU’s are inserted into the network at the same time;

G5) AC buses cannot be unpowered for more than a well-defined length of time;

G6) DC buses must always stay powered, at least in a “reduced performance” mode, which occurs when only one HVRU is used;

G7) The left AC bus $B_L$ must always be powered from the first available source from the ordered list ($G_1$, $A_C$, $A_8$, $G_6$);

G8) The right AC bus $B_R$ must always be powered from the first available source from the ordered list ($G_1$, $A_R$, $A_1$, $G_1$).
Designing controllers can be tricky and time consuming

Example: EPS “hand-written” controller
Designing controllers can be tricky and time consuming
Example: EPS “hand-written” controller
Design time ~ 1 week [Nuzzo] (but have to verify also)
For a real controller, it could be months [e.g., robotic controllers, Willow Garage]

Can design time be improved?

Declarative specification of controllers

At the outset the controller is just a box with inputs and outputs:
Declarative specification of controllers

At the outset the controller is just a box with inputs and outputs:

Example: EPS controller

We can specify the input-output behavior of the controller in a high-level language, e.g., in temporal logic.
Declarative specification of controllers

Example: LTL specification for EPS

~40 lines

# Assumptions

- (gl_healthy & gr_healthy & al_healthy & ar_healthy)
- [gl_healthy | gr_healthy | al_healthy | ar_healthy]
- ![gl_healthy -> X(!gl_healthy)]
- ![gr_healthy -> X(!gr_healthy)]
- ![al_healthy -> X(!al_healthy)]
- ![ar_healthy -> X(!ar_healthy)]

# Guarantees

- ![c1 & c2 & c3 & c4 & c5 & c6 & c7 & c8 & c9 & c10 & c11 & c12 & c13]
- ![X(c7) & X(c8) & X(c11) & X(c12) & X(c13)]
- ![!(c2 & c3)]
- ![!(c1 & c5 & (al_healthy | ar_healthy))]
- ![!(c4 & c6 & (al_healthy | ar_healthy))]
- ![((X(gl_healthy) & X(gr_healthy)) -> X(!c2) & X(!c3) & X(!c9) & X(!c10))]
- ![((X(!gl_healthy) & X(!gr_healthy)) -> X(c9) & X(c10))]
- ![X(!gl_healthy) -> X(!c1)]
- ![X(!gr_healthy) -> X(!c4)]
- ![X(!al_healthy) -> X(!c2)]
- ![X(!ar_healthy) -> X(!c3)]
- ![X(gl_healthy) -> X(c1)]
- ![X(gr_healthy) -> X(c4)]

A2) At least one power source is always “healthy” (i.e. it is operational and can be inserted into the network to deliver power):

\[ [(gl\_healthy | gr\_healthy | al\_healthy | ar\_healthy)] \]
The controller synthesis problem

Given formula specification (e.g., in LTL) synthesize controller (e.g., FSM) which implements the specification (or state that such a controller does not exist).

Automatic controller synthesis from declarative specifications
Example: controller for EPS synthesized from previous LTL spec using Tulip (Caltech) ~3k lines of Matlab
Automatic controller synthesis from declarative specifications

Example: controller for EPS synthesized using Tulip (Caltech), ~40 states – zooming in

```matlab
switch state
    case 2
        if isequal(p1_healthy, 1) && isequal(p2_healthy, 1) && isequal(a1_healthy, 1) && isequal(a2_healthy, 1)
            state = 0;
            c4 = 1;
            c5 = 1;
            c0 = 1;
            c2 = 1;
            c13 = 0;
            c12 = 0;
            c11 = 0;
            c10 = 0;
            c9 = 0;
            c8 = 0;
        else
            disp("Cannot find a valid successor, environment assumption is likely to be violated")
            c4 = 1;
            c5 = 1;
            c0 = 1;
            c2 = 1;
```

Synthesis in these two lectures

Part 1: Controller synthesis and game solving.

Part 2: Example-guided and syntax-guided synthesis.
Declarative specification of controllers

At the outset the controller is just a box with inputs and outputs:

We can specify the input-output behavior of the controller in a high-level language, e.g., in temporal logic.
Controller synthesis (reactive synthesis)
[Pnueli-Rosner, POPL 1989]

Given interface of controller:

\[
\begin{array}{c}
p_1 \\
\vdots \\
p_n \\
\end{array} \quad \begin{array}{c}
\vdots \\
\end{array} \quad \begin{array}{c}
q_1 \\
\vdots \\
q_m \\
\end{array}
\]

and given temporal logic formula \( \varphi \) over set of input/output variables,

synthesize a controller (= state machine) \( M \), such that all behaviors of \( M \) (for any sequence of inputs) satisfy \( \varphi \).

Note: other notions of controller synthesis exist in the literature. See “Bridging the gap” paper on the course web site for details.

Examples

Consider controller interface:

\[
p \quad \begin{array}{c}
\longrightarrow \\
\end{array} \quad q
\]

and specifications

\[
\varphi_1 = G(p \rightarrow Xq)
\]

\[
\varphi_2 = G(p \leftrightarrow Xq)
\]

\[
\varphi_3 = G(q \leftrightarrow Xp)
\]
Examples

Consider controller interface:

\[ p \rightarrow q \]

and specifications

\[ \varphi_1 = G(p \rightarrow Xq) \]

\[ \varphi_2 = G(p \leftrightarrow Xq) \]

\[ \varphi_3 = G(q \leftrightarrow Xp) \]

No solution: controller cannot foresee the future!

Satisfiability vs. realizability

Satisfiability: exists some behavior that satisfies the specification. (In this behavior, we may choose both inputs and outputs as we wish.)

Realizability: exists controller that implements the specification. Must work for all input sequences, since inputs are uncontrollable.

Inherently different problems, also w.r.t. complexity:

LTL satisfiability: PSPACE
LTL realizability: 2EXPTIME
Controller synthesis algorithms: computing strategies in games

Solving safety games

Solving reachability games

Solving deterministic Büchi games (liveness)

Remarks on the general LTL synthesis problem
Safety automata

In some fortunate cases, the LTL specification can be translated to a safety automaton.

Example: \( \varphi = G(p \rightarrow q) \)

Automaton:

\[ \tilde{p} + q \]

“bad” state

“Spreading” a safety automaton to a game

We need to separate the input moves from the output moves:

Automaton:

\[ \tilde{p} + q \]

Game:
Safety games

Input (environment) states:
Output (controller) states:
Bad state:

Goal: find **winning strategy** = avoiding bad state

Solving safety games

1. Compute set of losing states, starting with \( \text{Losing} := \{\circ\} \);
2. If initial state in \( \text{Losing} \), no strategy exists.
3. Otherwise, all remaining states are winning. Extract strategy from them by choosing outputs that avoid the losing states.
Solving safety games

1. Compute set of losing states, starting with \( \text{Losing} := \{ \emptyset \} \);
   - repeat
     - \( \text{UncontrollablyLosing} := \{ s \mid s \text{ has uncontrollable succ in } \text{Losing} \} \);
     - \( \text{ControllablyLosing} := \{ s \mid \text{all controllable succs of } s \text{ are in } \text{Losing} \} \);
     - \( \text{Losing} := \text{Losing} \cup \text{UncontrollablyLosing} \cup \text{ControllablyLosing} \);
   - until \( \text{Losing} \) does not change;
Solving safety games

- Extracting the strategy: “cut” controllable transitions in order to avoid losing states.
- Strategy is **state-based** (also called “positional”, or “memoryless”).

Controller synthesis algorithms

- Solving safety games
- **Solving reachability games**
  - Solving deterministic Büchi games (liveness)
  - Remarks on the general LTL synthesis problem
Reachability games: dual of safety games

Reachability game: trying to reach a target state.

Observation: what is Losing for the safety player is Winning for the reachability player (and vice versa).

Solving reachability games: direct algorithm

1. Compute set of Winning states;
   - **Winning** := {笑脸};
   - repeat
     - Winning := Winning U ForceNext(Winning);
   - until Winning does not change;
   - ForceNext(S) := { s | all uncontrollable succs of s are in S } U { s | s has controllable succ in S }
How to extract strategies in reachability games?

Similarly as for safety games:

Extract strategy from $\text{ForceNext}(S)$: ensure you choose the right controllable transition that leads in winning state.

Is strategy state-based?
Yes!

How to extract strategies in reachability games?

Similarly as for safety games: BUT, a subtlety:

Need to fix successor the first time state is added in $\text{Winning}$. 
Controller synthesis algorithms

Solving safety games

Solving reachability games

**Beyond safety and reachability games**

Remarks on the general LTL synthesis problem

What about other types of properties?

**Bounded response** specifications can be translated to safety automata/games:

\[ \varphi = G(p \rightarrow (q \lor Xq \lor XXq)) \]

Automaton:
What about liveness properties?

What about **unbounded response**?

\[ \varphi = G(p \rightarrow Fq) \]

More interesting example:

\[ \varphi = G(p_1 \rightarrow Fq_1) \land G(p_2 \rightarrow Fq_2) \land G(\neg(q_1 \land q_2)) \]

---

**Synthesis for general LTL specifications**

Given LTL specification \( \varphi \):

If \( \varphi \) can be translated to a **deterministic Büchi automaton**, then can extend the previous ideas to solving Büchi games.

Otherwise, solution involves more advanced topics, such as tree automata. Will not be covered in this course.

**Note:** LTL **cannot** always be translated to deterministic Büchi automata.
Büchi automata

Syntactically same as finite state automata:

\[ A = (\Sigma, S, s_0, \delta, F) \]

But Büchi automata accept **infinite words.**
A run must visit an accepting state **infinitely often.**

From LTL to Büchi automata

Consider unbounded response property:

\[ \varphi = G(p \rightarrow Fq) \]

Büchi automaton:

\[ \tilde{p} + q \quad \tilde{q} \quad p\tilde{q} \quad q \]

accepting state
From LTL to Büchi automata

Consider LTL formula:
\[ \varphi = FGq \]

Büchi automaton? (s.t. there exists an accepting run)

Is there a deterministic Büchi automaton for this spec?

Controller synthesis algorithms

Solving safety games

Solving reachability games

Solving deterministic Büchi games (liveness)

Remarks on the general LTL synthesis problem
Spreading Büchi automata to Büchi games

Büchi automaton:

Büchi game:

Solving deterministic Büchi games

1. Compute set of *RecurrentAccepting* states = accepting states from which controller can force returning to an accepting state infinitely often.
2. Solve reachability game with target = RecurrentAccepting.
Solving deterministic Büchi games

1. Compute set of RecurrentAccepting states = accepting states from which controller can force returning to an accepting state infinitely often.
   - $\text{RecAcc} := \text{set of all accepting states}$;
   - repeat
     - $\text{Revisit} := \{\}$;
     - repeat
       - $\text{Revisit} := \text{Revisit} \cup \text{ForceNext}(\text{Revisit} \cup \text{RecAcc})$;
       - until $\text{Revisit}$ does not change;
       - $\text{RecAcc} := \text{RecAcc} \cap \text{Revisit}$;
     - until set $\text{RecAcc}$ does not change;

Recall

$\text{ForceNext}(S) := \{ s \mid \text{all uncontrollable succs of } s \text{ are in } S \} 
\cup \{ s \mid s \text{ has controllable succ in } S \}$
Solving deterministic Büchi games – Example

- \( \text{RecAcc} := \) set of all accepting states;
- repeat
  - \( \text{Revisit} := \) \{ \};
  - repeat
    - \( \text{Revisit} := \text{Revisit} \cup \text{ForceNext}(\text{Revisit} \cup \text{RecAcc}); \)
    - until \( \text{Revisit} \) does not change;
    - \( \text{RecAcc} := \text{RecAcc} \cap \text{Revisit}; \)
- until set \( \text{RecAcc} \) does not change;

Computing recurrent accepting states: a subtle relation with reachability games

1. Compute set of \( \textbf{RecurrentAccepting} \) states = accepting states from which controller can force returning to an accepting state infinitely often.
   - \( \text{RecAcc} := \) set of all accepting states;
   - repeat
     - \( \text{Revisit} := \) \{ \};
     - repeat
       - \( \text{Revisit} := \text{Revisit} \cup \text{ForceNext}(\text{Revisit} \cup \text{RecAcc}); \)
       - until \( \text{Revisit} \) does not change;
       - \( \text{RecAcc} := \text{RecAcc} \cap \text{Revisit}; \)
     - until set \( \text{RecAcc} \) does not change;
Solving reachability games vs. computing Revisit

1. Compute set of **Winning** states:
   - \( \text{Winning} := \{ \} \);
   - repeat
     - \( \text{Winning} := \text{Winning} \cup \text{ForceNext}(\text{Winning}) \);
   - until \( \text{Winning} \) does not change;

2. Compute **Revisit**:
   - \( \text{Revisit} := \{ \} \);
   - repeat
     - \( \text{Revisit} := \text{Revisit} \cup \text{ForceNext} (\text{Revisit} \cup \text{RecAcc}) \);
   - until \( \text{Revisit} \) does not change;

Solving deterministic Büchi games – modified example

- \( \text{RecAcc} := \) set of all accepting states;
- repeat
  - \( \text{Revisit} := \{ \} \);
  - repeat
    - \( \text{Revisit} := \text{Revisit} \cup \text{ForceNext} (\text{Revisit} \cup \text{RecAcc}) \);
    - until \( \text{Revisit} \) does not change;
    - \( \text{RecAcc} := \text{RecAcc} \cap \text{Revisit} \);
  - until set \( \text{RecAcc} \) does not change;
How to extract strategies in deterministic Büchi games?

Similarly as for reachability games:

Extract strategy from \textbf{ForceNext}(S): ensure you choose the right controllable transition that leads in winning state.

Careful to choose the transition the first time state is added to S.

Is strategy state-based?
Yes!

What about non-deterministic Büchi games?
Does same algorithm work?

Not quite:
algorithm sound but incomplete.

Non-deterministic automaton for \((GFr \land GFG) \lor (FG \neg r \land FG \neg g)\)

[Paulin Chalons, PhD thesis, 2013]

Non-deterministic Büchi game
Controller synthesis algorithms

Solving safety games

Solving reachability games

Solving deterministic Büchi games (liveness)

Remarks on the general LTL synthesis problem

Controller synthesis: EE vs. CS?

CS: synthesize outputs to implement $\varphi$:

EE: synthesize inputs to stabilize a physical process/plant:

Not different: plant inputs = controller outputs (and vice versa).
Can we capture plants in the CS synthesis problem?

CS: given plant P (say, a FSM), synthesize controller C, so that closed-loop system satisfies $\varphi$:

Can we reduce this problem to the standard LTL synthesis problem?

Remarks, assessment

Despite some (mostly isolated) success stories, controller synthesis hasn’t really caught on yet in practice.

Why is that?

- Normal: things like that take time (c.f. model-checking)
- 2EXPTIME is a horrible (worst-case) complexity (remember: even linear is too expensive because of state explosion!)
- Tools still impractical
- Synthesis of real, complex systems from complete specs impractical (imagine full synthesis of complete Intel microchip from LTL specs …)
- Lack of good debugging (e.g., counter-examples)
- Need: better tools, better methods (incremental, interactive, …)
- Great opportunities for research!
References