Problem Description

Given a set of variables $x_1, \ldots, x_n$ and their primed versions $x'_1, \ldots, x'_n$, it is possbile to describe a loop which uses these variables by 3 boolean functions:

$$\mathrm{F}_{\mathrm{PRE}}(x_1, \ldots, x_n)$$
$$\mathrm{F}_{\mathrm{TRAN}}(x_1, \ldots, x_n, x'_1, \ldots, x'_n)$$
$$\mathrm{F}_{\mathrm{POST}}(x_1, \ldots, x_n)$$

With:

$\mathrm{F}_{\mathrm{PRE}}(x_1, \ldots, x_n) = 1$ denoting that the set of variables are a valid set of input variables to the loop;
$\mathrm{F}_{\mathrm{TRAN}}(x_1, \ldots, x_n, x'_1, \ldots, x'_n) = 1$ denoting that the unprimed set of input variables become its corresponding primed versions after one interation of loop
$\mathrm{F}_{\mathrm{POST}}(x_1, \ldots, x_n) = 1$ denoting that the set of input variables are a valid set of ending state of the loop

The problem is to find the invariant of the loop, a boolean function

$$\mathrm{F}_{\mathrm{INV}}(x_1, \ldots, x_n)$$

such that

$$\begin{aligned} \mathrm{F}_{\mathrm{PRE}}(x_1, \ldots, x_n) &\Rightarrow \mathrm{F}_{\mathrm{INV}}(x_1, \ldots, x_n) \\ \mathrm{F}_{\mathrm{INV}}(x_1, \ldots, x_n) \wedge \mathrm{F}_{\mathrm{TRAN}}(x_1, \ldots, x_n, x'_1, \ldots, x'_n) &\Rightarrow \mathrm{F}_{\mathrm{INV}}(x'_1, \ldots, x'_n) \\ \mathrm{F}_{\mathrm{INV}}(x_1, \ldots, x_n) &\Rightarrow \mathrm{F}_{\mathrm{POST}}(x_1, \ldots, x_n) \end{aligned}$$

Assumption and argument

Assume that the form of $\mathrm{F}_{\mathrm{PRE}}$ is

$$\mathrm{F}_{\mathrm{PRE}} \Leftrightarrow C_1^{(0)} \wedge C_2^{(0)} \wedge \ldots$$

And the form of $\mathrm{F}_{\mathrm{TRAN}}$ is:

$$\begin{aligned} \mathrm{F}_{\mathrm{TRAN}} \Leftrightarrow (&C_1^{(1)} \wedge C_2^{(1)} \wedge \ldots \\ &T_1^{(1)} \wedge T_2^{(1)} \wedge \cdots \wedge T_n^{(1)}) \vee \\ &(C_1^{(2)} \wedge C_2^{(2)} \wedge \ldots \\ &T_1^{(2)} \wedge T_2^{(2)} \wedge \cdots \wedge T_n^{(2)}) \vee \\ &\ldots \end{aligned}$$

with elements, or atoms $C_j^{(i)}$ having the form

$$C_j^{(i)} \Leftrightarrow \begin{cases} x_k \geq c \\ x_k \leq c \\ x_l - x_k \geq c \end{cases}$$

And atoms $T_j^{(i)}$ have the form

$$T_j^{(i)} \Leftrightarrow x'_j = x_j + c_j$$

We would like to prove the argument that given this assumption as a constraint, if there exists an invariant, there must exist another invariant that have the form

$$\mathrm{F}_{\mathrm{INV}} \Leftrightarrow C_1 \wedge C_2 \ldots$$

with C_i being in the same form as $C_j^{(i)}$

Terminology

We shall use certain terminology for the rest of our discussion. We will define them here.

Region A region is a set of constraints on variables.

$$f_i(x_1, x_2, \ldots, x_n) \geq 0$$

It represents a geometric region in N^n space. For CLIA problems, all region involved in the problem shall have linear boundaries. We could use a boolean function of these variables to denote a region, as a boolean function is effectively a set of constraints on it parameters. If the set of constraints of a region are all of linear forms, in other words, if f_i's are all linear functions, then we denote such a region as a **linear region**.

Subregion Given two Regions

$$R_1(x_i) \geq 0, R_2(x_i) \geq 0$$

if

$$R_1(x_i) \geq 0 \Rightarrow R_2(x_i) \geq 0$$

We denote that R_1 is a **subregion** of R_2

Regular Region A regular region is a region with the form:

$$C_1 \wedge C_2 \wedge \ldots$$

And with atomic constraints in the form being:

$$C_i \Leftrightarrow \begin{cases} x_k \geq c \\ x_k \leq c \\ x_l - x_k \geq c \end{cases}$$

Transformation A transformation is a set of constraints set on $(x_1, x_2, \ldots, x_n)$ (input variables) and $(x'_1, x'_2, \ldots, x'_n)$ (output variables) So that in one interation of the loop, given values of all variables in last interation as input variables, constraints on the new values of all variables could be determined as output variables

Linear Deterministic Transformation If a transformation T satisfies the following condition:

$$T \Leftrightarrow (x'_1 = x_1 + c_1) \wedge (x'_2 = x_2 + c_2) \wedge \cdots \wedge (x'_n = x_n + c_n)$$

with n input variables and n output variables on N^n space, then we call it a **Linear Deterministic Transformation**. We also denote the n-dimensional vector

$$(c_1, c_2, \ldots c_n)$$

as the **Transform Vector** of the transformation.

Envelope Given an input region and a transformation. A set of constraints on $(x'_1, x'_2, \ldots, x'_n)$ could be obtained from the constraints denoted by the region. These constraints actually form a region for the output variables. Denote this new region, unioned with the input region, as the envelope of the original region under one iteration of the transformation. And denote the transformation from the input region to its envelope as one **expanding** of the original region. An input region is always a subregion of its envelope.

Domains and Subdomains of a transformation If a transformation has certain conditions on its input variables that is a region:

$$T \Leftrightarrow R(\{x_k\}) \wedge T'(\{x_k, x'_k\})$$

denote that region as the **Domain** of the transformation. If a transformation is in the form of a disjunction, with each part being a domain transformation without any overlaying parts:

$$\begin{aligned} T \Leftrightarrow & (R_1(\{x_k\}) \wedge T'_1(\{x_k, x'_k\})) \\ & \vee (R_2(\{x_k\}) \wedge T'_2(\{x_k, x'_k\})) \\ & \ldots \end{aligned}$$

$$R_i \wedge R_j = \emptyset, \text{for any } i \neq j$$

Then denote this transformation as a **multi-domain** transformation, denote each of these regions as **subdomains** of the transformation and denote the transformations in subdomains as **subtransformations**.

Regular Multi-domain Transformation If the domains of a multi-domain transformation are regular regions, we denote that transformation as a regular multi-domain transformation.

Linear Deterministic Regular Multi-domain Transformation If for each domains of a regular multi-domain transformation, the subtransformations are linear Deterministic transformations, we denote the whole transformation as a linear deterministic regular multi-domain transformation.

Extended Transformation If a multi-domain transformation's subdomains do not cover the whole N^n space, then for the uncovered part of the space, or for the **undefined domain** of the transformation, constraints on output variables does not exist, so principally they could be any value. An **extended transformation** could be introduced, for which in the undfined domain of the original multi-domain transformation, $x'_k = x_k$ is enforced for all variable pairs. We still call that domain as undefined domain for convenience. Observe that this enforces the subtransformation to be linearly bounded for the undefined domains.

Contain Given a region and a transformation. If the envelope of the region under one iteration of that transformation is still a subregion of the region, we call that this transformation is **contained** with in such region. In other words, if a transformation is contained by certain region, expanding that region would not result in a region that's larger than the original region.

Equivalent expression for the problem

Using the terminology defined above, certain observations could be obtained for the problem:

- $\mathrm{F_{PRE}}, \mathrm{F_{POST}}, \mathrm{F_{INV}}$ denotes three regions in N^n space
- $\mathrm{F_{PRE}}$ should be a subregion of $\mathrm{F_{INV}}$
- $\mathrm{F_{INV}}$ should be a subregion of $\mathrm{F_{POST}}$
- Transform denoted by $\mathrm{F_{TRAN}}$ should be contained in $\mathrm{F_{INV}}$

These observations could serve as a set of equivalent expressions to the original invariant synthesis problem.

Lemmas

Certain lemmas could be obtained to help the proof of the argument as well.

Lemma 1 The envelope of a regular region under a linear deterministic regular multi-domain transformation is still a regular region.

Linear Deterministic Regular Multi-domain Transformation Conditions

Theorem 1 For an invariant synthesis problem with regular $\mathrm{F_{PRE}}$, regular $\mathrm{F_{POST}}$, and a linear deterministic regular multi-domain transformation as its $\mathrm{F_{INV}}$, if :

- there exisits a linear invariant $\mathrm{F_{INV}}'$ for this problem, and,
- the region of $\mathrm{F_{INV}}'$ has at least one complete subdomain of $\mathrm{F_{TRAN}}$ as its subregion

Then:

- Taking the combined region of all subdomains of $\mathrm{F_{TRAN}}$ that are subregions of $\mathrm{F_{INV}}'$, denoted as R_0
- The envelope of R_0, denoted as $\mathrm{F_{INV}}$, is a regular invariant of the synthesis problem

Proof:

Use proof by contradiction.

- Assume that $\mathrm{F_{INV}}$ is not an invariant
- Denote the subdomains of $\mathrm{F_{TRAN}}$ that are not subregions of $\mathrm{F_{INV}}'$ as **boundary domains** of $\mathrm{F_{TRAN}}$ for $\mathrm{F_{INV}}'$
- For input points from R_0, after one transformation, the output points have 2 possibilities:
  - They're still in R_0
    - These points are contained by R_0, thus certainly contained by $\mathrm{F_{INV}}$
  - They're in one of the boundary domains
- Thus, given that $\mathrm{F_{INV}}$ is not an invariant, there must exist some point in $\mathrm{F_{INV}}$ and also in the boundary domains of $\mathrm{F_{TRAN}}$ for $\mathrm{F_{INV}}'$, that transfers out of $\mathrm{F_{INV}}$ after one transformation
- ***KEY***: prove that this leads to points near the boundaries of $\mathrm{F_{INV}}'$ would transfer out of $\mathrm{F_{INV}}'$ as well, which would cause a contradiction
  - The directions of the boundaries may be important in providing this proof
  - Easy case: $\mathrm{F_{INV}}'$ boundaries are regular.