Problem Description

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

$$\mathrm{F}_{\mathrm{PRE}}(x_1, \dots, x_n)$$

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

$$\mathrm{F}_{\mathrm{POST}}(x_1, \dots, x_n)$$

With:

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

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

such that

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

General Terminology

Set A set, referred to in our context, is a set of points of Z^n space. It could be expressed as a set of expressions on the n variables.

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

It represents a geometric region in Z^n space. For CLIA problems, all set involved in the problem shall have linear boundaries. If the set of constraints of a set are all of linear forms, in other words, if f_i's are all linear functions, then we denote such a set as a **linearly bounded set**.

Finite Set If a set contains finite numbers of points from Z^n space, then we call it a finite set. In other words, if

$$\exists P \in Z^n, P \in R$$

has finite solutions, then R is a finite set.

Transformation A transformation is a set of constraints set on $(x_1, x_2, \dots, x_n)$ (input variables) and $(x'_1, x'_2, \dots, x'_n)$ (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

Deterministic Transformation A deterministic transformation is a transformation which could determine a set of values of the output variables with the values of input variables given. In other words, for a deterministic transformation T,

$$\exists \{x'_i\}, T(\{x_i\}, \{x'_i\})$$

has and only has one set of $\{x'_i\}$ as its solution. When T is a deterministic transformation, we denote that

$$T(\{x_i\}) = \{x'_i\}$$

or

$$T(P) = P'$$

Given that

$$P = \{x_i\}, P' = \{x'_i\}$$

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

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

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

$$\vec{c} = (c_1, c_2, ... c_n)$$

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

Using the notation of deterministic transformation above, this transformation could be expressed as

$$T(\{x_1, x_2, ..., x_n\}) = \{x_1 + c_1, x_2 + c_2, ..., x_n + c_n\}$$

Envelope Given an input set R and a deterministic transformation T. Define the envelope of R under T, $\text{Env}(R, T)$ as:

$$\text{Env}(R, T) = R \vee \{P' | P' = T(P), P \in R\}$$

We denote the transformation from a set to its envelope under certain deterministic transformation as one expansion of that set under such transformation, and we could keep doing that expansion on the expanded envelope.

Regions of a transformation If a transformation has certain conditions on its input variables that is a set:

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

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

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

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

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

Extended Transformation If a multi-region transformation's regions do not cover the whole Z^n space, then for the uncovered part of the space, or for the **undefined regions** 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 regions of the original multi-region transformation, $x'_k = x_k$ is enforced for all variable pairs. We still call that domain as undefined regions for convenience. Observe that this enforces the subtransformation to be linear deterministic for the undefined regions.

Contain Given a set R and a transformation T. If

$$\forall P \in R, T(P) \in R$$

Then we note that T is **contained** by R, this could also be expressed as:

$$T \wedge R \Rightarrow R(\{x'_i\} \rightarrow \{x_i\})$$

Equivalent expression for the problem

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

- $\mathrm{F}_{\mathrm{PRE}}, \mathrm{F}_{\mathrm{POST}}, \mathrm{F}_{\mathrm{INV}}$ denotes three sets in Z^n space
- $\mathrm{F}_{\mathrm{PRE}}$ should be a subset of $\mathrm{F}_{\mathrm{INV}}$
- $\mathrm{F}_{\mathrm{INV}}$ should be a subset of $\mathrm{F}_{\mathrm{POST}}$
- Transform denoted by $\mathrm{F}_{\mathrm{TRAN}}$ should be contained in $\mathrm{F}_{\mathrm{INV}}$

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

Proof on finite bound problems

Assumption and argument

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

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

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

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

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 that is a finite set, there must exist another invariant that have the form

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

with C_i being in the same form as $C_j^{(i)}$, and such invariant could be obtained by expanding $\mathrm{F}_{\mathrm{PRE}}$ for finite times.

Terminology

Octagon An Octagon is a set with the form:

$$C_1 \wedge C_2 \wedge ...$$

And with atomic constraints in the form being:

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

Combination of Octagons A combination of octagons is a set with the form:

$$R_1 \vee R_2 \vee ...$$

And with each of these R_i being an octagon.

Octagonal Multi-region Transformation If the regions of a multi-region transformation are octagons, we denote that transformation as a octagonal multi-region transformation.

Linear Deterministic Octagonal Multi-region Transformation If for each regions of a octagonal multi-region transformation, the subtransformations are linear Deterministic transformations, we denote the whole transformation as a linear deterministic octagonal multi-region transformation. ## Lemmas

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

Lemma 1 A set is a combination of octagons iff. the equations of the boundaries of this set is of form f_i, with f_i being:

$$f_i \Leftrightarrow \begin{cases} x_i = c_i \\ x_i - x_j = c_{ij} \end{cases}$$

Proof.

If set R is a combination of octagons, then the atomic expression of its logical form is $C_j^{(i)}$, so the boundary equation forms of R shall be the equation version of the inequalities in $C_j^{(i)}$, which is of form f_i

If set R has boundary equations in form of f_i, the logical form of R shall consist of inequality version forms of these equations as its atomic expression, which is $C_j^{(i)}$, and we could always convert this form into a disjunction normal form (DNF), which is the same notation as it is in the definition of combinations of octagons, thus R is a combination of octagons.

Lemma 2 Transformation T is contained by set R iff. the envelope of R under T should be R iff. $\{P'|T(P) = P', P \in R\} \subseteq R$

Proof.

$$\forall P \in R, T(P) \in R \Leftrightarrow \{P'|T(P) = P', P \in R\} \subseteq R \Leftrightarrow R \vee \{P'|T(P) = P', P \in R\} = R$$

Lemma 3 Conjunctions and disjunctions of combinations of octagons are still combinations of octagons.

Proof. Given combination of octagons:

$$R_1 = r_{11} \vee r_{12} ... r_{1n}$$
$$R_2 = r_{21} \vee r_{22} ... r_{2n}$$

$R_1 \vee R_2$ is in the same form of combinations of octagons definition, so it is a combination of octagons as well $R_1 \wedge R_2$ could be converted into disjunction normal form, which is in the same form of combinations of octagons definition as well, so it is a combination of octagons too.

Lemma 4 The envelope of a combination of octagons R under a linear deterministic octagonal multi-region transformation T, $\text{Env}(R, T)$, is still a combination of octagons

Proof.

Consider different portions in R that contributes to

$$R' = \{P'|P' = T(P), P \in R\}$$

As the whole Z^n space is divided by T's regions without any overlaying parts, it should be possible to split R into subsets without overlaying parts with each subset being in a different region of T.

Formally, denote the regions of T as $D_1, D_2, ... D_m$, R could be written as

$$R = R_1 \vee R_2 \vee ... R_m$$

with

$$R_i \Rightarrow D_i$$

and

$$R_i \wedge R_j = \emptyset, i \neq j$$

Then, for each these subsets, points in it have a contribution in R', denote them as

$$R'_i = \{P' | P' = T(P), P \in R_i\}$$

R_i is R separated by region boundaries of T, thus its boundaries shall be either a boundary from R's boundaries or a boundary from T's region boundaries. These boundaries all have the forms of f_i, thus according to **Lemma 1**, R_i is a combination of octagons.

As $R_i \Rightarrow D_i$, denote the transform vector in D_i as $\vec{t_i}$, all points in R_i are moved by vector $\vec{t_i}$ to form R'_i, thus the boundaries are just moved by $\vec{t_i}$ as well, they're still in forms of f_i, thus R'_is are combinations of octagons as well.

Then using **Lemma 3** $R' = R'_1 \vee R'_2 \vee ... \vee R'_m$ is a combination of octagons as well.

Also then $\text{Env}(R, T) = R \vee R'$ is a combination of octagons.

Lemma 5 If transformation T is contained in R, and $R_s \subseteq R$, then $\text{Env}(R_s, T) \subseteq R$

Proof.

T is contained in R, so $\{P' | P' = T(P), P \in R\} \subseteq R$ (**Lemma 2**)

And

$$R_s \subseteq R$$

thus

$$\{P' | P' = T(P), P \in R_s\} \subseteq \{P' | P' = T(P), P \in R\} \subseteq R$$

thus

$$\text{Env}(R_s, T) = R_s \vee \{P' | P' = T(P), P \in R_s\} \subseteq R$$

Proof

Theorem 1 For an invariant synthesis problem with F_{PRE} in the form of a combination of octagons, an arbitrary F_{POST} that makes sense, and a linear deterministic octagonal multi-region transformation as its F_{TRAN}, if :

- there exisits an invariant $\text{F}_{\text{INV}}{}'$ for this problem, and,
- the set of $\text{F}_{\text{INV}}{}'$ is a finite set

Then, there should exist another F_{INV} for the this problem, and F_{INV} shall be a combination of octagons, and such F_{INV} could be obtained by expanding F_{PRE} for finite times.

Proof.

First, we take the pre-condition F_{PRE} and expand it to its envelope $\text{Env}(\text{F}_{\text{PRE}}, T)$, it is obivous that $\text{F}_{\text{PRE}} \subseteq \text{Env}(\text{F}_{\text{PRE}}, T)$ according to the definition of envelopes.

We denote the number of points in set R as $|R|$, then we have $|R| \leq |\mathrm{Env}(R,T)|$ according to the definition of envelopes.

Denote that

$$\mathrm{Env}^n(R,T) = \mathrm{Env}(\mathrm{Env}^{n-1}(R,T),T)$$

and

$$\mathrm{Env}^0(R,T) = R$$

Assume that

$$\forall n \in Z, \mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T) \neq \mathrm{Env}^n(\mathrm{F_{PRE}},T)$$

.

This leads to

$$|\mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T)| \neq |\mathrm{Env}^n(\mathrm{F_{PRE}},T)|$$

We also have

$$|\mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T)| \leq |\mathrm{Env}^n(\mathrm{F_{PRE}},T)|$$

Thus

$$|\mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T)| < |\mathrm{Env}^n(\mathrm{F_{PRE}},T)|$$

We are on Z^n space, thus all these should be integer numbers, thus

$$|\mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T)| + 1 \leq |\mathrm{Env}^n(\mathrm{F_{PRE}},T)|$$

Expanding the set to its envelope shall at least increase the set size by 1.

On the other hand, according to the original problem, T shall be contained in $\mathrm{F_{INV}}'$, thus for any subset of T, its envelop under T shall still be a subset of T (**Lemma 5**).

So

$$\forall n \in Z, \mathrm{Env}^n(\mathrm{F_{PRE}},T) \subseteq \mathrm{F_{INV}}'$$

so

$$|\mathrm{Env}^n(\mathrm{F_{PRE}},T)| \leq |\mathrm{F_{INV}}'|$$

But as $\mathrm{F_{INV}}'$ is finite, $|\mathrm{F_{INV}}'|$ is finite as well, and the set size increases at least one after expansion.

$$\exists m \in Z, \mathrm{Env}^m(\mathrm{F_{PRE}},T) > |\mathrm{F_{INV}}'|$$

That raise a contradiction, so the assumption shall not hold, thus

$$\exists n \in Z, \mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T) = \mathrm{Env}^n(\mathrm{F_{PRE}},T)$$

We denote $\mathrm{F_{INV}} = \mathrm{Env}^{n-1}(\mathrm{F_{PRE}},T)$, thus

$$\mathrm{F_{INV}} = \mathrm{Env}(\mathrm{F_{INV}},T)$$

According to **Lemma 2**, this means T is contained by $\mathrm{F_{INV}}$ and thus $\mathrm{F_{INV}}$ is a invariant solution for the original problem.

According to **Lemma 4**, $\mathrm{F_{INV}}$ is generated by expanding $\mathrm{F_{PRE}}$ for finite times, as $\mathrm{F_{PRE}}$ is a combination of octagons, $\mathrm{F_{INV}}$ is a combination of octagons as well.

Q.E.D.

Intermediate ideas: Stable Regions and Safe Zones

- A region is stable if
  - A set expanding into such a region would either:
    - Be expanding infinitely in such region and covering all points in a direction.
    - Reach a fixed point
  - And either way, it would never exit such region again.
  - That property could be captured syntactically using constraints on the formations of the transformation regions and transformation vectors
- With stable regions in a transformation identified, we could define a safe zone for the transformation
  - A safe zone of a transforamtion is a set in the space such that it contains all points that, after a finite number of transforamtion steps, would step into a stable region
  - This could be obtained by "reverse expanding" the stable regions.
- We can defined the compliment of a safe zone as the unsafe zone of the corresponding transformation
- If the unsafe zone is finite, the strongest invariant shall be obtained by keep expanding from the pre condition set.
  - Expanding that way, a set would either
    - Expand into a stable region and yield a part of invariant in that region.
    - Reach a fixed point after some expansions
      - This could be proved in the same manner as the finite invariant proof.

General ideas: Any system that will not create a loop should work

Terminology

Transformation Graph For a deterministic multi-region transformation, define two sets:

$$V = \{R_i | R_i \text{ is a region of transformation } T\}$$

$$E = \{(R_i, R_j) | \exists P \in R_i, T(P) \in R_j\}$$

Then (V, E) effectively defined a directed graph. We note this graph as the **transformation graph** of transformation T

Loop-free transformation For a linear deterministic multi-region transformation, if its transformation graph is acyclic, then we denote this transformation as a **loop-free transformation**

Strong Invariant For a linear deterministic multi-region transformation T with $\mathrm{F}_{\mathrm{PRE}}$, $\mathrm{F}_{\mathrm{POST}}$ and one of its invariant $\mathrm{F}_{\mathrm{INV}}$, if in addition to the definition of invariants, this invariant satisfies:

$$\forall P \in \mathrm{F}_{\mathrm{INV}}, \exists P' \in \mathrm{F}_{\mathrm{PRE}}, \exists n \in Z^+, T^{(n)}(P') = P$$

Continuation For a deterministic multi-region transformation T, and a set S, if there exists another set S', so that

$$\forall P' \in S', \exists P \in S, \exists n \geq 0, T^{(n)}(P) = P'$$

and

$$\forall n \geq 0, \forall P \in S, \exists P' \in S', T^{(n)}(P) = P'$$

then we say that S' is a **continuation** of S under T, denoted as

$$\mathrm{Cont}(S, T) = S'$$

Note: as when $n = 0$, we have $T^{(0)}(P) = P$, it is obvious that a continuation of a set shall contain all the points in the original set, in other words, $S \subseteq \mathrm{Cont}(S, T)$

Modular Set For a set S, we call the set

$$S' = S \wedge (x_i = r_i \mod m_i)$$

as the **modular set** of S on x_i with $r_i \mod m_i$, denoted as

$$S' = \text{Modu}(S, x_i, r_i, m_i)$$

Modular Partitions For a set S, we call the series of set

$$\text{Modu}(S, x_i, 1, m_i), \text{Modu}(S, x_i, 2, m_i), \dots, \text{Modu}(S, x_i, m_i - 1, m_i)$$

as a series of **modular partition** of S on x_i with m_i

Modular Octagon We call the modular set of an octagon as a **modular octagon**

Modular Partition of a Set For a linear deterministic multi-region transformation T with a set S, we call the following procedure of partitioning set S' as determining the modular partition of S under T

First take partitions of S by the regions of T:

$$S_i = S \wedge R_i$$

Then, for each S_i, assume that the transformation vector in R_i is

$$(\delta x_1^{(i)}, \dots, \delta x_n^{(i)})$$

we partition S_i into $\delta x_1^{(i)} \times \cdots \times \delta x_n^{(i)}$ modular partitions:

$$S_i^{(m_1,\dots,m_n)} = \text{Modu}(\dots \text{Modu}(\text{Modu}(S, x_1, m_1, \delta x_1^{(i)}), x_2, m_2, \delta x_2^{(i)}) \dots, x_n, m_n, \delta x_n^{(i)})$$

Expressed equivalently:

$$S_i^{(m_1,\dots,m_n)} = S \wedge (x_1 = m_1 \mod \delta x_1^{(i)}) \wedge \dots (x_n = m_n \mod \delta x_n^{(i)})$$

And we denote this partition as:

$$S_i^{(m_1,\dots,m_n)} = \text{MPart}(S, T, R_i, \vec{m}), \vec{m} = (m_1, \dots, m_n)$$

Modular Expansion of a Octagon For a linear deterministic multi-region transformation T with a set S, we call the following procedure of determining set S' as determining the modular expansion of S under T

First, take the modular partitions of S under T, for a partition

$$S_i^{(m_1,\dots,m_n)}$$

Take its envelope,

$$\text{Env}(S_i^{(m_1,\dots,m_n)})$$

and taking the union of all these envelopes as the output

$$S' = \bigvee_{i,m_1,\dots m_n} \text{Env}(S_i^{(m_1,\dots,m_n)})$$

Denoted

$$S' = \text{MExp}(S, T)$$

Modular Extension of a Octagon For a linear deterministic octagonal multi-region transformation T with a set S, we call the following procedure of determining set S' as determining the modular extension of S under T

First, take the modular partitions of S under T, for a partition

$$S_i^{(m_1,...,m_n)}$$

It is trival to note that this set shall be a modular octagon, so it would be in the form of

$$C_1 \wedge C_2 \wedge ... \wedge (x_1 = m_1 \mod \delta x_1^{(i)}) \wedge ... (x_n = m_n \mod \delta x_n^{(i)})$$

Also note that R_i shall be an octagon, in form of

$$C_1' \wedge C_2' \wedge ...$$

We than do the following for this set:

This definition of extension is currently broken, the operations above could not guarantee that all extensible partitions are captured and are extented in a correct way

For each variable x_l in the problem, it has a corresponding δx_l in region R_i of T, for these values, if they all satisfy the following properties: - $\delta x_l = 0$, or - $\delta x_l > 0$, and R_i don't have forms of boundries like

$$x_l \leq c, x_l \pm x_m \leq c$$

, or - $\delta x_l < 0$, and R_i don't have forms of boundries like

$$x_l \geq c, x_l \pm x_m \geq c$$

Then this partition would be locally extensible, we obtain the extension by: - for any $\delta x_l > 0$, remove all boundries in $S_i^{(m_1,...,m_n)}$ that are in the form

$$x_l \leq c, x_l \pm x_m \leq c$$

, and - for any $\delta x_l < 0$, remove all boundries in $S_i^{(m_1,...,m_n)}$ that are in the form

$$x_l \geq c, x_l \pm x_m \geq c$$

, and

We denote the set that is obtained after doing these procedures above for each variable as the local extension of $S_i^{(m_1,...,m_n)}$

$$\text{LExt}(S_i^{(m_1,...,m_n)}, T, R_i)$$

The final output of modular extension is obtained by taking the union of the local extensions of all these partitions:

$$S' = \bigvee_{i,m_1,...m_n} \text{LExt}(S_i^{(m_1,...,m_n)}, T, R_i)$$

Denoted

$$S' = \text{MExt}(S, T)$$

Assumption and Argument

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

$$\mathrm{F_{PRE}} \Leftrightarrow C_1^{(0)} \wedge C_2^{(0)} \wedge ...$$

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

$$\begin{aligned}\mathrm{F_{TRAN}} \Leftrightarrow (&C_1^{(1)} \wedge C_2^{(1)} \wedge ... \\ &T_1^{(1)} \wedge T_2^{(1)} \wedge ... \wedge T_n^{(1)}) \vee \\ &(C_1^{(2)} \wedge C_2^{(2)} \wedge ... \\ &T_1^{(2)} \wedge T_2^{(2)} \wedge ... \wedge T_n^{(2)}) \vee \\ &...\end{aligned}$$

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

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

The argument we would like to prove is 2-fold. Firstly, we would like to prove that, if the transformation T is a loop-free, and we denote the operator O as

$$O(S, T) = \mathrm{MExp}(\mathrm{MExt}(S, T), T)$$

then there exists $n \in Z^+$, such that

$$O^{n+1}(S, T) = O^n(S, T)$$

Secondly, if this $O^n(S, T)$ satisfies $O^n(S, T) \subseteq \mathrm{F_{POST}}$, then this $O^n(S, T)$ is a strong invariant of this problem.

Lemmas

Lemma 6 For a deterministic multi-region transformation T, and a set S, if

$$S = S_1 \vee S_2 \vee ... \vee S_k$$

, and

$$S_i' = \mathrm{Cont}(S_i, T), i = 1, ..., k$$

then

$$S' = S_1' \vee S_2' \vee ... \vee S_k' = \mathrm{Cont}(S, T)$$

Proof.

$\forall P \in S'$, as $S' = S_1' \vee ... \vee S_k'$,

$$\exists S_i', P \in S_i'$$

And $S_i' = \mathrm{Cont}(S_i, T)$, so

$$\exists P' \in S_i, \exists n \geq 0, T^{(n)}(P') = P$$

As $S_i \subseteq S$, this proves

$$\exists P' \in S, \exists n \geq 0, T^{(n)}(P') = P$$

and thus justify the first part of continuation definition.

$\forall P \in S, \forall n \geq 0$, as $S = S_1 \vee ... \vee S_k$

$$\exists S_i, P \in S_i$$

And $S_i' = \text{Cont}(S_i, T)$, so

$$\exists P' \in S_i', T^{(n)}(P) = P'$$

As $S_i' \subseteq S'$, this proves

$$\exists P' \in S', T^{(n)}(P) = P'$$

and thus justify the second part of continuation definition.

So that,

$$S' = \text{Cont}(S, T)$$

Q.E.D.

Lemma 7 For a deterministic multi-region transformation T with $\text{F}_{\text{PRE}}, \text{F}_{\text{POST}}$ to form a problem, and a set F_{INV}.

$$\text{F}_{\text{INV}} \text{ is a strong invariant of the problem} \Leftrightarrow (\text{F}_{\text{INV}} = \text{Cont}(\text{F}_{\text{PRE}}, T)) \wedge (\text{F}_{\text{INV}} \subseteq \text{F}_{\text{POST}})$$

Proof.

The forward direction:

If F_{INV} is a strong invariant of the problem, then by definition we have $\text{F}_{\text{INV}} \subseteq \text{F}_{\text{POST}}$

And

$$\forall P \in \text{F}_{\text{INV}}, \exists P' \in \text{F}_{\text{PRE}}, \exists n \in Z^+, T^{(n)}(P') = P$$

This proves the first part of continuation definition.

For the second part, consider $\forall P \in \text{F}_{\text{PRE}}$, assume $\exists n \geq 0$

$$T^{(n)}(P) \notin \text{F}_{\text{INV}}$$

As $P \in \text{F}_{\text{PRE}} \subseteq \text{F}_{\text{INV}}$ there must exist a $n \geq m \geq 0$, so that

$$T^{(m)}(P) \in \text{F}_{\text{INV}}, T^{(m+1)}(P) \notin \text{F}_{\text{INV}}$$

This contradicts with the F_{INV} property of

$$\forall Q \in \text{F}_{\text{INV}}, T(Q) \in \text{F}_{\text{INV}}$$

So the assumption should not hold, thus

$$\forall n \geq 0, T^{(n)}(P) \in \text{F}_{\text{INV}}$$

This proves the second part of continuation definition.

So that the forward direction is proven.

Now the backward direction:

If $S = \text{Cont}(\text{F}_{\text{PRE}}, T)$, according to the first property of continuation, $\forall P \in \text{F}_{\text{INV}}$

$$\exists n \geq 0, \exists Q \in \text{F}_{\text{PRE}}, P = T^{(n)}(Q)$$

then according to the second property of continuation, we have

$$T(P) = T^{(n+1)}(Q) \in \mathrm{F}_{\mathrm{INV}}$$

This effectively proves

$$\forall P \in \mathrm{F}_{\mathrm{INV}}, T(P) \in \mathrm{F}_{\mathrm{INV}}$$

Together with $\mathrm{F}_{\mathrm{INV}} \subseteq \mathrm{F}_{\mathrm{POST}}$ this proves $\mathrm{F}_{\mathrm{INV}}$ is a invariant.

We already have the first property of continuation in the same form as the strong invariant additional property, thus this proves $\mathrm{F}_{\mathrm{INV}}$ is a strong invariant.

So that the backward direction is proven.

Q.E.D.

Lemma 8 This lemma is where I found the flaw, this lemma should be used to prove that, a set is extensible (S is extensible iff. all points in S would not leave the region S is in after arbitrary number of transformations) iff. the boundary conditions in the "Modular Extension" definition is met.

Lemma 9 For a linear deterministic octagonal multi-region transformation T with a octagon S, if S is the subset of a region R_i of T, $S \subseteq R_i$, and S satisfies:

$$\forall n \geq 0, \forall P \in S, T^{(n)}(P) \in R$$

then we take the modular extension of S,

$$S' = \mathrm{MExt}(S, T)$$

S' shall be a continuation of S under T:

$$S' = \mathrm{Cont}(S, T)$$

** As the flaw causes the definition of modular extension may need to be modified, the proof of this lemma needs to be rewritten**

Lemma 10 For a linear deterministic multi-region transformation T with a set S, S could be partitioned by regions of T:

$$S_i = S \wedge R_i, i = 1, ..., k$$
$$S = S_1 \vee ... \vee S_k$$

then modular expansion could be performed separately on these partions then unioned:

$$\mathrm{MExp}(S, T) = \mathrm{MExp}(S_1, T) \vee ... \vee \mathrm{MExp}(S_k, T)$$

Proof.

As the first step of modular expansion is to partition the input set, this argument is trival to prove

Lemma 11 For a linear deterministic octagonal multi-region transformation T with a octagon S, S could be partitioned by regions of T:

$$S_i = S \wedge R_i, i = 1, ..., k$$
$$S = S_1 \vee ... \vee S_k$$

then modular extension could be performed separately on these partions then unioned:

$$\mathrm{MExt}(S, T) = \mathrm{MExt}(S_1, T) \vee ... \vee \mathrm{MExt}(S_k, T)$$

Proof.

As the first step of modular extension is to partition the input set, this argument is trival to prove

the expression this lemma needs to be modified as modular extension definition is to be modified, but the proof should remain trival even after modification

Proof

For an octagonal $\mathrm{F_{PRE}}$ that is an octagon in a linear deterministic octagonal multi-region loop-free transformation T. As the transformation graph for T is loop-free, performing transformation continuously on any point in $\mathrm{F_{PRE}}$ shall end up in a region, in which any further transformation would not move the point out of the region.

Thus, for any point in $\mathrm{F_{PRE}}$ we could associate a finite path of regions with it

$$(R_{p_1}, R_{p_2}, ... R_{p_j}), p_i \neq p_j \text{ when } i \neq j$$

We could partition $\mathrm{F_{PRE}}$ based on the different paths associated with the points

We need an additional lemma here to prove that the modular extension operation is applicable to these partitions. I thought before that being an octagon should guarantee that, and the extension operation shall always preserve the octagon property so it is a trival argument, but now the flaw is that the extension operation may not preserve that property, so we need to modify both the extension operation's applicability conditions and the operation itself, then provide a concrete proof on this lemma

When the modular expansion and modular extension operation is performed on the whole set, take one partition with path $(R_{p_1}, R_{p_2}, ..., R_{p_j})$ to consider. Denote this partition as S

According to the path definition, we should have $S \subseteq R_{p_1}$, and

$$T^{(i)}(S) \subseteq R_{p_{i+1}}, i < j$$

$$T^{(i)}(S) \subseteq R_{p_j}, i \geq j$$

As $p_i \neq p_j$ when $i \neq j$, this means that

$$\forall i < j-1, \forall P \in T^{(i)}(S), \exists l \geq 0, T^{(l)}(P) \in R_{p_j} \neq R_{p_{i+1}}$$

So that according to lemma 8, $T^{(i)}(S), i < j-1$ would not satisfy the boundary conditions of modular extension.

This means $O^{(i)}(S), i < j-1$ would not satisfy the boundary conditions of modular extension, and when $i < j-1$ $O^{(i)}(S) = S \vee T(S) \vee ... T^{(i)}(S)$

Proof for this argument could be done by induction:

for $i = 0$, $O^{(i)}(S) = S = T^{(0)}(S)$ as $0 < j-1$, S would not satisfy the conditions.

Assume $O^{(k)}(S), k+1 < j-1$ does not satisfy the conditions, and $O^{(k)}(S) = S \vee T(S) \vee ... T^{(k)}(S)$ then $O^{(k+1)}(S) = O(O^{(k)}(S)) = \mathrm{MExp}(\mathrm{MExt}(O^{(k)}(S)))$ as $O^{(k)}(S)$ does not satisfy the conditions,

$$\mathrm{MExt}(O^{(k)}(S)) = O^{(k)}(S)$$

so

$$O^{(k+1)}(S) = \mathrm{MExp}(O^{(k)}(S)) = T(O^{(k)}(S)) \vee O^{(k)}(S)$$

put $O^{(k)}(S)$ expression in, and we've got

$$O^{(k+1)}(S) = S \vee T(S) \vee ... \vee T^{(k+1)}(S)$$

And this form shall not satisfy the conditions, either.

Thus by mathematical induction the original argument is proven

This means O operations do not apply MExt on $O^{(i)}(S)$ when $i < j-1$

When $i = j$,

$$O^{(i)}(S) = O^{(j)}(S) = O(O^{(j-1)}(S))$$

, And

$$O^{(j-1)}(S) = O(O^{(j-2)}(S)) = \text{MExp}(T \vee T(S) \vee ... \vee T^{(j-2)}(S)) = O^{(j-2)}(S) \vee T^{(j-1)}(S)$$

According to the definition of paths, $\forall P \in T^{(j-1)}(S), \forall n \geq 0$

$$T^{(n)}(P) \in R_{p_j}$$

So according to lemma 9

$$\text{MExt}(T^{(j-1)}(S)) = \text{Cont}(T^{(j-1)}(S))$$

As

$$\text{MExt}(O^{(j-2)}(S)) = O^{(j-2)}(S)$$

and

$$T^{(j-1)}(S) \subseteq R_{q_j}, O^{(j-2)}(S) \wedge R_{q_j} = \emptyset$$

if we partition $O^{(j-2)}(S)$ by the regions to $P_1, P_2, ..., P_t$ then $P_1, P_2, ..., P_t, T^{(j-1)}(S)$ shall be a valid partition by regions of $O^{(j-1)}(S)$

Then according to lemma 11, $\text{MExt}(O^{(j-1)}(S)) = \text{Cont}(T^{(j-1)}(S)) \vee O^{(j-2)}(S)$

As

$$O^{(j-2)}(S) = T \vee T(S) \vee ... \vee T^{(j-2)}(S)$$

$\text{MExt}(O^{(j-1)}(S))$ shall satisfy the two properties of continuation of S as well So

$$\text{MExt}(O^{(j-1)}(S)) = \text{Cont}(S)$$

Then

$$O^{(j)}(S) = \text{MExp}(\text{Cont}(S))$$

According to the definition of continuation, it is trival that

$$\text{MExp}(\text{Cont}(S)) = \text{Cont}(S)$$

So

$$O^{(j)}(S) = \text{Cont}(S)$$

Also we have that

$$O^{(i+1)}(S) = O^{(i)}(S), i \geq j$$

For this particular partition, after jth O operation, we obtain the continuation of the partition

Then for the entire F_{PRE}, after sufficient times of O operations, every partition transforms to the continuation of that partition

Thus according to lemma 6, the whole set of F_{PRE} after sufficient times of operations, turns into a continuation of F_{PRE}

According to lemma 7, this proves that, if this continuation C has $C \subseteq \text{F}_{\text{POST}}$, then it is a strong invariant to the problem.