AUTOMATIC SYNTHESIS OF OPTIMAL IN Variant ASSERTIONS:
MATHEMATICAL FOUNDATIONS

Patrick Cousot* and Radhia Cousot**
Laboratoire d'Informatique, U.S.M.G., BP.53
38041 Grenoble cedex, France

1. INTRODUCTION

The problem of discovering invariant assertions of programs is explored in light of the fixpoint approach in the static analysis of programs, Cousot [1977a], Cousot[1977b]. In section 2 we establish the lattice theoretic foundations upon which the synthesis of invariant assertions is based. We study the resolution of a fixpoint system of equations by Jacobi's successive approximations method. Under continuity hypothesis we show that any chaotic iterative method converges to the optimal solution. In section 3 we study the deductive semantics of programs. We show that a system of logical forward equations can be associated with a program using the predicate transformer rules which define the semantics of elementary instructions. The resolution of this system of semantic equations by chaotic iterations leads to the optimal invariants which exactly define the semantics of this program. Therefore these optimal invariants can be used for total correctness proofs (section 4). Next we show that usually a system of inequations is used as a substitute for the system of equations. Hence the solutions to this system of inequations are approximate invariants which can only be used for proofs of partial correctness (section 5). In section 6 we show that symbolic execution of programs consists in fact in solving the semantic equations associated with this program. The construction of the symbolic execution tree corresponds to the chaotic successive approximations method. Therefore symbolic execution permits optimal invariant assertions to be discovered provided that one can pass to the limit, that is consider infinite paths in the symbolic execution tree. Induction principles can be used for that purpose. In section 7 we show how difference equations can be utilized to discover the general term of the sequence of successive approximations so that optimal invariants are obtained by a mere passage to the limit. In section 8 we show that an approximation of the optimal solution to a fixpoint system of equations can be obtained by strengthening the term of a chaotic iteration sequence. This formalizes the synthesis of approximate invariants by heuristic methods. Various examples provide a helpful intuitive support to the technical sections.

2. RESOLUTION OF A FIXPOINT SYSTEM OF EQUATIONS BY
CHAOTIC ITERATIONS

We denote by \((L, \leq, 1, \bigcup, \bigcap)\) a complete lattice with respect to the partial ordering \(\leq\). We use the symbols \(\bigcup, \bigcap\) for the finite and infinite lattice operations of join and meet. The infimum \(1\) and supremum \(\tau\) of the lattice are defined by \(1 = \bigcap L\) and \(\tau = \bigcup L\) (Birkhoff[1967]).

A function \(\psi : L \to L\) of \(L\) into \(L\) is isotone (synonymously, order-preserving or monotone) if and only if \(\forall x, y \in L, (x \leq y) \Rightarrow (\psi(x) \leq \psi(y))\).

We define the limit of a chain \(x^0 \leq x^1 \leq \ldots \leq x^k \leq \ldots\) to be its least upper bound, \(\lim_{k \to \infty} x^k = \bigcup_{k=0}^{\infty} x^k\).

A function \(\psi : L \to L\) is continuous if and only if for any chain \(x^k, k \geq 0, \ldots\) we have \(\lim_{k \to \infty} \psi(x^k) = \psi(\lim_{k \to \infty} x^k)\). Note that a continuous function is necessarily isotone.

* Attached de Recherche au CNRS, Laboratoire Associé n°7.
** This work was supported by IRIA-SEISORI under grant 76-160.
We denote by $L^n$ the set of all vectors $X=(X_1, \ldots, X_n)$, the components of which belong to $L$. 
($L^n, \leq, \cup, \cap, 0, 1$) is a complete lattice with the usual "componentwise" definitions: 
$\{X \leq Y \iff \forall i (X_i \leq Y_i)\}$, $\{Y \leq F(X)\}$, $\{X \cup Y = ((X_1 \cup Y_1), \ldots, (X_n \cup Y_n))\}$, etc.
A function of several variable $f : L^n \to L$ is said to be isotope (continuous) in the variables jointly if and only if it is isotope (continuous) in the variables separately.

Hereafter we will consider a system of continuous equations with $n$ variables of the form:
$$\begin{align*}
X_1 &= F_1(X_1, \ldots, X_n) \\
& \vdots \\
X_n &= F_n(X_1, \ldots, X_n)
\end{align*}$$
This system can be abbreviated by a fixpoint equation $X=F(X)$ where $X$ is the vector $(X_1, \ldots, X_n)$ and $F$ a continuous function of type $L^n \to L^n$.

An element $X$ of $L^n$ is a fixpoint of $F : L^n \to L^n$ if and only if $F(X)=X$. The least fixpoint $\text{fp}(F)$ of $F$ is such that:
$$\{F(\text{fp}(F))=\text{fp}(F)\} \quad \text{and} \quad \{X \leq \text{fp}(F) \iff F(X) \leq X\}.$$

THEOREM (Tarski[1955]) Any monotone map $F$ of a complete lattice $L$ into itself has a least fixpoint defined by: $\text{fp}(F) = \cap \{X \leq L : F(X) \leq X\}$.

In practice this theorem is not constructive since in general the set $\{X \leq L : F(X) \leq X\}$ of post-fixpoints of $F$ is infinite and cannot be easily characterized. Yet, if $F$ is continuous Kleene[1952] and Tarski[1955] suggest that the least fixpoint of $F$ can be obtained as the limit of a sequence of successive approximations $X^0 = \bot, X^1 = F(X^0), \ldots, X^k = F(X^{k-1})$, ... that is $\text{fp}(F) = \lim_{k \to \infty} X^k$ where $X^k$ denotes the $k$-fold composition of $F$ with itself. This is nothing else than Jacobi's method of successive approximations:
$$X^k = F_1(X^{k-1}, X^{k-1}, \ldots, X^{k-1}) \quad (k=1,2,\ldots)$$
We now generalize this result by showing that any chaotic iteration method converges to the least fixpoint of $F$. Otherwise stated this signifies that one can arbitrarily determine at each step which are the components of the system of equations which will evolve and in what order (as long as no component is forgotten indefinitely).

Let $J$ be a non-empty subset of $\{1, \ldots, n\}$. We denote by $F_J$ the map $L^n \to L^n$ defined by:
$$F_J(X_1, \ldots, X_n) = (Y_1, \ldots, Y_n)$$
where $Y_i = F_i(X_i)$ if $i \in J$ then $F_J(X_1, \ldots, X_n)$ else $X_i$. $F_i$

**DEFINITION 2.1** A chaotic iteration corresponding to the operator $F$ and starting with a given vector $X^0$ such that $X^0 \leq F(X^0) \leq \text{fp}(F)$ is a sequence $X^k$, $k=0, 1, \ldots$ of vectors of $L^n$ defined recursively by $X^{k+1} = F_J(X^k)$ where $J^k$, $k=0, 1, \ldots$ is a sequence of subsets of $\{1, 2, \ldots, n\}$ such that $\forall \emptyset \neq M \subseteq \{1, 2, \ldots, n\}, \forall k \geq 0 : F(M, \ldots, X^n) \leq F(M, X^n)$.

**THEOREM 2.2** The limit $X^\infty$ of a chaotic iteration $X^0, \ldots, X^k, X^{k+1}, \ldots$ is equal to $\text{fp}(F)$.

**Lemma 2.2.1** \{$\forall k \geq 0, X^k \leq X^{k+1} \iff F(X^k) \leq \text{fp}(F)$\}.

**Proof**: Let us first remark that whenever $X \leq F(X) \leq \text{fp}(F)$ we have $\forall k \geq 0, X \leq F(X) \leq \text{fp}(F)$. Indeed $\forall k \geq 0, X \leq F(X) \leq \text{fp}(F)$ therefore if $x \leq F(x)$ then $x \leq F(x) = F(y)$, otherwise $F(x) = F(y)$. Since by hypothesis $X^0 \leq F(X^0) \leq \text{fp}(F)$ this implies $X^0 \leq F(X^0) \leq F(X^0) \leq \text{fp}(F)$. For the induction step let us assume that $X^{k+1} \leq X^k \leq F(X^{k+1}) \leq F(X^k)$. If $i \notin J^k$ then $X_{i+k} = X_{i+k}$, otherwise $X_{i+k} = F_{i+k}(X_{i+k})$, $F_{i+k}(X_{i+k}) \leq \text{fp}(F)$ by isotony. In both cases $\forall k \geq 0, X^k \leq F(X^k) \leq \text{fp}(F)$ proving that $X^k \leq \text{fp}(F)$. End of Proof.

**Lemma 2.2.2** \{$\forall \emptyset \neq M \subseteq \{1, 2, \ldots, n\}, \forall k \geq 0, (X^k) \leq X^{k+1}$\}.

**Proof**: The proof is by reductio ad absurdum. Let us suppose that $\forall \emptyset \neq M \subseteq \{1, 2, \ldots, n\}, \forall k \geq 0, (X^k) \leq X^{k+1}$ does not hold that $X^{k+1}$ is not comparable with $X^{k+1}$. We denote by $\text{fp}(X^k)$, $\forall k \geq 0$ such that $F(X^k)$ is not comparable with $X^{k+1}$. This must be true for $k=0$ which contradicts lemma 2.2.1.

**case 1**: Suppose that $\forall \emptyset \neq M \subseteq \{1, 2, \ldots, n\}, \forall k \geq 0, (X^k) \leq X^{k+1}$ does not hold that $X^{k+1}$ is not comparable with $X^{k+1}$. This implies that for some component $i \in \{1, 2, \ldots, n\}$ we have $X^{k+1} = F_i(X^k)$, while for the other components the inequality is not necessarily strict. By definition of
Proof of theorem 2.2:

Part 1: Let us prove that \( X^\infty \subseteq F(X^\infty) \). According to lemma 2.2.1 we have \( \forall k \in \mathbb{N}, X^k \subseteq F(X^k) \), thus passing to the limit we get \( \lim_{k \to \infty} X^k = \lim_{k \to \infty} F(X^k) \). The sequence of chaotic iterations is an increasing chain (lemma 2.2.1) and \( F \) is continuous, hence \( \lim_{k \to \infty} F(X^k) = F(\lim_{k \to \infty} X^k) \) and as \( X^k \subseteq F(X^k) \) for all \( k \), we conclude \( X^\infty \subseteq F(X^\infty) \). End of Proof.

Part 2: Let us now prove that \( F(X^\infty) = X^\infty \). By definition \( X^\infty = \lim_{k \to \infty} X^k \). Since \( X^k \subseteq F(X^k) \) for all \( k \), we have \( X^\infty \subseteq F(X^\infty) \). By continuity of \( F \), \( F(X^\infty) \subseteq X^\infty \). Thus \( X^\infty = F(X^\infty) \). End of Proof.

3. DEDUCTIVE SEMANTICS OF PROGRAMS

The deductive semantics of a program defines the logical invariant assertions associated with each program point. Once determined these assertions can be used to verify the program with respect to a specific program or to prove that the program is erroneous.

3.1. LOGICAL ASSERTIONS

We consider the set \( L \) of logical first order predicates \( P(X,\bar{X}) \) over the set \( X \) of program variables and the set \( \bar{X} \) of initial values of these program variables. \( X \) and \( \bar{X} \) are the free variables in the predicate \( P \). The assertion \( P(X,\bar{X}) \) associated with a point \( i \) of the program describes the values of the program variables at program point \( i \) during an execution starting with an initial state \( \bar{X} \) of the program variables. The set of predicates \( P(X,\bar{X}) \) forms a complete lattice \( (\varepsilon,\land,\lor,\top,\bot,\neg) \) by choosing respectively \( (\varepsilon,\top,\lor,\land,\neg) \).

3.2. SYSTEM OF LOGICAL FORWARD EQUATIONS

We use the notation \( (P(X,\bar{X})) \land (Q(X,\bar{X})) \) to mean that for every \( X,\bar{X}, \) if \( P(X,\bar{X}) \) holds prior to execution of the statement \( S \) then \( Q(X,\bar{X}) \) is the strongest post condition such that the statement \( S \) faultless executes and properly terminates leaving the program variables in a final state satisfying \( Q \) (Dijkstra [1976]). The deductive semantics of a programming language defines the rules which can be used to associate a system of equations with a sequential program.
Program entry point $j$:

$$P_j(X, Y) = \{X_i = X_i^j, i=1..m\}$$

The respective initial values of the variables $X=(X_1, \ldots, X_m)$ are the symbols $X_i^j=(X_i^1, \ldots, X_i^j, \ldots, X_i^m)$ (we may eventually have $X_i=\Pi$ when the variable $X_i$ is not initialized).

Assignment statements:

$$\{P(X, Y)\} X_i := E(X) \{P_i^v \text{ and } X_i = E_i^v\}$$
where

$$P_i^v = P(X_1, \ldots, X_{i-1}, v, X_{i+1}, \ldots, X_m, X_1^v, \ldots, X_m^v)$$
$$E_i^v = E(X_1, \ldots, X_{i-1}, v, X_{i+1}, \ldots, X_m)$$
The above rule must be enriched if one wants to take account of the fact that the execution of the assignment statement may fail, (e.g. the expression $E$ might overflow).

Test statements:

$$\{P(X, Y)\} \text{ if } Q(X) \text{ then } \{P(X, Y) \text{ and } Q(X)\} \ldots \text{ else } \{P(X, Y) \text{ and not } Q(X)\} \ldots \text{ end}$$

Go to statements and labels:

$$L : \{\text{OR } P_i(X, Y)\} \text{ where } \text{pred}(L)$$
the set of program points going to L sequentially or by jumps.

3.3. Example

We illustrate the application of the above rules to a very simple program (over the set $\Pi$ of integers augmented by $\Pi$).

$$\{P_1(x, y, R, y)\}, \{P_2(x, y, R, y)\} \text{ while } x<y \text{ do }$$
$$\{P_3(x, y, R, y)\} \text{ od}$$

Rewriting this program segment with branch and test primitives, and applying the rules of the deductive semantics we get a system of equations which can be simplified as follows:

$$P_1(x, y, R, y) = (x=R) \text{ and } (y=y)$$
$$P_2(x, y, R, y) = P_1(x, y, R, y) \text{ or } P_3(x, y, R, y)$$
$$P_3(x, y, R, y) = \{x=E: P_2(v, y, R, y) \text{ and } (x=v-y)\}$$
$$P_4(x, y, R, y) = (P_1(x, y, R, y) \text{ or } P_3(x, y, R, y))$$

(Hereafter we will write $P_1$ instead of $P_1(x, y, R, y)$ in order to simplify the notations).

3.4. Optimal Invariants

According to Tarski's theorem the above system of equations of the form $P=F(P)$ has a least solution $P^{\text{opt}}$ (least for ordering $\leq$ that is $\Rightarrow$). We call $P^{\text{opt}}$ the set of optimal invariants since they imply any other solution to the system of equations, (for all other sets of invariants $P$ such that $P=F(P)$,$P^{\text{opt}}$ is a lower bound therefore $P^{\text{opt}}$ $\Rightarrow$ $P$). The optimal invariants are the limit of any chaotic iterations starting from the infimum false (theorem 2.2). Let us choose Gauss-Seidel's method:

$$\begin{align*}
P^k_1 &= F(P^1_1, \ldots, P^k_{n-1}, P^k_n) \\
\vdots \\
P^k_1 &= F(P^k_1, \ldots, P^k_{n-1}, P^k_n) (p=1,2,\ldots) \\
P^k_1 &= F(P^k_1, \ldots, P^k_{n-1}, P^k_n) (p=1,2,\ldots)
\end{align*}$$

(Coming back to 2.1, this consists in choosing $P^i_1=\{((i \mod \Pi)+1)\}$ for $i=0,1,\ldots$ a step $k$ summarizing $n$ primitive iterations).

Initialization:

$$P^0_1 = \text{false} \quad (i=1,\ldots)$$

Step 1:

$$P^1_1 = (x=R) \text{ and } (y=y)$$
$$P^2_1 = (R>y) \text{ and } (x=R) \text{ and } (y=y)$$
$$P^3_1 = (R>y) \text{ and } (x=R) \text{ and } (y=y)$$
$$P^4_1 = (R>y) \text{ and } (x=R) \text{ and } (y=y)$$

Step 2:

$$P^1_2 = (x=R) \text{ and } (y=y)$$
$$P^2_2 = (R>y) \text{ and } (x=R) \text{ and } (y=y)$$
$$P^3_2 = (R>y) \text{ and } (x=R) \text{ and } (y=y)$$

By computing these first few terms we seek to discover the general term $P^i_1$ of the sequence:

Step 1:

$$P^1_1 = (x=R) \text{ and } (y=y)$$
$$P^2_1 = \text{OR} (AND (x=R) \text{ and } (x=R-\{j-1\}) \text{ and } (y=y))$$
$$P^3_1 = \text{OR} (AND (x=R) \text{ and } (x=R-j) \text{ and } (y=y))$$
$$P^4_1 = \text{OR} (AND (x=R) \text{ and } (x=R-j) \text{ and } (x=R-\{j-1\}) \text{ and } (y=y))$$

4
This general term $P^i$ of the chaotic iterations is proved to be correct by mathematical induction:

**Basis**: $P^1$ and $P^2$ are of the form specified by $P^i$ for $i=1$ and $i=2$.

**Induction Step**: assuming $P^i$ to be correct and substituting in the right-hand side of

---

5. **SYSTEMS OF IMPLICATIONS, APPROXIMATE INVARIANTS AND PROOFS OF PARTIAL CORRECTNESS**

Most program verification methods use inequalities of the form $P \Rightarrow F(P)$ whereas we used equalities $P=F(P)$. For example, instead of $(x>0) \ x:=x+2 \ (x>2)$
satisfying \( P \Rightarrow X(P) \). This is not surprising since this condition is based on Tarski’s theorem which does not provide an algorithmic construction of the least fixpoint of \( P \).

6. SYMBOLIC EXECUTION

The purpose of this section is to show that symbolic execution of a program consists in solving the semantic equations associated with this program by chaotic iterations.

6.1. SYMBOLIC CONTEXTS

Observe (3.4) that the invariant \( P_i \) associated with a program point i can be expressed in the normal form \( P = \bigvee \) \( \bigwedge \) \( p_j \) where each \( p_j \) is of the form \( (Q_j \land (X_{i_1} = E_{i_1}^{1j}) \land \ldots \land (X_{m_1} = E_{m_1})) \). Each \( p_j \) describes a program path which may lead to the point i.

For each program path \( p_j \) an assertion \( Q_j \) states the condition which had to be satisfied in order for that path to be executed. At point i on that path the value of the program variable \( X_k \), \( k = 1 \ldots m \) is given by \( E_{k,j} \). \( E_{k,j} \) is a formal expression depending on the initial values \( X \) of the variables on program entry. No \( X_k \) can appear as a free variable neither in \( Q_j \) nor in the \( E_{k,j} \). Slightly changing the notations we will call \( P_j \) a symbolic context and rewrite it as \( P = \{ p_j : j \in \Delta \} \) where \( p_j = Q_j \bigwedge E_{i_1}^{1j} \ldots E_{m_1} \).

6.2. SYSTEM OF SYMBOLIC FORWARD EQUATIONS

Using now the notation of symbolic contexts the rules of the deductive semantics (3.2) must be adapted so that they transform an input predicate in normal form into an output predicate in normal form. For example, the output predicate corresponding to the input predicate

\[
\{ Q_j \bigwedge E_{i_1}^{1j} \ldots E_{m_1} \} : j \in \Delta
\]

after the assignment statement \( X_k := E(X_1, \ldots, X_m) \) is:

\[
\{ \forall v : Q_j \bigwedge (X_{i_1} = E_{i_1}^{1j}) \land \ldots \land (X_{m_1} = E_{m_1}) \}
\]

Eliminating the free variables \( v \) we get:

\[
\{ \bigvee Q_j \bigwedge (X_{i_1} = E_{i_1}^{1j}) \land \ldots \land (X_{m_1} = E_{m_1}) \}
\]

We will denote this rule by the shorthand notation:

\[
\{ p \} \quad \forall k = \{ Q_k \} \quad \{ E(X_1, \ldots, X_m) \}
\]

However, when there is no ambiguity on which context must be used to evaluate the expression \( E \) we will write more simply:

\[
\{ p \} \quad X_k := E(X_1, \ldots, X_m)
\]

The other rules can be defined in the same way. In particular, the operation \( \lor \) describes the union \( P \lor Q \) of two symbolic contexts \( P = \{ p_1, \ldots, p_r \} \) and \( Q = \{ q_1, \ldots, q_s \} \) that is the set \( \{ p_1, \ldots, p_r, q_1, \ldots, q_s \} \) where superfluous equivalent program paths are eliminated whereas inaccessible paths (the path condition of which is false) are removed.

6.3. EXAMPLE

Using again the example 3.3:

\[
\begin{align*}
0 & \rightarrow \text{loop} \rightarrow \{ \}$$
1 & \rightarrow \text{if } x \neq y \text{ then }$
2 & \rightarrow \text{x := x - y }$
3 & \rightarrow \text{go to loop; }$
4 & \rightarrow \text{fi ;}$
\end{align*}
\]
we have the system of equations:

\[
\begin{align*}
P_0 &= \{ \text{true}, R, y \}$
\end{align*}
\]

\[
\begin{align*}
P_1 &= P_0 \lor P_3
\end{align*}
\]

\[
\begin{align*}
P_2 &= P_1 \land (x \neq y)
\end{align*}
\]

\[
\begin{align*}
P_4 &= P_1 \land (x < y)
\end{align*}
\]

6.4. SYMBOLIC EXECUTION TREE

As in 3.4 we solve these equations using chaotic iterations with a Gauss-Seidel policy:

Initialization:

\[
p_4^0 = \phi \quad (i = 0 \ldots 4)
\]

Step 1:

\[
\begin{align*}
p_1^0 &= \{ \text{true}, R, p \}$
\end{align*}
\]

\[
\begin{align*}
p_1^1 &= p_3 \bigwedge (x \neq y) = \{ \text{true}, R, y \}$
\end{align*}
\]

\[
\begin{align*}
p_1^2 &= p_1 \land (x < y) = \{ \text{true}, R, y \}$
\end{align*}
\]

\[
\begin{align*}
p_1^3 &= p_1 \land (x < y) = \{ \text{true}, R, y \}$
\end{align*}
\]

6
Step 2:

\[ P_2^* = \{ \text{true}, \overline{x}, \overline{y} \} \]
\[ P_2^1 = \{ \text{true}, \overline{x}, \overline{y} \}, <(\overline{x} \overline{y}), \overline{x} \overline{y}> \}
\[ P_2^2 = \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> \}
\[ P_2^3 = \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> \}
\]

So that at iteration 2 we have built the following symbolic execution tree (Hanlter & King[1976]):

\[ \text{true}, \overline{x}, \overline{y} \]
\[ <(\overline{x} \overline{y}), \overline{x} \overline{y}> \]
\[ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> \]
\[ <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> \]

We have represented the symbolic context \( P_1 \) associated with program point \( i \) by the set of paths associated with each of the nodes labelled \( i \) in the above execution tree. Equivalently we could have represented the symbolic context associated with program point \( i \) by the maximal subtree (of the above symbolic tree) the leaves of which are labelled 1. Then the union \( U \) of symbolic contexts performed at junction of program paths would be the merging of symbolic execution trees.

It is clear that the computation of the next terms of the sequence of chaotic iterations would cause the symbolic execution tree to grow. We can make the tree to grow in whatever direction we want, the result will be the same (2.2). Without particular hypothesis on \( X \) and \( Y \) this process would converge to the optimal invariants in infinitely many steps (2.3). Therefore we must be able either to reason about the limit without knowing it (6.4) or to directly pass to the limit (7).

6.5. Verification of Properties of Optimal Symbolic Contexts

Coming back to the notations of §2.3 in order to prove a property \( P(X^K) \) of the solution to the system of equations \( X = Y(X) \) we can prove by induction that all terms \( X^{km} \) of a chaotic iteration sequence have this property:

\[ \{(P(X) \lor P(X^{km})) \land (\forall k, P(X^{km}) \Rightarrow P(X^{(k+1)m})) \Rightarrow (P(\lim X^{km})) \}

(Yet \( P \) must be an admissible predicate chosen in order to remain true when passing to the limit. Rigorously we should apply the second principle of transfinite induction).

Example: Let us prove the trivial fact that \( \{\text{Wae}[i,(\overline{x} \mid x)]/y_i, \overline{R} \overline{z} \overline{a} \overline{y} \} \) at point 3 of program 6.3.

Base: For the single path of \( P_1 \) we have \( \{\text{Wae}[1,1], \overline{R} \overline{z} \overline{a} \overline{y} \} \).

Induction step: We assume that at step \( k \) the symbolic context \( P_k^\ast \) is equal to \( \{P_{1}^{k}, y_i \land x_i, y_i : i \in D \} \) with the induction hypothesis \( \{\text{Wic}D,(\text{Wae}[1,(\overline{x} \mid x)]/y_i, \overline{R} \overline{z} \overline{a} \overline{y} )\} \). The equations 6.3 allow the computation of \( P_{k+1}^\ast \):

\[ P_{k+1}^\ast = \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> : i \in D \}
\]

We must show that the hypothesis holds for all paths of \( P_k^\ast \). This is trivial for the path \( <(\overline{x} \overline{y}), \overline{x} \overline{y}> \). Otherwise we must show that \( \{\text{Wic}D,(\text{Wae}[1,(\overline{x} \mid x)]/y_i+1, \overline{R} \overline{z} \overline{a} \overline{y} )\} \). According to the induction hypothesis, this condition is true \( \text{Wae}[1,(\overline{x} \mid x)]/y_i \). Finally for \( x=(\overline{x} \mid x)/y_i+1 \), the path condition \( x_1 \overline{y} \overline{y}_i \) implies \( \overline{R} \overline{z} \overline{a} \overline{y} \).

This approach for reasoning about the limit of chaotic iterations is implicitly used in the technique of "cut-trees" of Hanlter & King[1976]. Indeed the induction step can be understood as consisting in reasoning on the cut tree for \( \{3\} \):

\[ \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> : i \in D \}
\]

\[ \{ \text{true}, \overline{x}, \overline{y} \}
\]

\[ \{ \text{true}, \overline{x}, \overline{y} \}, <(\overline{x} \overline{y}), \overline{x} \overline{y}> \}
\]

\[ \{<(\overline{x} \overline{y}), \overline{x} \overline{y}> \}
\]

\[ \{ \ldots \}
\]

\[ \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> : i \in D \}
\]

\[ \{ <(\overline{x} \overline{y}), \overline{x} \overline{y}>, <(\overline{x} \overline{y}) \land (\overline{x} \overline{y}), \overline{x} \overline{y}> : i \in D \}
\]

End of Example.
7. SYNTHESIS OF OPTIMAL INVARIANT ASSERTIONS: THE USE OF DIFFERENCE EQUATIONS

7.1. DISCOVERY OF OPTIMAL SYMBOLIC CONTEXTS

The equations of example 6.3 can be written as:
\[ P_i = P_i \cup \{ P_j \land x+y \} (x+x-y) \]
they are of the form:
\[ P_i = f_i(P_0) \cup f_2(P_i) \]
The resolution by successive approximations was:
\[ P_i^k = \emptyset \]
\[ P_1^1 = f_1(P_0) \cup f_2(\emptyset) = f_1(P_0) \]
\[ P_1^2 = f_1(P_0) \cup f_2(f_1(P_0)) \]
\[ P_1^3 = f_1(P_0) \cup f_2(f_1(P_0)) \cup f_2^2(f_1(P_0)) \]
\[ = f_1(P_0) \cup f_2(f_1(P_0)) \cup f_2^2(f_1(P_0)) \]
since \( f_2 \) is distributive over \( \cup \). (This comes from the fact that \( f_2 \) is the composition of elementary functions as defined in 6.2. Setting apart the difference in notations they are similar to the predicate transformers of the deductive semantics (3.2). Since the set of predicates form a complete boolean lattice the infinite distributive laws hold for OR

\[ \land \text{ AND} \]

The general term of the approximation sequence is:
\[ P_i^k = \bigcup_{i=0}^{k-1} f_1^i(P_0) \]

since:
\[ P_i^{k+1} = f_1(P_0) \cup f_2\bigcup_{i=0}^{k-1} f_1^i(P_0) = \bigcup_{i=0}^{k} f_1^i(P_0) \]

Passing to the limit we get:
\[ P_i^\infty = \bigcup_{i=0}^{\infty} f_1^i(P_0) \] This result can be obtained directly since the graph of dependence between \( P_0 \) and \( P_i \):

\[ f_1 \quad P_0 \quad P_i \quad f_2 \]

can be considered as (in general a non-deterministic) finite automaton which recognizes the Kleene's language \( f_1f_2^* \). We have obtained a symbolic formulation of the desired solution, but it remains to give the explicit formulation of the function \( f_1^i f_2 \). This can be done by solving the difference equations:
\[ \begin{cases}
    f_1^0 f_2(P_0) = P_0 \\
    f_1^i f_2^i f_1(P_0) = f_1(f_2 f_1(P_0))
\end{cases} \]

We have:
\[ f_2^0 f_1(P_0) = \{ \text{true,}x,y \} \]
\[ = \{ \text{true,}x,y \}, \quad x \neq y \} \]

Let \( f_2^i f_1(P_0) \) be \( \{ \text{true,}x,y \}, \quad x \neq y \} \), we have
\[ f_2^{i+1} f_1(P_0) = f_2(\{ \langle p_{ij} x_{ij}, y_{ij} \rangle ; j \in D_1 \}) \]
\[ = \{ \langle p_{ij} x_{ij}, y_{ij} \rangle ; j \in D_1 \} \]

First of all, we can determine the domain of \( j \) which indexes the possible paths. Since \( D_0 = \{ 1 \} \) and \( D_{i+1} = D_i \) (because there is a single path within the loop). Therefore we can simply ignore the path index and solve the difference equations (in the order of dependence):
\[ X_0 = x_0, \quad X_{i+1} = x_{i+1} x_i + (x_i y_i) \]
\[ P_0 = \text{true,} \quad P_{i+1} = P_i \text{ and } (x_i y_i) \]

These recurrence relations can be solved directly (e.g. Cohen & Katzoff (1976) yielding \( X_j = x_0 x_j y_0 \), \( X_{i+1} = X_i + y_0 \), and since \( P_0 = \text{true} \) and \( P_{i+1} = P_i \) we get \( P_0 \text{ and } (x_0 y_0) \) get \( P_0 \text{ and } (x_0 y_0) \). Finally the optimal loop invariant of program 6.3 is:
\[ P_1^\infty = \bigcup_{i=0}^{\infty} \{ \langle x_0, y_0 \rangle, x_0 \neq y_0 \} \]

The "difference equations method" was introduced by Elspas, Green, Levitt & Waldinger (1972), Elspas (1974). It is further used in Greif & Waldinger (1975), Katz & Manna (1976) (algorithmic approach), Cheatham & Townelay (1976). It has also been used in determining symbolic expression of program complexity (Wegbreit 1975). However, the technique was understood with respect to an operational semantics, i.e. by reasoning on (dummy) loop counters and on approximate invariants. In fact a reasoning in terms of denotational semantics clearly shows that (at least in theory) optimal invariants can be discovered and consequently program termination can be proved or disproved.

7.2. REMARK

We have proved that in theory all chaotic iteration sequences lead to the optimal solution to the system of equations. However, in practice a major difficulty consists in finding a form of the general term of the approximation sequence which is suitable for establishing the difference equations. Consider for example a system of equations with the following dependenc graph :
We can express $P_1^\infty$ by the following equivalent forms:

$$
P_1^\infty = \bigcup_{j \geq 0} (f_4 \circ f_3 \circ (f_6 \circ f_5 \circ f_3)^j \circ f_1)(P_0)
$$

(i and j correspond to individual counters for the loops)

$$
P_1^\infty = \bigcup_{k \geq 0} (f_1(P_0) \cup f_4 \circ (f_2 \circ f_4 \cup f_6 \circ f_5 \circ f_3)^k \circ f_2 \circ f_1)(P_0)
$$

(k is a common counter for the two loops).

Although these two forms of $P_1^\infty$ are equivalent one of them will be more suitable for generating the difference equations and the choice depends on the semantics of the considered program.

### 7.3. Example

Let us consider the following program (taken from King[1969]):

```plaintext
{0}  z := 1;
{1}  if y \neq 0 then
{2}    if odd(y) then
{3}      z := z * x;
{4}    fi;
{5}    (y,x) := (y \div 2, x^2);
{6}  go to loop;
{7}  fi;
```

The following holds:

$$
P_1 = P_0 \cup \begin{cases}
(\text{true} \land \text{even}(y)) \rightarrow (z = x \land \text{even}(x))^2, z + P_1(z) \\
(\text{false} \land \text{odd}(y)) \rightarrow (z = x \land \text{odd}(y) \rightarrow x)
\end{cases}
$$

This formulation uses the conditional expressions of Sintzoff[1975]:

- $(true \lor \neg v) \land (Q \lor v') = (true \land (Q \lor v'))$
- $(false \lor \neg v) \land (Q \lor v') = (Q \land (Q \lor v'))$
- $Q \lor Q' = Q \lor Q'$
- $Q \land Q' = Q \land Q'$
- $[Q \lor v) = (Q \lor \neg v')$
- $[Q \land v) = Q \land \neg v')$
- $Q \land \neg v = (Q \land \neg v')$
- $v \lor (Q \land v) = v \lor (Q \land v')$
- $f(v_1, ..., v_{n-1}, v_n) = \sum f(v_1, ..., v_{n-1}, v_n)$
- $f(v_1, ..., (Q \land v), ..., v_n) = (Q \land f(v_1, ..., v_n))$
- etc.

The general form of the solution for the equation defining $P_1$ is $P_1 = P_0 \cup \bigcup_{i \geq 0} f_i(P_0)$.

For determining $f_i(P_0)$ we use the difference equations:

$$
f_0(P_0) = \begin{cases}
\text{true} & \begin{cases}
\text{a}, \text{b}, 1
\end{cases} \\
\text{false} & \begin{cases}
\text{x_0}, \text{x_1}, \text{z_0}, \text{z_1}
\end{cases}
\end{cases}
$$

$$
f_i+1(P_0) = f_i(\begin{cases}
\text{q}_i \land \text{y_1} \land \text{z_1}
\end{cases})
= \begin{cases}
\text{x_0} \land \text{y_0} \land \text{z_0}
\end{cases}
$$

The formal resolution proceeds as follows:

$$
x_0 = a \Rightarrow x_i = a^i
$$

$$
x_i = x_i^2
$$
Finally the optimal output invariant of the program is:
\[ P_1 = P_1 \land (y=0) \]
\[ = \bigcup_{i=0}^{\infty} q_i \land (y_i=0,x_i,y_i,z_i) \]
\[ = (b=0,x=a,y=b,z=1) \]
\[ \cup (j>0 : (b \cdot 2^j-1 \cdot 0) \land (b \cdot 2^j=0)), \]
\[ x=a^j, \]
\[ y=b \cdot 2^j, \]
\[ z=\frac{i}{\bigcup_{j=0}^{\infty} (even(b \cdot 2^j) \lor odd(b \cdot 2^j) \Rightarrow a^j)} \]
Since the path condition at the halptpoint \( \{7\} : (b=0) \lor (j>0 : (b \cdot 2^j-1 \cdot 0) \land (b \cdot 2^j=0)) \) is true for any input value \( b \) of \( y \), the program always terminates.

It remains to show that \( P_1(z)=a \mid b \) to prove total correctness. In the non-obvious case \( b \neq 0 \), we have to know that every number \( b \) can be expressed in binary form:
\[ b = (b \cdot 2^j-1 \cdot 0) \land (b \cdot 2^j=0)) \]
\[ sign(b) \cdot \sum_{j=0}^{\infty} (even(b \cdot 2^j) \lor odd(b \cdot 2^j) \Rightarrow 2^j) \]
Evaluating \( a \mid b \) using the property that:
\[ a \mid \sum_{j=0}^{\infty} 2^j = a^j \]
we get:
\[ a \mid b = (b \cdot 2^j-1 \cdot 0) \land (b \cdot 2^j=0)) \]
\[ \sum_{j=0}^{\infty} (even(b \cdot 2^j) \lor odd(b \cdot 2^j) \Rightarrow a^j) \]
which is the desired result.

8. SYNTHESIS OF APPROXIMATE INVARIANTS

Let us consider a system of equations \( X=F(X) \) associated with a given program. We have seen that a set \( P \) of approximate invariants must satisfy \( lfp(F) \subseteq P \), that is \( lfp(F) = P \) with lattice notations. We can obtain such a \( P \) by "strengthening" the terms of a chaotic iteration sequence.

**DEFINITION 8.1** A strengthened chaotic iteration corresponding to the continuous operator \( F \in \mathbb{R}^n \rightarrow \mathbb{R}^n \) and starting with a given vector \( X_0 \) such that \( X^k \subseteq F(X^k) \) is a sequence \( X^k \), \( k=0,1, \ldots \) of vectors of \( \mathbb{R}^n \) defined recursively by \( X^{k+1}=F(X^k) \) where \( \{W_{k} \in \mathbb{R}^n \mid \forall \mathbb{W} \in \{1, \ldots, n\} \}
\[ f_i(X^k) \subseteq F(X^k) \subseteq X^k \]
and \( j^k \), \( k=0,1, \ldots \) is a sequence of subsets of \( \{1, \ldots, n\} \) such that \( \{W_{k} \in \mathbb{R}^n \mid \forall \mathbb{W} \in \{1, \ldots, n\} \}
\[ f_i(X^k) \subseteq F(X^k) \subseteq X^k \]

**DEFINITION 8.2** A strengthened chaotic iteration is said to stabilize after \( s \) steps if and only if \( \{W_{k} \in \mathbb{R}^n \mid \forall \mathbb{W} \in \{1, \ldots, n\} \}
\[ f_i(X^k) \subseteq F(X^k) \subseteq X^k \]
Notice that stabilization can always be enforced.
Proof: take \( X^s = \mathbb{T} \) (but this choice is of no practical interest).

**THEOREM 8.3** The limit \( X^\infty \) of a chaotic iteration sequence \( X^0, X^1, X^2, \ldots \) which stabilizes after \( s \) steps is such that \( lfp(F) \subseteq X^\infty \).

Proof: Let us first prove that a chaotic iteration sequence is an increasing chain.
Basis: since \( X^0 \subseteq F(X^0) \), we have \( X^0 \subseteq F(X^0) \subseteq F(X^0) \subseteq X^1 \).

Induction step: suppose that \( X^{k} \subseteq X^{k+1} \). We have \( X^{k+1} \subseteq F(X^k) \). Moreover, if \( (i \notin X_k \) and \( F_i(X^k) \subseteq X_k \) or \( (i \in X_k \) and \( F_i(X^k) \subseteq X_{k+1} \)) then \( X_{k+1} \subseteq X_k \; \Rightarrow \; F_i(X^k) \subseteq X_{k+1} \) proving that \( X^{k+1} \subseteq X^{k+1} \). Hence by recurrence on \( k \) we have \( F(X^k) \subseteq X^{k+1} \). According to the definition of a chaotic iteration which stabilizes we have \( X^s \subseteq X^{s+1} \subseteq \ldots \subseteq X^{\infty} \).

Therefore, if \( F_i(X^s) \subseteq X^s \) then \( F_i(X^s) \subseteq X^s \) since \( X^s \subseteq X^{s+1} \subseteq \ldots \subseteq X^{\infty} \). This implies \( X^s \subseteq X^s \subseteq \ldots \subseteq X^{\infty} \). Let us now prove that \( F(X^s) \subseteq X^s \).

**End of Proof.**

In practice the definition of \( \mathbb{T}^k \) models the use of heuristics for generating invariants (e.g. Katz & Mannal 1976).

**Example:** Coming back to the program of §3.3, we have given the first terms of the corresponding
approximation sequence at §3.4:

\[ P_2^0 = \text{false} \]

\[ P_2^1 = \langle x=\bar{y} \rangle \text{and} \langle x=R \rangle \text{and} \langle y=\bar{y} \rangle \]

\[ P_2^2 = \langle x=\bar{y} \rangle \text{and} \langle x=\bar{y} \rangle \text{and} \langle y=\bar{y} \rangle \]

or

\[ \langle \forall k \in \{1, 2\} : x=\bar{y} \rangle \text{and} \langle x=\bar{y} \rangle \text{and} \langle y=\bar{y} \rangle \]

The idea of solving these equations by means of chaotic successive approximations is so natural that it was first understood as a program execution on symbolic values. We think that even a semi-automatic resolution of the semantic equations is a terrific task which result can hardly be controlled by the program.


Sintzoff[1975]. Sintzoff,M. Vérification d'assertions pour des fonctions utilisables comme valeurs et affectant des variables extérieures.
The papers in this volume were presented at the ACM Symposium on Artificial Intelligence and Programming Languages, sponsored jointly by SIGART and SIGPLAN, and held at the University of Rochester, August 15-17, 1977.

The Program Committee wishes to thank all those who submitted papers for consideration.