CHAPTER THREE

Transformations Involving exit Statements

Introduction

In this chapter we build on the results of the last chapter to develop a set of transformations of programs which use unbounded loops and **exit** statements. These transformations will allow us to work directly with the programs without having to use the definitional transformations to prove the equivalence of two statements. In this chapter we consider statements to be compounds of "primitive statements" (which are either **exit** statements, or statements which cannot be terminated by the execution of an **exit** statement within them). These correspond loosely to the "basic blocks" of compiler terminology. All the transformations in this section treat primitive statements as atomic, indivisible units.

The complexity of interpreting **do** loops is a consequence of the "power" of such control structures; indeed they can be used to simulate any other form of control structure including arbitrary transfers of control. [Bohm & Jacopini 66] showed that any program using any control structures can be transformed to a functionally equivalent one which uses only composition, **if then else**, and **while do** control structures. This has been described as "perhaps the first major result of structured programming" [Ledgard & Marcotty 75].

However if one restricts the transformations to those which increase neither program length nor execution time then these basic control structures are not sufficient. S.R.Kosaraju in [Kosaraju 74] proved that the addition of infinite loops of arbitrary depth and **exit(n)** statements, where **n** can be any integer, is sufficient.

These statements are used by Arsac in [Arsac 79] and [Arsac 82] where several program transformations are developed for recursion removal. [Taylor 84] also discusses them and propounds their inclusion in programming languages as an alternative to current looping syntax.

The following transformations were inspired by Arsac's work in this area, we have generalised these transformations and proved them within our programming system (which unlike Arsac's allows nondeterministic programs and specifications as programs as well as a much wider range of control structures):

Incrementation (but not partial incrementation),
Simple Absorption, and a simple converse,
False Iteration, and a simple converse,
Inversion and Proper Inversion,
Loop Doubling,
First Step Unrolling,
Double Iteration,

Loop Absorption

As well as generalising these transformations, we have added the various "selective unrolling" and "selective unfolding" transformations which (as we shall demonstrate) cannot be derived from Arsac's set of transformations.

The rest of this section will concentrate on our proofs of these transformations together with the proofs of some lemmas which will be needed in the next chapter. First we give some notation:

Defn: Since an **exit** statement is not allowed to leave a block or a recursive procedure or loop (other than a **do** loop) we can regard such statements as single indivisible wholes as far as this section is concerned. Hence we define a primitive statement to be either an **exit** statement, an assignment, an assertion a block, a recursive procedure, a **while** loop, a **for** loop or a nondeterministic iteration. Thus a primitive statement cannot be terminated by the execution of an **exit** statement (unless it is an **exit** statement). All other statements are compound statements.

Primitive Statements: eg:
Exit Statements **exit(k)**
Assignments **x:=x′.Q**
Assertions **{Q}**
Blocks **beg x:S end**
Recursive Procedures **proc X** $\equiv$ **S**
Counted Repetition **for i:=b step s to f do S od**
Deterministic Iteration **while B do S od**
Nondeterministic iteration **do** $\mathbf{B}_1 \rightarrow \mathbf{S}_1 \square \dots \square \mathbf{B}_n \rightarrow \mathbf{S}_n$ **od**
Abstraction **rep x/y.Q:S per** and **beg x/y.Q:S per**

Compound Statements: eg:
Composition $\mathbf{S}_1;\mathbf{S}_2$
Deterministic Selection **if B then** $\mathbf{S}_1$ **else** $\mathbf{S}_2$ **fi**
Nondeterministic Selection **if** $\mathbf{B}_1 \rightarrow \mathbf{S}_1 \square \dots \square \mathbf{B}_n \rightarrow \mathbf{S}_n$ **fi**
Unbounded loops **do S od**
Nondeterministic Choice **oneof** $\mathbf{S}_1 \vee \mathbf{S}_2$ **foeno**

Defn: For any statements **T, S** where **T** is primitive the function **occ(T,S)** (the number of occurrences of **T** in **S**) is defined as follows:
If **T=S** then **occ(T,S)=1**.

Otherwise if **S** is primitive then **occ(T,S)=0**, (since in this section we regard all primitive statements as <u>indivisible</u>, so occurrences of a statement within a primitive statement are not counted).

Otherwise $\mathbf{occ(T,(S_1;S_2)) = occ(T,S_1)+occ(T,S_2)}$
$\mathbf{occ(T,\ \underline{if}\ B\ \underline{then}\ S_1\ \underline{else}\ S_2\ \underline{fi}) = occ(T,S_1)+occ(T,S_2)}$
$\mathbf{occ(T,\ \underline{oneof}\ S_1 \vee S_2\ \underline{foeno}) = occ(T,S_1)+occ(T,S_2)}$
$\mathbf{occ(T,\underline{if}\ B_1 \rightarrow S_1 \square \ldots \square B_n \rightarrow S_n\ \underline{fi})} = \sum_{1\leqslant i\leqslant n}\mathbf{occ(T,S_i)}$
$\mathbf{occ(T,\underline{do}\ S_1\ \underline{od}) = occ(T,S_1)}$

We will use the following simple program to illustrate the transformations developed in this section. The program sets **r** to the sum of all integers from **1** to **n**:

```
Prog= r:=0; i:=1;
  do if i>n then exit fi;
       t:=i;
       do r:=r+1; t:=t−1;
          if t=0 then exit fi od;
       i:=i+1 od.
```

This program has primitive statements: **r:=0**, **i:=1**, **t:=i**, **r:=r+1**, **t:=t−1**, **i:=i+1** each of which occurs once, and <u>**exit**</u> which occurs twice.

<u>**Defn:**</u> For any statements **T,S** (where **T** is primitive) and integers **n,d** the predicate **ts(n,T,S,d)** (which is interpreted "the **n**th occurrence of **T** in **S** is a terminal statement of **S** which will leave **d** enclosing loops") is defined recursively as follows:
If **S** is a primitive non-<u>**exit**</u> statement then $\mathbf{ts(n,T,S,d)} \iff \mathbf{n=1} \wedge \mathbf{d=0} \wedge \mathbf{T=S}$
$\mathbf{ts(n,T,\underline{exit}(k),d)} \iff \mathbf{n=1} \wedge \mathbf{d=k} \wedge \mathbf{T=\underline{exit}(k)}$
$\mathbf{ts(n,T,(S_1;S_2),d)} \iff \mathbf{ts(n,T,S_1,d)} \vee \mathbf{ts(n\text{-}occ(T,S_1),T,S_2,d)}$ if $\mathbf{d>0}$
$\iff \mathbf{ts(n\text{-}occ(T,S_1),T,S_2,d)}$ if $\mathbf{d=0}$
$\mathbf{ts(n,T,\underline{if}\ B\ \underline{then}\ S_1\ \underline{else}\ S_2\ \underline{fi},\ d)} \iff \mathbf{ts(n,T,S_1,d)} \vee \mathbf{ts(n\text{-}occ(T,S_1),T,S_2,d)}$
$\mathbf{ts(n,T,\underline{if}\ B_1 \rightarrow S_1 \square \ldots \square B_n \rightarrow S_n\ \underline{fi},\ d)} \iff \bigvee_{1\leqslant i\leqslant n}\mathbf{ts(n\text{-}}\sum_{1\leqslant j<i}\mathbf{occ(T,S_j),T,S_i,d)}$
$\mathbf{ts(n,T,\underline{do}\ S_1\ \underline{od},\ d)} \iff \mathbf{ts(n,T,S_1,d+1)}$

With our example the only terminal statement of **Prog** is the first occurrence of <u>**exit**</u>, which will leave zero enclosing <u>**do**</u> loops thus:
$\mathbf{ts(1,\underline{exit},Prog,0)} \iff \mathbf{true}$ while $\mathbf{ts(2,\underline{exit},Prog,0)} \iff \mathbf{false}$.

We write $\mathbf{ts(n,T,S)}$ for $\mathbf{ts(n,T,S,0)}$ and write $\mathbf{ts(S)}$ for $\{\mathbf{T}|\exists\mathbf{n.ts(n,T,S)}\}$ and $\mathbf{ts(S,d)}$ for $\{\mathbf{T}|\exists\mathbf{n.ts(n,T,S,d)}\}$. Thus $\mathbf{ts(Prog)}=\{\underline{\mathbf{exit}}\}$.

We say **T** is a terminal statement of **S**, or **T** is terminal in **S** if $\exists\mathbf{n.ts(n,T,S)}$.

<u>Theorem:</u> If $\mathbf{ts(S)}=\{\}$ then $\vdash\mathbf{S}\ \approx \mathbf{abort}$.
ie if **S** has no terminal statement then **S** cannot terminate.
Proof: By induction on **n** and on the structure of **S** prove:
If $\mathbf{ts(S,n)}=\{\}$ then $\vdash\mathbf{depth{:=}n;\ guard}_n\mathbf{(S);\ \{depth\leqslant 0\}}\ \approx\ \mathbf{abort}$

<u>Defn:</u> If $\mathbf{occ(T,S)\geqslant n\geqslant 1}$ then the depth of the **n**th occurrence of the primitive statement **T** in **S**, called $\delta\mathbf{(n,T,S)}$, is defined:
If **T**=**S** then $\delta\mathbf{(1,T,S)=0}$
$\delta\mathbf{(n,T,(S_1;S_2))} = \delta\mathbf{(n,T,S_1)}$ if $\mathbf{occ(T,S_1)\geqslant n}$
$\qquad\qquad\delta\mathbf{(n-occ(T,S_1),T,S_2)}$ otherwise
$\delta(\mathbf{n,T,\underline{oneof}}\ \mathrm{S}_1 \vee \mathrm{S}_2\ \mathbf{\underline{foeno}}) =$
$\delta(\mathbf{n,T,\underline{if}\ B\ \underline{then}}\ \mathrm{S}_1\ \mathbf{\underline{else}}\ \mathrm{S}_2\ \mathbf{\underline{fi}}) = \delta\mathbf{(n,T,S_1)}$ if $\mathbf{occ(T,S_1)\geqslant n}$
$\qquad\qquad\delta\mathbf{(n-occ(T,S_1),T,S_2)}$ otherwise
$\delta(\mathbf{n,T,\underline{if}\ B_1}\ \rightarrow \mathbf{S_1} \square \ldots \square\ \mathbf{B}_n\ \rightarrow \mathrm{S}_n\ \mathbf{\underline{fi}}) = \delta(\mathbf{n}\text{-}\sum_{1\leqslant j<i}\mathbf{occ(T,S}_j\mathbf{),T,S}_i)$ where **i** is the smallest integer such that $\mathbf{occ(T,S}_i\mathbf{)\geqslant n}\text{-}\sum_{1\leqslant j<i}\mathbf{occ(T,S}_j\mathbf{)}$
$\delta(\mathbf{n,T,\underline{do}}\ \mathrm{S}_1\ \mathbf{\underline{od}}) = \delta\mathbf{(n,T,S_1)+1}$

<u>Defn:</u> If **T** is primitive and $\mathbf{ts(n,T,S)}$ holds then the <u>terminal</u> <u>value</u> of the **n**th occurrence of **T** in **S**, $\tau\mathbf{(n,T,S)}$, is defined as $|\mathbf{T}|-\delta\mathbf{(n,T,S)}$ where $|\underline{\mathbf{exit}}\mathbf{(k)}| = \mathbf{k}$ and $|\mathbf{T}| = \mathbf{0}$ for all other primitive statements.
Note that if **T** is terminal then we must have $\tau\mathbf{(n,T,S)\geqslant 0}$.

The terminal value of a statement is the number of enclosing loops which would be terminated by the execution of that statement. This means that the next statement to be executed after the **n**th occurrence of **T** in **S** will be the first statement outside $\tau\mathbf{(n,T,S)}$ loops.
For example: $\delta(\mathbf{1,\underline{exit},Prog)=1}$, $\delta(\mathbf{2,\underline{exit},Prog)=2}$, $\delta\mathbf{(1,i{:=}1,Prog)=0}$ etc.
$\qquad\tau(\mathbf{1,\underline{exit},Prog}) = |\underline{\mathbf{exit}}| - \delta(\mathbf{1,\underline{exit},Prog}) = \mathbf{1-1 = 0}$.
If $\tau\mathbf{(n,T,S)=0}$ then the next statement executed after the execution of **T** in **S** will be the statement immediately following **S**. If $\tau\mathbf{(n,T,S)>0}$ then the execution of **T** in **S** will cause the termination of the first τ **<u>do</u>** loops enclosing **S**.

It often occurs that we wish to substitute certain occurrences of primitive statements by other statements, and do all the substitutions simultaneously. Such a substitution is defined as follows:

Defn: Global Substitution: If $\mathbf{P(n,T,S)}$ is a predicate on $\mathbf{n,T}$ and $\mathbf{S}$, and $\mathbf{S'(n,T,S)}$ is a statement for any $\mathbf{n,T}$ and $\mathbf{S}$ then the effect of replacing the $\mathbf{n}$th occurrence of the primitive statement $\mathbf{T}$ in $\mathbf{S}$ by $\mathbf{S'(n,T,S)}$ for every $\mathbf{n}$ and $\mathbf{T}$ such that $\mathbf{P(n,T,S)}$ holds is denoted:

$$\mathbf{S[S'(n,T,S)/(n,T)|P(n,T,S)]}$$

For any statement $\mathbf{S''}$, statement function $\mathbf{S'}$, integer $\mathbf{k}$ and predicate $\mathbf{P}$:
$\mathbf{S''[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$ is defined:

(i) $\mathbf{S''[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $= \mathbf{S''}$ if $\mathbf{S''}$ is primitive and $\mathbf{P(k{+}1,S'',S)}$ fails.

(ii) $\mathbf{S''[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $= \mathbf{S'(k{+}1,S'',S)}$ if $\mathbf{S''}$ is primitive and $\mathbf{P(k{+}1,S'',S)}$ holds.

(iii) $\mathbf{(S_1;S_2)[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $= \mathbf{S_1[S'(n,T,S)/(n{-}k,T)|P(n,T,S)\wedge]}$;
  $\mathbf{S_2[S'(n,T,S)/(n{-}k{-}occ(T,S_1),T)|P(n,T,S)]}$

(iv) **__if__ B __then__** $\mathbf{S_1}$ **__else__** $\mathbf{S_2}$ **__fi__**, similar to (iii).

(v) (**__if__** $\mathbf{B_1 \rightarrow S_1 \square \ldots \square B_m \rightarrow S_m}$ **__fi__**)$\mathbf{[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $=$ **__if__** $\mathbf{B_1 \rightarrow S_1[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $\square$ ...
  $\kappa\kappa\kappa\kappa\ \square\ \mathbf{B}_i \rightarrow \mathbf{S}_i\mathbf{[S'(n,T,S)/(n{-}k{-}\textstyle\sum_{1\leqslant j<i} occ(T,S_j),T)|P(n,T,S)]}\ \square$ ...**__fi__**

(vi) (**__do__** $\mathbf{S_1}$ **__od__**)$\mathbf{[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$
  $=$ **__do__** $\mathbf{S_1[S'(n,T,S)/(n{-}k,T)|P(n,T,S)]}$ **__od__**

We will often abbreviate $\delta\mathbf{(n,T,S)}$ by δ, $\mathbf{ts(n,T,S)} \wedge \mathbf{R}(\tau\mathbf{(n,T,S)})$ by $\mathbf{R}(\tau)$ (where $\mathbf{R}$ is a relation on integers) and $\mathbf{(n,T)}$ by $\mathbf{T}$ so for example:

$$\mathbf{S[S'(n,T,S)/(n,T)|ts(n,T,S)} \wedge \tau\mathbf{(n,T,S)=0]} \text{ becomes } \mathbf{S[S'(n,T,S)/T|}\tau\mathbf{=0]}$$

Such substitutions will be used extensively in the rest of this section to prove properties of statements and transformations of them by induction on their structure.

Note that for $\mathbf{n_0} < \omega$ the statement $\mathbf{S[S'/(n,T)|n{=}n_0 \wedge T{=}T_0]}$ is $\mathbf{S}$ with $\mathbf{S'}$ replacing the $\mathbf{n_0}$th occurrence of $\mathbf{T_0}$. We abbreviate this to $\mathbf{S[S'/(n_0,T_0)]}$.

Defn: Incrementation:
An example of global substitution is incrementation: if $\mathbf{S}$ is a statement and $\mathbf{k}$ an integer then $\mathbf{S{+}k}$

denotes the substitution of all terminal statements **exit(m)** by **exit(m+k)** and all other primitive terminal statements **T** by **T;exit(k)**. ie:

$$\mathbf{S+k} =_{DF} \mathbf{S[T+k/(n,T)|\tau(n,T,S)\geqslant 0] = S[T+k/T|\tau \geqslant 0]}$$

Thus **Prog+1** is identical to **Prog** except that the first occurrence of **exit** is replaced by **exit(2)**. Note that the second occurrence of **exit** is not a terminal statement of **Proc** so is not incremented.

Example: If **P** is
if B then exit fi;
do do a; if C then exit fi od;
b; if D then exit(2) fi; od; c.

where **a,b** and **c** are primitive then **P+3** is
if B then exit(4) fi;
do do a; if C then exit fi od;
b; if D then exit(5) fi; od; c; exit(3).

Defn: Partial Incrementation:

This is similar to incrementation except that only those terminal statements which have a terminal value greater than some given value are incremented.

$$\mathbf{S+(k,d)} =_{DF} \mathbf{S[T+k/(n,T)|ts(n,T,S) \wedge \tau(n,T,S)\geqslant d]}$$

For example:

do S **od**+(k,d) = **do** S[T+k/(n,T)|ts(n,T,S) $\wedge$ τ(n,T,S)$\geqslant$d+1] **od**
= **do** S+(k,d+1) **od**

Clearly **S+(k,0) = S+k**.
Also $(\mathbf{S_1;S_2})\mathbf{+(k,d) = S_1+(k,d); S_2+(k,d)}$ if $\mathbf{d>0}$
$= \mathbf{S_1+(k,1); S_2+(k,d)}$ if $\mathbf{d=0}$.
This is because terminal statements of $\mathbf{S_1}$ with terminal value zero lead to the execution of $\mathbf{S_2}$ so are not terminal statements of $\mathbf{S_1;S_2}$ but those with terminal value $>\mathbf{0}$ are terminal statements of $\mathbf{S_1;S_2}$.
For the other compounds we can apply the **+(k,d)** directly to each component.
For primitive non-**exit** statements **S+(k,d) = S; exit(k)**.
For **exit** statements: **exit(l)+(k,d) = exit(l+k)**.

Using the example above, **P+(3,1)** is:

$\underline{\textbf{if}}$ **B** $\underline{\textbf{then}}$ $\underline{\textbf{exit}}$ $\underline{\textbf{fi}}$**;**
$\underline{\textbf{do}}$ $\underline{\textbf{do}}$ **a;** $\underline{\textbf{if}}$ **C** $\underline{\textbf{then}}$ $\underline{\textbf{exit}}$ $\underline{\textbf{fi}}$ $\underline{\textbf{od}}$**;**
b; $\underline{\textbf{if}}$ **D** $\underline{\textbf{then}}$ $\underline{\textbf{exit}}$**(5)** $\underline{\textbf{fi}}$**;** $\underline{\textbf{od}}$**; c.**

For most of our substitutions we will not want to replace the non-**exit** primitive statements but only to add another statement after them. This is to ensure that adding **exit(0)** (ie **skip**) after a non-**exit** primitive does not affect our substitutions. For example the definition of simple absorption is:

$$\mathbf{S;S'} \approx \mathbf{S[S'} + \delta/\mathbf{T}|\tau = \mathbf{0]}$$

which should be interpreted as:

$$\mathbf{S;S'} \approx \mathbf{S[S'(n,T,S)/(n,T)|ts(n,T,S)} \wedge \tau\mathbf{(n,T,S)=0]}$$

where $\mathbf{S'(n,T,S)} = \mathbf{T;\ S'} + \delta\mathbf{(n,T,S)}$ if **T** is a non-**exit** primitive
$= \mathbf{S'} + \delta\mathbf{(n,T,S)}$ otherwise.

TRANSFORMATIONS:

Lemma A: For all integers **d**,**k**
$\Delta \vdash$ **{depth=k+l}; guard**$_{k+l}$**(S+(k,l))**
$\approx$ **{depth=k+l}; guard**$_{k+l}$**(S);** $\underline{\textbf{if}}$ **depth**$\leqslant$**k** $\underline{\textbf{then}}$ **depth:=depth−k** $\underline{\textbf{fi}}$
This says that if after executing **S** the depth is $\leqslant$**k** then the last terminal statement executed corresponds to a one of the statements of **S+(k,l)** which has been incremented by **l**. To get the same effect we execute **depth:=depth−k** in this case. If the depth is >**k** then the corresponding terminal statement of **S+(k,l)** would not be incremented so we do nothing. This lemma will be used in the proofs of several important transformations.

Proof: By induction on the structure of **S**:
Let **IF** = $\underline{\textbf{if}}$ **depth**$\leqslant$**k** $\underline{\textbf{then}}$ **depth:=depth−k** $\underline{\textbf{fi}}$
Note that **{depth=k+l}; depth:=depth−n** $\approx$ **{depth=k+l}; guard**$_{k+l}$**(**$\underline{\textbf{exit}}$**(n))**

Case (i): **S** is an **exit** statement and **l**$\leqslant$ |**S**| -say **S** is **exit(n)** with **n**$\geqslant$**l**.
{depth=k+l}; guard$_{k+l}$**(S+(k,l))** $\approx$ **{depth=k+l}; depth:=depth−(n+k)**
$\approx$ **{depth=k+l}; depth:=depth−n;** $\underline{\textbf{if}}$ **depth**$\leqslant$**k** $\underline{\textbf{then}}$ **depth:=depth−k** $\underline{\textbf{fi}}$

Case (ii): **S** is an **exit** statement and **l**> |**S**| -say **S** is **exit(n)** with **n**<**l**.

$\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S+(k,l))}$

$\approx$ $\mathbf{\{depth=k+l\};\ depth{:=}depth-n}$ since the terminal value $\mathbf{n}$ is $<\mathbf{l}$.

$\approx$ $\mathbf{\{depth=k+l\};\ depth{:=}depth-n;\ \{depth>k\}}$

$\approx$ $\mathbf{\{depth=k+l\};\ depth{:=}depth-n;}$ $\underline{\mathbf{if}}$ $\mathbf{depth\leqslant k}$ $\underline{\mathbf{then}}$ $\mathbf{depth{:=}depth-k}$ $\underline{\mathbf{fi}}$

Case (iii): **S** is a non-**exit** primitive and $\mathbf{l=0}$. Thus **S** does not change **depth**.

$\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S+(k,l))}$ $\approx$ $\mathbf{\{depth=k+l\};\ S;\ depth{:=}depth-k}$

$\approx$ $\mathbf{\{depth=k+l\};\ S;}$ $\underline{\mathbf{if}}$ $\mathbf{depth\leqslant k}$ $\underline{\mathbf{then}}$ $\mathbf{depth{:=}depth-k}$ $\underline{\mathbf{fi}}$

Case (iv): **S** is a non-**exit** primitive and $\mathbf{l>0}$. Thus **S** does not change **depth** and the incrementation does not take place.

$\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S+(k,l))}$ $\approx$ $\mathbf{\{depth=k+l\};\ S;\ \{depth>k\}}$

$\approx$ $\mathbf{\{depth=k+l\};\ S;}$ $\underline{\mathbf{if}}$ $\mathbf{depth\leqslant k}$ $\underline{\mathbf{then}}$ $\mathbf{depth{:=}depth-k}$ $\underline{\mathbf{fi}}$

Case (v): $\mathbf{S=S_1;S_2}$ and $\mathbf{l=0}$.

$\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{((S_1;S_2)+(k,l))}$

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1+(k,1));\ guard}_{k+l}\mathbf{(S_2+k)}$

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1);\ IF;}$

$\underline{\mathbf{if}}$ $\mathbf{depth=k+l}$ $\underline{\mathbf{then}}$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_2+k)}$ $\underline{\mathbf{fi}}$

by induction hypothesis and properties of **guard**.

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1);}$

$\underline{\mathbf{if}}$ $\mathbf{depth\leqslant k}$ $\underline{\mathbf{then}}$ $\mathbf{depth{:=}depth-k;\ \{depth\leqslant 0\}}$ $\underline{\mathbf{fi}}$;

$\underline{\mathbf{if}}$ $\mathbf{depth=k+l}$ $\underline{\mathbf{then}}$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_2);\ IF}$ $\underline{\mathbf{fi}}$

by induction hypothesis again.

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1);}$

$\underline{\mathbf{if}}$ $\mathbf{depth\leqslant k}$

$\underline{\mathbf{then}}$ $\mathbf{depth{:=}depth-k}$

$\underline{\mathbf{else}}$ $\underline{\mathbf{if}}$ $\mathbf{depth=k+l}$ $\underline{\mathbf{then}}$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_2);\ IF}$ $\underline{\mathbf{fi}}$ $\underline{\mathbf{fi}}$

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1);}$

$\underline{\mathbf{if}}$ $\mathbf{depth=k+l}$ $\underline{\mathbf{then}}$ $\mathbf{guard}_{k+l}\mathbf{(S_2)}$ $\underline{\mathbf{fi}}$; $\mathbf{IF}$

by forward contraction of $\underline{\mathbf{if}}$.

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1);\ guard}_{k+l}\mathbf{(S_2);\ IF}$

$\approx$ $\mathbf{\{depth=k+l\};\ guard}_{k+l}\mathbf{(S_1;S_2);\ IF}$

Case (vi): $\mathbf{S{=}S_1;S_2}$ and $\mathbf{l{>}0}$.
$\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}((\mathbf{S_1;S_2}){+}(\mathbf{k,l}))$
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}(\mathbf{S_1}{+}(\mathbf{k,l}))$; $\mathbf{guard}_{k+l}(\mathbf{S_2}{+}(\mathbf{k,l}))$
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}(\mathbf{S_1})$; **IF**;
if **depth=k+l** **then** $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}(\mathbf{S_2}{+}(\mathbf{k,l}))$ **fi**
by induction hypothesis and properties of **guard**.
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}(\mathbf{S_1;S_2})$; **IF**
as for last case.

Case (vii): $\mathbf{S}{=}$ **if** $\mathbf{B_1} \rightarrow \mathbf{S_1} \ \square \ \ldots \ \square \ \mathbf{B}_n \rightarrow \mathbf{S}_n$ **fi**
Use case analysis on $\mathbf{B}_1, \ldots, \mathbf{B}_n$ and the induction hypothesis on $\mathbf{S}_1, \ldots, \mathbf{S}_n$ to get:
$\{\mathbf{depth{=}k{+}l}\}$; **if** $\mathbf{B_1} \rightarrow \mathbf{guard}_{k+l}(\mathbf{S_1})$; **IF**
$\square$ ...
$\square$ $\mathbf{B}_n \rightarrow \mathbf{guard}_{k+l}(\mathbf{S}_n)$; **IF** **fi**
Then backward and forward expansion of the outer **if** gives the result.

Case (viii): $\mathbf{S}{=}$**do** $\mathbf{S_1}$ **od**.
$\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}($**do** $\mathbf{S_1}$ **od**$+(\mathbf{k,l}))$
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}($**do** $\mathbf{S_1}{+}(\mathbf{k,l{+}1})$ **od**$)$ by a previous result
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; **depth:=depth+1**;
while **depth=k+l+1** **do** $\{\mathbf{depth{=}k{+}l{+}1}\}$; $\mathbf{guard}_{k+l+1}(\mathbf{S_1}{+}(\mathbf{k,l{+}1}))$ **od**
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; **depth:=depth+1**;
while **depth=k+l+1** **do** $\{\mathbf{depth{=}k{+}l{+}1}\}$; $\mathbf{guard}_{k+l+1}(\mathbf{S_1})$; **IF** **od**
by induction hypothesis.
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; **depth:=depth+1**;
while **depth=k+l+1** **do** $\{\mathbf{depth{=}k{+}l{+}1}\}$; $\mathbf{guard}_{k+l+1}(\mathbf{S_1})$ **od**; **IF**
by forward expansion of **do**.
$\approx$ $\{\mathbf{depth{=}k{+}l}\}$; $\mathbf{guard}_{k+l}($**do** $\mathbf{S_1}$ **od**$)$; **IF**
This proves the Lemma.

Cor A: $\Delta \vdash \{\mathbf{depth{=}d}\}; \mathbf{guard}_d(\mathbf{S{+}d}) \approx \{\mathbf{depth{=}d}\}; \mathbf{depth{:=}depth{-}d}; \mathbf{guard}_0(\mathbf{S})$
Proof: From Lemma A
$\{\mathbf{depth{=}d}\}$; $\mathbf{guard}_d(\mathbf{S{+}d})$
$\approx$ $\{\mathbf{depth{=}d}\}$; $\mathbf{guard}_d(\mathbf{S})$; **if** $\mathbf{depth \leqslant d}$ **then** **depth:=depth−d** **fi**
$\approx$ $\{\mathbf{depth{=}d}\}$; $\mathbf{guard}_d(\mathbf{S})$; **depth:=depth−d** since **S** cannot increase **depth**
$\approx$ $\{\mathbf{depth{=}d}\}$; **depth:=depth−d**; $\mathbf{guard}_0(\mathbf{S})$ from a property of **guard**.

Lemma B: If $\mathbf{S}$ is $\mathbf{d}$-reducible and has no terminal statement with terminal value $\mathbf{d}$ then:
$\Delta \vdash \{\mathbf{depth{=}d{+}1}\}; \mathbf{guard}_{d+1}(\mathbf{S})$
$\approx \{\mathbf{depth{=}d{+}1}\}; \mathbf{guard}_{d+1}(\mathbf{S}[\mathbf{T}{-}\mathbf{1}/\mathbf{T}|\tau \geqslant \mathbf{d}{+}\mathbf{1}]);$
$\underline{\mathbf{if}}$ **depth**$\leqslant$**1** $\underline{\mathbf{then}}$ **depth:=depth−1** $\underline{\mathbf{fi}}$
Proof: By induction on the structure of **S** using the same cases as Lemma A.

Simple Absorption: $\Delta \vdash \mathbf{S;S'} \approx \mathbf{S}[\mathbf{S'} + \delta/\mathbf{T}|\tau = \mathbf{0}]$
The statement **S′** following **S** is "absorbed" into it by replacing all of the terminal statements of **S** which would lead to **S′** by **S′** incremented by the depth of the terminal statement. This is used a great deal when restructuring an unstructured program.

For our example program: **Prog;** **do** **r:=r−1;** **if** **r=0** **then** **exit** **fi**
is equivalent to **Prog** with the first occurrence (only) of **exit** replaced by:
do **r:=r−1;** **if** **r=0** **then** **exit(2)** **fi**

Proof of Simple Absorption: Prove that for all **d**
$\{\mathbf{depth{=}d}\}; \mathbf{guard}_d(\mathbf{S}); \mathbf{guard}_0(\mathbf{S'}) \approx \{\mathbf{depth{=}d}\}; \mathbf{guard}_d(\mathbf{S}[\mathbf{S'} + \delta{+}\mathbf{d}/\mathbf{T}|\tau = \mathbf{d}])$
See the proof of the converse for the cases used.

Defn: **S′** is a term of **S** if for each **k** the replacement of **S′+k** by **exit(k)** in **S** produces a terminal statement with terminal value zero.
This is a generalisation of Arsac's definition of a term in [Arsac 79]. A further generalisation is:

Defn: For $\mathbf{d} \in \mathbb{N}$, **S′** is a **d**-term of **S** if for any **k** each replacement of **S′+k** by **exit(k)** in **S** produces a terminal statement with terminal value **d**.
Thus a term (defined by the previous definition) is a **0**-term.

Lemma: **S′** is a **d**-term of **do** $\mathbf{S}_1$ **od** iff **S′** is a **(d+1)**-term of $\mathbf{S}_1$.
Proof: If some occurrence **exit(k)** is a terminal statement of **do** **S** **od** with terminal value **d** then the same occurrence is a terminal statement of **S** with terminal value **d+1** and vice versa. Thus if replacing some occurrence of **S′+k** by **exit(k)** in **do** **S** **od** gives a terminal statement with terminal value **d** then the same substitution in **S** gives a terminal statement with terminal value **d+1**. Conversely if replacing **S′+k** in **S** gives a terminal statement with terminal value **d+1** then this will be a terminal statement of **do** **S** **od** with **S′+k** replaced by **exit(k)** having terminal value **d**. For $\mathbf{S}_1;\mathbf{S}_2$, a **d**-term of $\mathbf{S}_1$ is a **d**-term of the compound iff **d>0**. A **d**-term of $\mathbf{S}_2$ is always a **d**-term of the compound. For all other compound statements, a **d**-term of any component is a **d**-term of the

compound.

Theorem: If $\mathbf{S'}$ is a term of $\mathbf{S}$ and every terminal statement of $\mathbf{S}$ with terminal value zero occurs within an occurrence of $\mathbf{S'}$+$\mathbf{k}$ in $\mathbf{S}$ (for some $\mathbf{k}$) then

$$\Delta \vdash \mathbf{S} \;\approx\; \mathbf{S}[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}];\mathbf{S'}$$

This is a converse to simple absorption, it is a generalisation of Arsac's version, which makes it more practically useful.

Proof: Prove the following by induction on the structure of $\mathbf{S}$:
If $\mathbf{S'}$ is a $\mathbf{d}$-term of $\mathbf{S}$ and any terminal statement of $\mathbf{S}$ with terminal value $\mathbf{d}$ is within an occurrence of $\mathbf{S'}$+$\mathbf{k}$ in $\mathbf{S}$ (for some $\mathbf{k}$) then

$$\mathbf{S} = \mathbf{S}[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}].$$

We may assume $\mathbf{S'}$ is not primitive or of the form $\mathbf{S'_1};\mathbf{S'_2}$ since otherwise we may replace $\mathbf{S'}$+$\mathbf{k}$ throughout $\mathbf{S}$ by **<u>if</u> true <u>then</u>** $\mathbf{S'}$ **<u>fi</u>** + $\mathbf{k}$ which is not primitive and not a sequence.

<u>Case</u> (i): $\mathbf{S}=\mathbf{S'}+\mathbf{n}$ for some $\mathbf{n}$. We must have $\mathbf{n}=\mathbf{d}$ since $\mathbf{S'}$ is a $\mathbf{d}$-term of $\mathbf{S}$:

$$(\mathbf{S'}+\mathbf{d})[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$
$$= \underline{\mathbf{exit}}(\mathbf{d})[\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}] = \mathbf{S'}+\mathbf{d}$$

<u>Case</u> (ii): $\mathbf{S}$ is primitive. Hence $\mathbf{S}\neq\mathbf{S'}+\mathbf{k}$ for any $\mathbf{k}$. Thus:

$$\mathbf{S}[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}] = \mathbf{S}[\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$

$= \mathbf{S}$ since $\mathbf{S}$ cannot be $\underline{\mathbf{exit}}(\mathbf{d})$ by premise.

<u>Case</u> (iii): $\mathbf{S}=\mathbf{S}_1;\mathbf{S}_2$.

$$(\mathbf{S}_1;\mathbf{S}_2)[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$
$$= (\mathbf{S}_1[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}];\ \mathbf{S}_2[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}])[\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$

since each occurrence of $\mathbf{S'}$+$\mathbf{k}$ must be within $\mathbf{S}_1$ or $\mathbf{S}_2$ since $\mathbf{S'}$+$\mathbf{k}$ is not a sequence.

$$= \mathbf{S}_1[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}];\ \mathbf{S}_2[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$

$= \mathbf{S}_1;\mathbf{S}_2$ by induction hypothesis

<u>Case</u> (iv): $\mathbf{S}=$ **<u>if</u> B <u>then</u>** $\mathbf{S}_1$ **<u>else</u>** $\mathbf{S}_2$ **<u>fi</u>** and $\mathbf{S}\neq\mathbf{S'}+\mathbf{k}$. Any occurrence of $\mathbf{S'}$+$\mathbf{k}$ must be within either $\mathbf{S}_1$ or $\mathbf{S}_2$. Use the induction hypothesis and forward expansion of **<u>if</u>**.

<u>Case</u> (v): $\mathbf{S}=$ **<u>do</u>** $\mathbf{S}_1$ **<u>od</u>**. By Lemma $\mathbf{S}_1$ is a $(\mathbf{d}+\mathbf{1})$-term of $\mathbf{S}_1$ so

$$(\underline{\mathbf{do}}\ \mathbf{S}_1\ \underline{\mathbf{od}})[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$
$$= (\underline{\mathbf{do}}\ \mathbf{S}_1[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}]\ \underline{\mathbf{od}})[\mathbf{S'}+\delta+\mathbf{d}/\mathbf{T}|\tau=\mathbf{d}]$$
$$= \underline{\mathbf{do}}\ \mathbf{S}_1[\underline{\mathbf{exit}}(\mathbf{k})/\mathbf{S'}+\mathbf{k}][\mathbf{S'}+\delta+\mathbf{d}+\mathbf{1}/\mathbf{T}|\tau=\mathbf{d}+\mathbf{1}]\ \underline{\mathbf{od}}$$

$= \underline{\mathbf{do}}\ \mathbf{S_1}\ \underline{\mathbf{od}}$ by induction hypothesis
Which proves the Theorem.

<u>False</u> <u>Iteration:</u> $\Delta \vdash \mathbf{S} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S{+}1}\ \underline{\mathbf{od}}$
Proof: $\mathbf{\{depth{=}1\};\ guard_1(S{+}1)}$
$\approx\ \mathbf{\{depth{=}1\};\ guard_1(S);\ depth{:=}depth{-}1}$
by a previous result.
Thus $\mathbf{\{depth{=}0\};\ depth{:=}1;}\ \underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}\ \mathbf{\{depth{=}1\};\ guard_1(S{+}1)}\ \underline{\mathbf{od}}$
$\approx\ \mathbf{\{depth{=}0\};\ depth{:=}1;}$
$\underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}$
$\mathbf{\{depth{=}1\};\ guard_1(S);\ depth{:=}depth{-}1}\ \underline{\mathbf{od}}$
By loop unrolling this is:
$\approx\ \mathbf{\{depth{=}0\};\ depth{:=}1;}$
$\underline{\mathbf{if}}\ \mathbf{depth{=}1}$
$\underline{\mathbf{then}}\ \mathbf{\{depth{=}1\};\ guard_1(S);\ \{depth{\leqslant}1\};\ depth{:=}depth{-}1;\ \{depth{\leqslant}0\};}$
$\underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}$
$\mathbf{\{depth{=}1\};\ guard_1(S);\ \{depth{\leqslant}1\};}$
$\mathbf{depth{:=}depth{-}1;\ \{depth{\leqslant}0\}}\ \underline{\mathbf{od}}$
$\approx\ \mathbf{\{depth{=}0\};\ depth{:=}1;\ guard_1(S);\ depth{:=}depth{-}1}$
$\approx\ \mathbf{\{depth{=}0\};\ guard_0(S)}$ by the following Lemma.

<u>Lemma:</u> For any $\mathbf{n} \in \mathbb{N}$ and any statement $\mathbf{S}$:
$$\Delta \vdash \mathbf{depth{:=}depth{+}1;\ guard_{\mathit{n}+1}(S);\ depth{:=}depth{-}1}\ \approx\ \mathbf{guard_{\mathit{n}}(S)}$$
Proof: By induction on the structure of $\mathbf{S}$:

<u>Cor:</u> By induction on $\mathbf{m}$ we have the more general form:
$$\Delta \vdash \mathbf{guard_{\mathit{n}}(S)}\ \approx\ \mathbf{depth{:=}depth{+}m;\ guard_{\mathit{n+m}}(S);\ depth{:=}depth{-}m}$$

<u>Defn:</u> $\mathbf{S}$ is <u>reducible</u> if replacing any terminal statement $\underline{\mathbf{exit}}\mathbf{(k)}$, which has terminal value one, by $\underline{\mathbf{exit}}\mathbf{(k{-}1)}$ gives a terminal statement of $\mathbf{S}$.

Note that any statement can be made reducible by the use of absorption. For example:
$\underline{\mathbf{if}}\ \mathbf{i{=}n}\ \underline{\mathbf{then}}\ \underline{\mathbf{exit}}\ \underline{\mathbf{fi}}\mathbf{;\ i{:=}i{+}1.}$
is not reducible, but by absorption we get:
$\underline{\mathbf{if}}\ \mathbf{i{=}n}\ \underline{\mathbf{then}}\ \underline{\mathbf{exit}}$
$\underline{\mathbf{else}}\ \mathbf{i{:=}i{+}1}\ \underline{\mathbf{fi}}\mathbf{.}$

which is reducible. It reduces to:
if i=n **then** skip
    else i:=i+1 **fi**.

Defn: **S** is **d**-reducible if replacing any terminal statement **exit(k)**, which has terminal value **d+1**, by **exit(k−1)** gives a terminal statement of **S**. Note that this is always the case for **d>0**.

Theorem: If **S** is reducible and all terminal statements of **S** have terminal value greater than zero then:

$$\Delta \vdash \textbf{do S od} \;\approx\; \mathbf{S[T{-}1/T} | \tau > \mathbf{0]} = \mathbf{S{-}1}$$

where **exit(k)−1** = **exit(k−1)** for **k>0**. In the substitution **T** must be an **exit(k)** with **k>0** for it to have $\tau > \mathbf{0}$ so **T−1** is always defined. This is a converse to false iteration.
Proof: From Lemma A with **k=1** and **l=d** we have:
$\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S{+}(1,d)})$
    $\approx$ $\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S})$; **if** depth$\leqslant$1 **then** depth:=depth−1 **fi**
From Lemma B we have:
$\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S})$
    $\approx$ $\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S{-}(1,d{+}1)})$; **if** depth$\leqslant$1 **then** depth:=depth−1 **fi**
Hence if **S** is **d**-reducible and has no terminal statement with terminal value **d** then:
$\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}((\mathbf{S{-}(1,d{+}1)){+}(1,d)})$
    $\approx$ $\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S{-}(1,d{+}1)})$; **if** depth$\leqslant$1 **then** depth:=depth−1 **fi**
    $\approx$ $\{\mathbf{depth{=}d{+}1}\}$; $\mathbf{guard}_{d+1}(\mathbf{S})$
ie $(\mathbf{S{-}(1,d{+}1)){+}(1,d)} \approx \mathbf{S}$.
Putting **d=1** we get: $\mathbf{S} \approx (\mathbf{S{-}(1,1)){+}1}$
Hence **do** S **od** $\approx$ **do** (S−(1,1))+1 **od** $\approx$ S−(1,1) = S−1 (by false iteration).

A consequence of these two results is:

Theorem: If **S′** is a term of **S** then:

$$\Delta \vdash \mathbf{S} \;\approx\; \textbf{do } \mathbf{(S{+}1)[S'{+}k{+}1/exit(k)];\ S'{+}1} \textbf{ od}$$

This can be used to combine multiple copies of a statement into a single copy by putting a false loop around the program, replacing each copy of the statement by an **exit** and putting a single copy at the end of the loop body. Multiple copies of a statement often occur during the removal of recursion and during the restructuring of an unstructured program.
Proof: If **S′** is a term of **S** then **S′+1** is a term of **S+1** and **S+1** has no terminal statement with terminal value zero, so by absorption:

$$\mathbf{S{+}1} \;\approx\; \mathbf{(S{+}1)[S'{+}k{+}1/\underline{exit}(k)];\ S'{+}1}$$

And by false iteration: $\mathbf{S} \;\approx\; \mathbf{\underline{do}\ S{+}1\ \underline{od}}$.

Defn: **S** is a proper sequence iff every terminal statement of **S** has terminal value zero, ie

$$\forall \mathbf{T,n.}\ \mathbf{ts(n,T,S)} \Rightarrow \tau\mathbf{(n,T,S)=0}$$

Thus a proper sequence cannot change **depth**.

If the body of a loop has no terminal statement with terminal value zero then the loop is a "false loop" (the body is only executed once since the execution of any terminal statement in the body will cause termination of the loop). If the body is reducible then the loop can br removed. Note that a statement can always be made reducible by absorption so this is always possible: but the absorption may cause an increase in the program text length. Such "false loops" are useful in "factoring out" several occurrences of a statement into a single occurrence. For example:

$\mathbf{\underline{if}\ B_1\ \underline{then}\ S_1;\ \underline{if}\ B_2\ \underline{then}\ S_2} \;\approx\; \mathbf{\underline{do}\ \underline{if}\ B_1\ \underline{then}\ S_1;\ \underline{if}\ B_2\ \underline{then}\ S_2{+}1\ \underline{fi}\ \underline{fi};}$
$\quad\quad \mathbf{\underline{else}\ S\ \underline{fi}\ S{+}1\ \underline{od}}$
$\quad \mathbf{\underline{else}\ S\ \underline{fi}}$

where the second version has only one copy of **S**. If we make the body of the loop on the RHS reducible by absorbing **S+1** and then remove the false iteration we get the LHS.

Loop inversion: $\Delta \vdash \mathbf{\underline{while}\ B\ \underline{do}\ S_1;\ \underline{if}\ B\ \underline{then}\ S_2\ \underline{fi}\ \underline{od}}$
$\quad\quad\quad \approx\; \mathbf{\underline{if}\ B\ \underline{then}\ S_1\ \underline{fi};\ \underline{while}\ B\ \underline{do}\ S_2;\ \underline{if}\ B\ \underline{then}\ S_1\ \underline{fi}\ \underline{od}}$

Proof: Since the assertion $\mathbf{\{B\}}$ can be inserted in the loop **while B do ... od** it is sufficient to prove:
$\Delta \vdash \mathbf{\underline{while}\ B\ \underline{do}\ \underline{if}\ B\ \underline{then}\ S_1\ \underline{fi};\ \underline{if}\ B\ \underline{then}\ S_2\ \underline{fi}\ \underline{od}}$
$\quad \approx\; \mathbf{\underline{if}\ B\ \underline{then}\ S_1\ \underline{fi};\ \underline{while}\ B\ \underline{do}\ \underline{if}\ B\ \underline{then}\ S_2\ \underline{fi};\ \underline{if}\ B\ \underline{then}\ S_1\ \underline{fi}\ \underline{od}}$
Let $\mathbf{IF_1} = \mathbf{\underline{if}\ B\ \underline{then}\ S_1\ \underline{fi}}$, $\mathbf{IF_2} = \mathbf{\underline{if}\ B\ \underline{then}\ S_2\ \underline{fi}}$. So we are trying to prove

$$\Delta \vdash \mathbf{\underline{while}\ B\ \underline{do}\ IF_1;\ IF_2\ \underline{od}} \;\approx\; \mathbf{IF_1;\ \underline{while}\ B\ \underline{do}\ IF_2;\ IF_1\ \underline{od}}$$

where the two statements inside the loop have been reversed–hence the name of the theorem. Use induction to show that:
$\Delta \vdash \mathbf{\underline{while}\ B\ \underline{do}\ IF_1;\ IF_2\ \underline{od}}^n \leqslant \mathbf{IF_1;\ \underline{while}\ B\ \underline{do}\ IF_2;\ IF_1\ \underline{od}}^n$ for $\mathbf{n{>}1}$.
Then show that:
$\Delta \vdash \mathbf{IF_1;\ \underline{while}\ B\ \underline{do}\ IF_2;\ IF_1\ \underline{od}}^n \leqslant \mathbf{\underline{while}\ B\ \underline{do}\ IF_1;\ IF_2\ \underline{od}}^{n+1}$ for $\mathbf{n{\geqslant}1}$.
The theorem follows from the general induction rule for iteration.

Inversion:
$\Delta \vdash \mathbf{\underline{do}\ S_1;S_2\ \underline{od}} \;\approx\; \mathbf{\underline{do}\ S_1;\ \underline{do}\ S_2;S_1\ \underline{od}{+}1\ \underline{od}}$

Proof: Let $\mathbf{IF}_1$ = if depth=1 then guard$_1$(S_1) fi, $\mathbf{IF}_2$ = if depth=1 then guard$_1$(S_2) fi
{depth=0}; guard$_0$(do S_1;S_2 od)
$\approx$ {depth=0}; depth:=1; while depth=1 do guard$_1$(S_1;S_2) od
$\approx$ {depth=0}; depth:=1; while depth=1 do $\mathbf{IF}_1$; $\mathbf{IF}_2$ od
$\approx$ {depth=0}; depth:=1; $\mathbf{IF}_1$; while depth=1 do $\mathbf{IF}_2$; $\mathbf{IF}_1$ od
by loop inversion.
$\approx$ {depth=0}; depth:=1; guard$_1$(S_1); while depth=1 do guard$_1$(S_2;S_1) od
$\approx$ {depth=0}; depth:=1; guard$_1$(S_1);
if depth=1 then {depth=1}; while depth=1 do guard$_1$(S_2;S_1) od fi
$\approx$ {depth=0}; depth:=1; guard$_1$(S_1);
if depth=1
then depth:=2; while depth=2 do guard$_2$(S_2;S_1);
if depth$\leqslant$1 then depth:=depth$-$1 fi; od;
{depth$<$1} fi
$\approx$ {depth=0}; depth:=1; guard$_1$(S_1);
if depth=1
then depth:=2 while depth=2 do guard$_2$((S_2;S_1)+(1,1)) od;
{depth$<$1} fi
$\approx$ {depth=0}; depth:=1; guard$_1$(S_1); guard$_1$(do S_2;S_1 od+1); {depth$<$1}
$\approx$ {depth=0}; depth:=1;
if depth=1
then guard$_1$(S_1); guard$_1$(do S_2;S_1 od+1);
while depth=1 do guard$_1$(S_1; do S_2;S_1 od+1) od fi
$\approx$ {depth=0}; depth:=1; while depth=1 do guard$_1$(S_1; do S_2;S_1 od+1) od
by loop rolling.
$\approx$ {depth=0}; guard$_0$(do S_1; do S_2;S_1 od+1 od)

Hence: do S_1;S_2 od $\approx$ do S_1; do S_2;S_1 od+1 od as required.

This transformation is often used in converting a **do** loop with an **exit** in the middle into a **while** loop by moving some statements outside the loop. For example if S_1 and S_2 are proper sequences then:
do S_1; if B then exit fi; S_2 od $\approx$ do S_1; do if B then exit fi; S_2; S_1 od+1 od
$\approx$ S_1; do if B then exit fi; S_2; S_1 od (since S_1 is a proper sequence)
$\approx$ S_1; while $\neg$B do S_2; S_1 od. (since S_1 and S_2 are proper sequences).

Theorem: If $\mathbf{S}_1$ is reducible then

$$\Delta \vdash \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \ \approx\ \mathbf{S}_1[\underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\delta+\mathbf{1/T}|\tau=\mathbf{0}]-\mathbf{1}$$

Proof: By inversion:
$\underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\mathbf{1}\ \underline{\mathbf{od}}$
By absorption $\mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\mathbf{1} \ \approx\ \mathbf{S}_1[\underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\delta+\mathbf{1/T}|\tau=\mathbf{0}]$

Claim: $\mathbf{S}_1[\underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\delta+\mathbf{1/T}|\tau=\mathbf{0}]$ is reducible and has no terminal statement with terminal value zero. To prove this claim, prove the following by induction on the structure of $\mathbf{S}$:
For any $\mathbf{k}$, if $\mathbf{S}$ is $\mathbf{d}$-reducible then $\mathbf{S}[\mathbf{S}'+\mathbf{k}+\delta+\mathbf{d/T}|\tau=\mathbf{d}]$ is also $\mathbf{d}$-reducible and has no terminal statement with terminal value $\mathbf{d}$.
Then by false iteration: $\underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S}_1[\underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\delta+\mathbf{1/T}|\tau=\mathbf{0}]\ \underline{\mathbf{od}}$

$$\approx\ \mathbf{S}_1[\underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\delta+\mathbf{1/T}|\tau=\mathbf{0}]-\mathbf{1}$$

which proves the theorem.

Proper Inversion:
If $\mathbf{S}_1$ is a proper sequence then: $\Delta \vdash \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \ \approx\ \mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}$
Proof: If $\mathbf{S}_1$ is a proper sequence then for any statement $\mathbf{S}$:

$$(\mathbf{S}_1;\mathbf{S})+\mathbf{1} = \mathbf{S}_1+(\mathbf{1},\mathbf{1});\ \mathbf{S}_2+\mathbf{1} = \mathbf{S}_1;\ \mathbf{S}+\mathbf{1}$$

since all of the terminal statements of $\mathbf{S}_1$ have terminal value zero.
Thus $\underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}+\mathbf{1}\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ (\mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}})+\mathbf{1}\ \underline{\mathbf{od}}$
$\approx\ \mathbf{S}_1;\ \underline{\mathbf{do}}\ \mathbf{S}_2;\mathbf{S}_1\ \underline{\mathbf{od}}$ by false iteration.

Repetition:
(a) $\Delta \vdash \mathbf{S}_1 \leqslant \mathbf{S}\ \wedge \mathbf{S}_2 \leqslant \mathbf{S} \Rightarrow \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}$
(b) $\Delta \vdash \mathbf{S} \leqslant \mathbf{S}_1 \wedge \mathbf{S} \leqslant \mathbf{S}_2 \Rightarrow \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}}$

Cor: $\Delta \vdash \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S};\mathbf{S}\ \underline{\mathbf{od}}$ (Loop doubling)
$\Delta \vdash \mathbf{S}_2 \leqslant \mathbf{S}_1 \Rightarrow \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S}_1\ \underline{\mathbf{od}}$
$\Delta \vdash \mathbf{S}_1 \leqslant \mathbf{S}_2 \Rightarrow \underline{\mathbf{do}}\ \mathbf{S}_1\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}}$

Proof: These are in fact all consequences of **loop doubling:**
(a) If $\mathbf{S}_1 \leqslant \mathbf{S}$ and $\mathbf{S}_2 \leqslant \mathbf{S}$ then $\mathbf{S}_1;\mathbf{S}_2 \leqslant \mathbf{S};\mathbf{S}$ and hence $\underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S};\mathbf{S}\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}$
(b) If $\mathbf{S} \leqslant \mathbf{S}_1$ and $\mathbf{S} \leqslant \mathbf{S}_2$ then $\mathbf{S};\mathbf{S} \leqslant \mathbf{S}_1;\mathbf{S}_2$ and hence $\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathbf{S};\mathbf{S}\ \underline{\mathbf{od}} \leqslant \underline{\mathbf{do}}\ \mathbf{S}_1;\mathbf{S}_2\ \underline{\mathbf{od}}$

Proof of Loop Doubling:
$\{\mathbf{depth=0}\};\ \mathbf{guard}_0(\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}) \ \approx\ \{\mathbf{depth=0}\};\ \mathbf{depth{:=}1};\ \underline{\mathbf{while}}\ \mathbf{depth=1}\ \underline{\mathbf{do}}\ \mathbf{guard}_1(\mathbf{S})\ \underline{\mathbf{od}}$

Let **IF** $\equiv$ **<u>if</u> depth=1 <u>then</u> guard$_1$(S) <u>fi</u>** $\approx$ **guard$_1$(S)**.
Let **DO$_1$** $\equiv$ **<u>while</u> depth=1 <u>do</u> IF <u>od</u>**
DO$_2$ $\equiv$ **<u>while</u> depth=1 <u>do</u> IF;IF <u>od</u>**
We need to prove **DO$_1$** $\approx$ **DO$_2$**.
Proof is by induction rule for loops:

Claim: $\mathbf{DO}_1^{2n} \leqslant \mathbf{DO}_2$ for all $\mathbf{n} < \omega$.
Trivial for **n=0** so suppose it holds for **n**.
$\mathbf{DO}_1^{2(n+1)} \approx \mathbf{DO}_1^{2n+2} \approx$ **<u>if</u> depth=1 <u>then</u> IF; <u>if</u> d=1 <u>then</u> IF; $\mathbf{DO}_1^{2n}$ <u>fi</u> <u>fi</u>**
$\leqslant$ **<u>if</u> depth=1 <u>then</u> IF; <u>if</u> d=1 <u>then</u> IF; DO$_2$ <u>fi</u> <u>fi</u>** by induction hyp
$\approx$ **<u>if</u> depth=1 <u>then</u> IF; IF; DO$_2$ <u>fi</u>** by case analysis on inner **<u>if</u>**
$\approx$ **DO$_2$** by loop rolling.

Claim: $\mathbf{DO}_2^{n} \leqslant \mathbf{DO}_1$ for all $\mathbf{n} < \omega$.
Trivial for **n=0** so suppose it holds for **n**.

$\mathbf{DO}_2^{n+1} \approx$ **<u>if</u> depth=1 <u>then</u> IF; IF; $\mathbf{DO}_2^{n}$ <u>fi</u>**
$\kappa\kappa\kappa \leqslant$ **<u>if</u> depth=1 <u>then</u> IF; IF; DO$_1$ <u>fi</u>** by induction hypothesis
$\approx$ **<u>if</u> depth=1 <u>then</u> IF; <u>if</u> depth=1 <u>then</u> IF; DO$_1$ <u>fi</u> <u>fi</u>** by case analysis
$\approx$ **<u>if</u> depth=1 <u>then</u> IF; DO$_1$ <u>fi</u>** by loop rolling
$\approx$ **DO$_1$**.
Hence by induction rule for loops **DO$_1$** $\approx$ **DO$_2$**.

<u>Arsac's Version of the Repetition Transformation</u>
Arsac in [Arsac 79] gives the following, more general, version of this transformation:

<u>do</u> S$_1$ **<u>od</u>** $\approx$ **<u>do</u>** S$_2$ **<u>od</u>** $\iff$ **<u>do</u>** S$_1$ **<u>od</u>** $\approx$ **<u>do</u>** S$_1$;S$_2$ **<u>od</u>**

However, this fails in general, to see this take **S$_2$ =skip**. Then the **RHS** is:
<u>do</u> S$_1$ <u>od</u> $\approx$ **<u>do</u> S$_1$; skip <u>od</u>** which holds for any **S$_1$** while the **LHS** is:
<u>do</u> S$_1$ <u>od</u> $\approx$ **<u>do</u> skip <u>od</u>** $\approx$ **abort** which is clearly not true in general.

The other implication, namely:
<u>do</u> S$_1$ <u>od</u> $\approx$ **<u>do</u> S$_2$ <u>od</u>** $\Rightarrow$ **<u>do</u> S$_1$ <u>od</u>** $\approx$ **<u>do</u> S$_1$;S$_2$ <u>od</u>**
looks more convincing but also fails in general. Take
S$_1$ = <u>if</u> x$\leqslant$0 <u>then</u> <u>exit</u> <u>fi</u>; x:=x−1

$\mathbf{S_2} = \underline{\mathbf{if}}\ \mathbf{x{\leqslant}0}\ \underline{\mathbf{then}}\ \underline{\mathbf{exit}}\ \underline{\mathbf{fi}}\mathbf{;\ x{:=}x-2}$

Then it is easy to see that: $\{\mathbf{x{\geqslant}0} \wedge \mathbf{even(x)}\} \vdash \underline{\mathbf{do}}\ \mathbf{S_1}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S_2}\ \underline{\mathbf{od}} \approx \mathbf{x{:=}0}$

But if $\mathbf{x{=}2}$ initially then $\underline{\mathbf{do}}\ \mathbf{S_1;S_2}\ \underline{\mathbf{od}} \approx \mathbf{x{:=}{-1}}$

So $\underline{\mathbf{do}}\ \mathbf{S_1}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S_1;S_2}\ \underline{\mathbf{od}}$ cannot be true.

Arsac uses this transformation to derive a version of "selective unrolling" (see next Chapter) which cannot in fact be derived from the transformations he gives. This invalidates his claim that his set of transformations is "complete" in the sense that any syntactic transformation (ie a transformation that preserves the sequence of states) can be derived from them. For example, the following example of selective unrolling cannot be derived from the transformations given by Arsac:

$$\begin{array}{lcl} \underline{\mathbf{do}}\ \underline{\mathbf{if}}\ \mathbf{B}\ \underline{\mathbf{then}}\ \mathbf{S_1} & \approx & \underline{\mathbf{do}}\ \underline{\mathbf{if}}\ \mathbf{B}\ \underline{\mathbf{then}}\ \mathbf{S_1};\ \underline{\mathbf{if}}\ \mathbf{B}\ \underline{\mathbf{then}}\ \mathbf{S_1}\ \underline{\mathbf{fi}} \\ \quad \underline{\mathbf{else}}\ \mathbf{S_2}\ \underline{\mathbf{fi}}\ \underline{\mathbf{od}}. & & \quad \underline{\mathbf{else}}\ \mathbf{S_2}\ \underline{\mathbf{fi}}\ \underline{\mathbf{od}}. \end{array}$$

This is because each of his transformations preserves the property that the number of copies of $\mathbf{S_1}$ within any loop equals the number of copies of $\mathbf{S_2}$. This property holds for the first version, but for the second version we have two copies of $\mathbf{S_1}$ and only one of $\mathbf{S_2}$. Hence no sequence of Arsac's transformations will convert the LHS into the RHS.

<u>First</u> <u>Step</u> <u>Unrolling:</u>

$\Delta \vdash \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S;}\ \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}{+}\mathbf{1}\ \underline{\mathbf{od}}$

Proof: $\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S;S}\ \underline{\mathbf{od}}$ loop doubling.

$\approx \underline{\mathbf{do}}\ \mathbf{S;}\ \underline{\mathbf{do}}\ \mathbf{S;S}\ \underline{\mathbf{od}}{+}\mathbf{1}\ \underline{\mathbf{od}}$ inversion.

$\approx \underline{\mathbf{do}}\ \mathbf{S;}\ \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}{+}\mathbf{1}\ \underline{\mathbf{od}}$ loop doubling.

If $\mathbf{S}$ is reducible then $\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \approx \mathbf{S}[\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}{+}\mathbf{1}{+}\delta/\mathbf{T}|\tau = \mathbf{0}]{-}\mathbf{1}$

Proof: $\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S;S}\ \underline{\mathbf{od}}$ loop doubling.

$\approx \mathbf{S}[\underline{\mathbf{do}}\ \mathbf{S;S}\ \underline{\mathbf{od}}{+}\mathbf{1}{+}\delta/\mathbf{T}|\tau = \mathbf{0}]{-}\mathbf{1}$ inversion.

$\approx \mathbf{S}[\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}{+}\mathbf{1}{+}\delta/\mathbf{T}|\tau = \mathbf{0}]{-}\mathbf{1}$ loop doubling.

<u>Double</u> <u>Iteration:</u>

If $\mathbf{S}$ is reducible then: $\Delta \vdash \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S}[\mathbf{T}{-}\mathbf{1}/\mathbf{T}|\tau > \mathbf{0}]\ \underline{\mathbf{od}} \approx \underline{\mathbf{do}}\ \mathbf{S}{-}\mathbf{1}\ \underline{\mathbf{od}}$

Note that any statement can be made reducible by the repeated application of absorption, hence any double loop can be converted to a single loop if required. However in general this will cause an increase in program text length. The choice of whether to use a single loop or a double loop can be made on the basis of which version best expresses the solution of the problem.

Defn: If $\mathbf{k} \leqslant \mathbf{d}$ then $\mathbf{S}-(\mathbf{k},\mathbf{d}) =_{DF} \mathbf{S}[\mathbf{T}-\mathbf{k}/\mathbf{T}|\tau \geqslant \mathbf{d}]$.
Note $(\mathbf{S}+(\mathbf{k},\mathbf{d}))-(\mathbf{k},\mathbf{d}) = \mathbf{S}$, in fact $(\mathbf{S}+(\mathbf{k},\mathbf{d}))-(\mathbf{k},\mathbf{d}') = \mathbf{S}$ holds for any $\mathbf{d}'$ with $\mathbf{d} \leqslant \mathbf{d}' < \mathbf{d}+\mathbf{k}$.
The converse $(\mathbf{S}-(\mathbf{k},\mathbf{d}))+(\mathbf{k},\mathbf{d}) = \mathbf{S}$ is not valid: for example $\mathbf{S}-(\mathbf{k},\mathbf{k})$ is the same as $\mathbf{S}-\mathbf{k}$.

Lemma A: If $\mathbf{k} \leqslant \mathbf{d}$ then

$$\{\mathbf{depth}=\mathbf{d}\};\ \mathbf{guard}_d(\mathbf{S}-(\mathbf{k},\mathbf{d})) \approx \mathbf{guard}_d(\mathbf{S});\ \underline{\mathbf{if}}\ \mathbf{depth} \leqslant 0\ \underline{\mathbf{then}}\ \mathbf{depth}:=\mathbf{depth}+\mathbf{k}\ \underline{\mathbf{fi}}$$

The proof is similar to the corresponding Lemma for partial incrementation.

The following Lemma is also used in the next Chapter in the theorem on transforming a regular action system to iterative form:

Lemma B: The following are equivalent:
(i) **{x=a}; while x=a do x:=b; S; if x=b then x:=a fi od**.
(ii) **{x=a}; while x=a ∨ x=b do x:=b; S od**.
(iii) **{x=a}; while x=a do x:=b; while x=b do S od od**.
Proof: For (i) ≈ (ii) prove that the **n**th truncations are equivalent and use the induction rule for iteration.

For (iii) ⩽ (ii) we also use induction to prove
{x=a}; while x=a do x:=b; while x=b do S od od^n
⩽ **{x=a}; while x=a ∨ x=b do x:=b; S od** -the base case (**n=1**) is trivial.
{x=a}; while x=a do x:=b; while x=b do S od od^{n+1}
≈ **{x=a}; if x=a then x:=b; while x=b do S od;**
while x=a do x:=b; while x=b do S od od^n **fi**
n⩾1 so {x≠a} ⊢ **while x=a do ... od**^{n} ≈ **skip**. So this is
≈ **{x=a}; x:=b; while x=b do S od; {x≠b};**
if x=a then while x=a do x:=b; while x=b do S od od^n **fi**
⩽ **{x=a}; x:=b; while x=b do S od; {x≠b};**
if x=a then while x=a ∨ x=b do x:=b; S od fi
by induction hypothesis.
≈ **{x=a}; x:=b; while x=b do S od; {x≠b};**
if x=a ∨ x=b then while x=a ∨ x=b do x:=b; S od fi
≈ **{x=a}; x:=b; S; while x=b do S od; while x=a ∨ x=b do x:=b; S od**
by loop unrolling and removing the **if**.
≈ **{x=a}; x:=b; S; while x=a ∨ x=b do x:=b; S od** by loop merging.

$\approx$ **{x=a}; while x=a $\vee$ x=b do x:=b; S od** by loop unrolling.

Finally to prove (ii) $\leqslant$ (iii) use induction to prove
{x=a}; while x=a $\vee$ x=b do x:=b; S od^n
$\leqslant$ **{x=a}; while x=a do x:=b; while x=b do S od od**

Proof: of double iteration:
{depth=0}; guard$_0$**(do do S od od)**
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do depth:=2; while depth=2 do guard$_2$**(S) od od**
{depth=0}; guard$_0$**(do S od−1)**
$\approx$ **{depth=0}; guard**$_0$**(do S[T−1/T|**τ **>0] od)**
$\approx$ **{depth=0}; depth:=1; while depth=1 do guard**$_1$**(S[T−1/T|**τ **>0]) od**

Let **IF** $\equiv$ **if depth$\leqslant$0 then depth:=depth+1 fi**. Then by Lemma A:
{depth=0}; guard$_0$**(do S od−1)**
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do guard$_1$**(S); if depth$\leqslant$0 then depth:=depth+1 fi od**
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do depth:=2; guard$_2$**(S); depth:=depth−1;**
if depth$\leqslant$0 then depth:=depth+1 fi od
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do depth:=2; guard$_2$**(S);**
if depth>1 then depth:=depth−1 fi od
by case analysis on **depth:=depth−1; if depth$\leqslant$0 then depth:=depth+1 fi**.
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do depth:=2; guard$_2$**(S);**
if depth=2 then depth:=depth−1 fi od
since **depth** can only be decreased.
$\approx$ **{depth=0}; depth:=1;**
while depth=1 do depth:=2; while depth=2 do guard$_2$**(S) od od**
by Lemma B.
$\approx$ **guard**$_0$**(do do S od od)**.

Cor: For any **S**:
$\Delta \vdash$ **do do do S od od od** $\approx$ **do do S od−1 od**

Proof: any terminal statement of **do** **S** **od** with terminal value one must be a terminal statement of **S** with terminal value two. So reducing such a statement by one gives a terminal statement with terminal value one of **S** and hence a terminal statement of **do** **S** **od**. Hence **do** **S** **od** is reducible and we can apply the last result.
Thus more than two nested **do** loops around the same statement are never needed.

Loop Absorption:
If $\mathbf{S}_1$ is reducible then
$\Delta \vdash$ $\underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathrm{S}_1\ \underline{\mathbf{od}};\ \mathrm{S}_2\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathrm{S}_1[\mathrm{S}_2 + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}]\mathbf{-1}\ \underline{\mathbf{od}}$
Proof: $\underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathrm{S}_1\ \underline{\mathbf{od}};\ \mathrm{S}_2\ \underline{\mathbf{od}}$
$\approx\ \underline{\mathbf{do}}\ (\underline{\mathbf{do}}\ \mathrm{S}_1\ \underline{\mathbf{od}})[\mathrm{S}_2 + \delta\mathbf{/T}|\tau\ \mathbf{=0}]\ \underline{\mathbf{od}}$ by absorption.
$\approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathrm{S}_1[\mathrm{S}_2 + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}]\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$
Now $\mathbf{S}_1[\mathbf{S}_2 + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}]$ is reducible and has no terminal statement with terminal value zero (by a previous Lemma). So we can apply double iteration to get:
$\underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathrm{S}_1\ \underline{\mathbf{od}};\ \mathrm{S}_2\ \underline{\mathbf{od}} \ \approx\ \underline{\mathbf{do}}\ \mathrm{S}_1[\mathrm{S}_2 + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}]\mathbf{-1}\ \underline{\mathbf{od}}$

This can often be used to replace a double-nested loop by a single loop. For example, suppose we have:
$\underline{\mathbf{do}}\ \mathrm{S}_1;\ \underline{\mathbf{do}}\ \mathrm{S}_2\ \underline{\mathbf{od}};\ \mathrm{S}_3\ \underline{\mathbf{od}}$ where $\mathbf{S}_1$ and $\mathbf{S}_2$ are reducible.
Move the inner loop to the beginning by proper inversion to give:
$\mathrm{S}_1;\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathrm{S}_2\ \underline{\mathbf{od}};\ \mathrm{S}_3;\ \mathrm{S}_1\ \underline{\mathbf{od}}$
Apply loop absorption to give:
$\mathrm{S}_1;\ \underline{\mathbf{do}}\ \mathrm{S}_2[(\mathrm{S}_3;\mathrm{S}_1) + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}]\ \underline{\mathbf{od}}\ \mathbf{-1}$
which is now a single loop.

This can also be used to combine several copies of one statement inside a single loop by transforming it to a double loop. We replace the single loop by a double loop, replace each copy of the statement by an **exit** of the inner loop and put a single copy of the statement between the two loops, after the inner loop

Lemma 1: If S' is a term of **S** then:
$\Delta \vdash \mathbf{S+1}\ \approx\ (\mathbf{S+(1,1)})[\underline{\mathbf{exit}}\mathbf{(k+1)/S'+(1,1)+k}][\mathbf{S'} + \delta\mathbf{+1/T}|\tau\ \mathbf{=1}][\mathbf{T+1/T}|\tau\ \mathbf{=0}]$
Proof: We use induction on the structure of **S** and prove the more general result:
$\mathbf{S+1}\ \approx\ (\mathbf{S+(1,d)})[\underline{\mathbf{exit}}\mathbf{(k+1)/S'+(1,1)+k}][\mathbf{S'} + \delta\mathbf{+d/T}|\tau\ \mathbf{=d}][\mathbf{T+1/T}|\tau\ \mathbf{<d}]$
where $\mathbf{d}\geqslant\mathbf{1}$ and $\mathbf{S}'$ is a $(\mathbf{d-1})$-term of **S**. As usual we may assume $\mathbf{S}'$ is compound and not a sequence since otherwise we may replace $\mathbf{S'+k}$ by
if **true** **then** $\mathrm{S}'\mathbf{+k}$ **fi**.

Let $[\mathbf{A}] = [\underline{\mathbf{exit}}(\mathbf{k+1})/\mathbf{S}'+(\mathbf{1,1})+\mathbf{k}]$, $[\mathbf{B}] = [\mathbf{S}' + \delta + \mathbf{d}/\mathbf{T}|\tau = \mathbf{d}]$, $[\mathbf{C}] = [\mathbf{T+1/T}|\tau < \mathbf{d}]$.
The only difficult case is:
<u>Case</u> (iv): $\mathbf{S} = \mathbf{S}_1;\mathbf{S}_2$ and $\mathbf{d}>\mathbf{1}$.
$(\mathbf{S}+(\mathbf{1,d}))[\mathbf{A}][\mathbf{B}][\mathbf{T+1/T}|\tau < \mathbf{d}]$
$\quad \approx\ (\mathbf{S}_1+(\mathbf{1,d}))[\mathbf{A}][\mathbf{B}][\mathbf{T+1/T}|\mathbf{0}< \tau < \mathbf{d}];\ (\mathbf{S}_2+(\mathbf{1,d}))[\mathbf{A}][\mathbf{B}][\mathbf{T+1/T}|\tau < \mathbf{d}]$
Claim: If $\mathbf{d}>\mathbf{1}$ then $(\mathbf{S}_1+(\mathbf{1,d}))[\mathbf{A}][\mathbf{B}][\mathbf{T+1/T}|\mathbf{0}< \tau < \mathbf{d}] \ \approx\ \mathbf{S}_1+(\mathbf{1,1})$
Then by induction hypothesis
$(\mathbf{S}+(\mathbf{1,d}))[\mathbf{A}][\mathbf{B}][\mathbf{T+1/T}|\tau < \mathbf{d}]$
$\quad \approx\ \mathbf{S}_1+(\mathbf{1,1});\ \mathbf{S}_2+\mathbf{1}\ \approx\ (\mathbf{S}_1;\mathbf{S}_2)+\mathbf{1}\ \approx\ \mathbf{S+1}.$
Proof of Claim: Prove by induction on the structure of $\mathbf{S}$ that:
If $\mathbf{d}>\mathbf{1}$ and $\mathbf{0}<\mathbf{l}<\mathbf{d}$ and $\mathbf{S}'$ is a $(\mathbf{d}-\mathbf{1})$-term of $\mathbf{S}$ then
$\quad \Delta \vdash (\mathbf{S}+(\mathbf{1,d}))[\underline{\mathbf{exit}}(\mathbf{k+1})/\mathbf{S}'+(\mathbf{1,1})+\mathbf{k}][\mathbf{S}' + \delta + \mathbf{d}/\mathbf{T}|\tau = \mathbf{d}][\mathbf{T+1/T}|\mathbf{l}< \tau < \mathbf{d}]\ \approx\ \mathbf{S}+(\mathbf{1,l})$

This claim is also used in <u>Case</u> (vi): $\mathbf{S} = \underline{\mathbf{do}}\ \mathbf{S}_1\ \underline{\mathbf{od}}$.

<u>**Lemma**</u> <u>**2:**</u> $\underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathbf{S};\ \underline{\mathbf{exit}}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}\ \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$.
Proof: Consider:
$\{\mathbf{depth{=}0}\};\ \mathbf{depth{:=}1};\ \underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}$
$\qquad\qquad \mathbf{depth{:=}2};\ \underline{\mathbf{while}}\ \mathbf{depth{=}2}\ \underline{\mathbf{do}}\ \mathbf{guard}_2(\mathbf{S});$
$\qquad\qquad\qquad\qquad \underline{\mathbf{if}}\ \mathbf{depth{=}2}\ \underline{\mathbf{then}}\ \mathbf{depth{:=}1}\ \underline{\mathbf{fi}}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}.$
By Lemma B ((iii)$\Rightarrow$(i))this is equivalent to:
$\{\mathbf{depth{=}0}\};\ \mathbf{depth{:=}1};\ \underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}$
$\qquad\qquad \mathbf{depth{:=}2};\ \mathbf{guard}_2(\mathbf{S});\ \underline{\mathbf{if}}\ \mathbf{depth{=}2}\ \underline{\mathbf{then}}\ \mathbf{depth{:=}1}\ \underline{\mathbf{fi}};\ \{\mathbf{depth}\neq\mathbf{2}\}$
$\qquad\qquad \underline{\mathbf{if}}\ \mathbf{depth{=}2}\ \underline{\mathbf{then}}\ \mathbf{depth{:=}1}\ \underline{\mathbf{fi}}\ \underline{\mathbf{od}}.$
The second $\underline{\mathbf{if}}$ can be removed and then Lemma B ((i)$\Rightarrow$(iii)) gives:
$\{\mathbf{depth{=}0}\};\ \mathbf{depth{:=}1};\ \underline{\mathbf{while}}\ \mathbf{depth{=}1}\ \underline{\mathbf{do}}$
$\qquad\qquad \mathbf{depth{:=}2};\ \underline{\mathbf{while}}\ \mathbf{d{=}2}\ \underline{\mathbf{do}}\ \mathbf{guard}_2(\mathbf{S})\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}.$
Hence the result.

<u>**Loop**</u> <u>**Expansion:**</u>
If $\mathbf{S}'$ is a term of $\mathbf{S}$ then
$\Delta \vdash \underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}\ \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ (\mathbf{S}+(\mathbf{1,1}))[\underline{\mathbf{exit}}(\mathbf{k+1})/\mathbf{S}'+(\mathbf{1,1})+\mathbf{k}]\ \underline{\mathbf{od}};\ \mathbf{S}'\ \underline{\mathbf{od}}$
Proof: $\underline{\mathbf{do}}\ \mathbf{S}\ \underline{\mathbf{od}}\ \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ \mathbf{S+1}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$ by false iteration.
$\qquad \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ (\mathbf{S}+(\mathbf{1,1}))[\mathbf{A}][\mathbf{S}' + \delta + \mathbf{1}/\mathbf{T}|\tau = \mathbf{1}][\mathbf{T+1/T}|\tau = \mathbf{0}]\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$ by Lemma 1.
$\qquad \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ (\mathbf{S}+(\mathbf{1,1}))[\mathbf{A}][\mathbf{S}' + \delta + \mathbf{1}/\mathbf{T}|\tau = \mathbf{1}];\ \underline{\mathbf{exit}}\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$ by the inverse of absorption.
$\qquad \approx\ \underline{\mathbf{do}}\ \underline{\mathbf{do}}\ (\mathbf{S}+(\mathbf{1,1}))[\mathbf{A}][\mathbf{S}' + \delta + \mathbf{1}/\mathbf{T}|\tau = \mathbf{1}]\ \underline{\mathbf{od}}\ \underline{\mathbf{od}}$ by Lemma 2.

$\approx$ **<u>do</u> <u>do</u> (S+(1,1))[A] <u>od</u>; S′ <u>od</u>** by the inverse of absorption.

The following Lemma provides a form of induction rule for unbounded loops:

<u>Lemma:</u> If $\Delta \vdash$ **<u>do</u> (S;)**^{n}**; abort <u>od</u>** $\leqslant$ **S′** for all **n**$< \omega$ then **<u>do</u> S <u>od</u>** $\leqslant$ **S′**.
Proof: Prove by induction on **n**:
{depth=k}; guard$_k$**(<u>do</u> (S;)**^{n}**; abort <u>od</u>)** $\approx$ **{depth=k}; depth:=k+1;**
<u>while</u> depth=k+1 <u>do</u> guard$_{k+1}$**(S) <u>od</u>**^{n}
Then the induction rule for loops gives the result.