9. PROOF CHARTS

The idea of presenting program proofs by diagrams was introduced by Lamport[77] and later developed by Owicki & Lamport[82] and Manna & Pnueli[82]. However because of a number of restrictions (such as impossibility of making infinite inductions) the method was not semantically complete.

This motivates our generalization which can be introduced by the self-explanatory :

Example 9-1 :

The "à la Burstall" total correctness proof of program 2-1 considered at paragraph 5.2 can be presented as follows (we write at L as a shorthand for [c=L]) :

Proposition 1 :

at Start $\wedge\ \underline{n}\geq 0 \wedge n=\underline{n}$
$\downarrow$ at Loop $\wedge\ \underline{n}\geq 0 \wedge n=\underline{n} \wedge p=1$ $\downarrow$ *lemma 0* at Loop $\wedge\ n=0 \wedge p=2^{\underline{n}}$ $\downarrow$
at Finish $\wedge\ p=2^{\underline{n}}$

Lemma 0 :

at Loop $\wedge\ \underline{n}\geq 0 \wedge n=\underline{n} \wedge p=\underline{p}$	
at Loop $\wedge\ \underline{n}>0 \wedge n=\underline{n} \wedge p=\underline{p}$ $\downarrow$ at Loop $\wedge\ \underline{n}>0 \wedge n=\underline{n}-1 \wedge p=2\mathrm{x}\underline{p}$ $\downarrow$ *lemma 0*, $0\leq n<\underline{n}$	at Loop $\wedge\ \underline{n}=0 \wedge n=\underline{n} \wedge p=\underline{p}$ $\Downarrow$
at Loop $\wedge\ n=0 \wedge p=\underline{p}\mathrm{x}2^{\underline{n}}$	

□

A proof chart for a transition system (S,t) will be formalized using a finite set of finite well-structured single-entry single-exit labelled graphs. We write $I^{\varepsilon} \leadsto I^{\sigma}$ to denote such a graph with a unique entry vertex labelled I^{ε} and a unique exit vertex labelled I^{σ}.

The set of admissible graphs will be defined by a graph grammar. Elementary graphs are of the form $I \longrightarrow J$ where I is the entry vertex, J is the exit vertex and there is a single edge from vertex I to vertex J. There are different types of edges (drawn by different arrows) some of which can be labelled (the label is then written on the corresponding arrow). Composite graphs are obtained using the following graph composition operations :

. If $I \leadsto J$ and $K \leadsto L$ are two graphs such that J=K then $I \leadsto J \leadsto L$ denotes the graph such that the entry vertex K is identified with the exit vertex J, there are no other mixtures of the vertices of the original graphs and the entry (respectively exit) vertex of the composite graph is the vertex labelled I (respectively L).

. If $I \leadsto J$ and $K \leadsto L$ are two graphs such that I=K and J=L then $I \overset{\leadsto}{\leadsto} J$ denotes the composite graph where the entry (respectively exit) vertices of the original graphs have been identified.

. If $I \leadsto J$ and $K \leadsto L$ are two graphs such that I=K then the loop

$$\begin{tikzcd} I \arrow[r, squiggly] \arrow[dr, squiggly] & J \\ & L \arrow[ul, bend left] \end{tikzcd}$$

is the composite graph with entry vertex I identified with K, with exit vertex J and with a new arc from vertex L to entry vertex I.

We write $I(s_0,\underline{s},\vec{s},s)$ (respectively $I(s_0,\underline{s},\vec{s}.\tilde{s},s)$ and $I(s_0,\underline{s},s)$) to mean that the label I attached to a graph vertex belongs to $(S \times S \times S^m \times S \rightarrow \{tt,ff\})$ where $m=n$ (respectively $m=n+1$, $m=0$) is the number of enclosing loops. Informally s_0 is the value of the state on program entry, $\underline{s}$ (respectively $\vec{s}_i$) is the value of the state corresponding to the entry of the graph (respectively to the entry of the i-th enclosing loop in the graph) and s is the value of the current state.

DEFINITION 9-2 *(Proof charts)*

A *proof chart* for (S,t) is a pair $((\Lambda,\vdash),\{(G_\ell,(f_\ell,W_\ell,\prec_\ell)) : \ell\in\Lambda\})$ such that $(\Lambda,\vdash)$ is a finite well-founded set (of graph names) and for all $\ell\in\Lambda$, $f_\ell\in(S^2\to W_\ell)$, $Wf(W_\ell,\prec_\ell)$ and G_ℓ is a well-formed chart $I_\ell^{\varepsilon\ell}(s_0,\underline{s},s) \rightsquigarrow I_\ell^{\sigma\ell}(s_0,\underline{s},s)$ generated by the following graph grammar :

$J(s_0,\underline{s},\vec{s},s) \rightsquigarrow K(s_0,\underline{s},\vec{s},s)$ ::=

$J(s_0,\underline{s},\vec{s},s) \longrightarrow K(s_0,\underline{s},\vec{s},s)$

when $\forall s_0,\underline{s},s\in S,\vec{s}\in S^n.[J(s_0,\underline{s},\vec{s},s) \Rightarrow (\exists s'\in S.t(s,s') \wedge \forall s'\in S.\ (t(s,s') \Rightarrow K(s_0,\underline{s},\vec{s},s')))]$

| $J(s_0,\underline{s},\vec{s},s) \overset{\ell'}{\rightsquigarrow} K(s_0,\underline{s},\vec{s},s)$

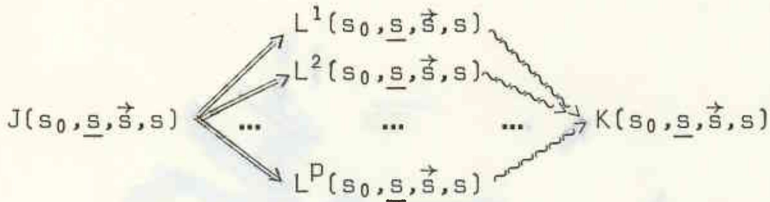
when $\ell'\vdash\ell \wedge \forall s_0,\underline{s},s\in S,\vec{s}\in S^n.[J(s_0,\underline{s},\vec{s},s) \Rightarrow (I_{\ell'}^{\varepsilon\ell'}(s_0,s,s) \wedge \forall s'\in S.\ (I_{\ell'}^{\sigma\ell'}(s_0,s,s') \Rightarrow K(s_0,\underline{s},\vec{s},s')))]$

| $J(s_0,\underline{s},\vec{s},s) \overset{\ell,(f_\ell,W_\ell,\prec_\ell)}{\rightsquigarrow} K(s_0,\underline{s},\vec{s},s)$

when $\forall s_0,\underline{s},s\in S,\vec{s}\in S^n.[J(s_0,\underline{s},\vec{s},s) \Rightarrow (f_\ell(s_0,s) \prec_\ell f_\ell(s_0,\underline{s}) \wedge I_\ell^{\varepsilon\ell}(s_0,s,s) \wedge \forall s'\in S.(I_\ell^{\sigma\ell}(s_0,s,s') \Rightarrow K(s_0,\underline{s},\vec{s},s')))]$

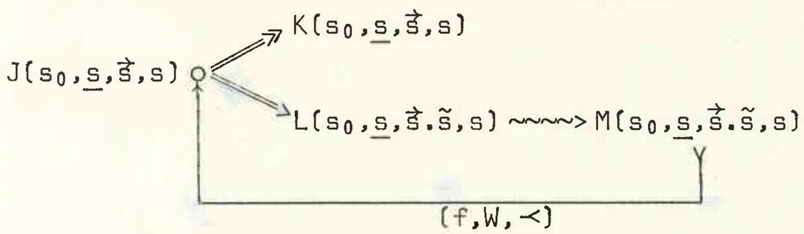
| $J(s_0,\underline{s},\vec{s},s) \Longrightarrow K(s_0,\underline{s},\vec{s},s)$

when $\forall s_0,\underline{s},s\in S,\vec{s}\in S^n.[J(s_0,\underline{s},\vec{s},s) \Rightarrow K(s_0,\underline{s},\vec{s},s)]$

| 

when $\forall s_0,\underline{s},s\in S,\vec{s}\in S^n.[J(s_0,\underline{s},\vec{s},s) \Rightarrow \bigvee_{i=1}^{p} L^i(s_0,\underline{s},\vec{s},s)]$

| $J(s_0,\underline{s},\vec{s},s) \rightsquigarrow L(s_0,\underline{s},\vec{s},s) \rightsquigarrow K(s_0,\underline{s},\vec{s},s)$

| 

when $f\in(S^3\to W) \wedge Wf(W,\prec) \wedge \forall s_0,\underline{s},s,\tilde{s}\in S,\vec{s}\in S^n.($

$[J(s_0,\underline{s},\vec{s},s) \Rightarrow (K(s_0,\underline{s},\vec{s},s) \vee L(s_0,\underline{s},\vec{s}.s,s))]$

$\wedge$ $[M(s_0,\underline{s},\vec{s}.\tilde{s},s) \Rightarrow ([f(s_0,\underline{s},s) \prec f(s_0,\underline{s},\tilde{s}) \wedge L(s_0,\underline{s},\vec{s}.s,s)]$

$\vee K(s_0,\underline{s},\vec{s},s))])$

(Observe that proof-charts are reducible graphs whence could also be formalized using a well-structured logical language).

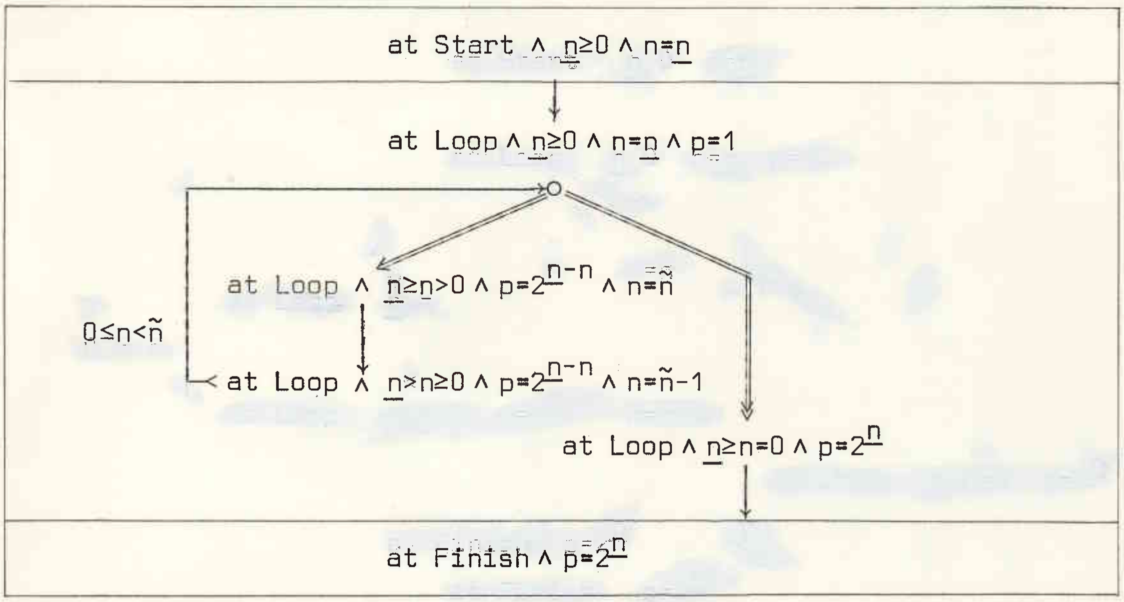
We can prove the inevitability of ψ for (S,t,ϕ) by showing that :

(14) There exists a proof chart $(I_{\ell}^{\varepsilon\ell}(s_0,\underline{s},s) \rightsquigarrow I_{\ell}^{\sigma\ell}(s_0,\underline{s},s),\ (f_{\ell},W_{\ell},\prec_{\ell}))$, $\ell\in(\Lambda,\vdash)$ and $\pi\in\ell$ such that :
$\forall s_0,\underline{s},s\in S.(I_{\pi}^{\varepsilon}\pi(s_0,s,s) = [s_0=s \wedge \phi(s)] \wedge I_{\pi}^{\sigma}\pi(s_0,\underline{s},s) = [s_0=\underline{s} \wedge \psi(\underline{s},s)])$

"A la Floyd" inevitability proofs can also be presented using proof charts as shown by the following :

Example 9-3 :

An "à la Floyd" total correctness proof of program 2-1 can also be presented as follows :



□

THEOREM 9-4 *(Soundness of proof charts)*

(14) $\Rightarrow$ ((2), with $n\in(\Lambda\rightarrow Ord)$)

Proof :

Let $((\Lambda,\vdash),\{(G_\ell,(f_\ell,W_\ell,\prec_\ell)),\ell\in\Lambda\})$ be a proof chart. Since $Wf(W_\ell,\prec_\ell)$ we can assume without loss of generality that $W_\ell\in Ord$ and $\prec_\ell=<$ (otherwise we can use rank-functions). Since Λ is finite we can also assume that $\Lambda\in\omega$ and $\vdash\,=<$. Since each graph G_ℓ is finite we can suppose that its vertices are named by elements of some finite set N_ℓ, the vertex named j being labelled by $J_\ell^j\in(S\times S\times S^{e(j)}\times S\rightarrow\{tt,ff\})$ where e(j) is the number of loops enclosing vertex j. We let ε_ℓ and σ_ℓ be the respective names of the unique entry and exit vertices of G_ℓ.

For each $\ell\in\Lambda$ we consider the set T_ℓ of tuples $<j,s_0,\underline{s},\vec{s},s>$ such that $j\in N_\ell$, $s_0,\underline{s},s\in S$, $\vec{s}\in S^{e(j)}$ and $J_\ell^j(s_0,\underline{s},\vec{s},s)$ holds. The binary relation $\ll_\ell$ on T_ℓ is defined by $<j',s'_0,\underline{s}',\vec{s}',s'>\ll_\ell<j,s_0,\underline{s},\vec{s},s>$ if and only if

either $J_\ell^j\longrightarrow J_\ell^{j'}\ \wedge\ s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}'=\vec{s}\wedge t(s,s')$

or $J_\ell^j\rightsquigarrow\xrightarrow{\ \ell'\ }J_\ell^{j'}\ \wedge\ s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}'=\vec{s}\wedge J_{\ell'}^{\sigma\ell'}(s_0,s,s')$

or $J_\ell^j\rightsquigarrow\xrightarrow{\ \ell,(f_\ell,W_\ell,\prec_\ell)\ }J_\ell^{j'}\ \wedge\ s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}'=\vec{s}\wedge J_\ell^{\sigma\ell}(s_0,s,s')$

or $((J_\ell^j\Longrightarrow J_\ell^{j'})\vee(J_\ell^j\circ\!\!\Longrightarrow J_\ell^{j'})\vee(J_\ell^j\rightarrowtail\!\!\circ\!\!\Longrightarrow J_\ell^{j'}))\wedge s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}'=\vec{s}\wedge s'=s$

or $J_\ell^j\circ\!\!\Longrightarrow J_\ell^{j'}\ \wedge\ s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}'=\vec{s}.s\wedge s'=s$

or else $J_\ell^j\rightarrowtail\!\!\circ\!\!\Longrightarrow J_\ell^{j'}\ \wedge\ s'_0=s_0\wedge\underline{s}'=\underline{s}\wedge\vec{s}=\vec{s}'.s\wedge s'=s$

Assume that $<<j_k,s_{0k},\underline{s}_k,\vec{s}_k,s_k>:\ k\geq 0>$ is an infinite decreasing sequence for $\ll_\ell$. It follows that $<j_k:k\geq 0>$ is an infinite path in the finite graph G_ℓ, hence a cycle. Therefore there is some vertex j of G_ℓ (of type $J_\ell^j\rightarrowtail\!\!\circ$) such that the sequence $<<j,s_{0i_k},\underline{s}_{i_k},\vec{s}_{i_k},\vec{s}'_{i_k}.\tilde{s}_{i_k},s_{i_k}>:\ k\geq 0>$ of elements of $<<j_k,s_{0k},\underline{s}_k,\vec{s}_k,s_k>:k\geq 0>$ such that $j_k=j$ is infinite. This is in contradiction with $\forall k\geq 0.f(s_{0i_k},\underline{s}_{i_k},s_{i_k})\prec f(s_{0i_k},\underline{s}_{i_k},\tilde{s}_{i_k})$, $f\in(S^3\rightarrow W)$ and $Wf(W,\prec)$. By reductio ad absurdum, we have $Wf(T_\ell,\ll_\ell)$.

We choose $\Lambda_2=\Lambda$, $\varepsilon 2_\ell(s_0,s)=J_\ell^{\varepsilon\ell}(s_0,s,s)$, $\theta 2_\ell(s_0,\underline{s},s)=J_\ell^{\sigma\ell}(s_0,\underline{s},s)$, $\Delta_2=Sup^+\{rk(W_\ell,\prec_\ell):\ell\in\Lambda\}$, $f2_\ell(s_0,s)=rk(W_\ell,\prec_\ell)(f_\ell(s_0,s))$, $n_\ell=rk(T_\ell,\ll_\ell)\dotplus 1$, $\pi_2=\pi$, $I2_\ell^i(s_0,\underline{s},s)=[\exists j\in N_\ell,\vec{s}\in S^{e(j)}.(J_\ell^j(s_0,\underline{s},\vec{s},s)\wedge i=rk(T_\ell,\ll_\ell)(<j,s_0,\underline{s},\vec{s},s>))]$ when $i<n_\ell$ and $I2_\ell^{n_\ell}(s_0,\underline{s},s)=J_\ell^{\varepsilon\ell}(s_0,\underline{s},s)$.

□

THEOREM 9-5 *(Semantic completeness of proof charts)*

(2) ⟹ (14)

Proof :

A proof by (2) can be presented by the proof chart $(G_\ell,(f_\ell,Ord,<))$, $\ell\in\Lambda$ where each G_ℓ, $\ell\in\Lambda$ is the following chart :

$$\varepsilon_\ell(s_0,\underline{s}) \wedge s=\underline{s}$$

$$I_\ell^{n_\ell}(s_0,\underline{s},s)$$

$$(\exists i\in n_\ell . I_\ell^i(s_0,\underline{s},s) \wedge \forall k\in n_\ell . [I_\ell^k(s_0,\underline{s},s) \Rightarrow k\leq i]$$
$$\wedge \neg\theta_\ell(s_0,\underline{s},s) \wedge s=\tilde{s})$$

$$(\exists i\in n_\ell . I_\ell^i(s_0,\underline{s},s) \wedge \forall k\in n_\ell . [I_\ell^k(s_0,\underline{s},s) \Rightarrow k\leq i]$$
$$\wedge\ s=\tilde{s} \wedge \exists s'\in S . t(s,s') \wedge \forall s'\in S . [t(s,s') \Rightarrow$$
$$\exists j<i . I_\ell^j(s_0,\underline{s},s')]])$$

$$(\exists i\in n_\ell . I_\ell^i(s_0,\underline{s},s) \wedge \forall k\in n_\ell . [I_\ell^k(s_0,\underline{s},s) \Rightarrow k\leq i]$$
$$\wedge\ s=\tilde{s} \wedge \exists \ell'<\ell . [\varepsilon_{\ell'}(s_0,s) \wedge \forall s'\in S . (\theta_{\ell'}(s_0,s,s') \Rightarrow$$
$$\exists j<i . I_\ell^j(s_0,\underline{s},s'))])$$

$$(\exists i\in n_\ell . I_\ell^i(s_0,\underline{s},s) \wedge \forall k\in n_\ell . [I_\ell^k(s_0,s,s) \Rightarrow k\leq i]$$
$$\wedge\ s=\tilde{s} \wedge f_\ell(s_0,s)<f_\ell(s_0,\underline{s}) \wedge \varepsilon_\ell(s_0,s) \wedge$$
$$\forall s'\in S . [\theta_\ell(s_0,s,s') \Rightarrow \exists j<i . I_\ell^j(s_0,\underline{s},s')])$$

ℓ'

$\ell,\ f_\ell(s_0,s)<f_\ell(s_0,\underline{s})$

$$(\exists i,j\in n_\ell .\ j<i \wedge I_\ell^j(s_0,\underline{s},s) \wedge I_\ell^i(s_0,\underline{s},\tilde{s}) \wedge \forall k\in n_\ell . [I_\ell^k(s_0,\underline{s},\tilde{s}) \Rightarrow k\leq i])$$

$$\min\{j\in n_\ell : I_\ell^j(s_0,\underline{s},s)\} < \min\{i\in n_\ell : I_\ell^i(s_0,\underline{s},\tilde{s})\}$$

$$\theta_\ell(s_0,\underline{s},s)$$

□

10. PROVING INEVITABILITY PROPERTIES OF PARALLEL PROGRAMS

Since parallel programs can be represented by non-deterministic transitions systems, proof charts can also be applied to inevitability proofs of parallel programs.

Example 9-6 : (Total correctness of a parallel program)

We consider an asynchronous parallel version of program 2-1 to compute 2^n when $n \geq 0$:

```
1:
      N1:=0; N2:=N;
2:
      [
        11:
             P1:=1
        12:
             if N1+1 < N2 then
        13:
                  T1:=N1+1; P1:=2xP1;
        14:
                  N1:=T1;
        15:
                  goto 12;
             fi;
        16:
      ||
        21:
             P2:=1;
        22:
             if N1+1 < N2 then
        23:
                  T2:=N2-1; P2:=2xP2;
        24:
                  N2:=T2;
        25:
                  goto 22;
             fi;
        26:
      ];
3:
      P :=  if N1+1=N2 then 2xP1xP2 else P1xP2 fi;
4:
```

We write at j (respectively at ij) to stand for $c=j$ ($c_i=j$) where c (c_i) is the program location counter (of process i when control is in the parallel command). We write in E for $\vee\{at\ \ell : \ell \in E\}$, $(P \Rightarrow Q \mid R)$ is the abbreviation of $((P \wedge Q) \vee (\neg P \wedge R))$ whereas if P holds then $(P \rightarrow a \mid b)$ denotes value a else value b. In particular $\min(a,b) = (a \leq b \rightarrow a \mid b)$.

$$\begin{tikzcd}[column sep=small] & P \arrow[d] & \\ & Q \vee R \arrow[dl] \arrow[dr] & \\ Q & & R \end{tikzcd}$$

will be shortened to

$$\begin{tikzcd}[column sep=small] & P \arrow[dl] \arrow[dr] & \\ Q & & R \end{tikzcd}$$

In the total correctness proof chart $P:(at1 \wedge n_0 \geq 0 \leadsto at4 \wedge p=2^{n_0})$ we distinguish two cases :

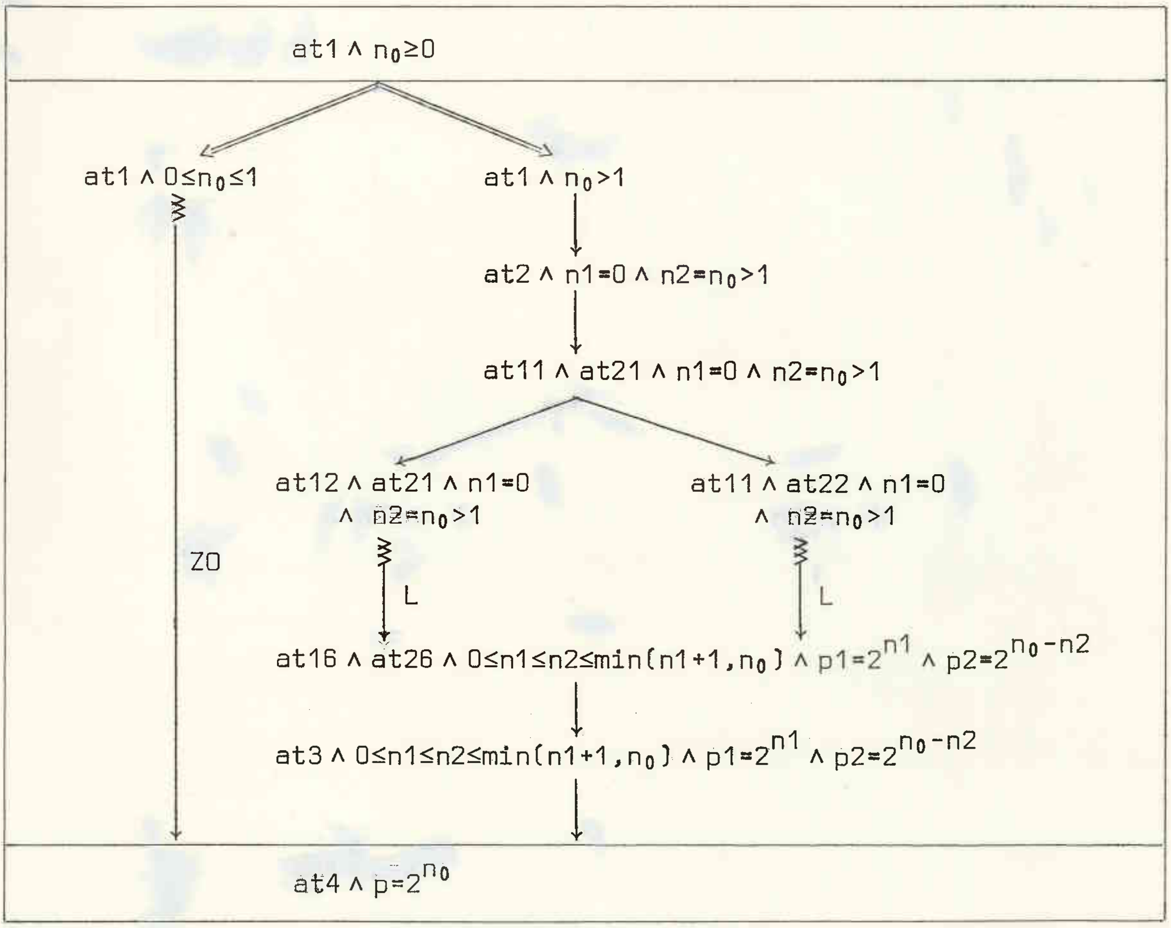
. The case $n_0 \leq 1$ is handled by lemma $ZO:(at1 \wedge 0 \leq n_0 \leq 1 \leadsto at4 \wedge p=2^{n_0})$. This lemma can be proved by hand-simulation and the corresponding chart is left to the reader.

. The main case $n_0>1$ is handled by lemma $L:(Atloop \wedge n1=\underline{n1} \wedge n2=\underline{n2} \wedge \underline{n1}+1<\underline{n2} \wedge Inv \leadsto at16 \wedge at26 \wedge \underline{n1} \leq n1 \leq n2 \leq min(n1+1,\underline{n2}) \wedge p1=2^{n1} \wedge p2=2^{n_0-n2})$ where Atloop stands for $([at12 \wedge in\{21,\ldots,25\}] \vee [in\{11,\ldots,15\} \wedge at22])$ and Inv is the following invariant :

$$Inv \equiv [(at11 \Rightarrow n1=0 \mid p1=2^{n1} \times (at14 \rightarrow 2 \mid 1)]) \wedge (at14 \Rightarrow t1=n1+1)$$
$$\wedge (at21 \Rightarrow n2=n_0 \mid p2=2^{n_0-n2} \times (at24 \rightarrow 2 \mid 1)]) \wedge (at24 \Rightarrow t2=n2-1)]$$

The proof chart P is the following :

P



The proof of lemma L is by induction on n2-n1 which is strictly decreased after one iteration in the loop of one of the two processes. This iteration is described by lemma I: $(\mathrm{Atloop} \wedge n1=\underline{n1} \wedge n2=\underline{n2} \wedge \underline{n1}+1<\underline{n2} \wedge \mathrm{Inv} \rightsquigarrow \mathrm{Atloop} \wedge 0\le n2-n1<\underline{n2}-\underline{n1} \wedge \underline{n1}\le n1 \wedge n2\le \underline{n2} \wedge \underline{n1}+1<\underline{n2} \wedge \mathrm{Inv} \wedge (n1=n2 \Rightarrow at15 \vee at25))$. When execution is about to leave the loops we have $n1\le n2\le n1+1$. The case $n1=n2$ is handled by lemma E: $(in\{12,15,16\} \wedge in\{22,25,26\} \wedge n1=\underline{n1} \wedge p1=\underline{p1} \wedge n2=\underline{n2} \wedge p2=\underline{p2} \wedge n1+1\ge n2 \rightsquigarrow at16 \wedge at26 \wedge n1=\underline{n1} \wedge p1=\underline{p1} \wedge n2=\underline{n2} \wedge p2=\underline{p2})$. The proof is trivial by hand-simulation and the corresponding chart is left to the reader. The case $n2=n1+1$ is handled by lemma B: $(\mathrm{Atloop} \wedge n1=\underline{n1} \wedge n1+1=n2=\underline{n2} \wedge \mathrm{Inv} \rightsquigarrow at16 \wedge at26 \vee \underline{n1}\le n1\le n2\le \min(n1+1,\underline{n2}) \wedge p1=2^{n1} \wedge p2=2^{n_0-n2})$. the proof chart L is the following :

L

$$\mathrm{Atloop} \wedge n1=\underline{n1} \wedge n2=\underline{n2} \wedge \underline{n1}+1<\underline{n2} \wedge \mathrm{Inv}$$

$$\Big\downarrow \mathrm{I}$$

$$\mathrm{Atloop} \wedge 0\le n2-n1<\underline{n2}-\underline{n1} \wedge \underline{n1}\le n1 \wedge n2\le\underline{n2} \wedge (n1=n2 \Rightarrow at15 \vee at25) \wedge \mathrm{Inv}$$

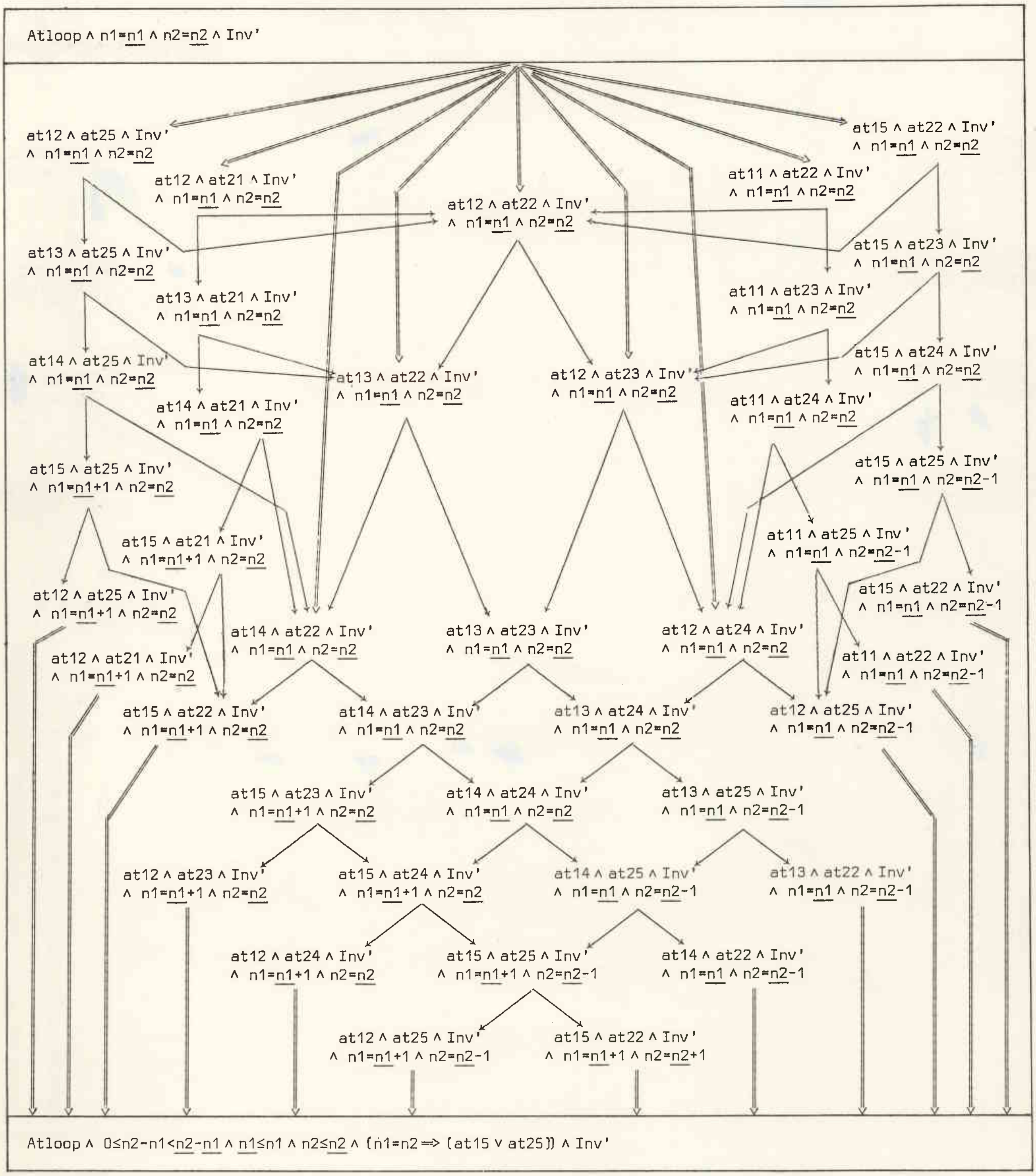
$[(at22 \wedge at25)\vee(at15 \wedge at12)] \wedge \underline{n1}\le n1=n2\le\underline{n2} \wedge \mathrm{Inv}$	$\mathrm{Atloop} \wedge \underline{n1}\le n1 \wedge n1+1=n2\le\underline{n2} \wedge \mathrm{Inv}$	$0\le n2-n1\le\underline{n2}-\underline{n1} \wedge \underline{n1}\le n1 \wedge n2\le n2 \wedge \mathrm{Atloop} \wedge n1+1<n2 \wedge \mathrm{Inv}$
$\downarrow$ E	$\downarrow$ B	$\downarrow$ L, $0\le n2-n1<\underline{n2}-\underline{n1}$

$$at16 \wedge at26 \wedge \underline{n1}\le n1\le n2\le\min(n1+1,\underline{n2}) \wedge p1=2^{n1} \wedge p2=2^{n_0-n2}$$

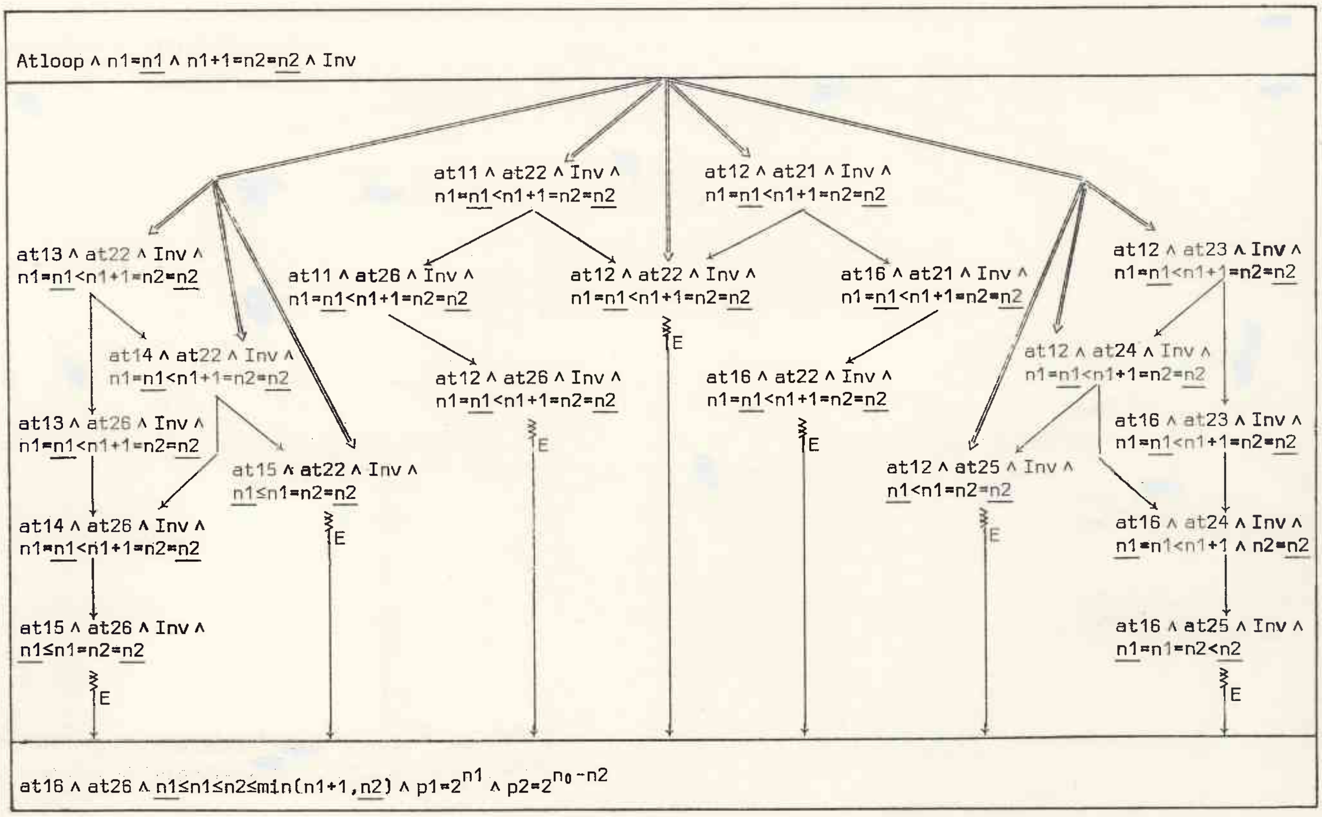
There is no difficulty about the proofs of lemmas I and B which can entirely be done by hand simulation.

We let Inv' be $\mathrm{Inv} \wedge \underline{n1}+1<\underline{n2}$ in the proof chart I :

I


Atloop ∧ n1=n1 ∧ n2=n2 ∧ Inv'
at12 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at21 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at11 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at15 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at21 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at11 ∧ at23 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at15 ∧ at23 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at14 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at23 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at15 ∧ at24 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at14 ∧ at21 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at11 ∧ at24 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at15 ∧ at25 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at15 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at15 ∧ at21 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at11 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at12 ∧ at25 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at15 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at14 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at23 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at24 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at21 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at11 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at15 ∧ at22 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at14 ∧ at23 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at24 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at12 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at15 ∧ at23 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at14 ∧ at24 ∧ Inv' ∧ n1=n1 ∧ n2=n2
at13 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at12 ∧ at23 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at15 ∧ at24 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at14 ∧ at25 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at13 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at12 ∧ at24 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2
at15 ∧ at25 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2-1
at14 ∧ at22 ∧ Inv' ∧ n1=n1 ∧ n2=n2-1
at12 ∧ at25 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2-1
at15 ∧ at22 ∧ Inv' ∧ n1=n1+1 ∧ n2=n2+1
Atloop ∧ 0≤n2-n1<n2-n1 ∧ n1≤n1 ∧ n2≤n2 ∧ (n1=n2 ⟹ (at15 ∨ at25)) ∧ Inv'

B



Atloop ∧ n1=n1 ∧ n1+1=n2=n2 ∧ Inv
at11 ∧ at22 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at12 ∧ at21 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at13 ∧ at22 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at11 ∧ at26 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at12 ∧ at22 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at16 ∧ at21 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at12 ∧ at23 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at14 ∧ at22 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at12 ∧ at26 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at16 ∧ at22 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at12 ∧ at24 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at13 ∧ at26 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at15 ∧ at22 ∧ Inv ∧ n1≤n1=n2=n2
at12 ∧ at25 ∧ Inv ∧ n1<n1=n2=n2
at16 ∧ at23 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at14 ∧ at26 ∧ Inv ∧ n1=n1<n1+1=n2=n2
at16 ∧ at24 ∧ Inv ∧ n1=n1<n1+1 ∧ n2=n2
at15 ∧ at26 ∧ Inv ∧ n1≤n1=n2=n2
at16 ∧ at25 ∧ Inv ∧ n1=n1=n2<n2
E
at16 ∧ at26 ∧ n1≤n1≤n2≤min(n1+1,n2) ∧ p1=2^n1 ∧ p2=2^(n0-n2)

□