Use of a Variant to Measure New Events Converging

variables: a, b, c

invariants:
- **inv1_1** : $a \in \mathbb{N}$
- **inv1_2** : $b \in \mathbb{N}$
- **inv1_3** : $c \in \mathbb{N}$
- **inv1_4** : $a + b + c = n$
- **inv1_5** : $a = 0 \lor c = 0$

```
ML_out
  when
    a + b < d
    c = 0
  then
    a := a + 1
  end
```

```
ML_in
  when
    c > 0
  then
    c := c − 1
  end
```

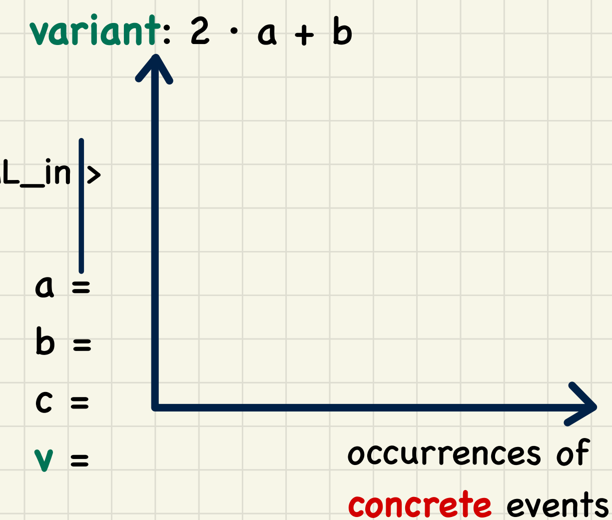
```
IL_in
  when
    a > 0
  then
    a := a − 1
    b := b + 1
  end
```

```
IL_out
  when
    b > 0
    a = 0
  then
    b := b − 1
    c := c + 1
  end
```

Variants for New Events: 2 · a + b

<init, ML_out, ML_out, IL_in, IL_out, IL_in, IL_out, ML_in, ML_in>

a =	a =	a =	a =	a =	a =	a =	a =	a =
b =	b =	b =	b =	b =	b =	b =	b =	b =
c =	c =	c =	c =	c =	c =	c =	c =	c =
v =	v =	v =	v =	v =	v =	v =	v =	v =



Use of a Variant to Measure New Events Converging

fixed

variables: a, b, c

invariants:
- **inv1_1** : $a \in \mathbb{N}$
- **inv1_2** : $b \in \mathbb{N}$
- **inv1_3** : $c \in \mathbb{N}$
- **inv1_4** : $a + b + c = n$
- **inv1_5** : $a = 0 \lor c = 0$

ML_out
when
$a + b < d$
$c = 0$
then
$a := a + 1$
end

ML_in
when
$c > 0$
then
$c := c - 1$
end

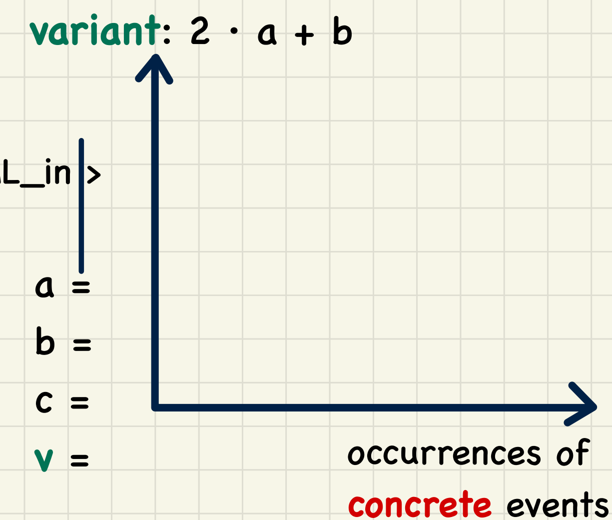
IL_in
when
$a > 0$
then
$a := a - 1$
$b := b + 1$
end

IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

Variants for New Events: 2 · a + b

<init, ML_out, ML_out, IL_in, IL_in, IL_out, IL_out, ML_in, ML_in>

a =	a =	a =	a =	a =	a =	a =	a =	a =
b =	b =	b =	b =	b =	b =	b =	b =	b =
c =	c =	c =	c =	c =	c =	c =	c =	c =
v =	v =	v =	v =	v =	v =	v =	v =	v =



PO of Convergence/Non-Divergence/Livelock Freedom

Variants for New Events: $2 \cdot a + b$

Variant Stays Non-Negative

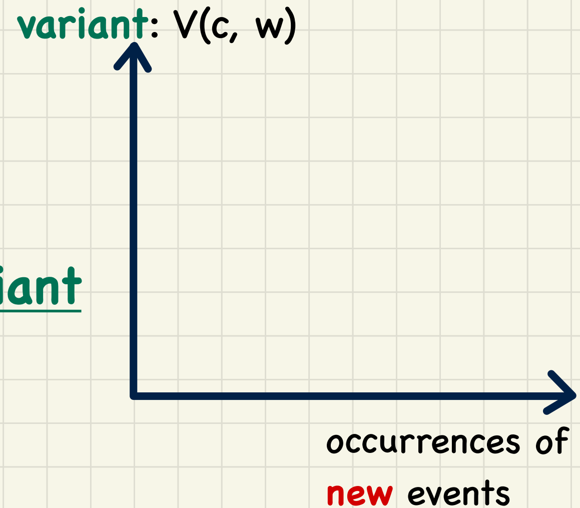
IL_in/NAT

$$\frac{A(c) \quad I(c,v) \quad J(c,v,w) \quad H(c,w) \quad \vdash \quad V(c,w) \in \mathbb{N}}{} \; \text{NAT}$$

A New Event Occurrence Decreases Variant

IL_in/VAR

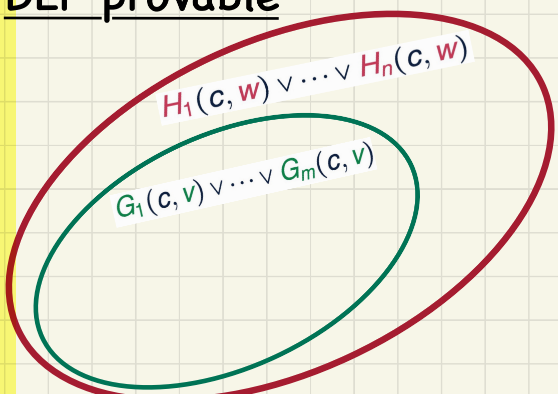
$$\frac{A(c) \quad I(c,v) \quad J(c,v,w) \quad H(c,w) \quad \vdash \quad V(c,F(c,w)) < V(c,w)}{} \; \text{VAR}$$



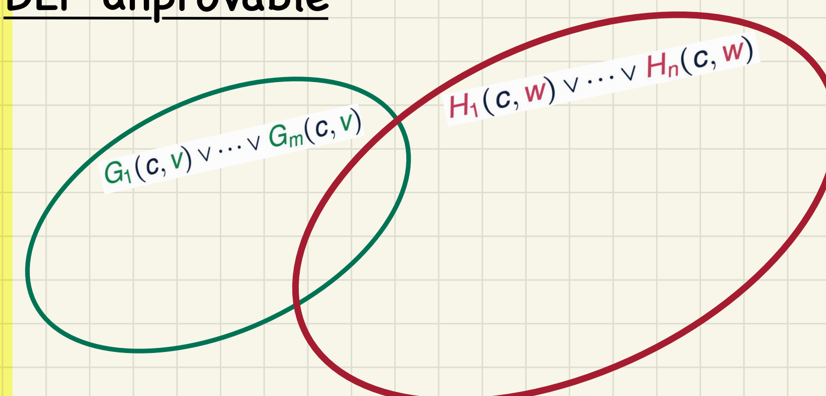
Idea of Relative Deadlock Freedom

$$\frac{\begin{array}{l} A(c) \\ I(c, v) \\ J(c, v, w) \\ G_1(c, v) \vee \cdots \vee G_m(c, v) \\ \vdash \\ H_1(c, w) \vee \cdots \vee H_n(c, w) \end{array}}{} \ \underline{\text{DLF}}$$

DLF provable



DLF unprovable



PO of Relative Deadlock Freedom

Abstract m0

variables: n

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

ML_out
when
$n < d$
then
$n := n + 1$
end

ML_in
when
$n > 0$
then
$n := n - 1$
end

Concrete m1

variables: a, b, c

invariants:
inv1_1 : $a \in \mathbb{N}$
inv1_2 : $b \in \mathbb{N}$
inv1_3 : $c \in \mathbb{N}$
inv1_4 : $a + b + c = n$
inv1_5 : $a = 0 \vee c = 0$

ML_out
when
$a + b < d$
$c = 0$
then
$a := a + 1$
end

ML_in
when
$c > 0$
then
$c := c - 1$
end

IL_in
when
$a > 0$
then
$a := a - 1$
$b := b + 1$
end

IL_out
when
$b > 0$
$a = 0$
then
$b := b - 1$
$c := c + 1$
end

$$
\begin{array}{l}
A(c) \\
I(c, v) \\
J(c, v, w) \\
G_1(c, v) \vee \cdots \vee G_m(c, v) \\
\vdash \\
H_1(c, w) \vee \cdots \vee H_n(c, w)
\end{array}
\quad \underline{\text{DLF}}
$$

Example Inference Rules

$$\frac{H, \neg P \vdash Q}{H \vdash P \vee Q}\ \textbf{OR\_R}$$

$$\frac{H, P, Q \vdash R}{H, P \wedge Q \vdash R}\ \textbf{AND\_L}$$

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q}\ \textbf{AND\_R}$$

Discharging POs of m1: Relative Deadlock Freedom

Part 1

$$\frac{H1 \vdash G}{H1, H2 \vdash G} \text{ MON}$$

$$\frac{H(F), E = F \vdash P(F)}{H(E), E = F \vdash P(E)} \text{ EQ\_LR}$$

$$\frac{H, \neg P \vdash Q}{H \vdash P \lor Q} \text{ OR\_R}$$

$d \in \mathbb{N}$
$d > 0$
$n \in \mathbb{N}$
$n \leq d$
$a \in \mathbb{N}$
$b \in \mathbb{N}$
$c \in \mathbb{N}$
$a + b + c = n$
$a = 0 \lor c = 0$
$n < d \lor n > 0$
$\vdash$
$\quad a + b < d \land c = 0$
$\lor \quad c > 0$
$\lor \quad a > 0$
$\lor \quad b > 0 \land a = 0$

Discharging POs of m1: Relative Deadlock Freedom

Part 2

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R} \quad \textbf{OR\_L}$$

$$\frac{H \vdash P}{H \vdash P \vee Q} \quad \textbf{OR\_R1}$$

$$\frac{}{P \vdash E = E} \quad \textbf{EQ}$$

$$\frac{H \vdash P \qquad H \vdash Q}{H \vdash P \wedge Q} \quad \textbf{AND\_R}$$

$$\frac{H \vdash Q}{H \vdash P \vee Q} \quad \textbf{OR\_R2}$$

$$\frac{}{H, P \vdash P} \quad \textbf{HYP}$$

$$
\begin{array}{l}
d > 0 \\
b = 0 \vee b > 0 \\
\vdash \\
\qquad b < d \wedge 0 = 0 \\
\vee \quad b > 0 \wedge 0 = 0
\end{array}
$$

Initial Model and 1st Refinement: Provably Correct

Abstract m0

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

variables: n

invariants:
inv0_1 : $n \in \mathbb{N}$
inv0_2 : $n \leq d$

```
init
  begin
    n := 0
  end
```

```
ML_out
  when
    n < d
  then
    n := n + 1
  end
```

```
ML_in
  when
    n > 0
  then
    n := n - 1
  end
```

Concrete m1

constants: d

axioms:
axm0_1 : $d \in \mathbb{N}$
axm0_2 : $d > 0$

variables: a, b, c

invariants:
inv1_1 : $a \in \mathbb{N}$
inv1_2 : $b \in \mathbb{N}$
inv1_3 : $c \in \mathbb{N}$
inv1_4 : $a + b + c = n$
inv1_5 : $a = 0 \lor c = 0$

variants:
$2 \cdot a + b$

```
init
  begin
    a := 0
    b := 0
    c := 0
  end
```

```
ML_out
  when
    a + b < d
    c = 0
  then
    a := a + 1
  end
```

```
ML_in
  when
    c > 0
  then
    c := c - 1
  end
```

```
IL_in
  when
    a > 0
  then
    a := a - 1
    b := b + 1
  end
```

```
IL_out
  when
    b > 0
    a = 0
  then
    b := b - 1
    c := c + 1
  end
```

Correctness Criteria:

- Guard Strengthening
- Invariant Establishment
- Invariant Preservation
- Convergence
- Relative Deadlock Freedom