Combining Widening and Acceleration in Linear Relation Analysis

(work in progress)

Laure Gonnord, Nicolas Halbwachs

VERIMAG

Motivation

Linear Relation Analysis (LRA)

- widening:
  - approximate results,
  - can be arbitrarily refined by delaying the wideniing
  - but delaying the widening is expensive
- acceleration:
  - Boigelot/Wolper, Common/Jurski, Finkel/Sutre/Leroux
  - compute the exact effect of loops
  - only works for a quite restricted class of programs, high complexity

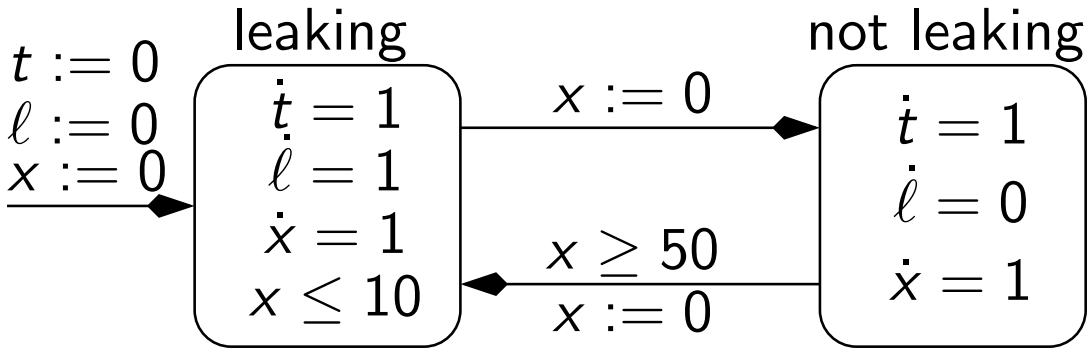
Motivation

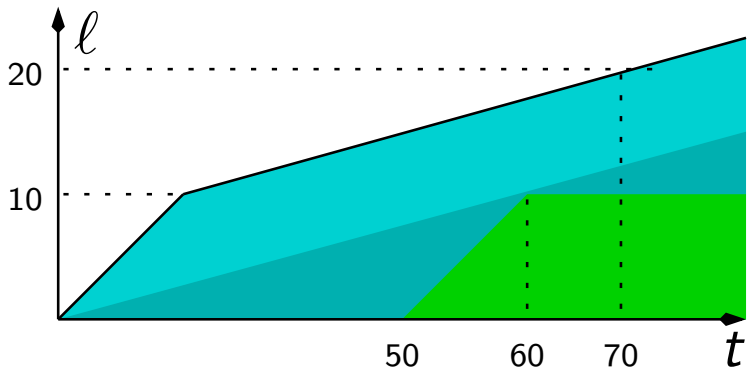
Linear Relation Analysis (LRA)

- widening:
  - approximate results,
  - can be arbitrarily refined by delaying the wideniing
  - but delaying the widening is expensive
- acceleration:
  - Boigelot/Wolper, Common/Jurski, Finkel/Sutre/Leroux
  - compute the exact effect of loops
  - only works for a quite restricted class of programs, high complexity

A motivating example: the gaz burner

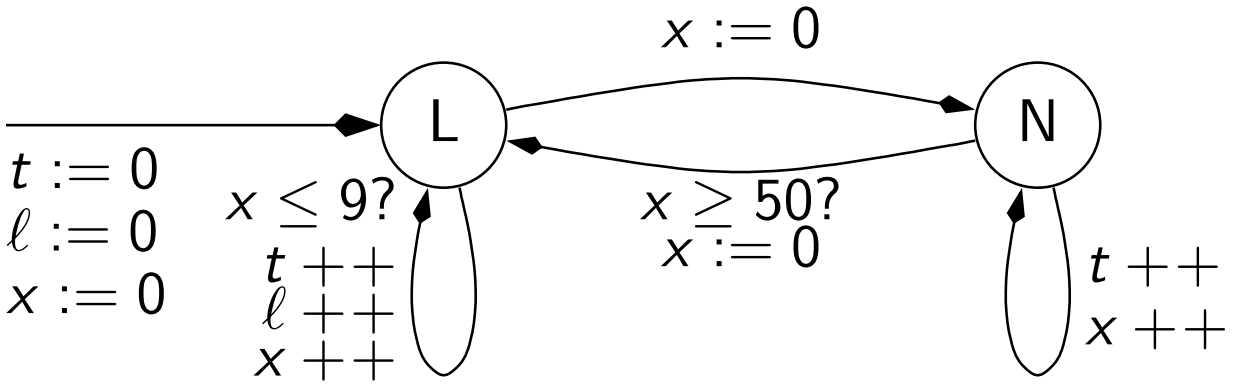
Continuous behaviour

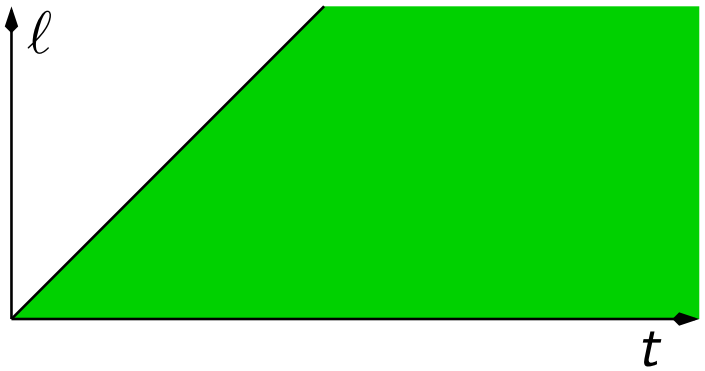




The gaz burner (cont.)

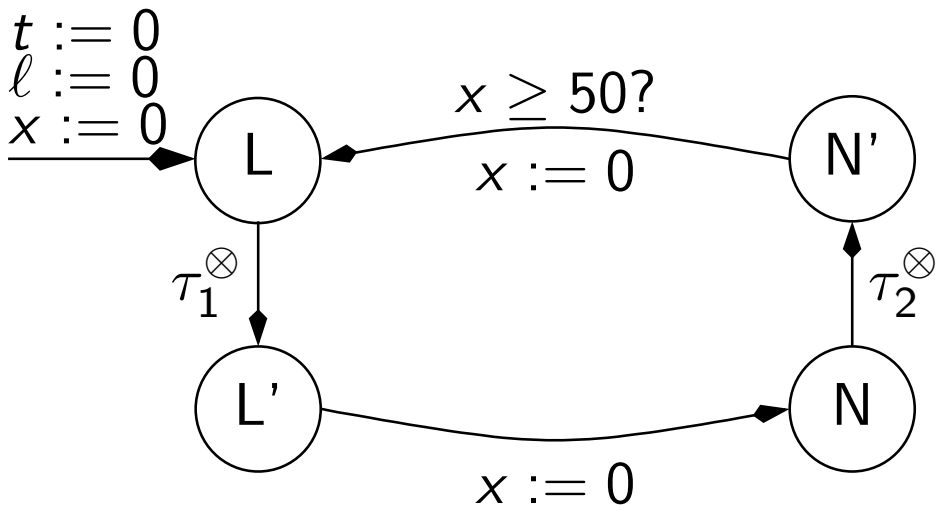
Discretizing





The gaz burner (end.)

We want to replace the loops ...



Simple loops

We want to caracterise $P = \tau^*(P_0)$, where :

$$\tau(x) = \text{ if } Ax \leq B \text{ then } Cx + D \text{ else } x$$

with (A, B) "guard" and (C, D) "action"

$$x \in P \Leftrightarrow \exists i \in \mathbb{N}, \exists x_0 \in P_0, x = \tau^i(x_0)$$

i.e., if we define the sequence (x_k) by $x_i = C^i x_0 + \sum_{j=0}^{i} C^j D$:

$$x \in \tau^*(x_0) \Leftrightarrow \exists i \in \mathbb{N}, x = x_i \text{ and } \forall j \in [0, i-1], Ax_j \leq B$$

Some simple cases

Computing C^k is too expensive

- [Leroux02] : the linear functions $\lambda x.CX + D$ with $\{C^k, k \in \mathbb{N}\}$ finite are *effectively* Presburger-definable.
- Simplest case: $C = \mathrm{Id}$ ("translation")
- Some cases hwre $C^2 = C$ (incrementation / assignment to constant).

Single translation loop

$$\tau(x) = \text{ if } Ax \leq B \text{ then } x + D \text{ else } x$$

(obvious) Proposition If $C = Id$, then $x \in \tau^*(P_0)$ iff

$$\exists i \in \mathbb{N}, \exists x_0 \in P_0, Ax_0 \leq B, A(x - D) \leq B, x = x_0 + iD$$

Abstract acceleration

$$\tau^{\otimes}(P_0) = \bigsqcup \{x \mid \exists i \in \mathbb{Q}, \exists x_0 \in P_0, Ax_0 \leq B, A(x - D) \leq B, x = x_0 + iD\}$$

Computation

$$\tau^{\otimes}(P_0) = ((P_0 \cap (Ax \leq B)) \nearrow D) \cap (A(x - D) \leq B)$$

Single translation loop

$$\tau(x) = \text{ if } Ax \leq B \text{ then } x + D \text{ else } x$$

(obvious) Proposition If $C = Id$, then $x \in \tau^*(P_0)$ iff

$$\exists i \in \mathbb{N}, \exists x_0 \in P_0, Ax_0 \leq B, A(x - D) \leq B, x = x_0 + iD$$

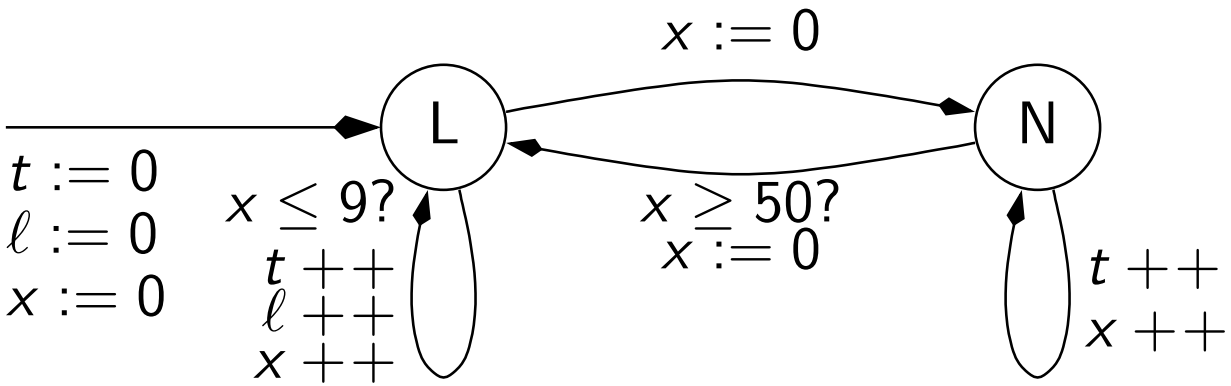
Abstract acceleration

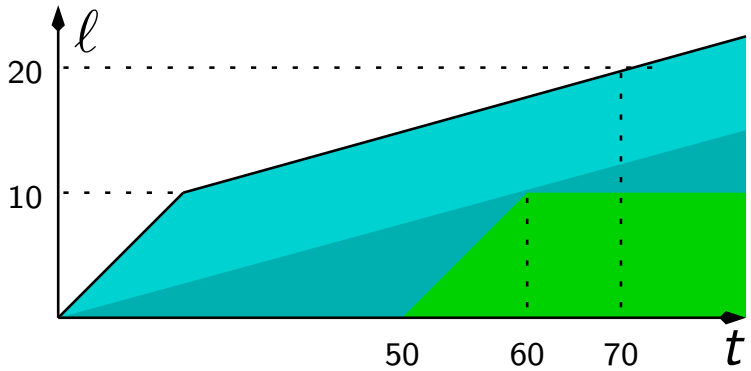
$$\tau^{\otimes}(P_0) = \bigsqcup \{x \mid \exists i \in \mathbb{Q}, \exists x_0 \in P_0, Ax_0 \leq B, A(x - D) \leq B, x = x_0 + iD\}$$

Computation

$$\tau^{\otimes}(P_0) = ((P_0 \cap (Ax \leq B)) \nearrow D) \cap (A(x - D) \leq B)$$

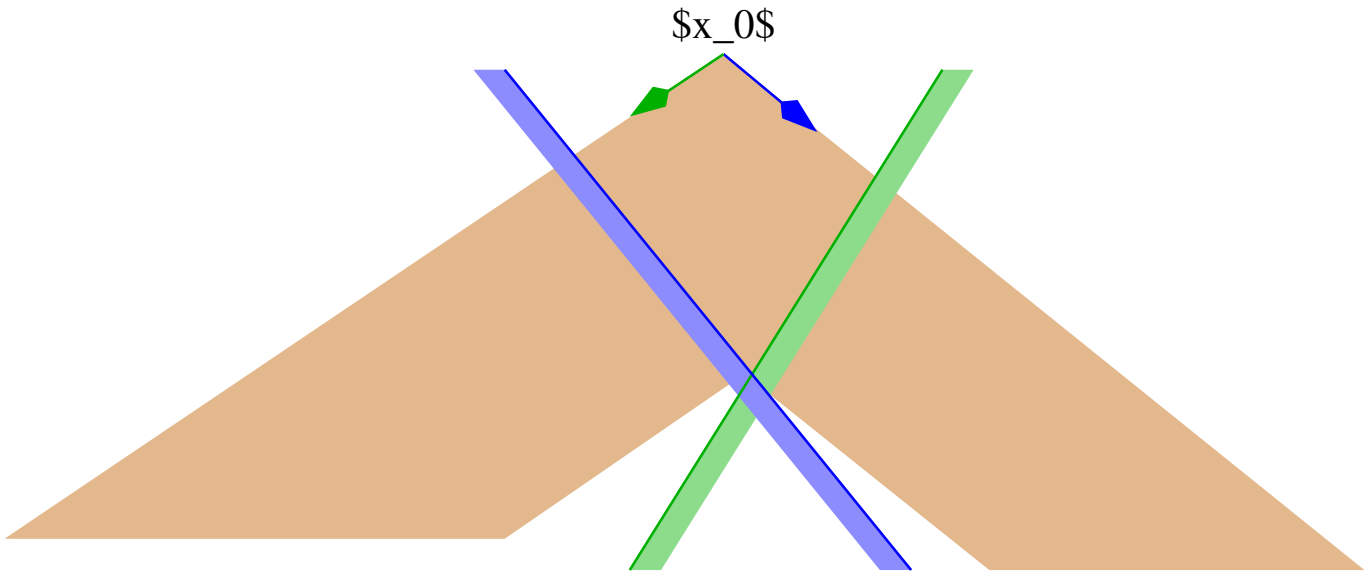
Ex.: gaz burner





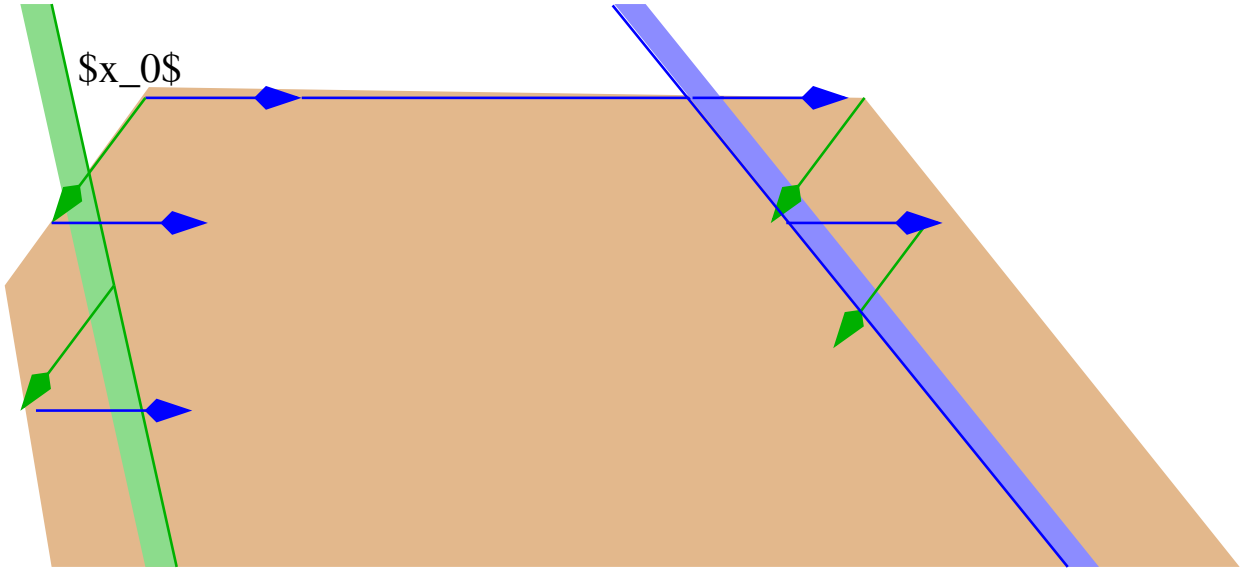
Two loops - First remarks

$(\tau_1 + \tau_2)^*(P_0)$ is not necessarily convex :

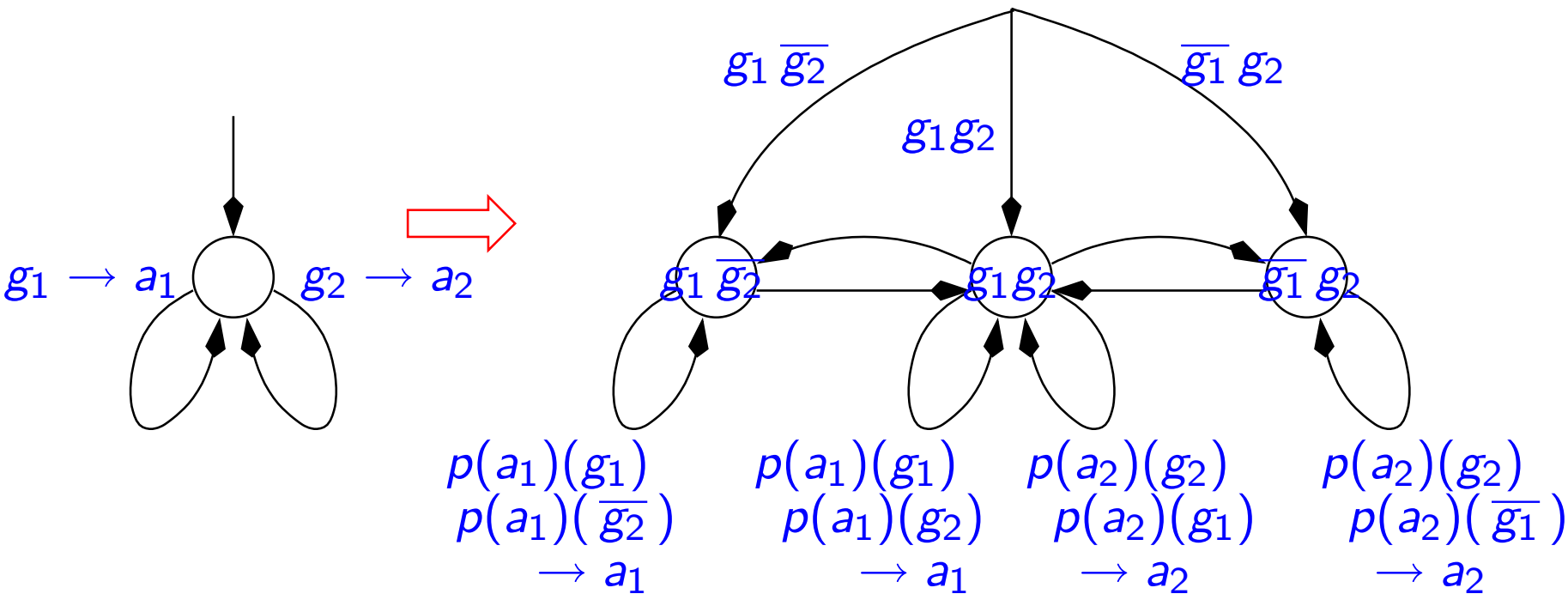


Two loops - First remarks

There can be quite complex oscillations



Several loops: partitionning



(at least conceptually)

Two simple translation loops – results

Simple translation loops: simple guards $g = ax \leq b$

$$\tau_i(x) = \text{ if } g_i \text{ then } x + D_i \text{ else } x \ , \ i = 1, 2$$

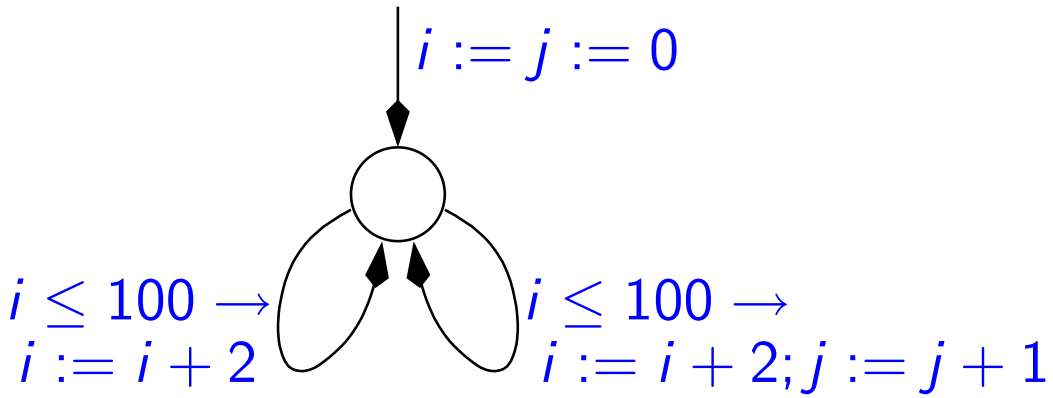
We know how to abstractly accelerate two simple loops as long as both guards are satisfied (not completely obvious)

Result: if $P_0 \subseteq g_1 \cap g_2$ then

$$(\tau_1 + \tau_2)^{\otimes}(P_0) \cap g_1 \cap g_2 = (P_0 \nearrow \{D_1, D_2\}) \cap g_1 \cap g_2$$

Old Cousot&Halbwachs78 example

```
i:=j:=0;
while i<= 100 do
1    if ? then i:=i+2
     else i:=i+2; j:=j+1
     fi
od
```

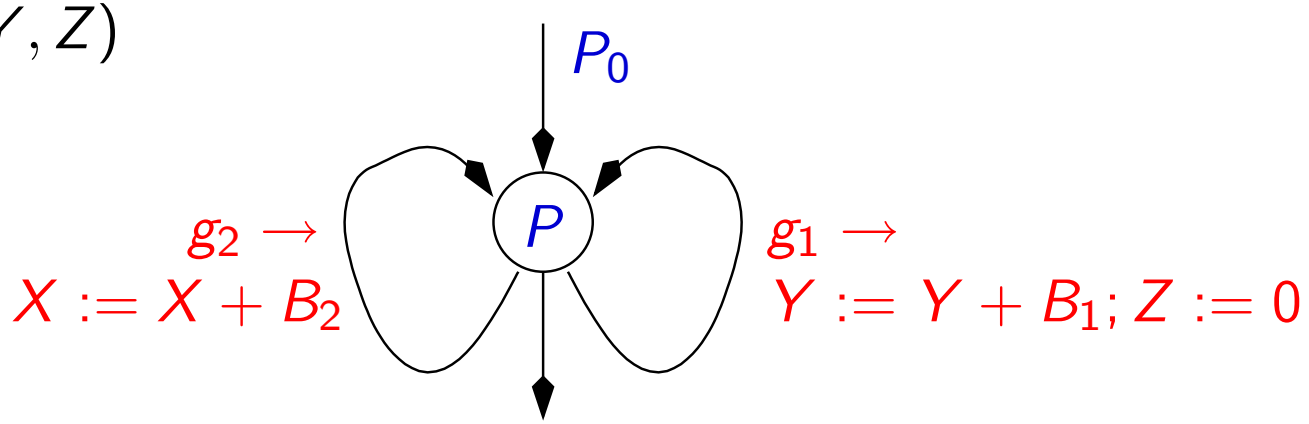


Immediate result at 1:

$$(0,0) \nearrow \{(2,0),(2,1)\} \cap (i \leq 100)$$
$$= 0 \leq 2j \leq i \leq 100$$

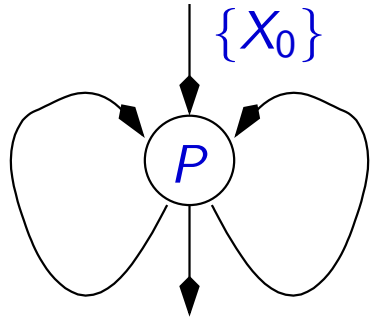
Two loops with reset (or constant assignments)

$X = (Y, Z)$



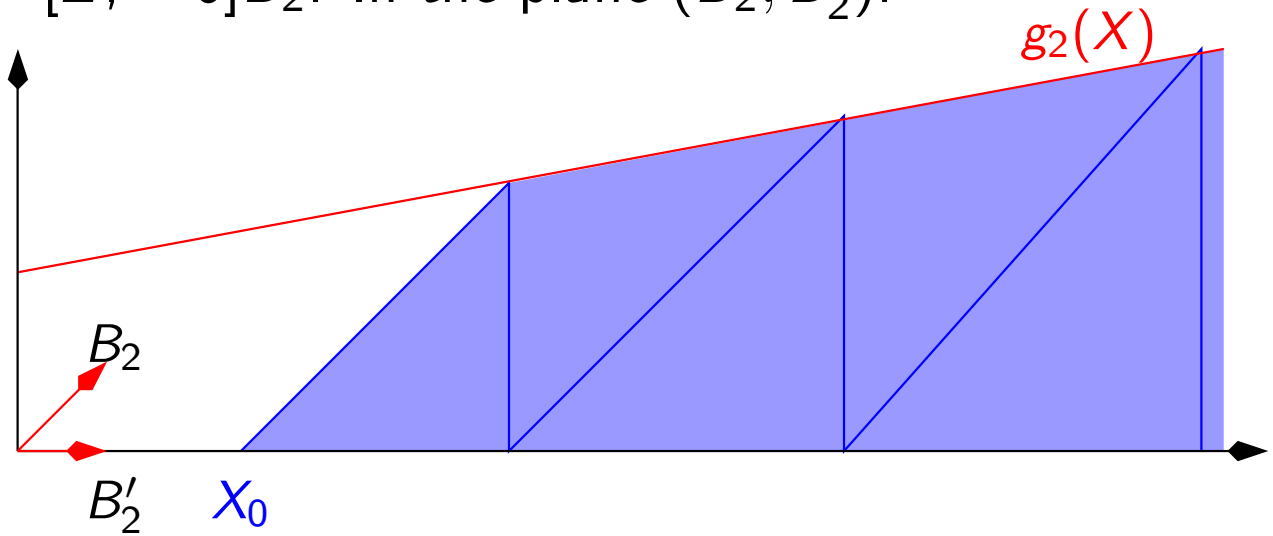
Unconditional simple reset

$X = (Y, Z)$



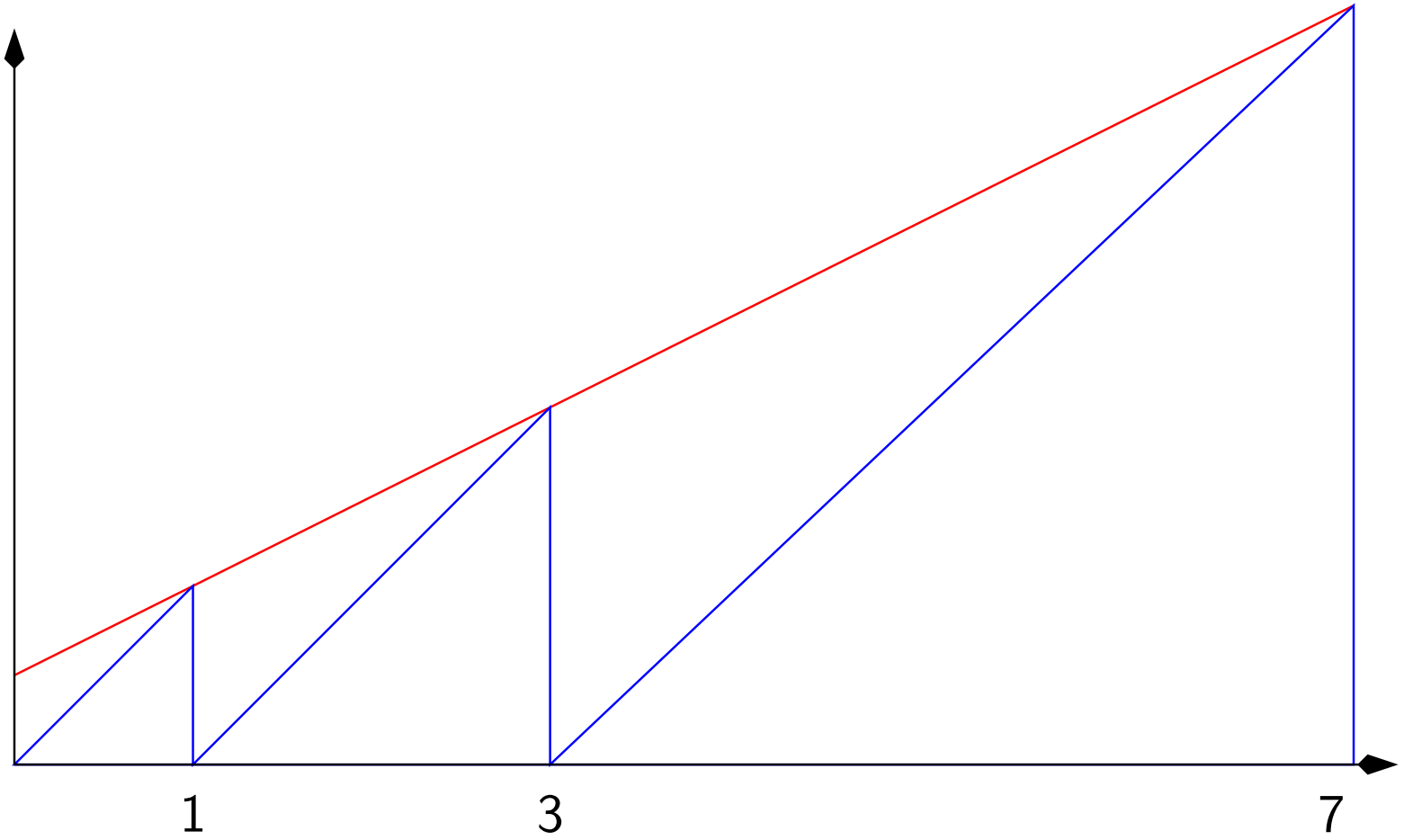
$g_2 \to X := X + B_2$ $\quad$ $true \to Z := 0$

Let $B_2' = [Z; = 0]B_2$. In the plane (B_2, B_2'):



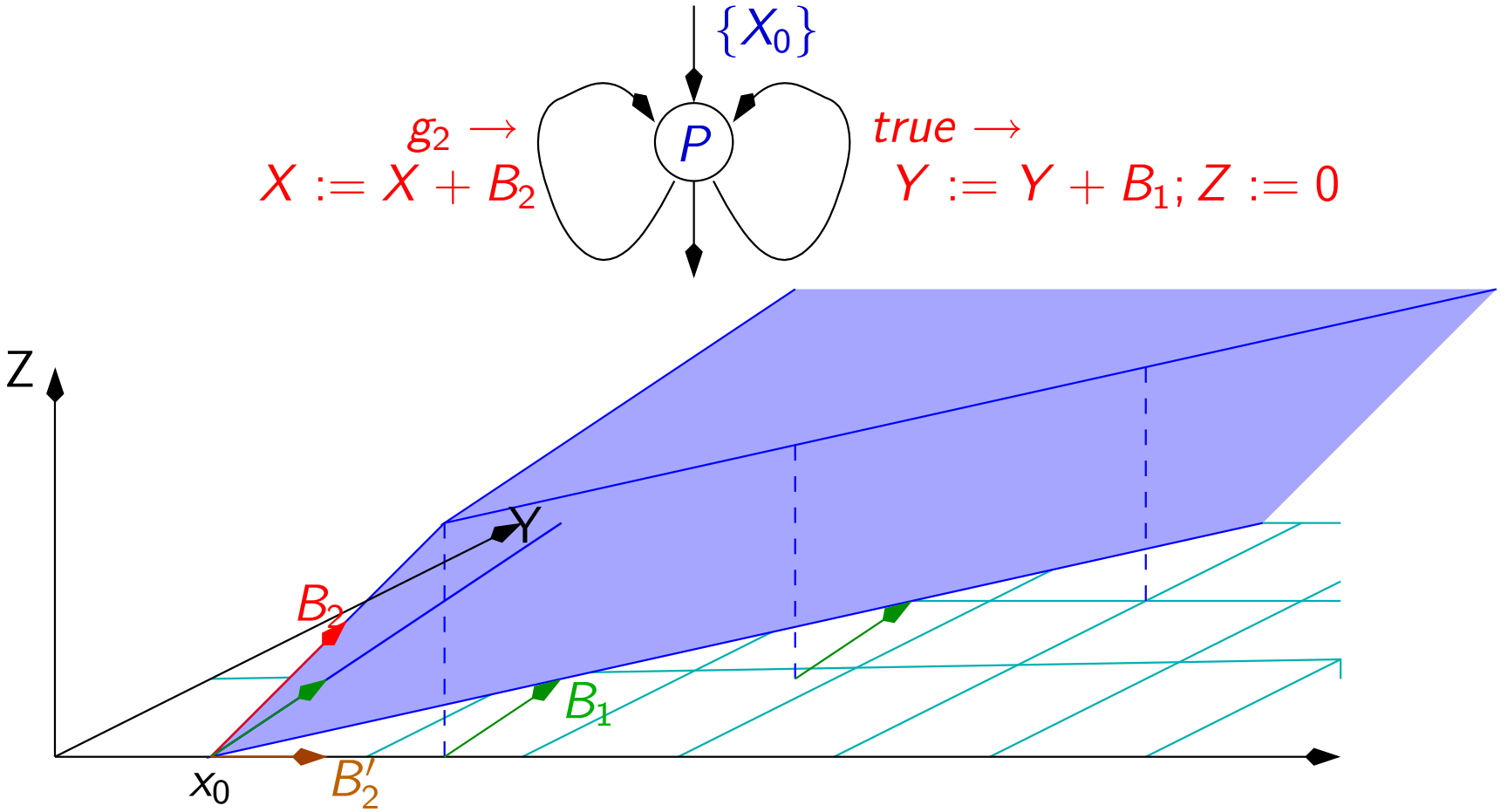
$$P = \{X_0\} \nearrow \{B_2, B_2'\} \cap g_2$$

Remark:



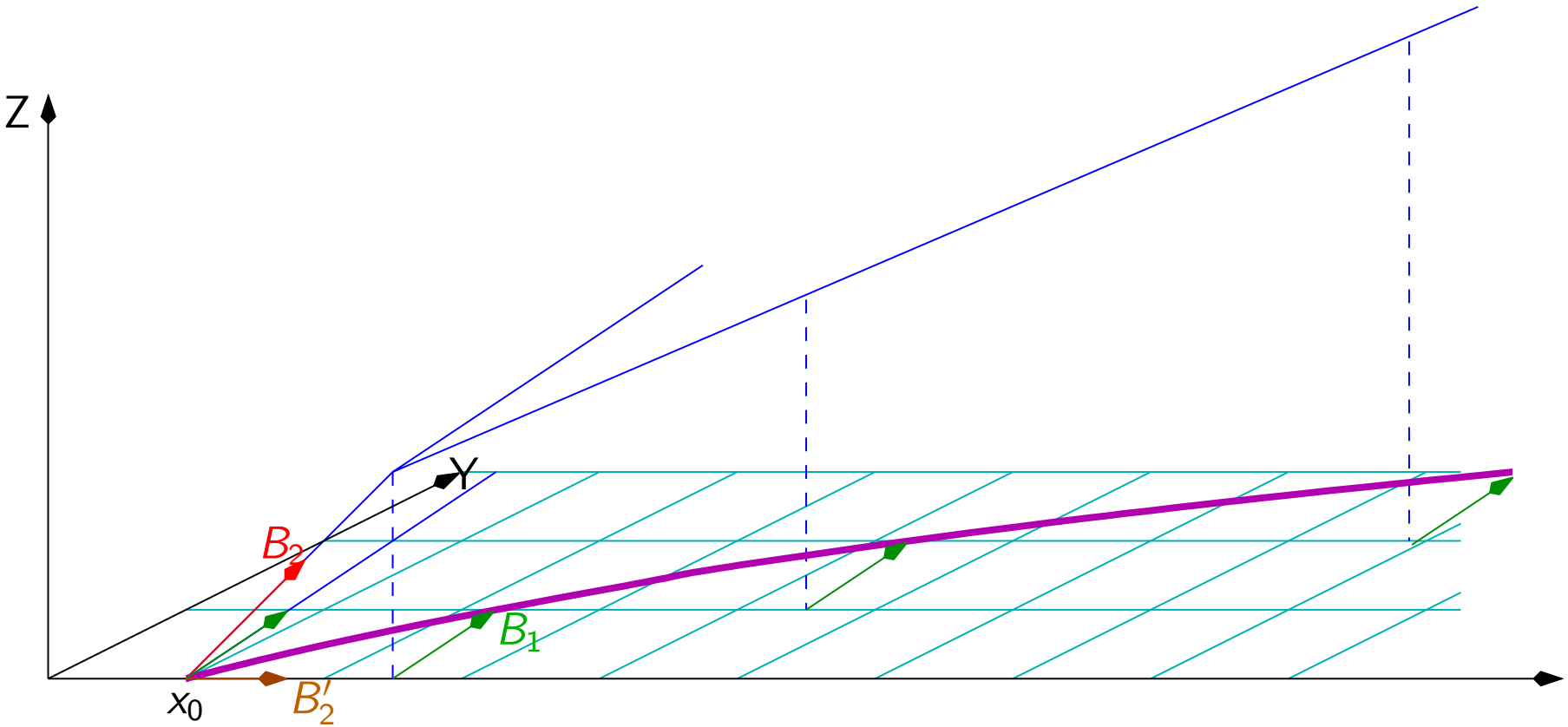
The exact set is not semi-linear

Unconditional translation/reset

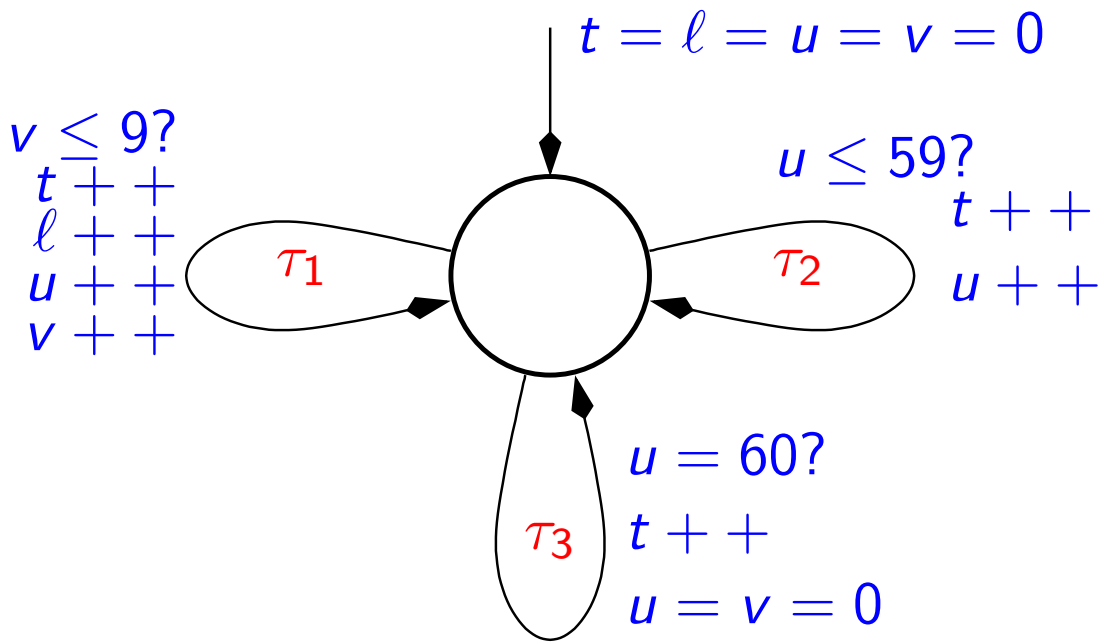


$$P = P_0 \nearrow \{B_1, B_2, k_{max} B_2' + B_1\} \cap g_2$$

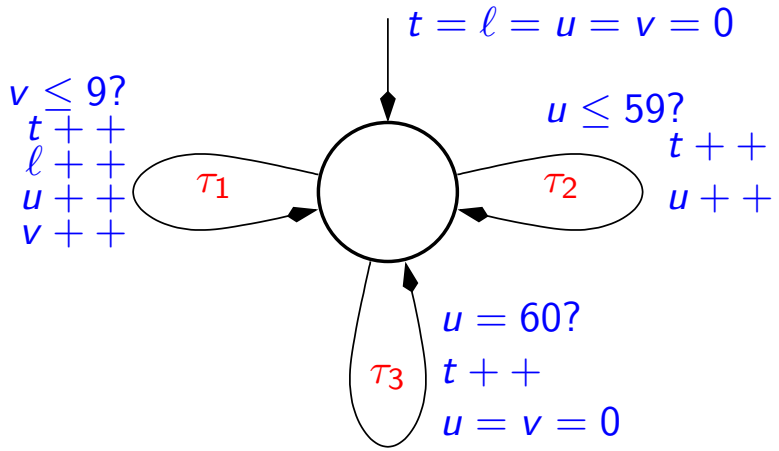
Only works if $g_2 = Z \leq C$ (modulo variable change)



An other (more difficult) version of the gaz burner



Let $X = (t, \ell, u, v)$, $Z = \{u, v\}$. $X_0 = (0, 0, 0, 0)$.



We compute

$F_1 = (\tau_1 + \tau_2)^*(X_0) = \{\ell = v, t = u, 0 \leq \ell \leq 10, \ell \leq t \leq 60\}$

(two simple translation loops).

Then, $\tau_3(F_1) = \{u = v = 0, t = 60, 0 \leq \ell \leq 10\}$, thus

$D_3 + k_1^{max} D_1^Y = (0, 60, 0, 0)$ and $D_3 + k_2^{max} D_2^Y = (0, 60, 10, 0)$

And we finally get :

$F(X_0) = \{\ell \geq v, u \leq 60, 0 \leq v \leq 10, u \geq v, u + 6\ell \leq t + 6y\}$

whose projecton onto $\{t, \ell\}$ gives $\{t + 50 \geq 6\ell, \ell \geq 0, t \geq \ell\}$.