Verificação e Falsificação de Sist. Híbridos: uma perspectiva histórica

Guilherme A. Pinto

7 dezembro 2007

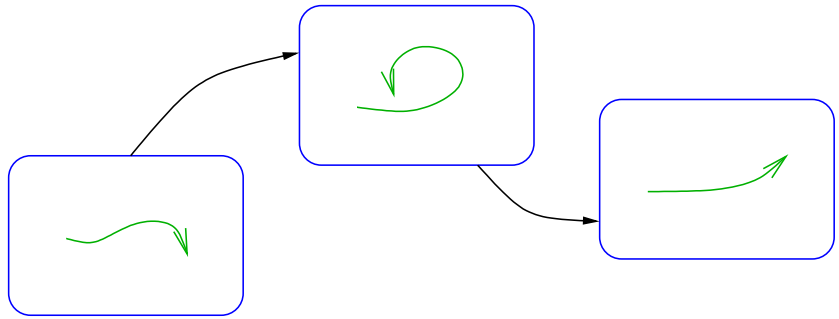
CIC – Departamento de Ciência da Computação
UnB – Universidade de Brasília

Roteiro

1. Motivação: Sistema Híbrido
   - Exemplo: joguinho do perseguidor
2. Verificação – 14 anos atrás
   - Alcançabilidade em Autômatos Híbridos (AH)
   - HyTech – Eliminação de Quantificadores
   - HyTech – Enumeração de Vértices
3. Falsificação – Hoje
   - *Bounded Model Checking* para AH
   - HySAT – DPLL + Prog. Linear

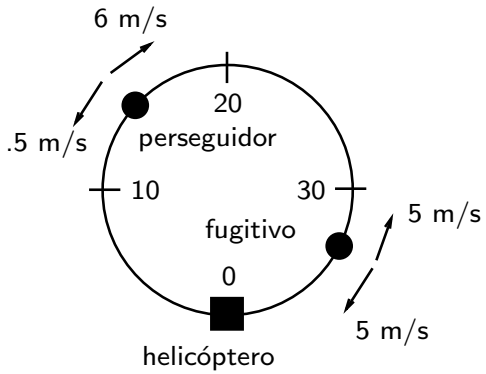
Sistema Híbrido

- Sistema dinâmico (software, protocolos, avião, carro, ...) onde há:
  - Variáveis discretas e contínuas;
  - Evolução discreta e contínua;

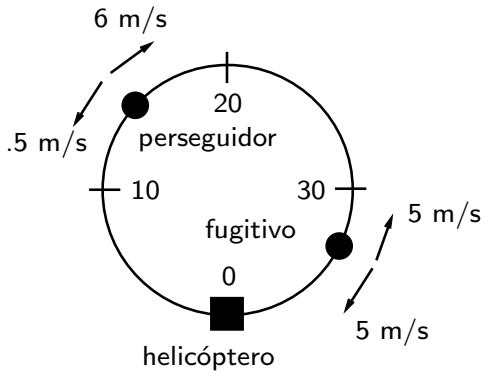


- Mesmo em sistemas físicos discretizados, há argumentos para se usar um modelo híbrido...
- Qual formalismo usamos aqui? Autômatos Híbridos

Exemplo: joguinho do perseguidor [Alur,et al.,1997]

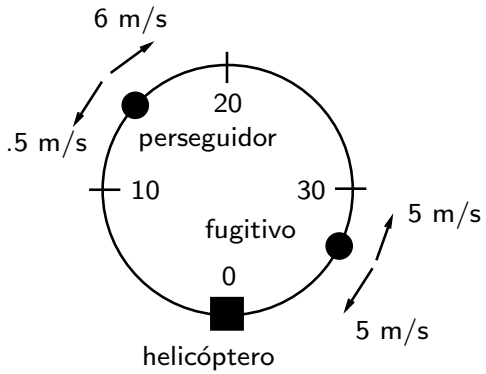


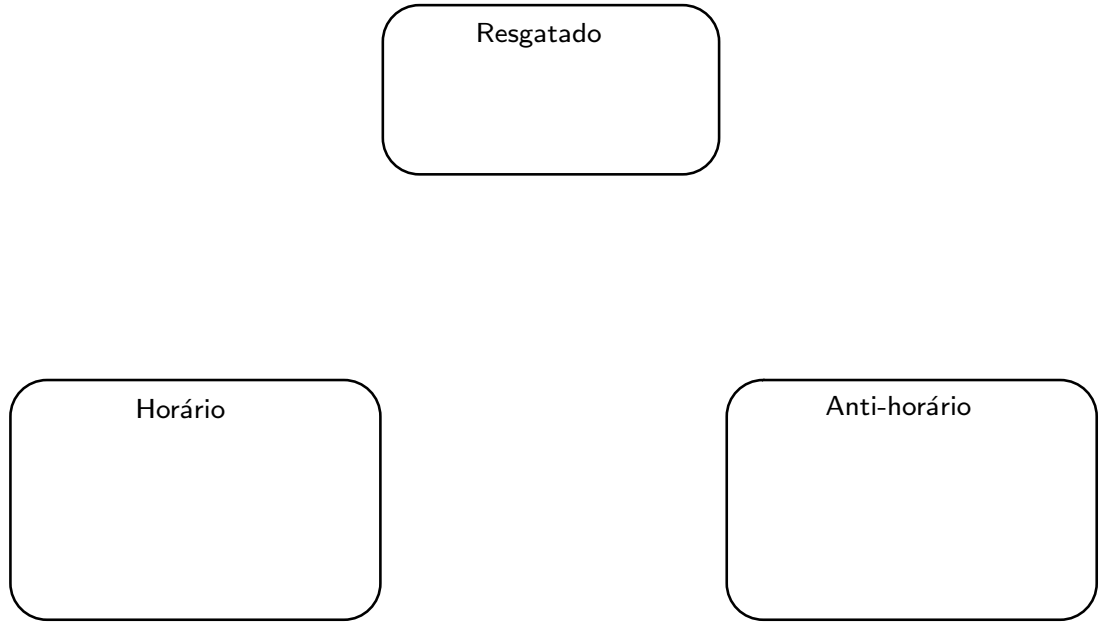
Exemplo: joguinho do perseguidor [Alur,et al.,1997]



Sistema híbrido: variáveis (f, p, t)

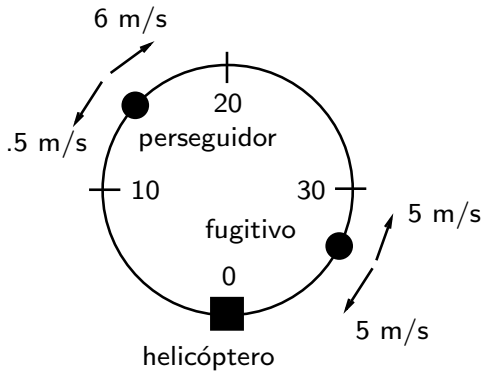
Exemplo: joguinho do perseguidor [Alur,et al.,1997]

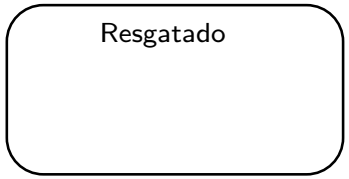


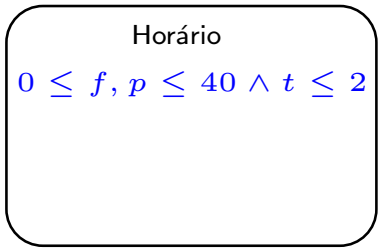


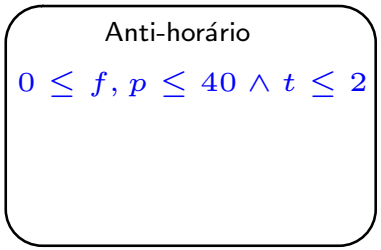
Sistema híbrido: variáveis (f, p, t) , modos de operação

Exemplo: joguinho do perseguidor [Alur,et al.,1997]



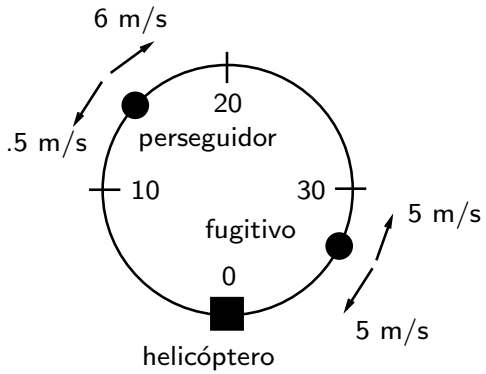


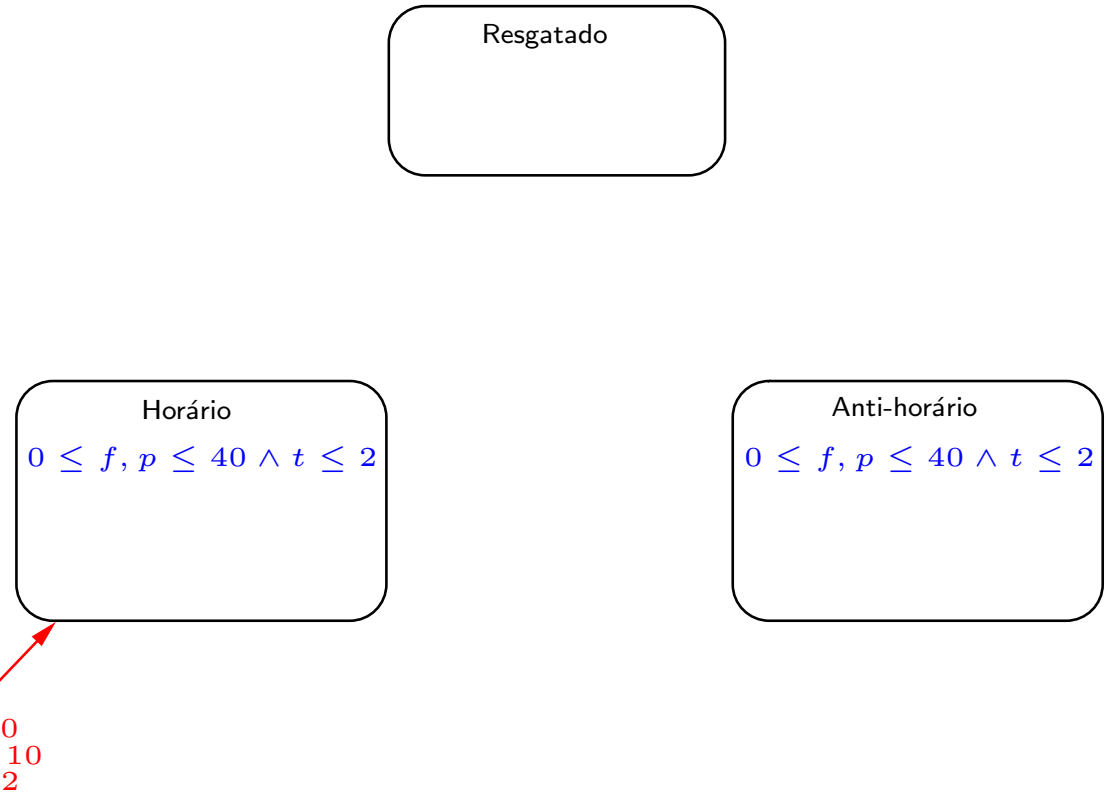




Sistema híbrido: variáveis (f, p, t) , modos de operação , invariantes

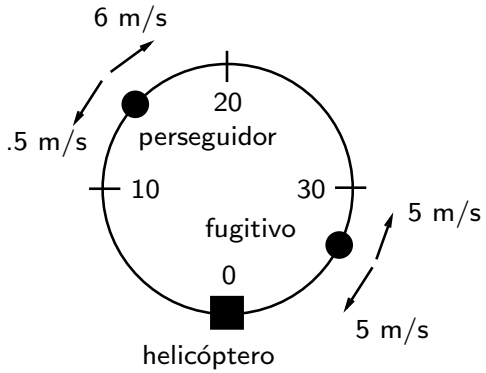
Exemplo: joguinho do perseguidor [Alur,et al.,1997]





Sistema híbrido: variáveis (f, p, t) , modos de operação , invariantes , condições iniciais

Exemplo: joguinho do perseguidor [Alur,et al.,1997]



Resgatado

$\dot{f} = \dot{p} = \dot{t} = 0$

Horário

$0 \leq f, p \leq 40 \wedge t \leq 2$

$\dot{f} = 5 \wedge -\frac{1}{2} \leq \dot{p} \leq 6 \wedge \dot{t} = 1$

Anti-horário

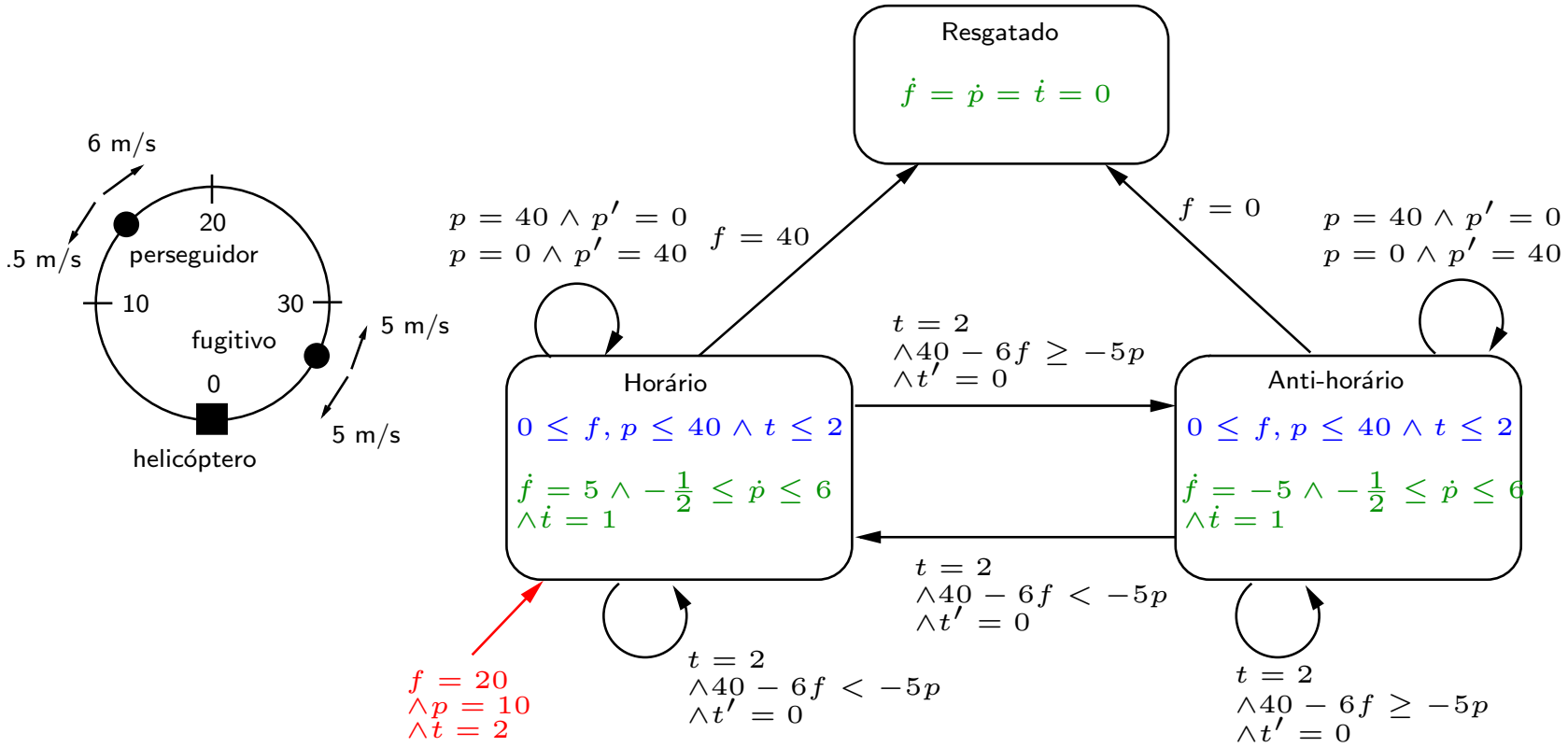
$0 \leq f, p \leq 40 \wedge t \leq 2$

$\dot{f} = -5 \wedge -\frac{1}{2} \leq \dot{p} \leq 6 \wedge \dot{t} = 1$

$f = 20 \wedge p = 10 \wedge t = 2$

Sistema híbrido: variáveis (f, p, t) , modos de operação , invariantes , condições iniciais , evolução contínua

Exemplo: joguinho do perseguidor [Alur,et al.,1997]



Sistema híbrido: variáveis (f, p, t) , modos de operação , invariantes , condições iniciais , evolução contínua , transições discretas.

Autômato Híbrido Linear

Todos os predicados são **convexos**:
$P = \{x \mid Ax \geq b\}$ ⟵ um Poliedro

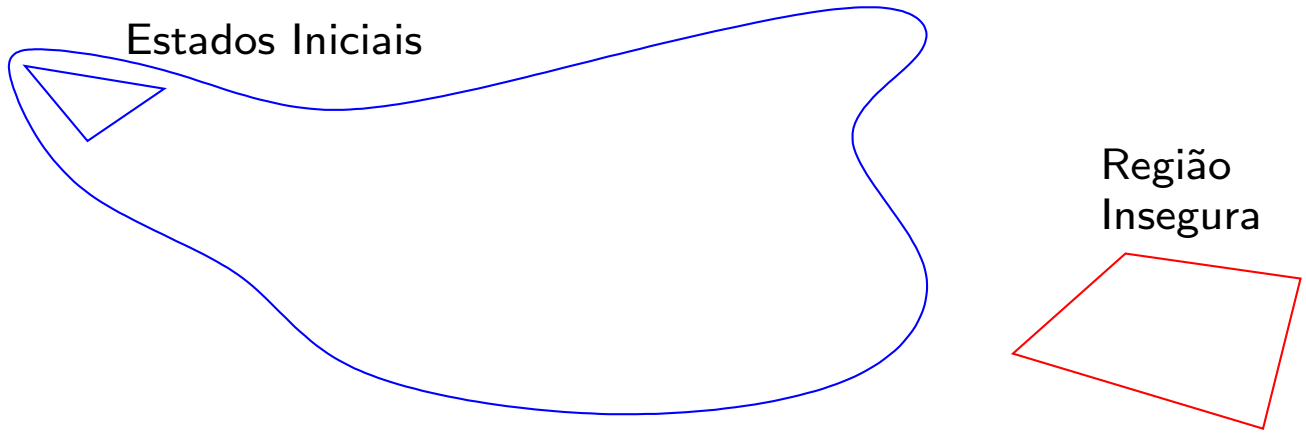
- Variáveis: X
- Modos
- Invariantes: um poliedro sobre X por modo
- Cond. iniciais: um poliedro sobre X por modo
- Evol. contínuas: um poliedro sobre $\dot{X}$ por modo ⟵ !!!
- Trans. discretas: conjunto de poliedros sobre $X \cup X'$

Alcançabilidade

- Verificação:
  - O sistema satisfaz a propriedade?
  - O sistema é seguro?
- Falsificação:
  - O sistema alcança um estado inseguro?

Alcançabilidade

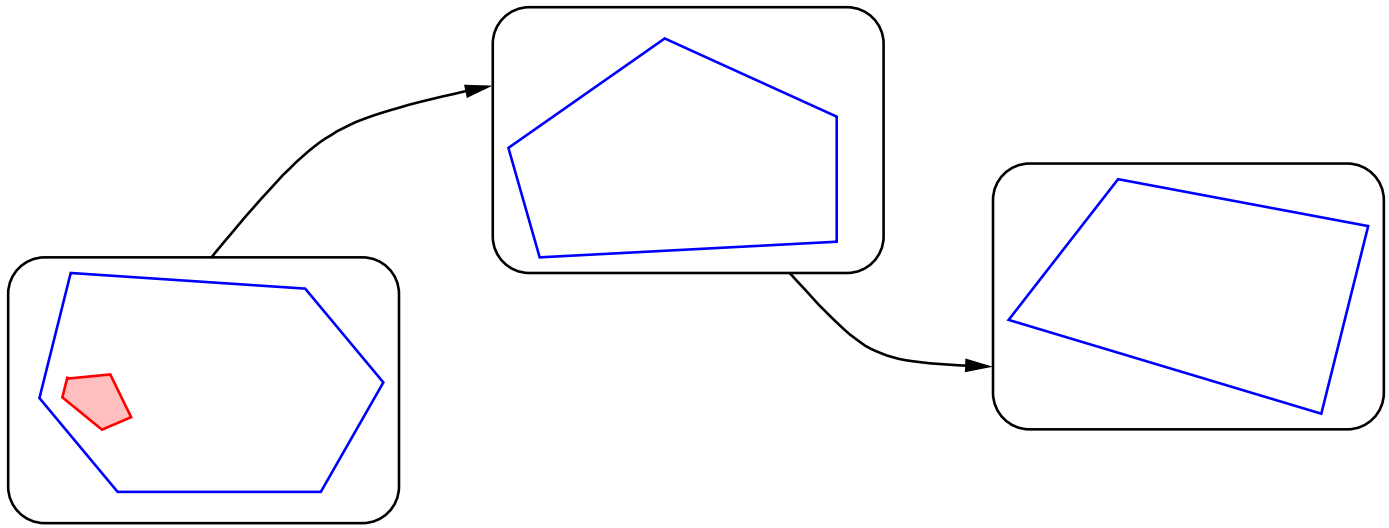
- Verificação:
  - O sistema satisfaz a propriedade?
  - O sistema é seguro?
- Falsificação:
  - O sistema alcança um estado inseguro?



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

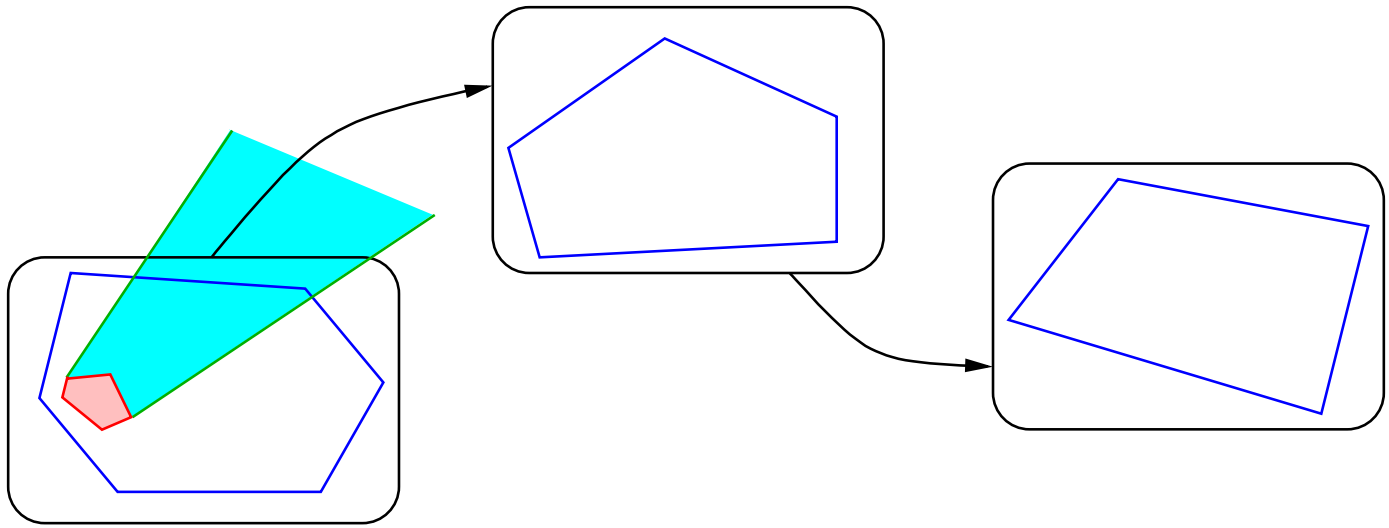
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

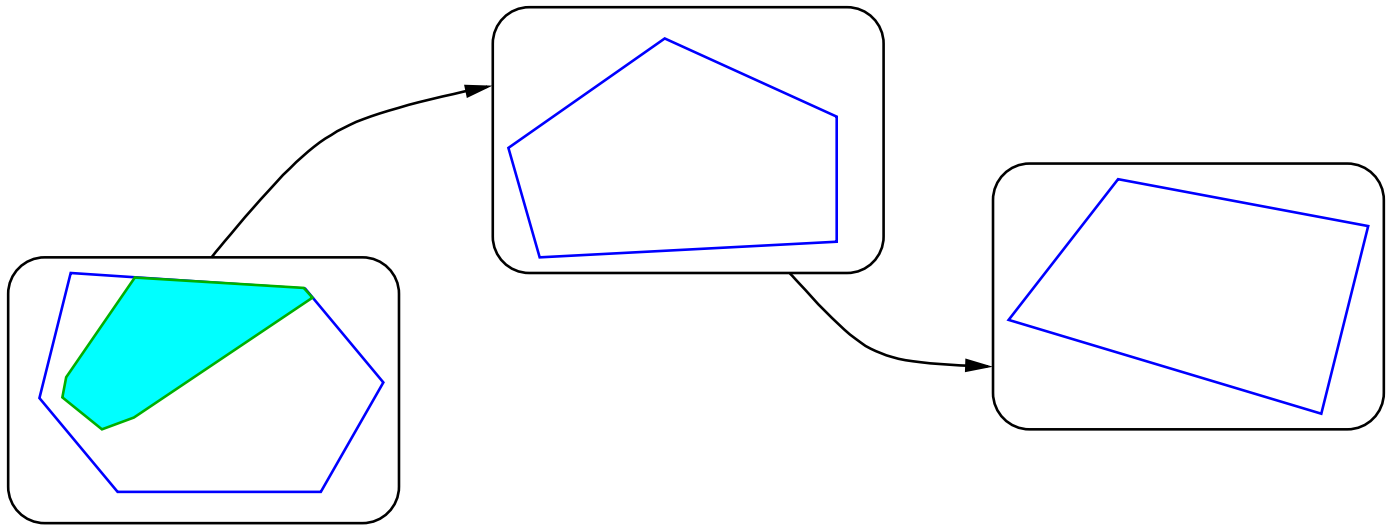
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

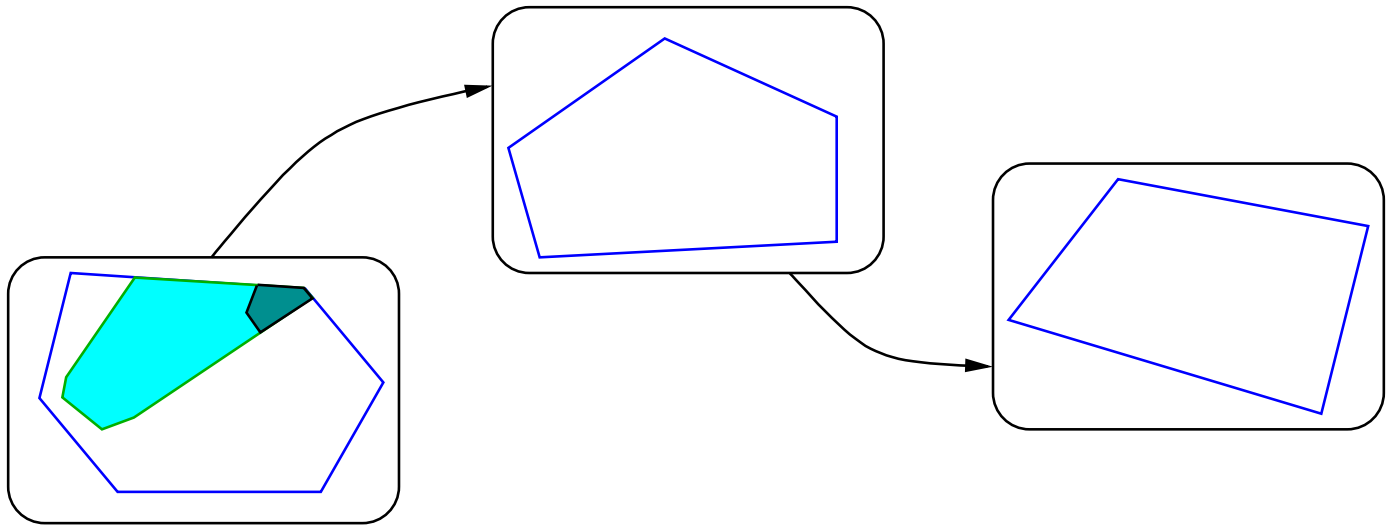
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

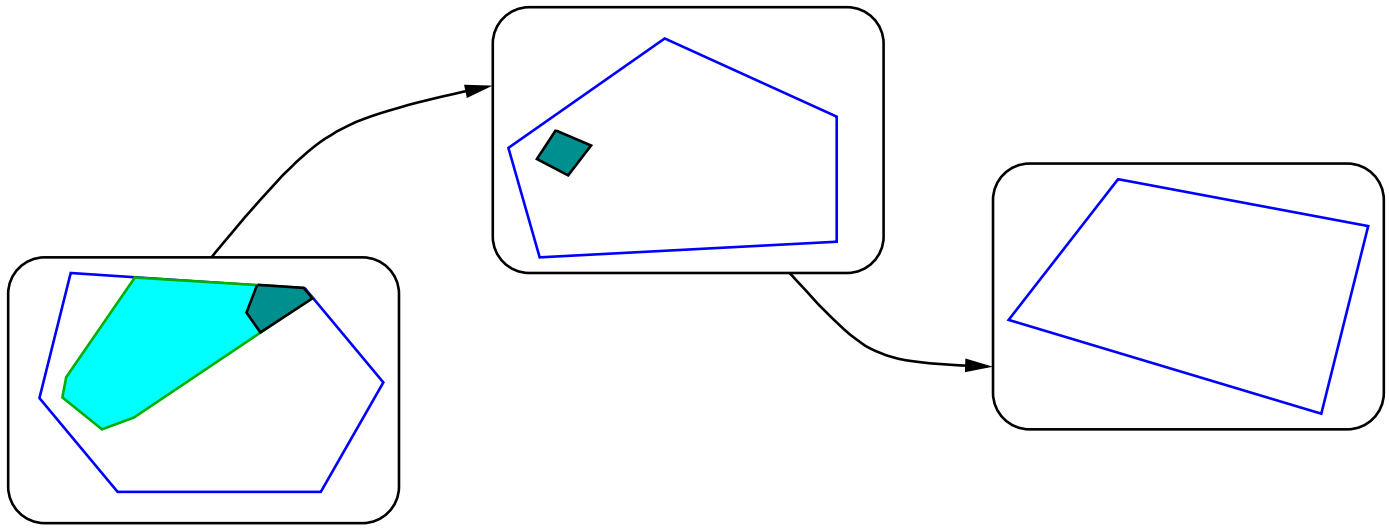
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

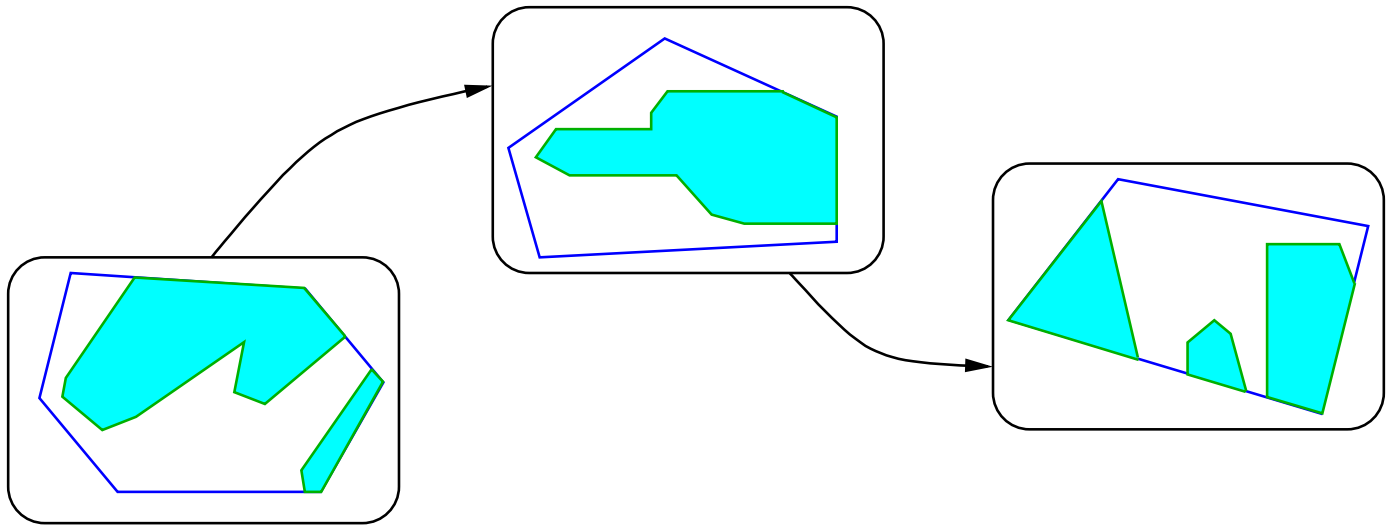
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

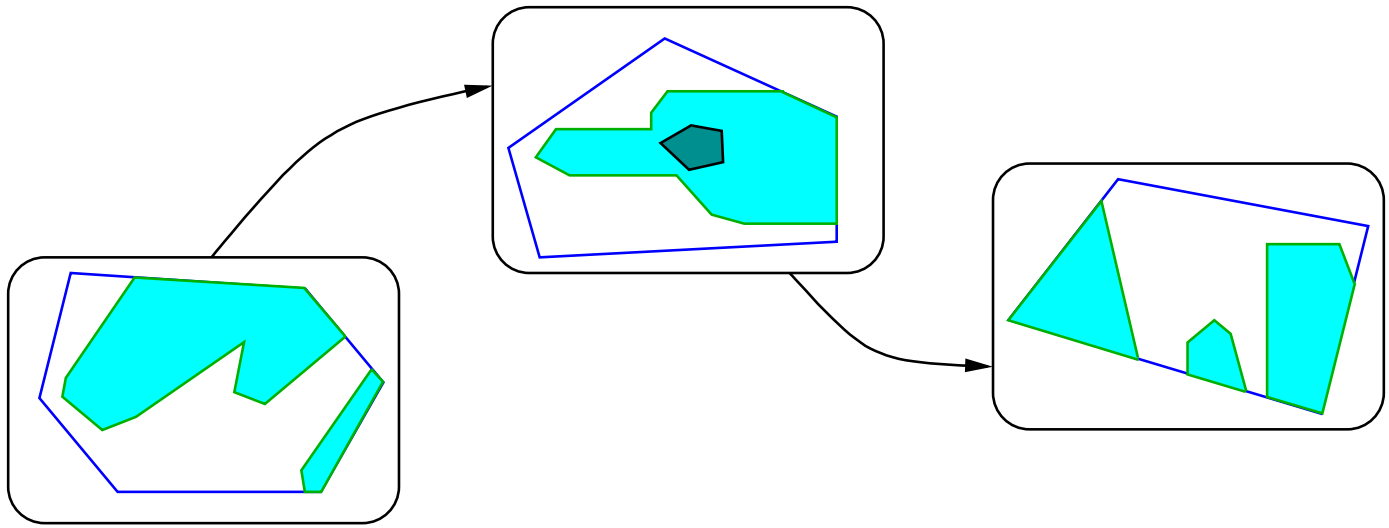
  $\longrightarrow$ a evolução é linear!



Alcançabilidade

- Objetivo: calcular **todos** os estados alcançáveis a partir de algum estado inicial

  $\longrightarrow$ a evolução é linear!



HyTech [Henzinger,et al.,∼1994]

- Implementado em Berkeley e Cornell, entre 1992 e 1994
- Primeira versão, usando eliminação de quantificadores e Mathematica era muuuuuito lenta...

Primitiva: Eliminação de Quantificadores

- Entrada: P, Q, E e T são poliedros (na forma $Ax \geq b$) sobre $X, X, \dot{X}$ e $X \cup X'$, respectivamente
- Saída: R é poliedro sobre X

Primitivas (Mathematica):

- **Interseção:** $R = P \cap Q$:
- **Evol. cont.:** $R = P$ evoluído por E:
- **Trans. disc.:** $R = P$ transitado por T:

- **Inclusão:** $P \subseteq Q$?:
- **Viabilidade:** $P = \emptyset$?:

Primitiva: Eliminação de Quantificadores

- Entrada: P, Q, E e T são poliedros (na forma $Ax \geq b$) sobre $X, X, \dot{X}$ e $X \cup X'$, respectivamente
- Saída: R é poliedro sobre X

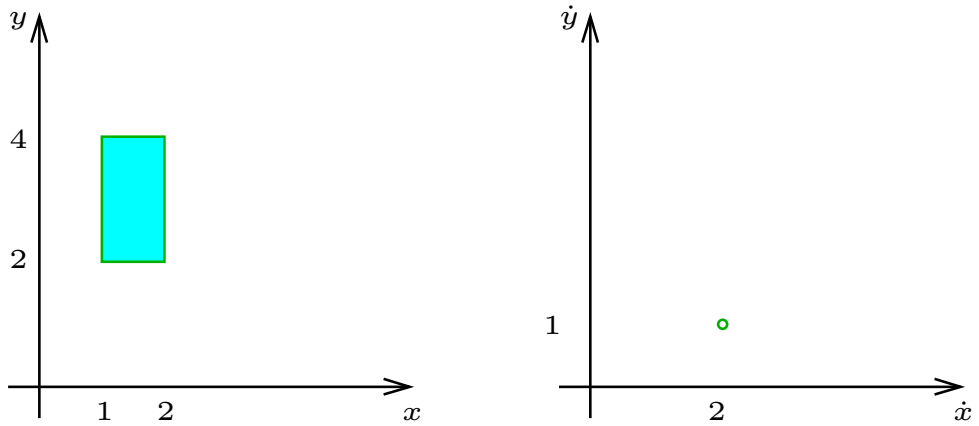
Primitivas (Mathematica):

- **Interseção:** $R = P \cap Q$: trivial
- **Evol. cont.:** $R = P$ evoluído por E: elim. de quant.
- **Trans. disc.:** $R = P$ transitado por T: elim. de quant.

- **Inclusão:** $P \subseteq Q$?: prog. linear
- **Viabilidade:** $P = \emptyset$?: prog. linear

Primitiva: Eliminação de Quantificadores

Exemplo de evolução cont.: $R = P$ evoluído por E



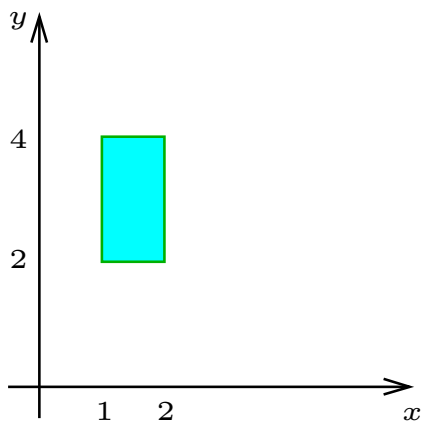
P E

- $P = 1 \leq x \leq 2 \wedge 2 \leq y \leq 4, \quad E = \dot{x} = 2 \wedge \dot{y} = 1$
- $R = \exists \delta \ (\ \delta \geq 0 \wedge 1 \leq x - 2\delta \leq 2 \wedge 2 \leq y - \delta \leq 4)$

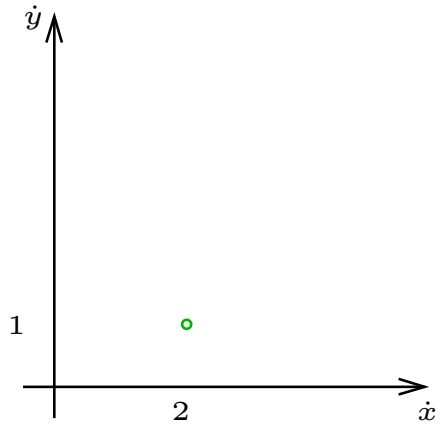
eliminando o quantificador

Primitiva: Eliminação de Quantificadores

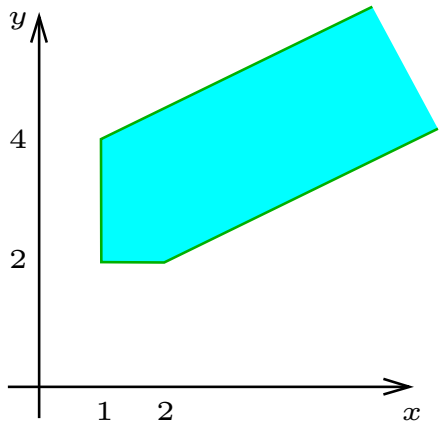
Exemplo de evolução cont.: $R = P$ evoluído por E



P



E



R

- $P = 1 \leq x \leq 2 \wedge 2 \leq y \leq 4, \quad E = \dot{x} = 2 \wedge \dot{y} = 1$
- $R = \exists \delta \ (\ \delta \geq 0 \wedge 1 \leq x - 2\delta \leq 2 \wedge 2 \leq y - \delta \leq 4)$

eliminando o quantificador

- $R = x \geq 1 \wedge y \geq 2 \wedge x - 2y + 2 \leq 0 \wedge x - 2y + 7 \geq 0$

HyTech

- Henzinger conversou, então, em 1995, com Halbwachs (Verimag, França)...
- Halbwachs — Meu, não vale a pena fazer eliminação de quantificadores. É melhor adicionar "raios" na representação interna do poliedro.
- Henzinger — Hã???

Poliedros

- Representação EXTERNA (conj. de inequações)

$$P = \{x \mid Ax \geq b\}$$

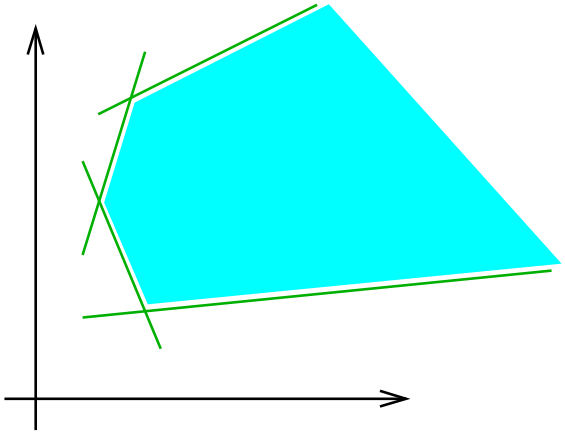
- Representação INTERNA (conj. de vértices e raios)

$$P = \{x \mid x = \text{conv}\{x_1, \ldots, x_v\} + \text{cone}\{y_1, \ldots, y_r\}\}$$

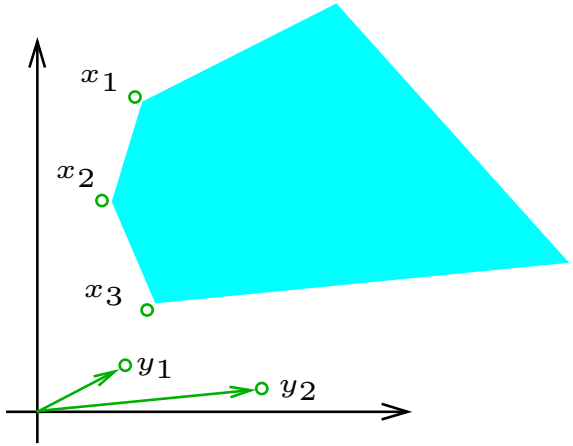
$$\text{conv}\{x_1, \ldots, x_v\} = \sum_{i=1}^{v} \lambda_i x_i, \quad \lambda_i \geq 0, \quad \sum_{i=1}^{v} \lambda_i = 1$$

$$\text{cone}\{y_1, \ldots, y_r\} = \sum_{j=1}^{r} \mu_j y_j, \quad \mu_j \geq 0$$

Exemplo



EXTERNA



INTERNA

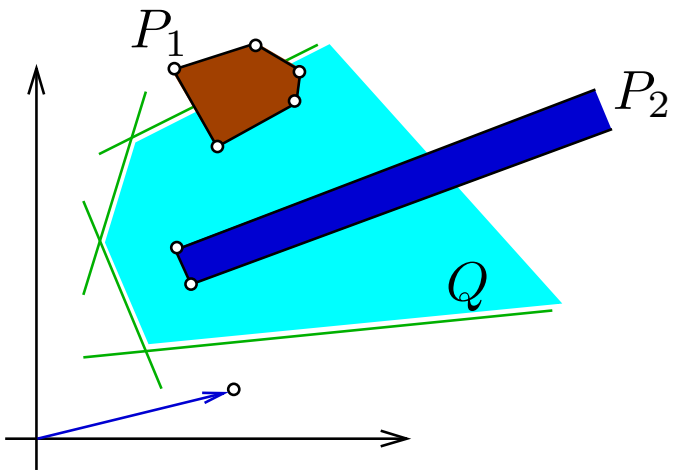
Primitivas para alcançabilidade

- **Interseção:** $P \cap Q$: trivial
- **Viabilidade:** $P = \emptyset$?: sse a representação interna de P não tiver nenhum vértice, nem raio :-)

Primitivas para alcançabilidade

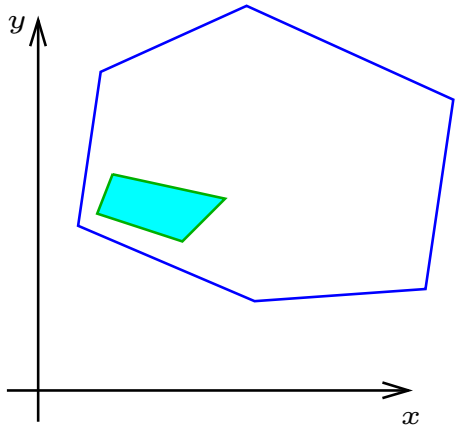
- **Inclusão:** $P \subseteq Q$?:
  - $P = \text{conv}\{x_1, \ldots, x_v\} + \text{cone}\{y_1, \ldots, y_r\}$
  - $Q = \{x \mid Ax \geq b\}$

  - $P \subseteq Q$ sse $Ax_i \geq b,\ 1 \leq i \leq v$
    e $Ay_j \geq 0,\ 1 \leq j \leq r$

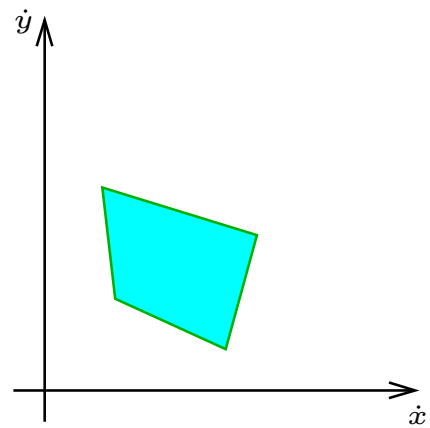


Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



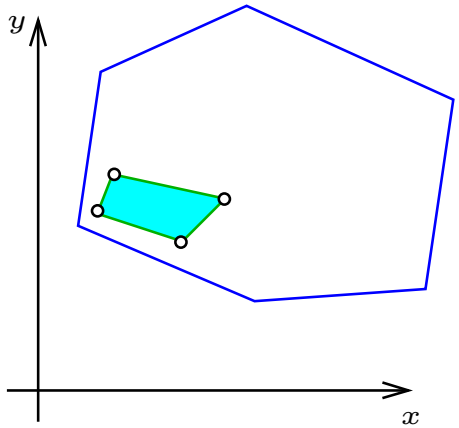
P



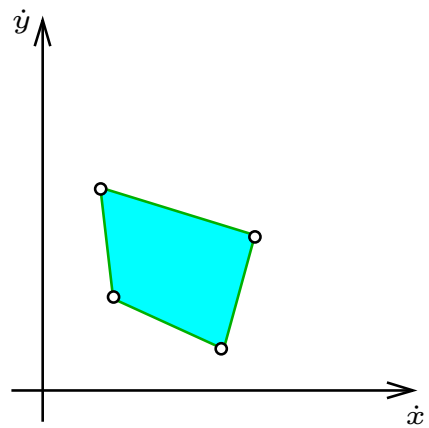
E

Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



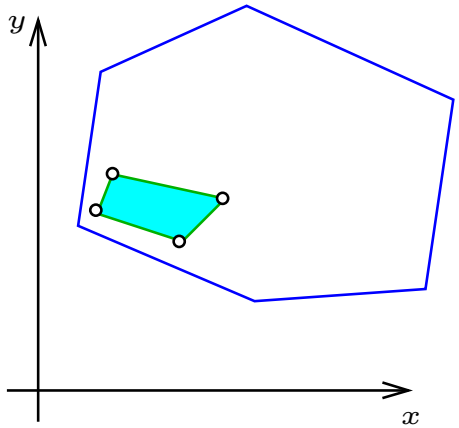
P



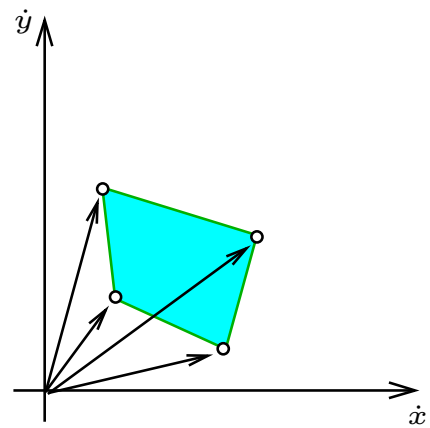
E

Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



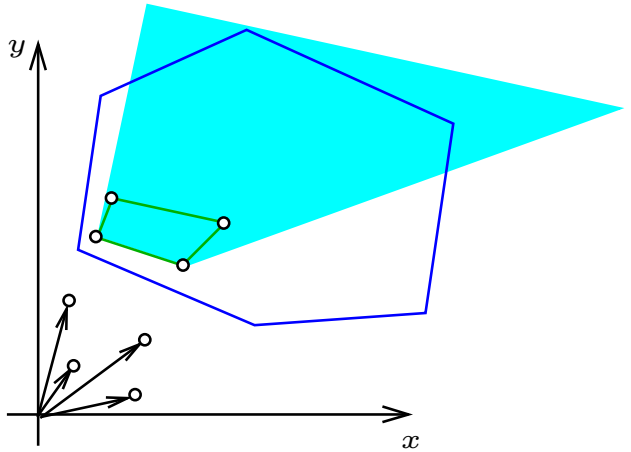
P



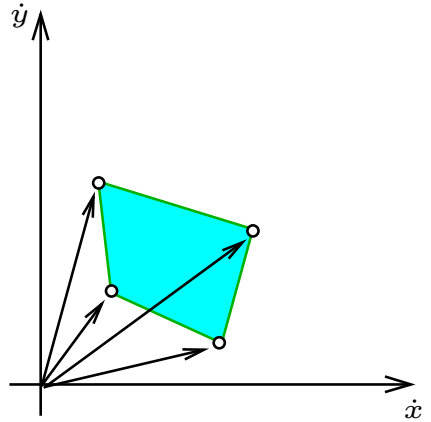
E

Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



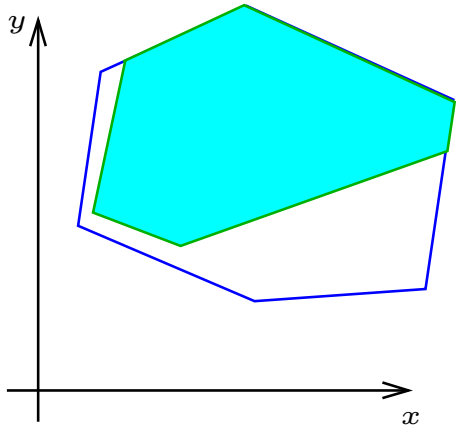
P



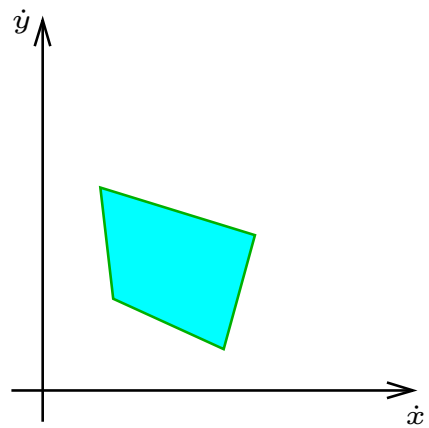
E

Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



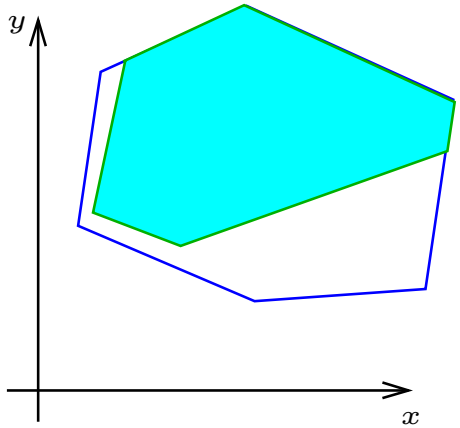
P



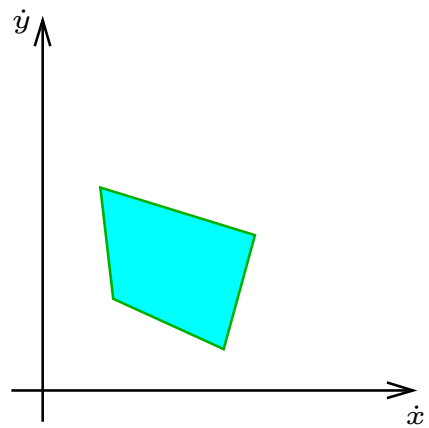
E

Primitivas para alcançabilidade

- **Evolução contínua:** $R = P$ evoluído por E



P



E

- **Transição discreta:** $R = P$ transitado por T: semelhante...

Primitivas: Enumeração de Vértices

- Todas as primitivas necessárias para alcançabilidade ficam trivializadas se tenho um algoritmo de conversão entre as representações:

  externa $\longrightarrow$ interna: enumeração de vértices
  interna $\longrightarrow$ externa: enumeração de facetas

Primitivas: Enumeração de Vértices

- Todas as primitivas necessárias para alcançabilidade ficam trivializadas se tenho um algoritmo de conversão entre as representações:

  externa $\longrightarrow$ interna: enumeração de vértices
  interna $\longrightarrow$ externa: enumeração de facetas

- Mas, as representações são DUAIS
  - dualidade cônica, tradicional da geometria;
  - não a dualidade tradicional de PL

Primitivas: Enumeração de Vértices

- Todas as primitivas necessárias para alcançabilidade ficam trivializadas se tenho um algoritmo de conversão entre as representações:

  externa $\longrightarrow$ interna: enumeração de vértices
  interna $\longrightarrow$ externa: enumeração de facetas

- Mas, as representações são DUAIS
  - dualidade cônica, tradicional da geometria;
  - não a dualidade tradicional de PL

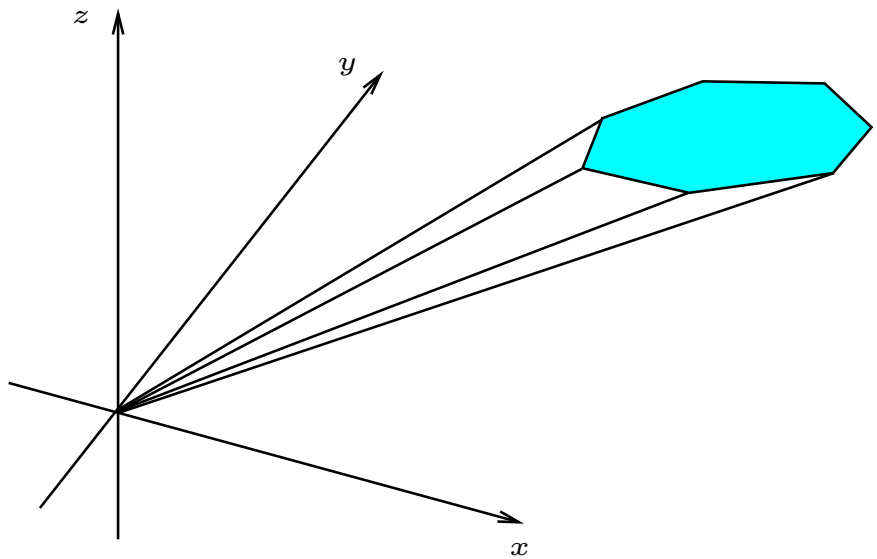
- Ficamos com um só problema: enumeração de vértices

Enumeração de Vértices

- pivotação (baseado no Simplex, Dantzig, 1947)
- incremental (Double Description Method, Motzkin, 1933)
  - Fourier, 1824
- Open problem: existe algoritmo polinomial para o problema? (polinomial na entrada e na saída)
- Algoritmo de Chernikova (três artigos em 1965,1966 e 1967) é uma "reencarnação" do DDM incremental de Motzkin

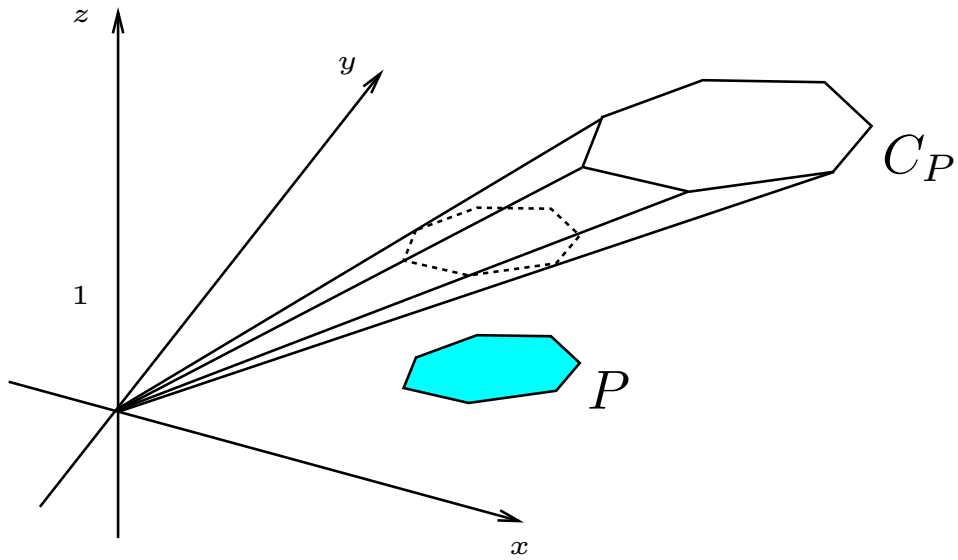
Cones

$\longrightarrow$ Poliedros da forma: $P = \{x \mid Ax \geq 0\}$ ou
$P = \{x \mid x = \text{cone}\{y_1, \ldots, y_r\}\}$



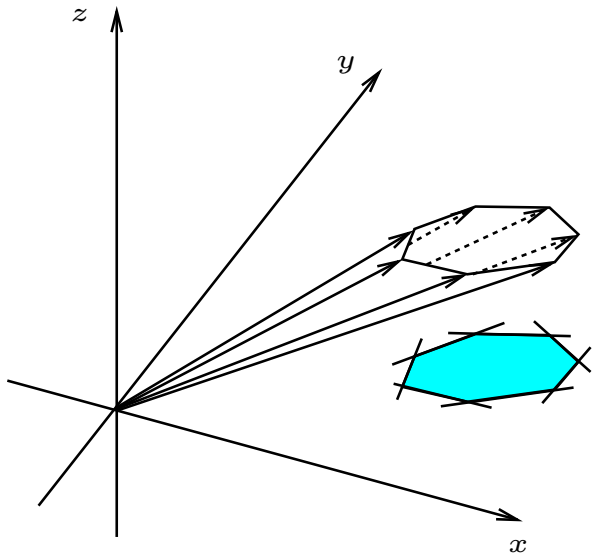
Cones

$\longrightarrow$ A todo poliedro, na dimensão d, $P = \{x \mid Ax \geq b\}$,
onde A é matriz $m \times d$,
está associado o cone, na dimensão $d+1$,
$C_P = \{x \mid [A \ -b]x \geq 0\}$, onde $[A \ -b]$ é matriz $m \times (d+1)$



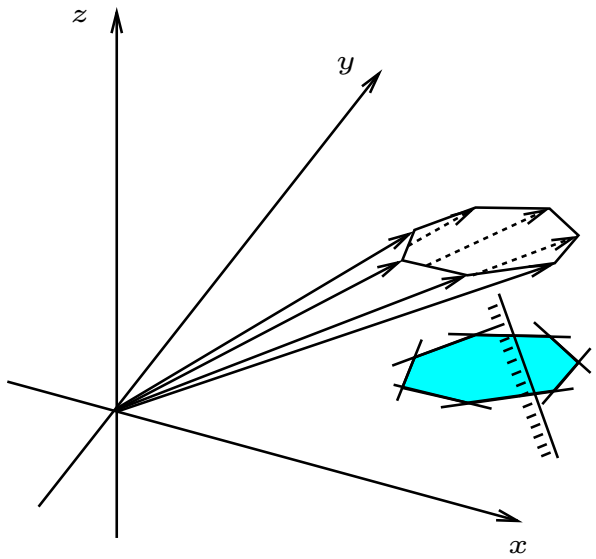
Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



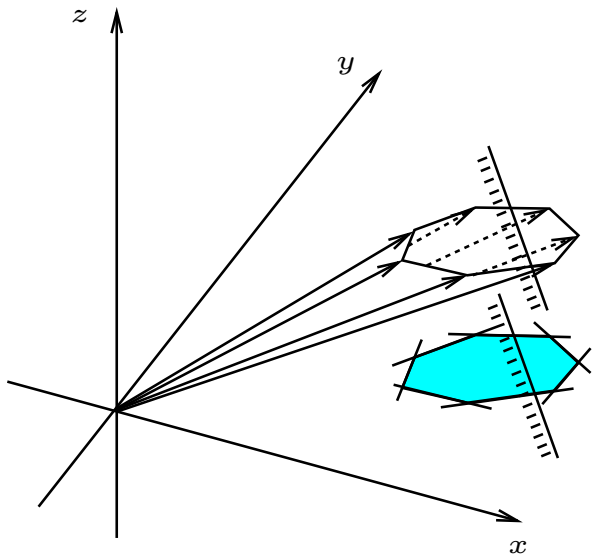
Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



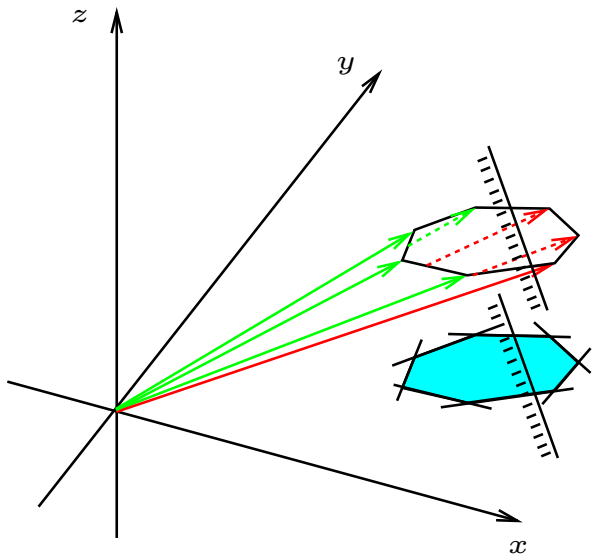
Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



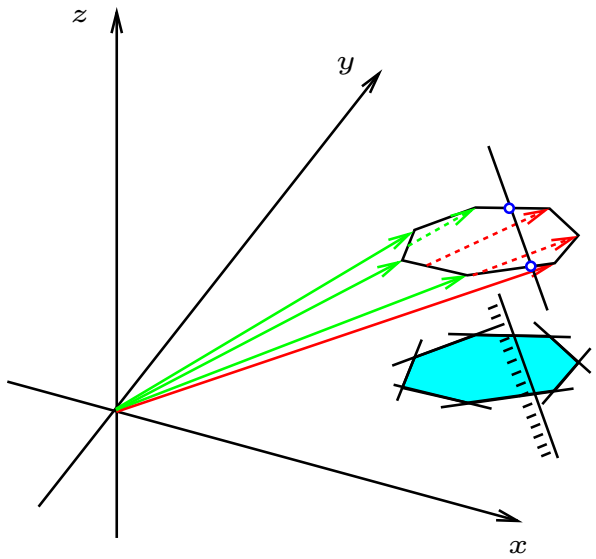
Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



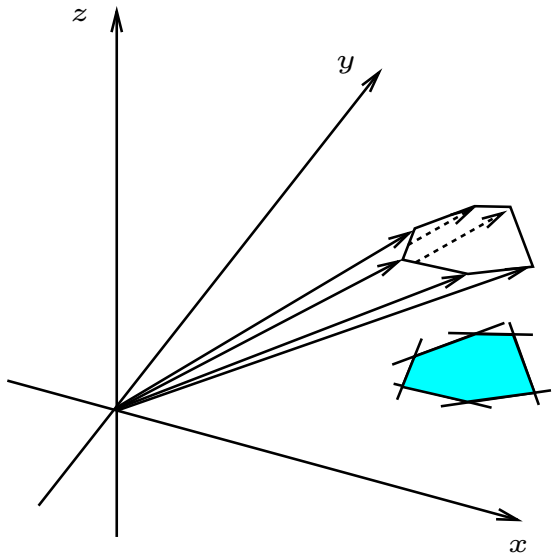
Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



Chernikova (DDM)

- Trabalha no cone C_P, e não em P, para evitar casos especiais no tratamento de poliedros ilimitados



Um balanço sobre Verificação em AH

- A mudança de elim. de quantificadores para poliedros no HyTech tornou a alcançabilidade entre 100 e 1000 vezes mais rápida, tipicamente
- Na prática, os sistemas são modelados como o produto de vários autômatos $\longleftarrow$ exponencialidade!
- Na prática, limitado a dimensão sete (?)
- Na prática, a memória se esgota antes de o tempo se esgotar ...

Bounded Model-Checking: SAT para AH

- Ao invés de calcular toda a área alcançável,
- Expressamos a existência de um contra-exemplo de k passos:

Propriedade é falsificada em k passos sse

$$I(s_0) \wedge T(s_0, s_1) \wedge T(s_1, s_2) \wedge \cdots \wedge T(s_{k-1}, s_k)$$
$$\wedge (unsafe(s_0) \vee \cdots \vee unsafe(s_k))$$

é satisfatível!

Exemplo: dois passos para o perseguidor

$$H^0 \rightarrow (f^0 = 20 \wedge p^0 = 10 \wedge t^0 = 2)$$
$$\wedge R^0 \rightarrow \text{false}$$
$$\wedge A^0 \rightarrow \text{false}$$

$$\wedge(H^0 \vee R^0 \vee A^0) \wedge ((\overline{H^0} \wedge \overline{R^0}) \vee (\overline{R^0} \wedge \overline{A^0}) \vee (\overline{H^0} \wedge \overline{A^0}))$$

$$\wedge H^0 \rightarrow (\delta^0 \geq 0 \wedge f'^0 = f^0 + 5\delta^0 \wedge t'^0 = t^0 + \delta^0$$
$$\wedge p'^0 \geq f^0 - \tfrac{1}{2}\delta^0 \wedge p'^0 \leq p^0 + 6\delta^0)$$

$$\wedge H^0 \rightarrow (t^0 \leq 2 \wedge t'^0 \leq 2 \cdots)$$

$$\wedge(t_1^0 \vee t_2^0 \vee t_3^0 \vee t_4^0 \vee t_5^0 \vee t_6^0 \vee t_7^0 \vee t_8^0) \wedge (\cdots) \leftarrow \text{problema!}$$

$$\vdots$$

$$\wedge(f^0 = p^0 \vee f'^0 = p'^0 \vee f^1 = p^1 \vee f'^1 = p'^1)$$

Como decidir Satisfatibilidade?

$$H^0 \rightarrow (f^0 = 20 \wedge p^0 = 10 \wedge t^0 = 2)$$
$$\wedge R^0 \rightarrow \text{false}$$
$$\wedge A^0 \rightarrow \text{false}$$

$$\wedge(H^0 \vee R^0 \vee A^0) \wedge ((\overline{H^0} \wedge \overline{R^0}) \vee (\overline{R^0} \wedge \overline{A^0}) \vee (\overline{H^0} \wedge \overline{A^0}))$$

$$\wedge H^0 \rightarrow (\delta^0 \geq 0 \wedge f'^0 = f^0 + 5\delta^0 \wedge t'^0 = t^0 + \delta^0$$
$$\wedge p'^0 \geq f^0 - \tfrac{1}{2}\delta^0 \wedge p'^0 \leq p^0 + 6\delta^0)$$

$$\wedge H^0 \rightarrow (t^0 \leq 2 \wedge t'^0 \leq 2 \cdots)$$

$$\wedge(t_1^0 \vee t_2^0 \vee t_3^0 \vee t_4^0 \vee t_5^0 \vee t_6^0 \vee t_7^0 \vee t_8^0) \wedge (\cdots) \leftarrow \text{problema!}$$

$$\vdots$$

$$\wedge(f^0 = p^0 \vee f'^0 = p'^0 \vee f^1 = p^1 \vee f'^1 = p'^1)$$

- Em tese:
  - Eliminação de quantificadores
  - Abordagem *eager*: converter em DNF e eliminar as desigualdades antes de falar qualquer coisa sobre SAT...
- Na prática: os famosos *lazy* SMT-Solvers

HySAT – Codificação Pseudo-Booleana

Fórmula de Entrada

$$\begin{aligned}\phi = &(\overline{e} \rightarrow C \wedge D)\\ &\wedge(\overline{f} \rightarrow A \wedge B)\\ &\wedge(\overline{f} \vee g \vee e)\\ &\wedge(\overline{g} \vee \overline{f})\\ &\wedge(e \rightarrow (C \vee D) \wedge g)\\ &\wedge(A \rightarrow (4x - 2y \geq 9))\\ &\wedge(B \rightarrow (2x - 4y \leq -7))\\ &\wedge(C \rightarrow (x + y \leq 5))\\ &\wedge(D \rightarrow (x \leq 7))\end{aligned}$$

HySAT – Codificação Pseudo-Booleana

Fórmula de Entrada

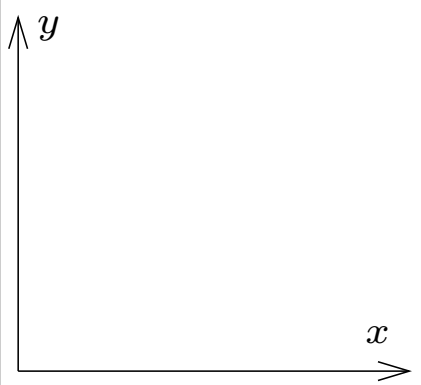
$$\begin{aligned}\phi = &(\overline{e} \rightarrow C \wedge D)\\ &\wedge(\overline{f} \rightarrow A \wedge B)\\ &\wedge(\overline{f} \vee g \vee e)\\ &\wedge(\overline{g} \vee \overline{f})\\ &\wedge(e \rightarrow (C \vee D) \wedge g)\\ &\wedge(A \rightarrow (4x - 2y \geq 9))\\ &\wedge(B \rightarrow (2x - 4y \leq -7))\\ &\wedge(C \rightarrow (x + y \leq 5))\\ &\wedge(D \rightarrow (x \leq 7))\end{aligned}$$

$\longrightarrow$

DPLL

$$2e + C + D \geq 2$$
$$2f + A + B \geq 2$$
$$\overline{f} + g + e \geq 1$$
$$\overline{g} + \overline{f} \geq 1$$
$$3\overline{e} + 2g + C + D \geq 3$$

Prog. Linear



HySAT [Fränzle,Herde,2006]

DPLL

$$2e + C + D \geq 2$$

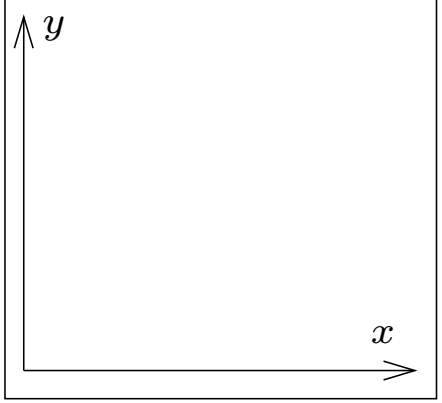
$$2f + A + B \geq 2$$

$$\overline{f} + g + e \geq 1$$

$$\overline{g} + \overline{f} \geq 1$$

$$3\overline{e} + 2g + C + D \geq 3$$

Prog. Linear



HySAT [Fränzle,Herde,2006]

DPLL

$$2e + C + D \geq 2$$

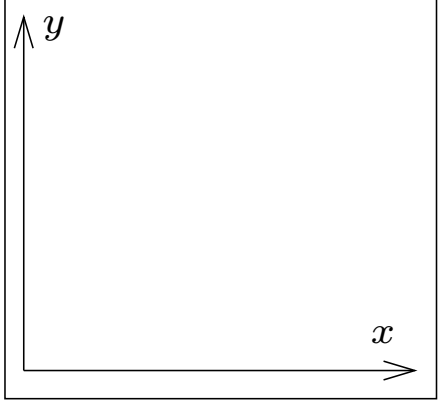
$$2f + A + B \geq 2$$

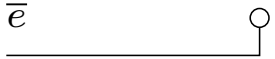
$$\overline{f} + g + e \geq 1$$

$$\overline{g} + \overline{f} \geq 1$$

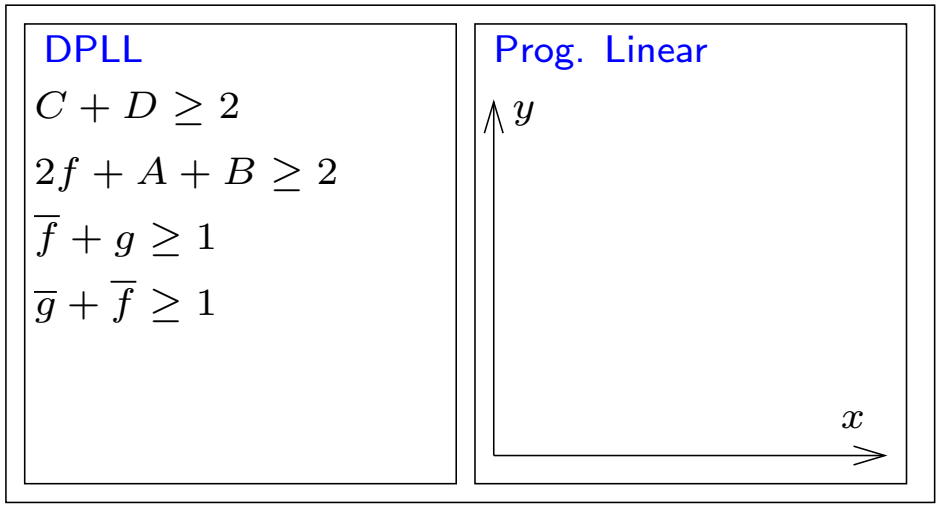
$$3\overline{e} + 2g + C + D \geq 3$$

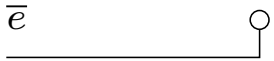
Prog. Linear



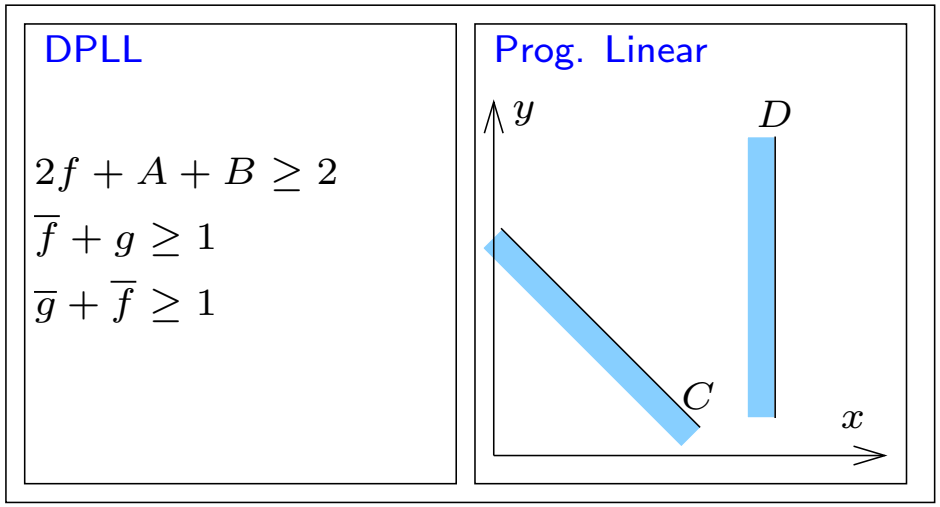


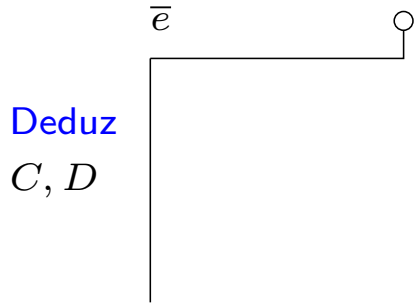
HySAT [Fränzle,Herde,2006]



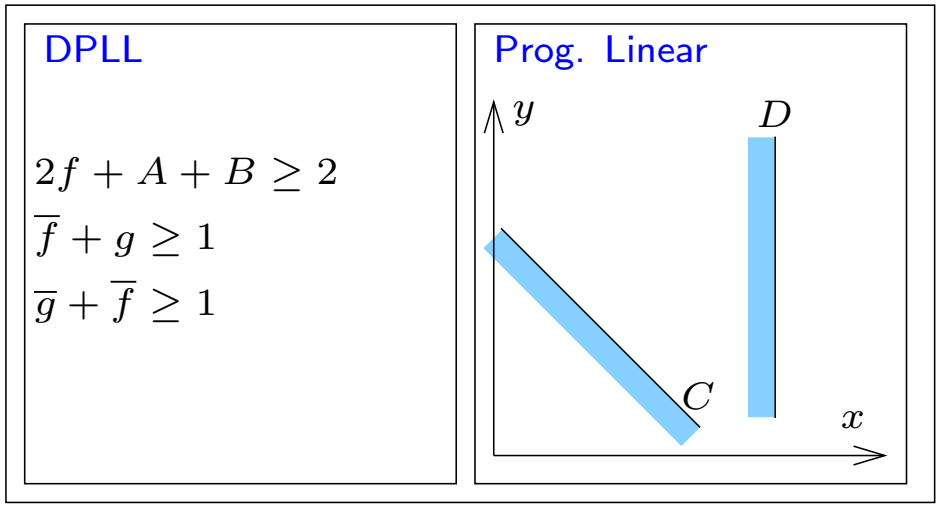


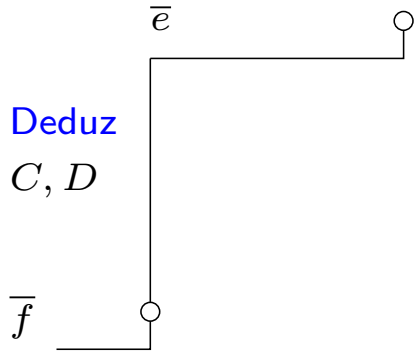
HySAT [Fränzle,Herde,2006]



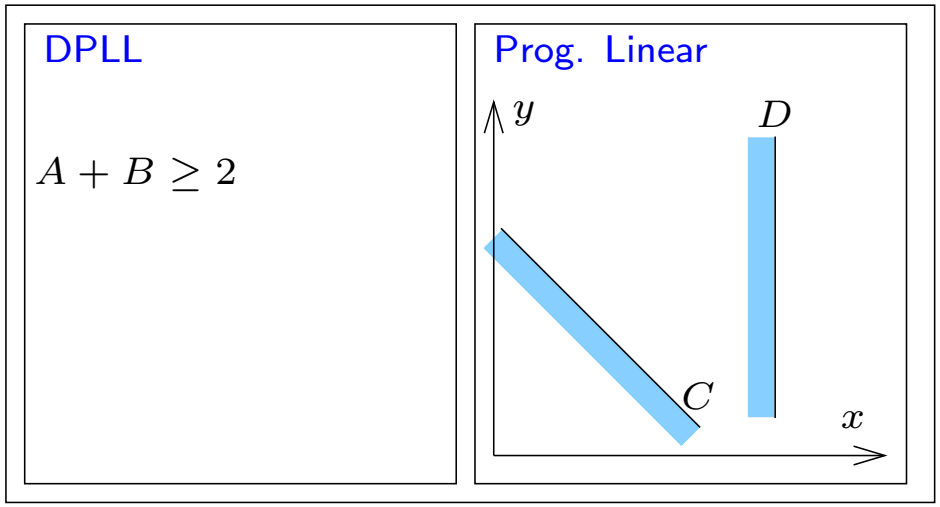


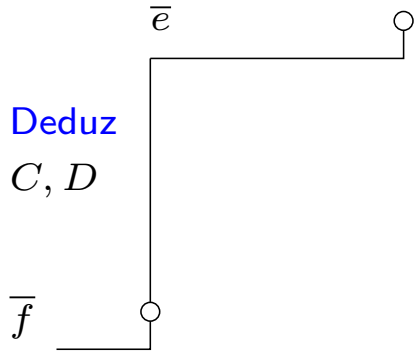
HySAT [Fränzle,Herde,2006]



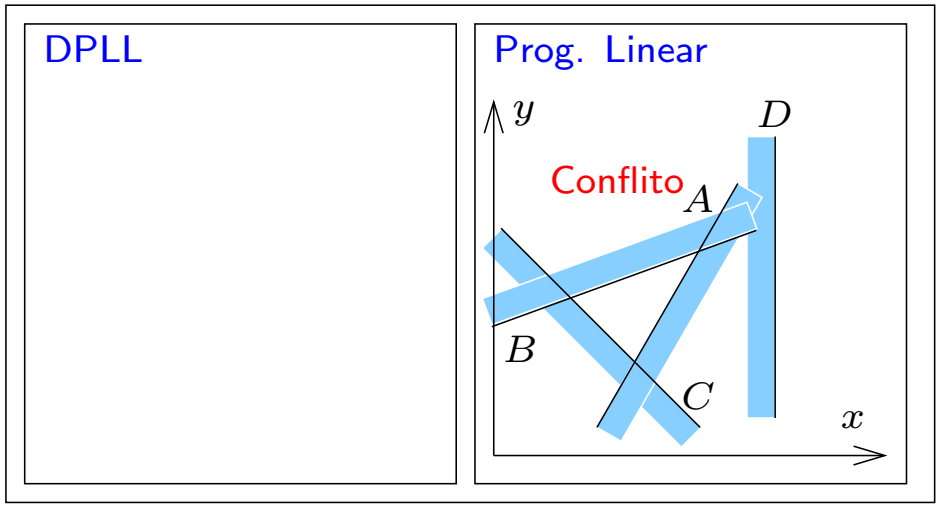


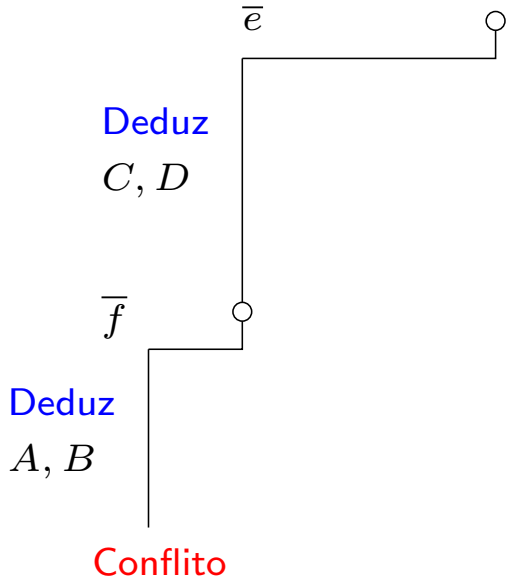
HySAT [Fränzle,Herde,2006]



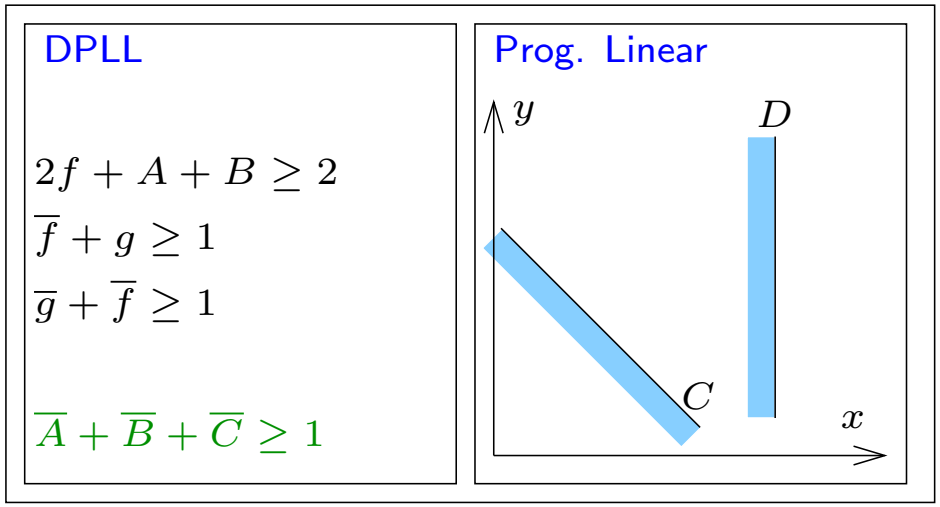


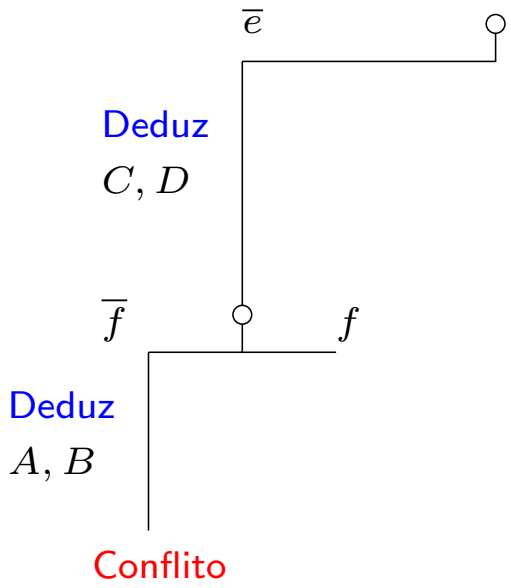
HySAT [Fränzle,Herde,2006]



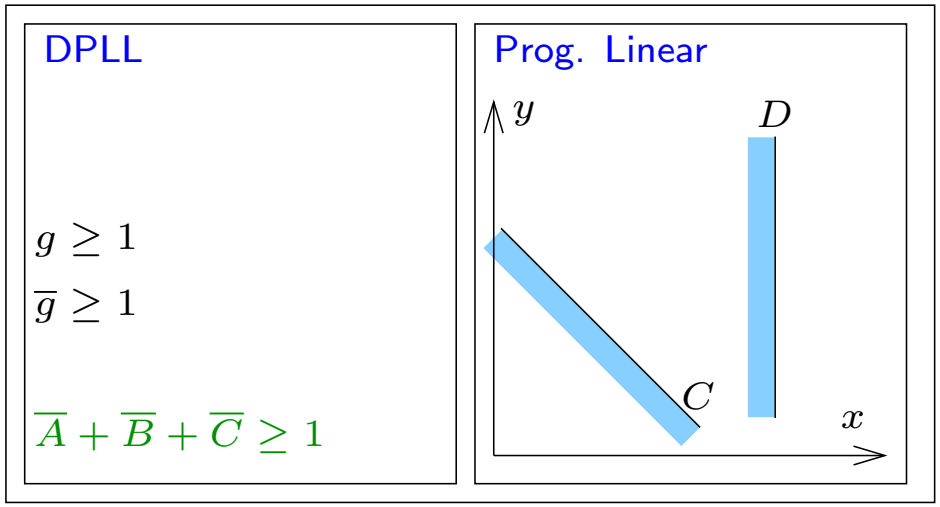


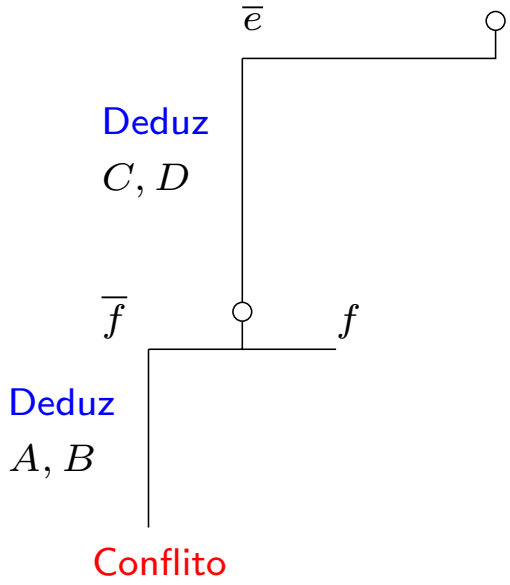
HySAT [Fränzle,Herde,2006]



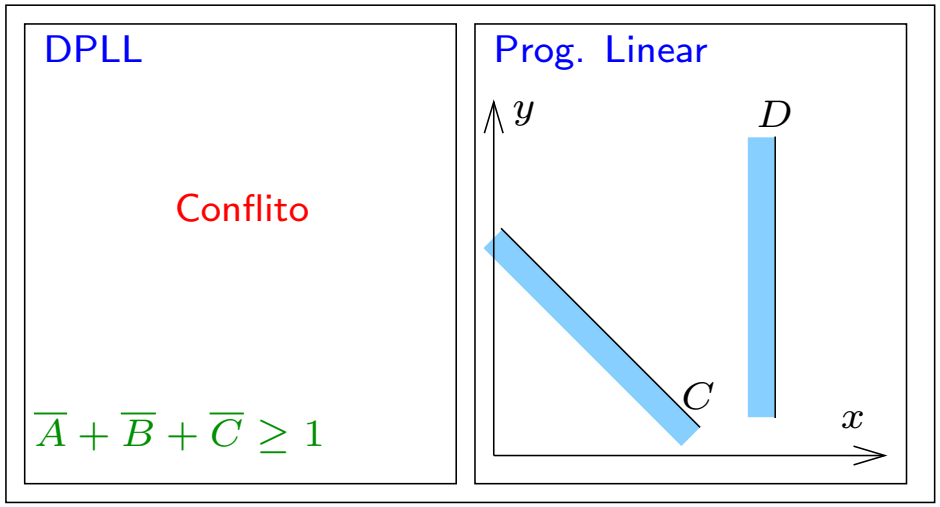


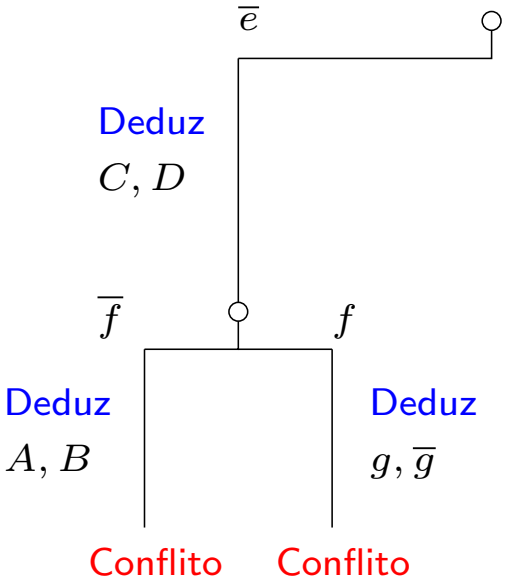
HySAT [Fränzle,Herde,2006]



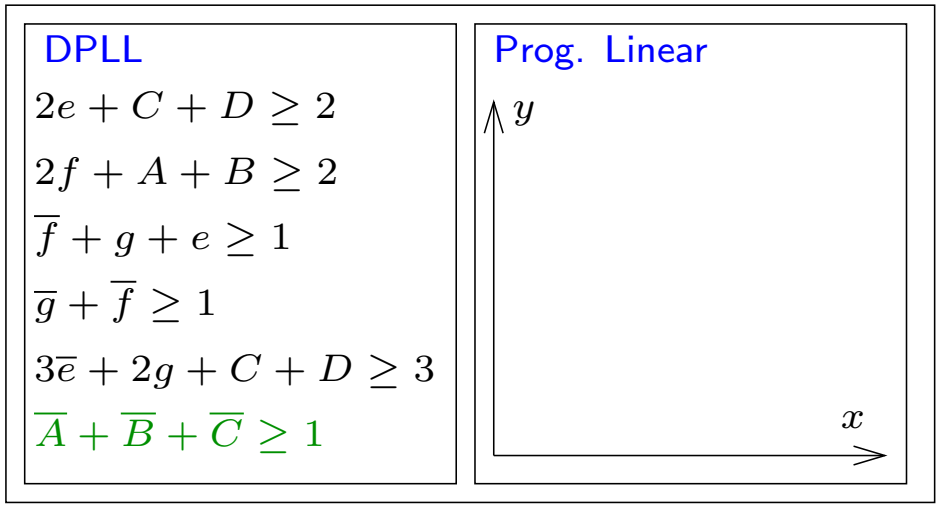


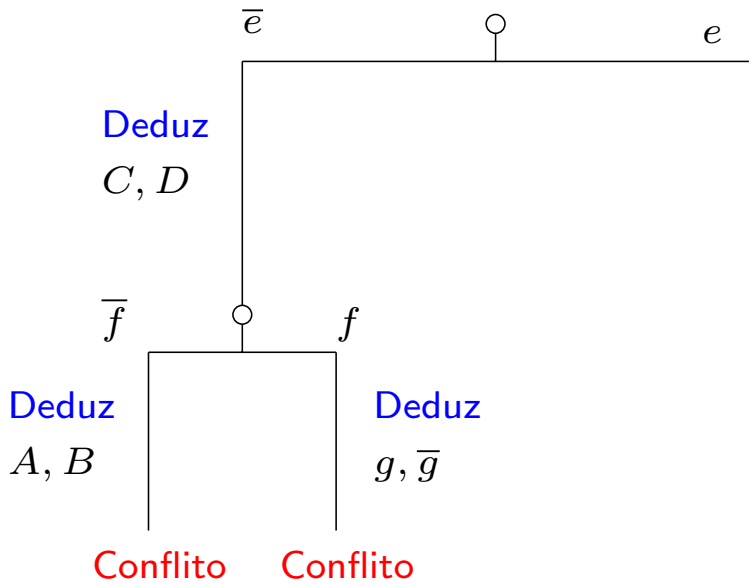
HySAT [Fränzle,Herde,2006]



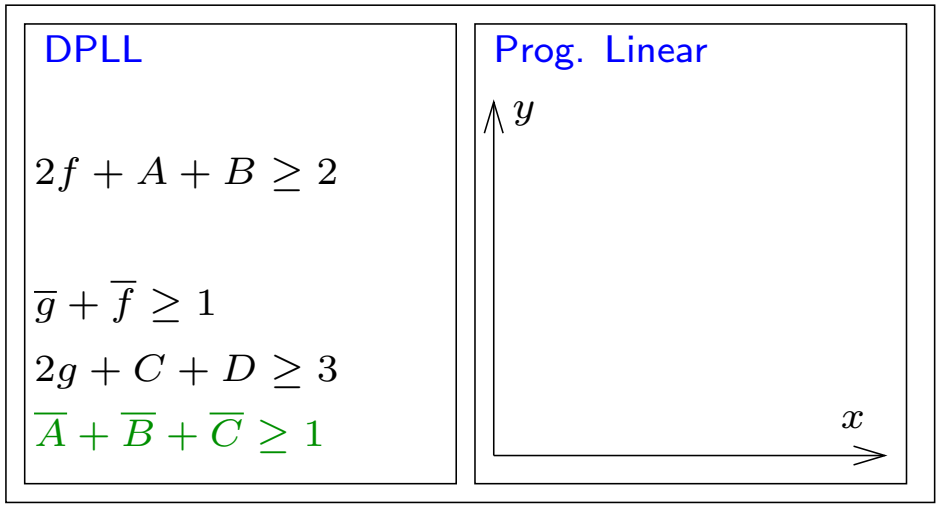


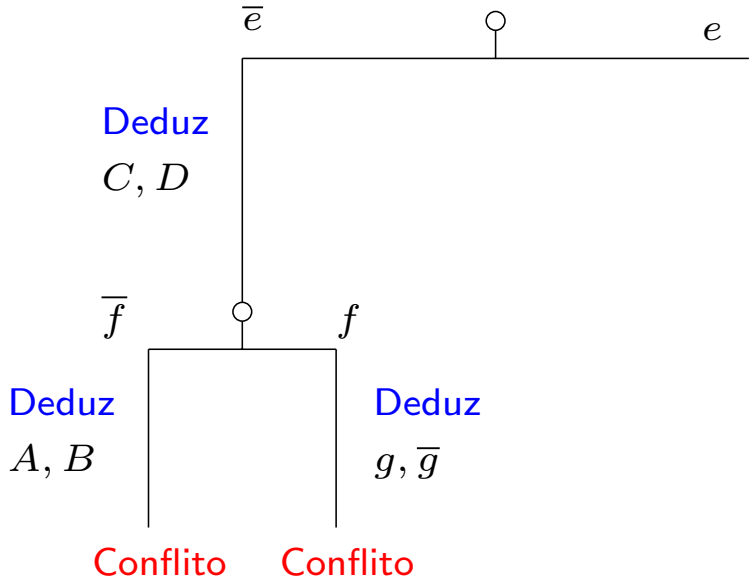
HySAT [Fränzle,Herde,2006]



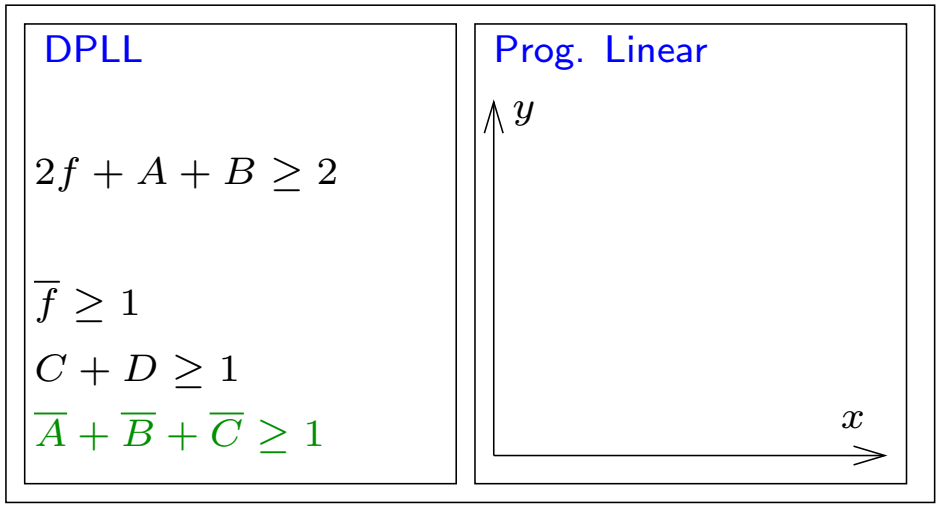


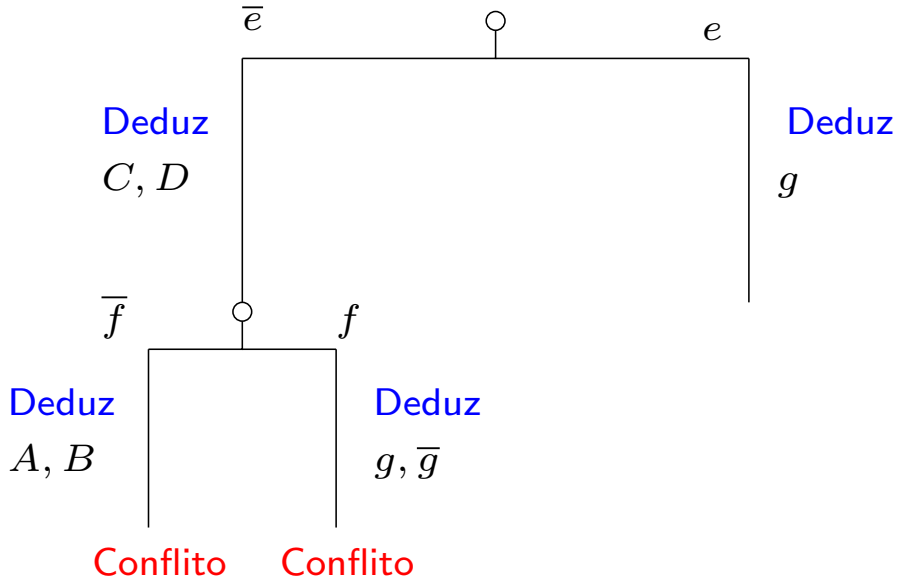
HySAT [Fränzle,Herde,2006]



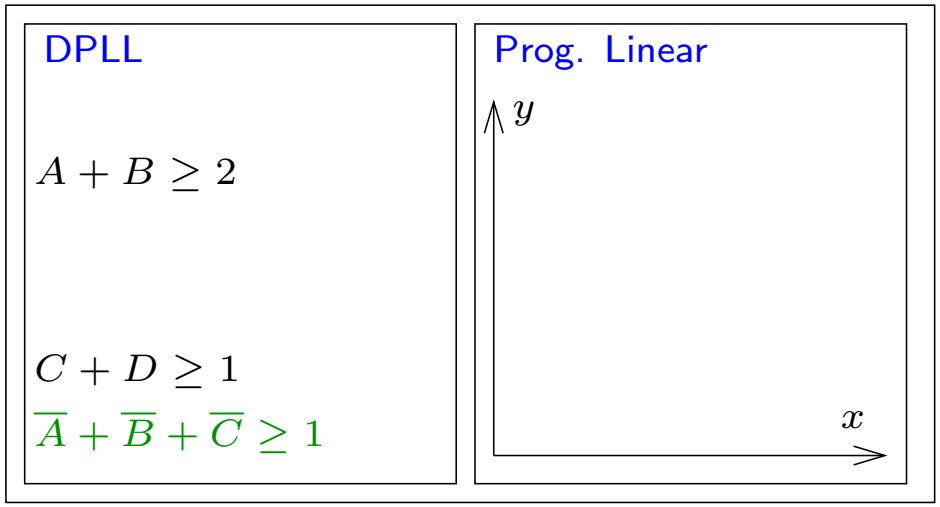


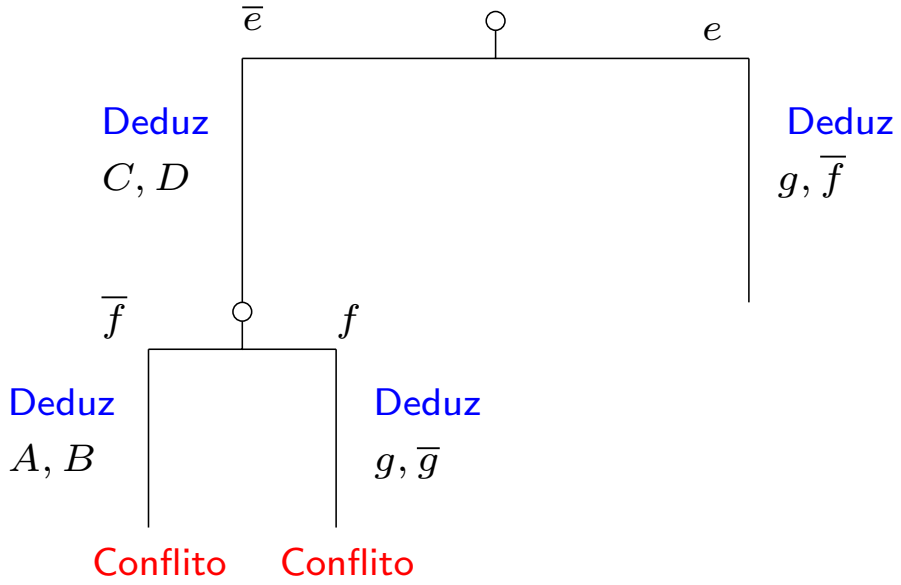
HySAT [Fränzle,Herde,2006]



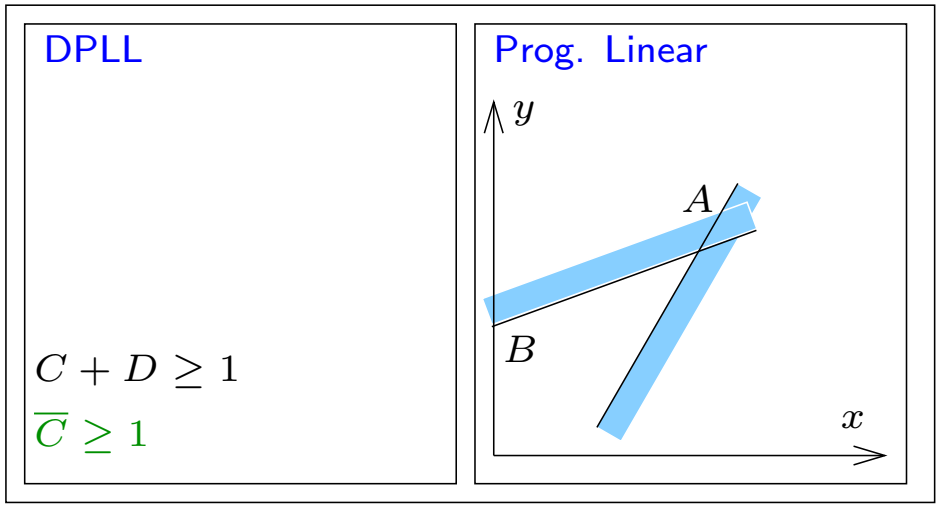


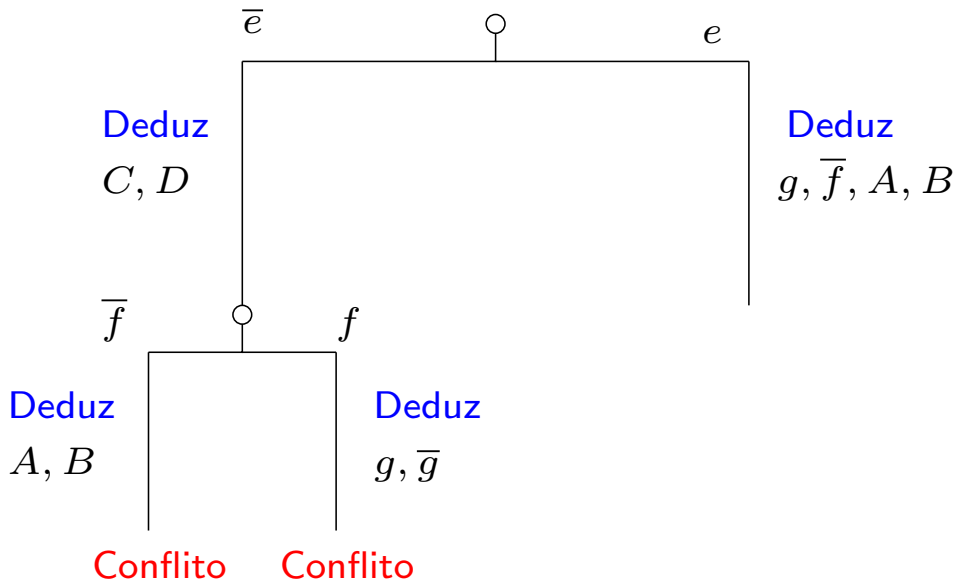
HySAT [Fränzle,Herde,2006]



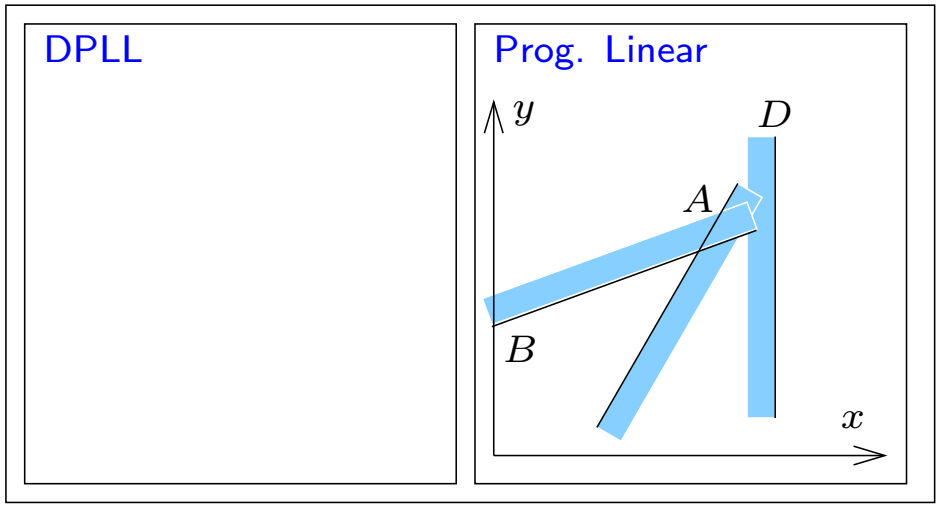


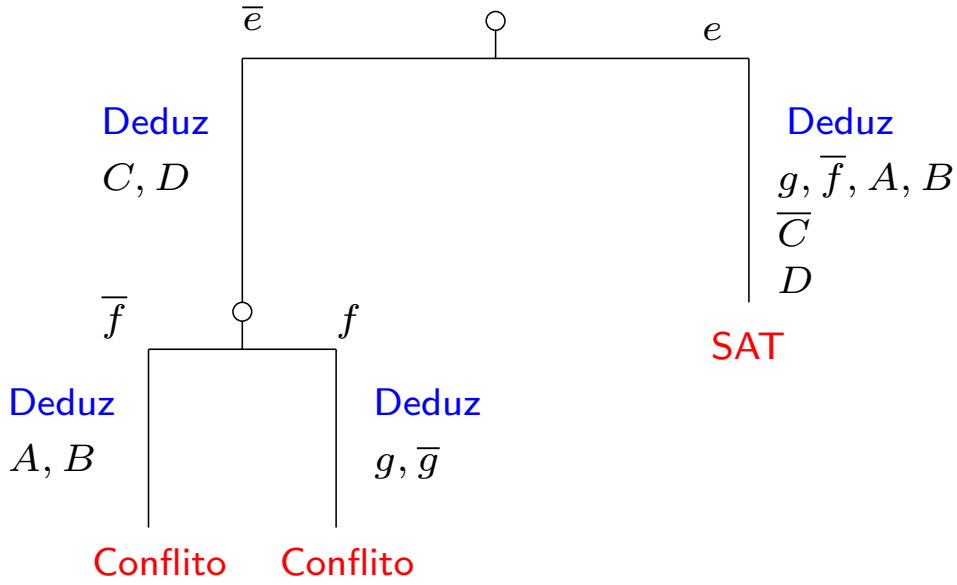
HySAT [Fränzle,Herde,2006]





HySAT [Fränzle,Herde,2006]





Conclusão

- Antigamente: Verificação exata
- Hoje: Verificação aproximada (refinamento de abstração...) e Falsificação exata