Verificação Formal em PVS do Sistema KB2D de Resolução de Conflitos de Tráfego Aéreo

André Luiz Galdino[1]

Universidade de Brasília
Departamento de Matemática

[1]Universidade Federal de Goiás
Campus de Catalão
Liberado, para cursar doutorado, pelo
Departamento de Matemática

Orientador: Mauricio Ayala-Rincón

01 de Dezembro de 2005, 3^o Seminário Informal (mas Formal!)

Plano da Apresentação

- Problema
- Solução 2-dimensional
- Descrição da Ferramenta de Verificação: PVS
- Conclusões e Trabalho Futuro

Problema

- **TCAS** - *Traffic Alert and Collision Avoidance System*.
- **RR3D** - Algoritmo de Resolução e Recuperação desenvolvido pelo *ICASE - NASA Langley Research Center*, atual NIA.
- **KB3D** - combina Mudança de Direção e Mudança de Velocidade Horizontal.

Problema

- **TCAS** - *Traffic Alert and Collision Avoidance System*.
- **RR3D** - Algoritmo de Resolução e Recuperação desenvolvido pelo *ICASE - NASA Langley Research Center*, atual NIA.
- **KB3D** - combina Mudança de Direção e Mudança de Velocidade Horizontal.

Problema

- **TCAS** - *Traffic Alert and Collision Avoidance System*.
- **RR3D** - Algoritmo de Resolução e Recuperação desenvolvido pelo *ICASE - NASA Langley Research Center*, atual NIA.
- **KB3D** - combina Mudança de Direção e Mudança de Velocidade Horizontal.

Problema

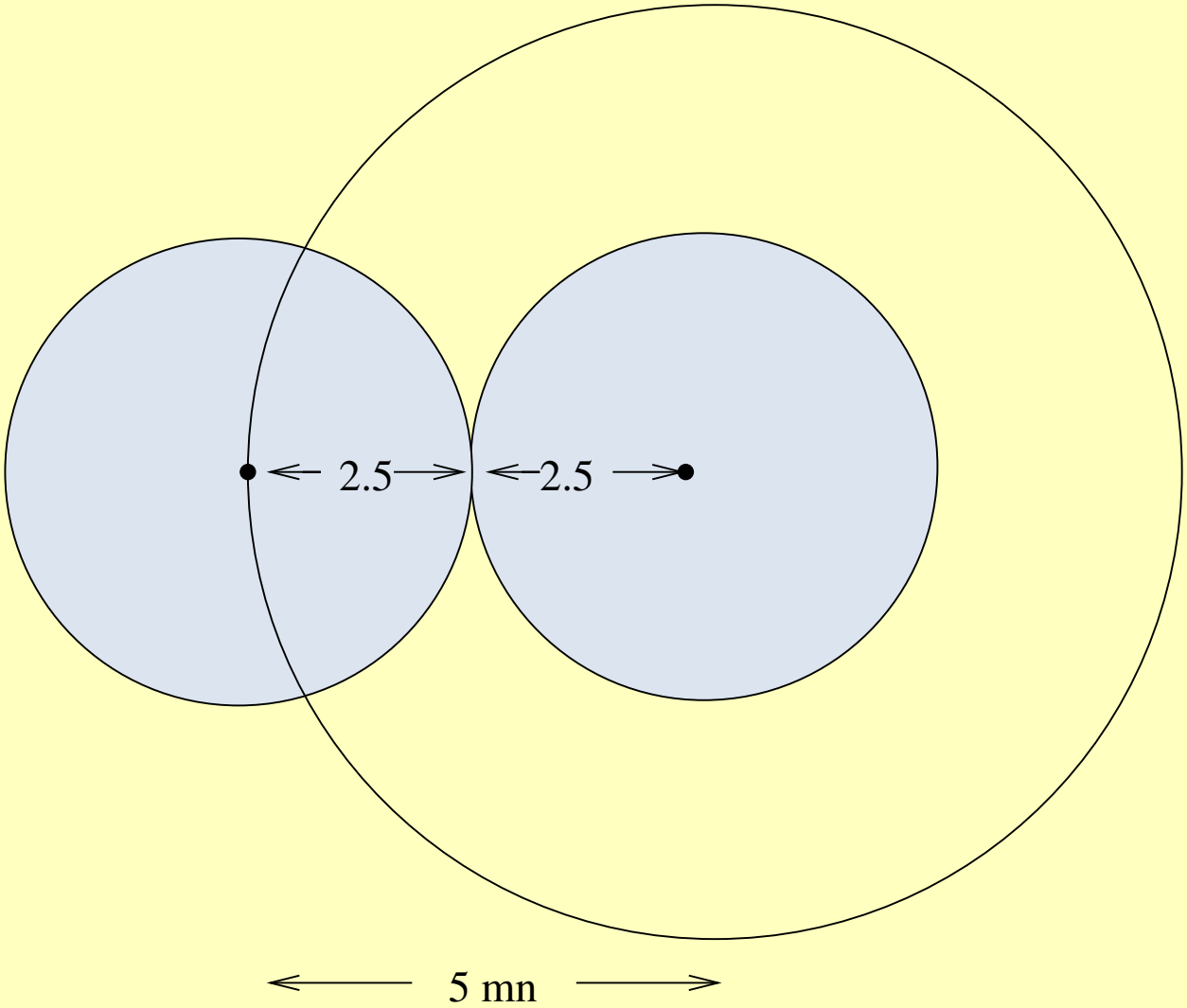
- **TCAS** - *Traffic Alert and Collision Avoidance System*.
- **RR3D** - Algoritmo de Resolução e Recuperação desenvolvido pelo *ICASE - NASA Langley Research Center*, atual NIA.
- **KB3D** - combina Mudança de Direção e Mudança de Velocidade Horizontal.

Definições e Conceitos Básicos

Figure: Zona de Exclusão e Zona de Proteção

- **Zona de Exclusão:** é um cilíndro centrada na aeronave.
- **Zona de Proteção:** é um cilíndro com o dobro das medidas da *Zona de Exclusão*.

Definições e Conceitos Básicos



Definições e Conceitos Básicos

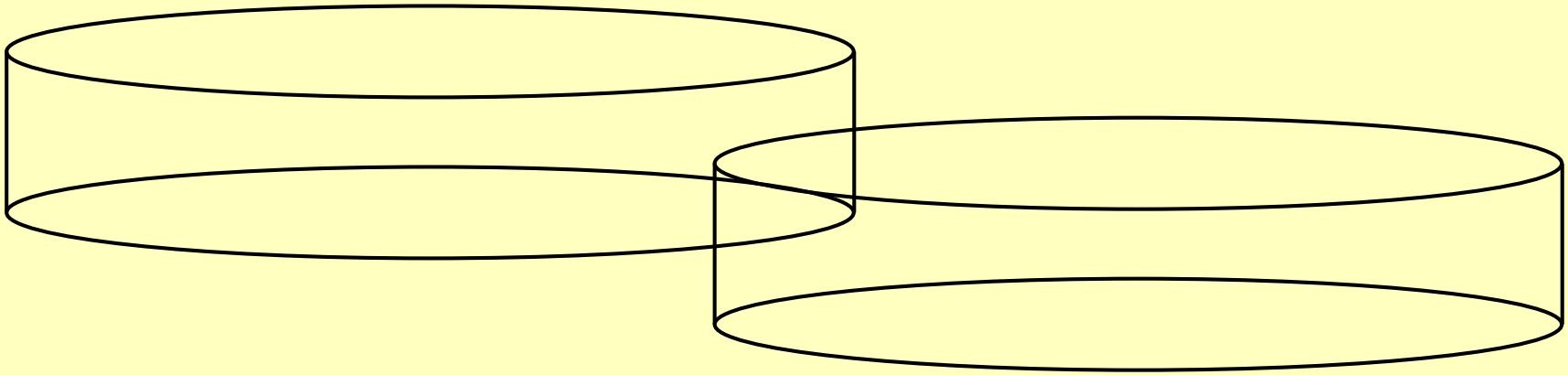
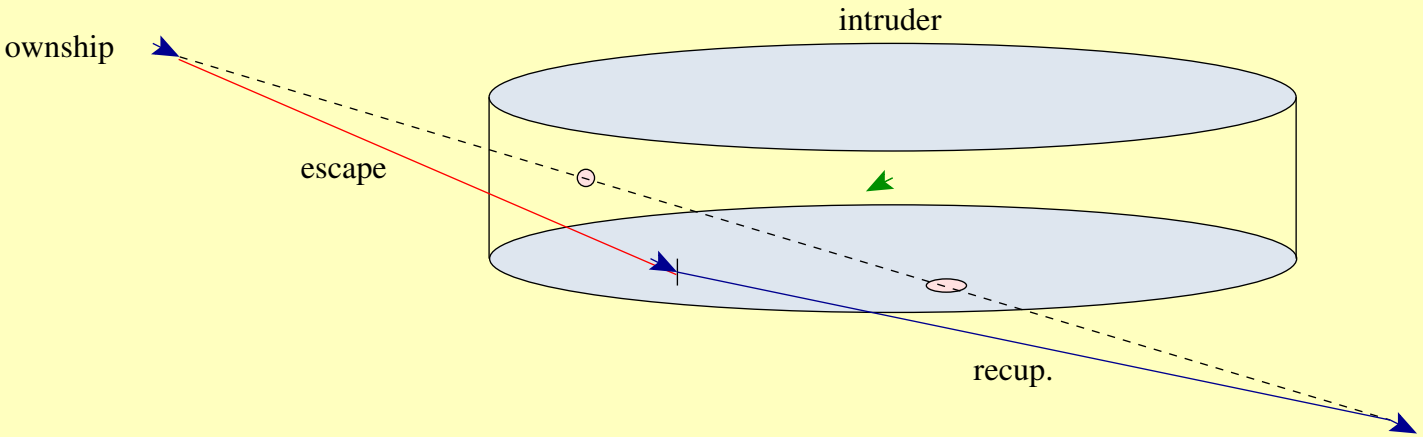


Figure: Conflito

- **Conflito:** Considera-se um conflito entre duas aeronaves a sobreposição de suas zonas de exclusão.

Definições e Conceitos Básicos



- **Trajetória de Escape** para a aeronave *ownship*, fornecida imediatamente após detectar um possível conflito com a aeronave *intruder*
- **Trajetória de Recuperação** para a aeronave *ownship* que redireciona-a ao seu caminho original, após, finalizada a trajetória de escape

Algoritmo de Detecção e Resolução de Conflitos

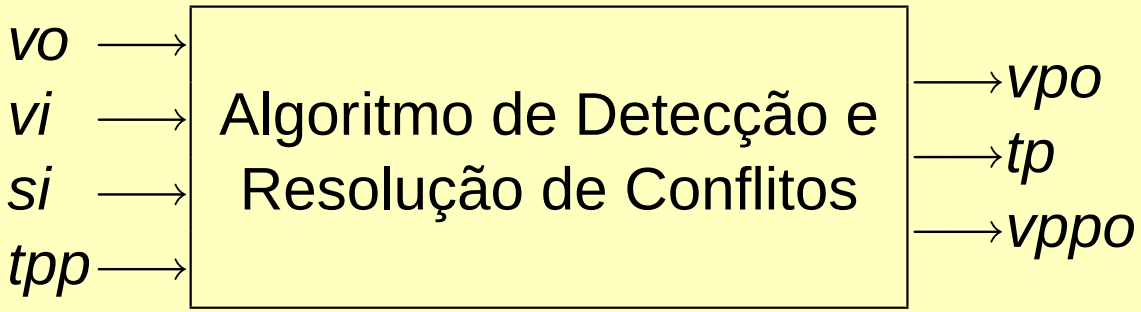
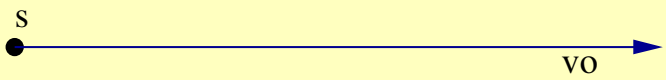
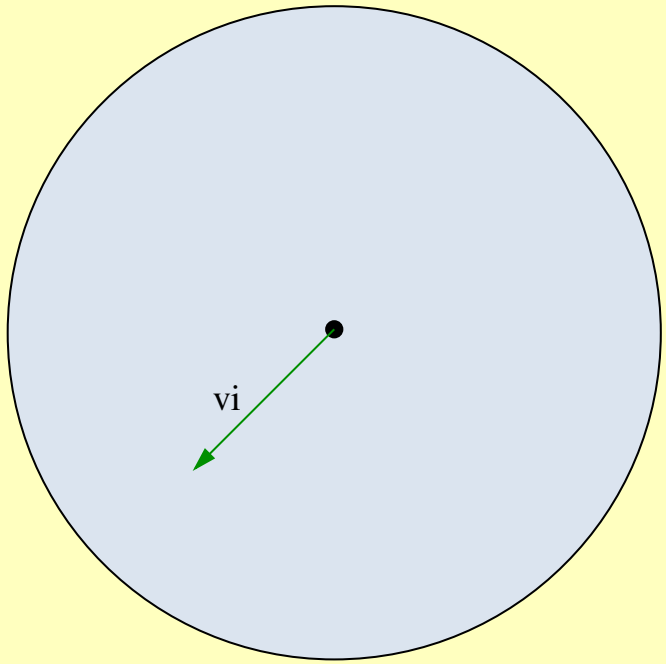


Figure: Entradas/Saídas do Algoritmo Detecção e Resolução de Conflitos

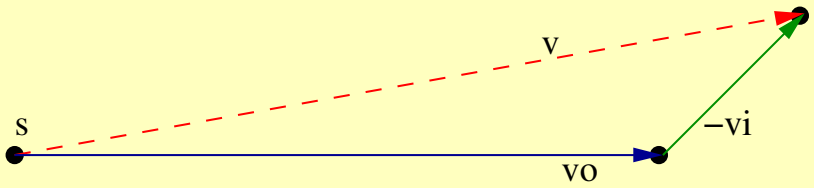
vo	Vel. do *ownship*	*vpo*	Vel. escape
vi	Vel. do *intruder*	*tp*	Tempo de troca
si	Posição do *intruder*	*vppo*	Vel. recuperação
tpp	Tempo final da trajetória		

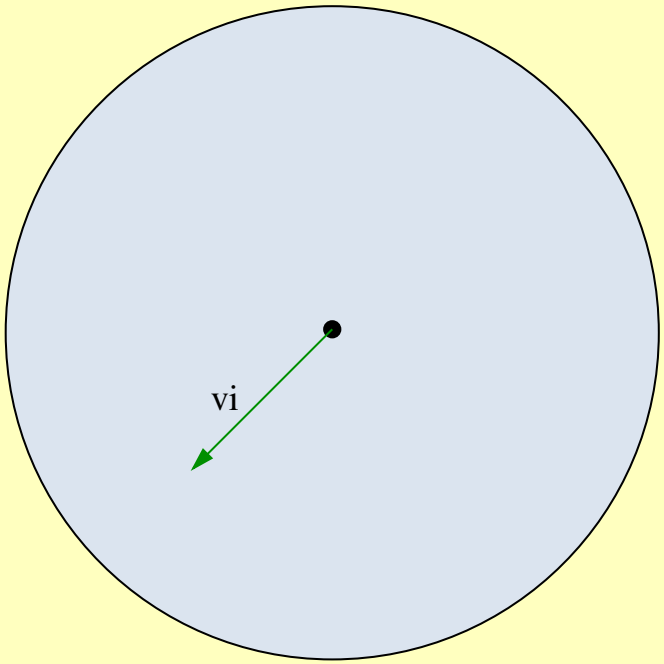
Solução Geométrica 2-dimensional



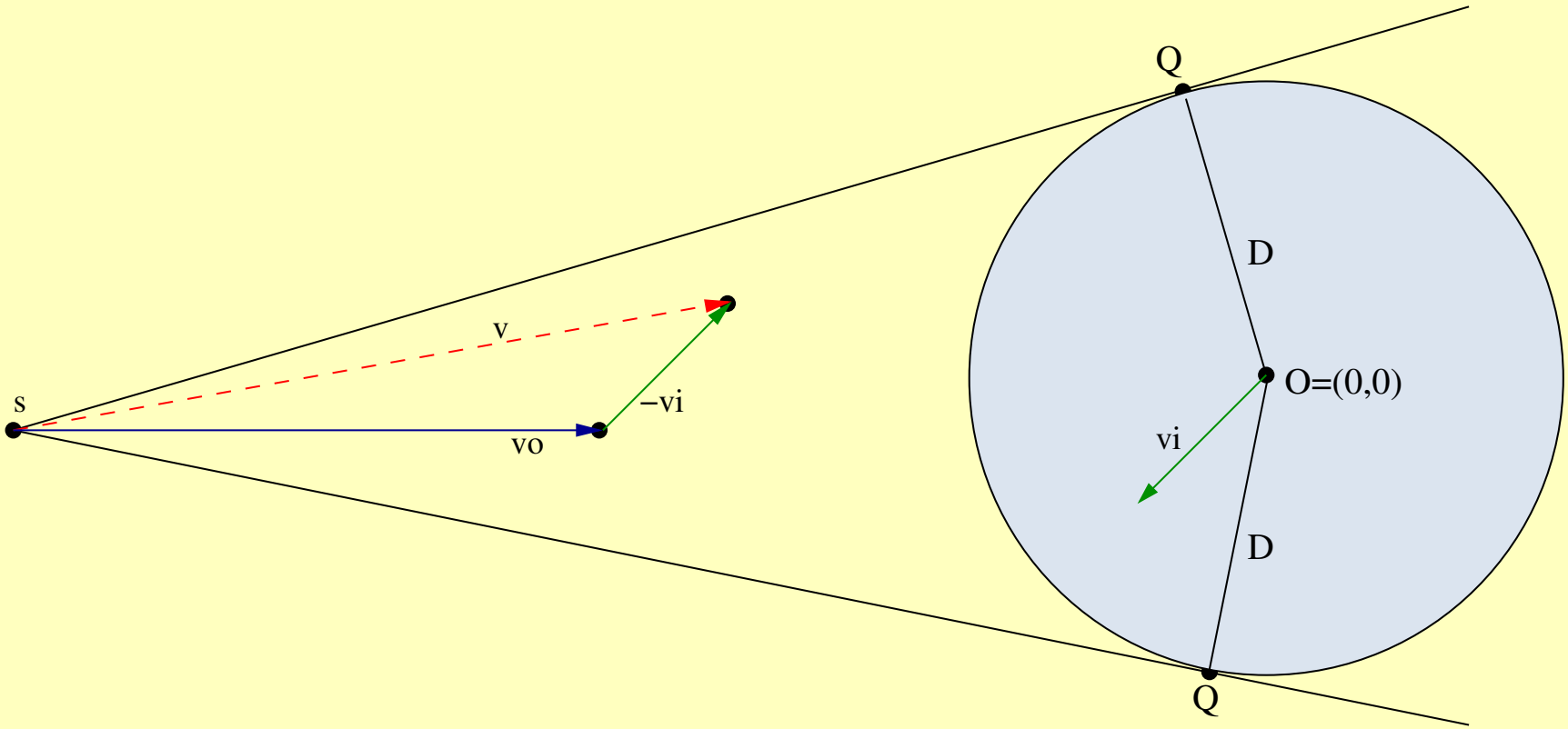


Solução Geométrica 2-dimensional

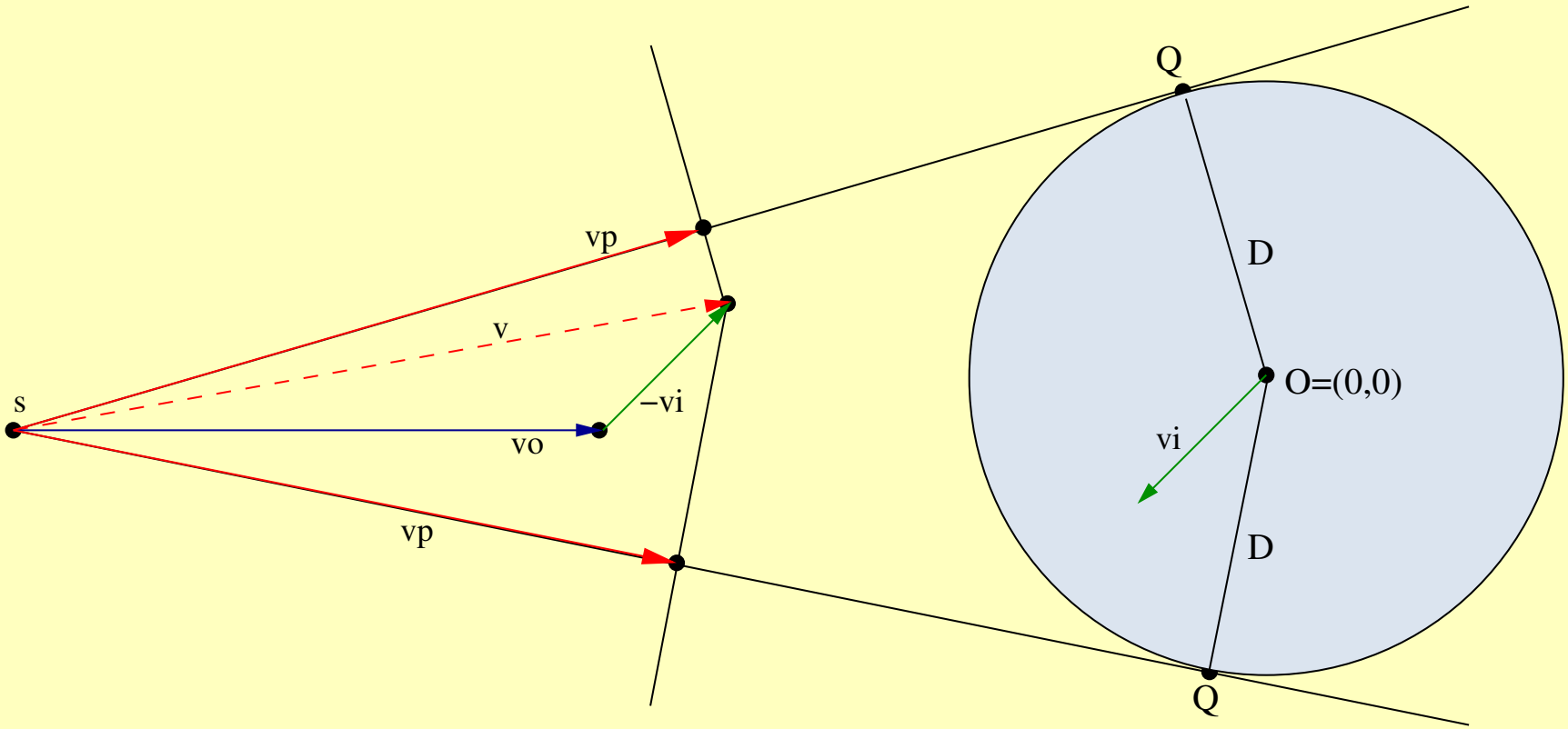




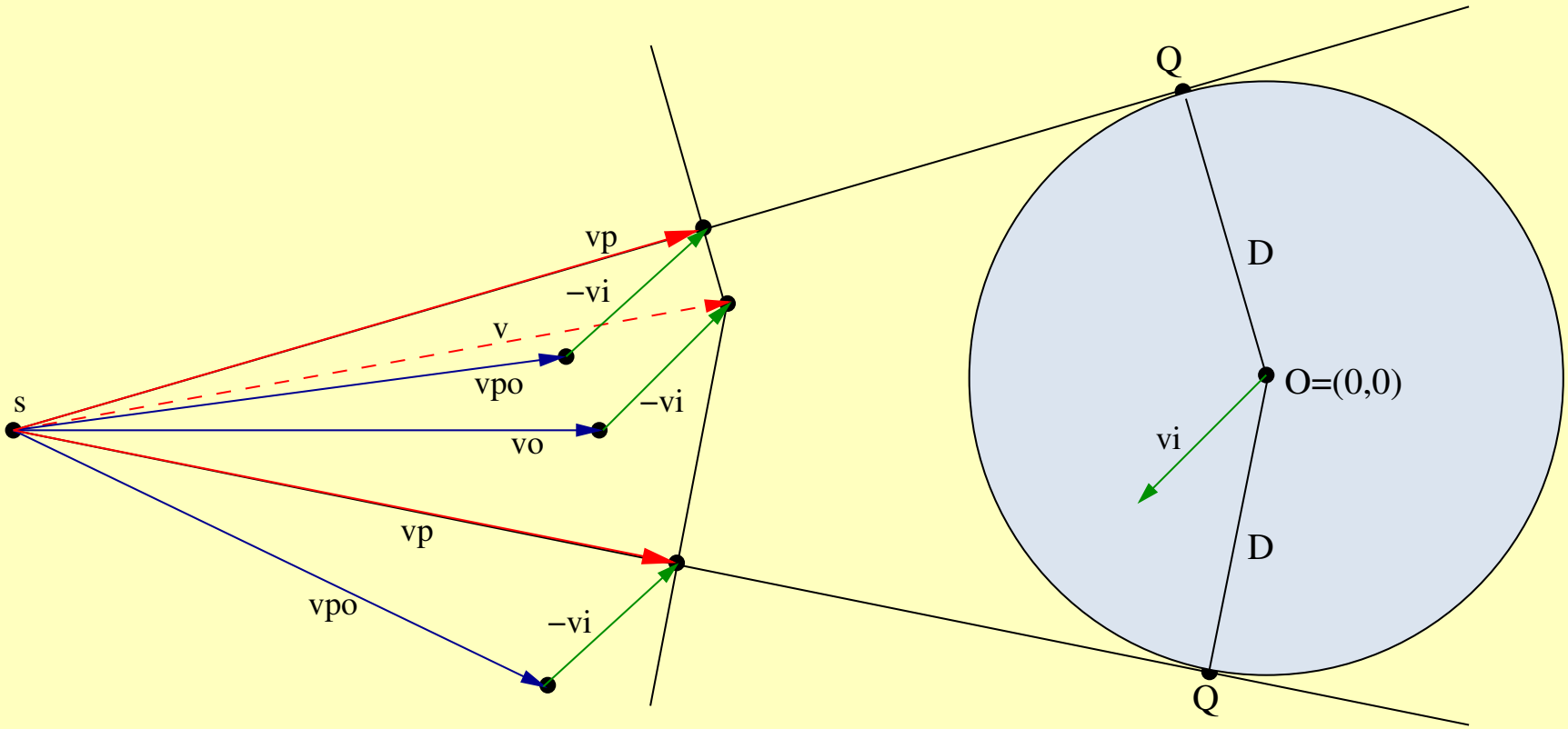
Solução Geométrica 2-dimensional



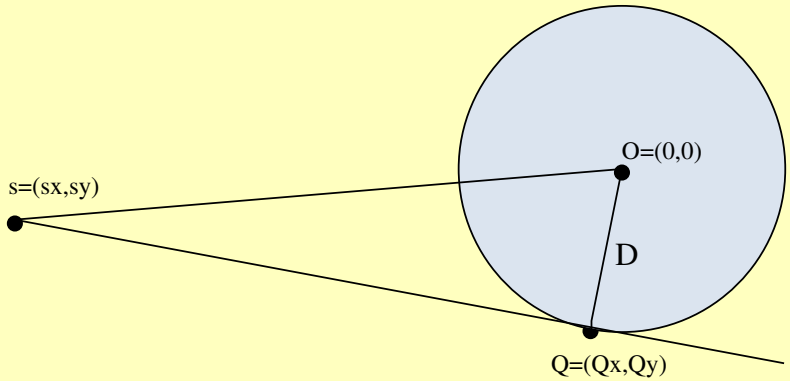
Solução Geométrica 2-dimensional



Solução Geométrica 2-dimensional



Solução Analítica



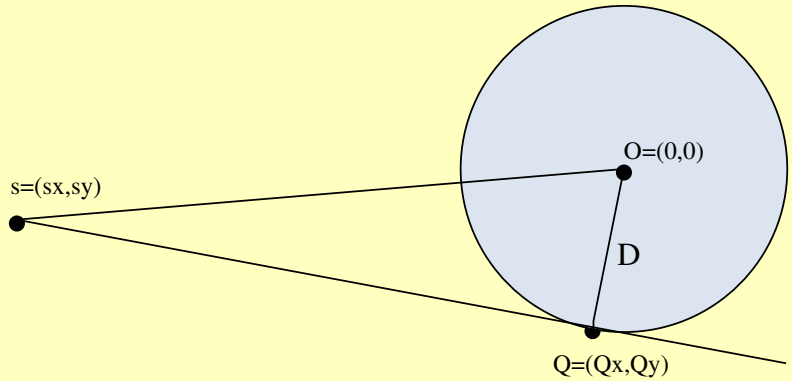
- Teorema de Pitágoras:

$$(Qx-sx)^2+(Qy-sy)^2+D^2 = sx^2+sy^2 \Rightarrow sx.Qx+sy.Qy = D^2$$

- Q ponto de tangência: $Qx^2 + Qy^2 = D^2$

$$\begin{cases} sx.Qx + sy.Qy &= D^2 \\ Qx^2 + Qy^2 &= D^2 \end{cases}$$

Solução Analítica



- Teorema de Pitágoras:

$$(Qx-sx)^2+(Qy-sy)^2+D^2 = sx^2+sy^2 \Rightarrow sx.Qx+sy.Qy = D^2$$

- Q ponto de tangência: $Qx^2 + Qy^2 = D^2$

$$\begin{cases} sx.Qx + sy.Qy &= D^2 \\ Qx^2 + Qy^2 &= D^2 \end{cases}$$

Solução Analítica

Após algumas simplificações e fazendo

- $alpha = \frac{D^2}{sx^2+sy^2}$
- $beta = \frac{D\sqrt{sx^2+sy^2-D^2}}{sx^2+sy^2}$

obtemos, com $eps = 1, -1$:

- $Qx(eps) = alpha.sx + eps.beta.sy$
- $Qy(eps) = alpha.sy - eps.beta.sx$

Solução Analítica

Após algumas simplificações e fazendo

- $alpha = \frac{D^2}{sx^2+sy^2}$
- $beta = \frac{D\sqrt{sx^2+sy^2-D^2}}{sx^2+sy^2}$

obtemos, com $eps = 1, -1$:

- $Qx(eps) = alpha.sx + eps.beta.sy$
- $Qy(eps) = alpha.sy - eps.beta.sx$

Solução Analítica

Após algumas simplificações e fazendo

- $alpha = \frac{D^2}{sx^2+sy^2}$
- $beta = \frac{D\sqrt{sx^2+sy^2-D^2}}{sx^2+sy^2}$

obtemos, com $eps = 1, -1$:

- $Qx(eps) = alpha.sx + eps.beta.sy$
- $Qy(eps) = alpha.sy - eps.beta.sx$

Solução Analítica

Após algumas simplificações e fazendo

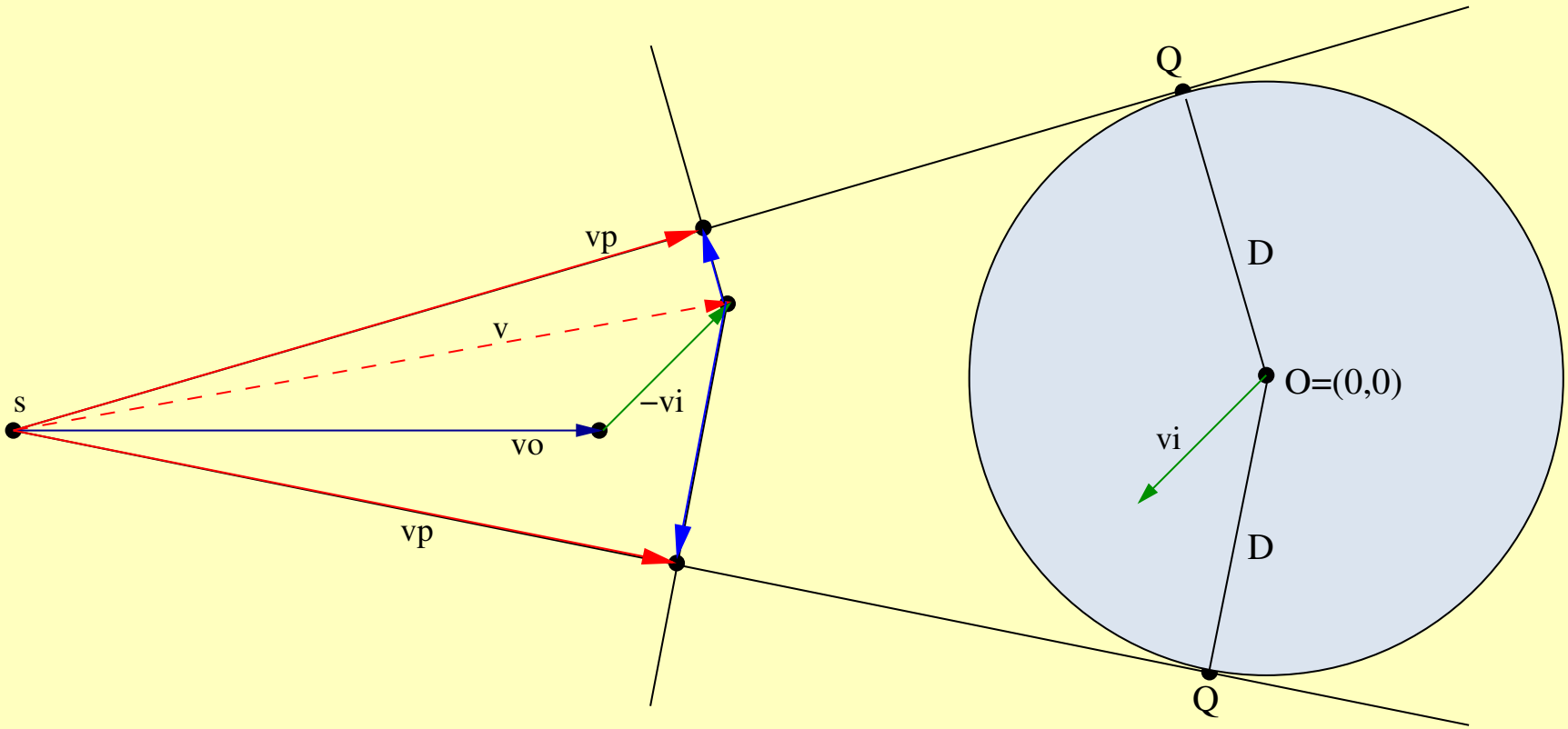
- $alpha = \frac{D^2}{sx^2+sy^2}$
- $beta = \frac{D\sqrt{sx^2+sy^2-D^2}}{sx^2+sy^2}$

obtemos, com $eps = 1, -1$:

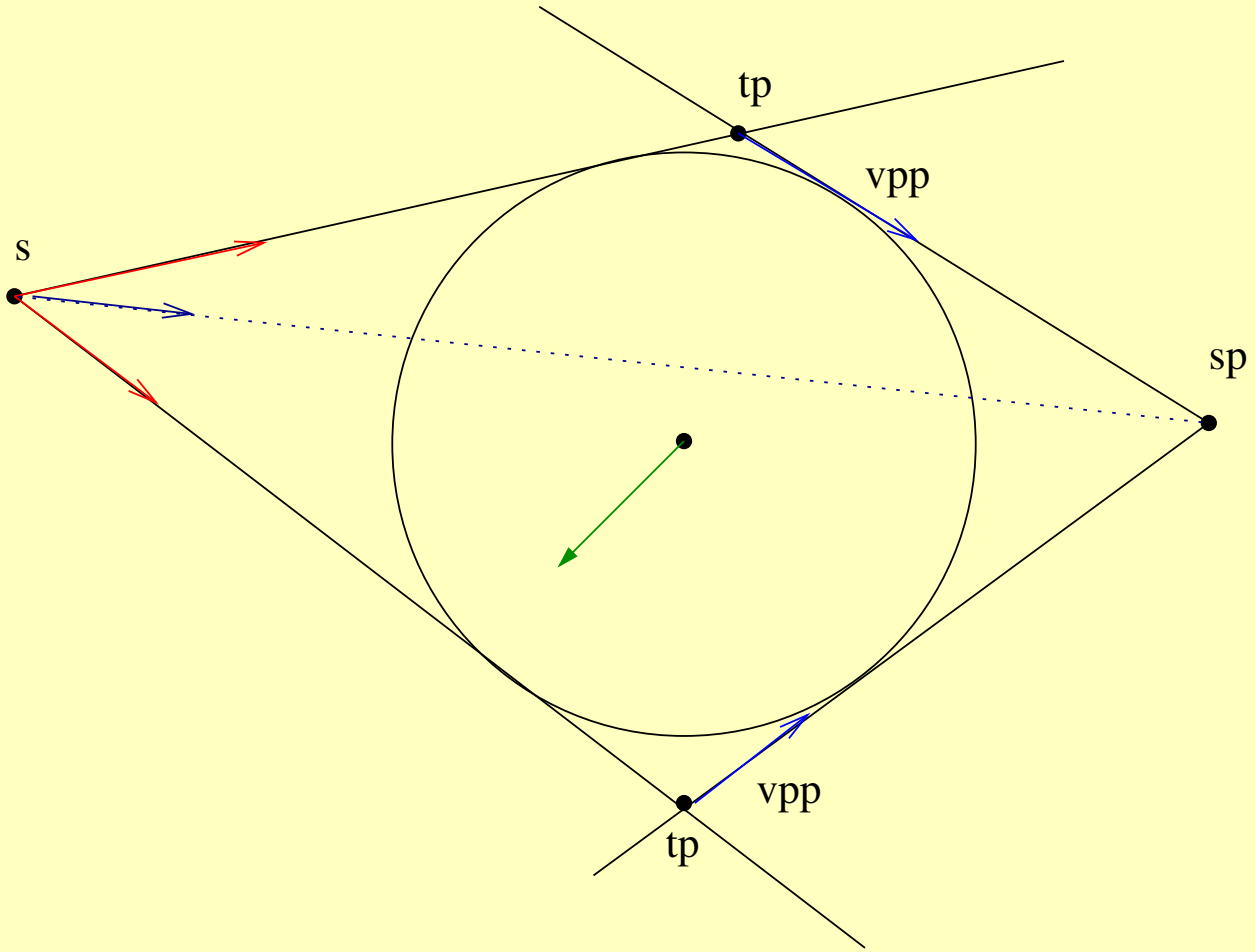
- $Qx(eps) = alpha.sx + eps.beta.sy$
- $Qy(eps) = alpha.sy - eps.beta.sx$

Solução Analítica

Observe que: $\begin{cases} vp &= t.(Q-s) \\ vp \cdot u &= 0 \end{cases}$



Solução Geométrica e Analítica (Recuperação)



$$\vec{v}pp = \frac{1}{tpp - tp}(tp\vec{p}v - tpp\vec{v})$$

O que é PVS?

- O PVS (Prototype Verification System) é um ambiente para especificação e verificação interativa semi-automática desenvolvido, por volta da década de 80, pelo SRI International Computer Science Laboratory;
- O PVS oferece estratégias para provar teoremas não-triviais passo a passo e cada passo que o sistema oferece é logicamente correto;
- O usuário tem que selecionar o comando apropriadamente e fornecer argumentos.

O que é PVS?

- O PVS (Prototype Verification System) é um ambiente para especificação e verificação interativa semi-automática desenvolvido, por volta da década de 80, pelo SRI International Computer Science Laboratory;
- O PVS oferece estratégias para provar teoremas não-triviais passo a passo e cada passo que o sistema oferece é logicamente correto;
- O usuário tem que selecionar o comando apropriadamente e fornecer argumentos.

De que consiste o PVS?

- uma linguagem de especificação baseada sobre lógica de ordem superior fortemente tipada;
- um provador interativo de teoremas baseado sobre cálculo sequente:

$$\Sigma \vdash_\Gamma \Delta$$

Σ: antecedentes (com rótulo negativo);
Δ:consequentes (com rótulo positivo);
Γ: Contexto.

- uma biblioteca de especificações (teorias) com definições e lemas.

De que consiste o PVS?

- uma linguagem de especificação baseada sobre lógica de ordem superior fortemente tipada;
- um provador interativo de teoremas baseado sobre cálculo sequente:

$$\Sigma \vdash_\Gamma \Delta$$

Σ: antecedentes (com rótulo negativo);
Δ:consequentes (com rótulo positivo);
Γ: Contexto.

- uma biblioteca de especificações (teorias) com definições e lemas.

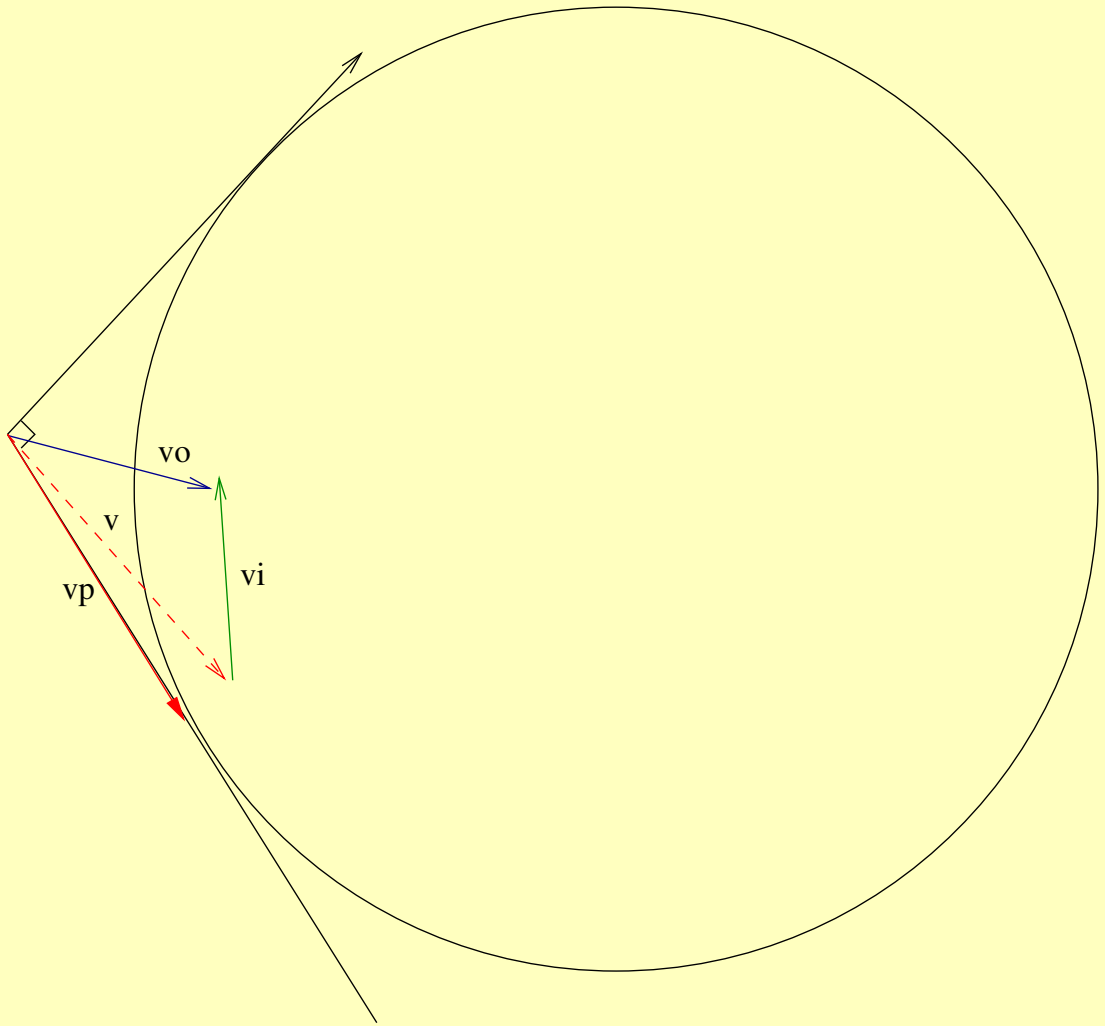
De que consiste o PVS?

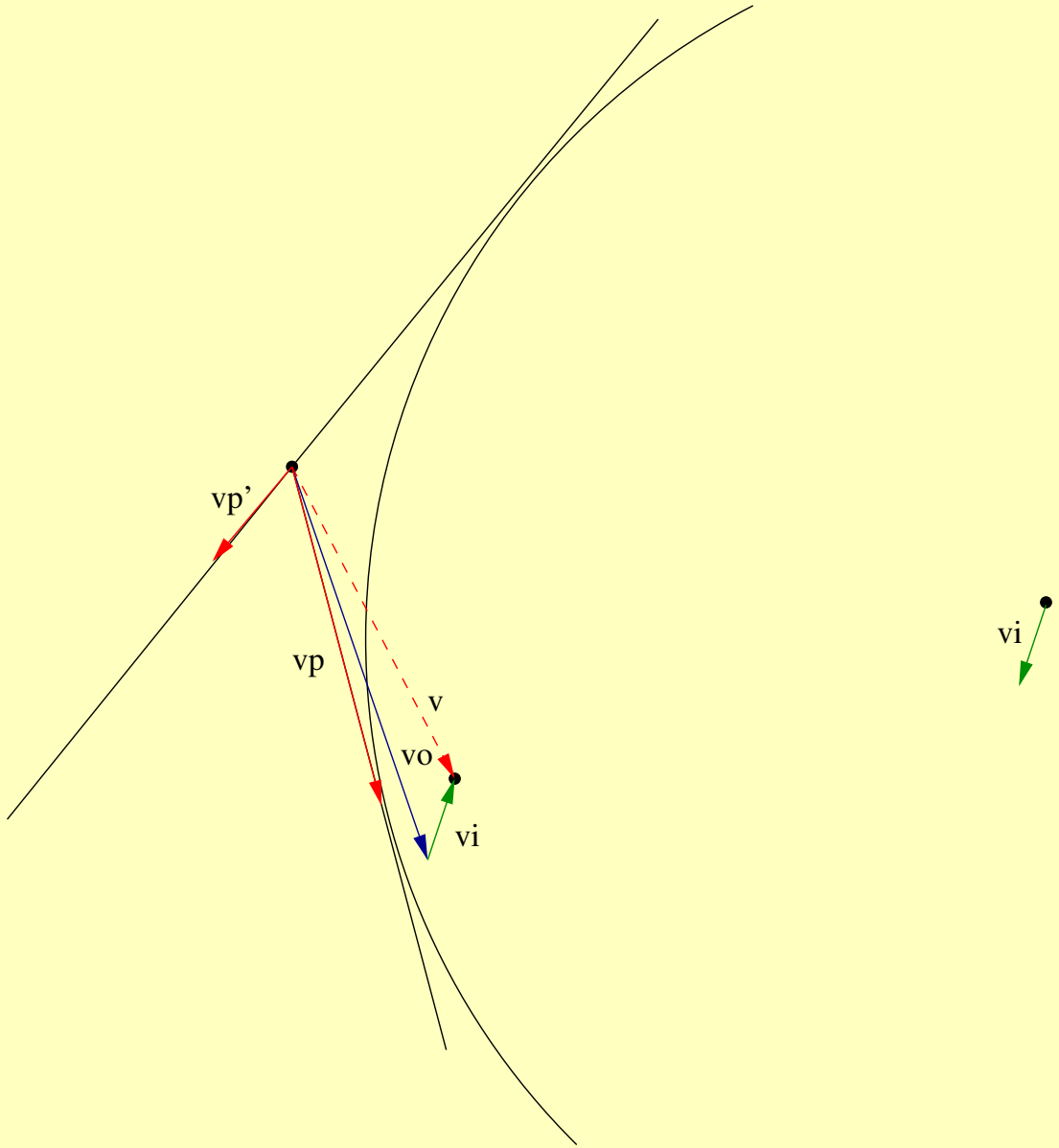
- uma linguagem de especificação baseada sobre lógica de ordem superior fortemente tipada;
- um provador interativo de teoremas baseado sobre cálculo sequente:

$$\Sigma \vdash_\Gamma \Delta$$

Σ: antecedentes (com rótulo negativo);
Δ:consequentes (com rótulo positivo);
Γ: Contexto.

- uma biblioteca de especificações (teorias) com definições e lemas.


vo
v
vi
vp


vp'
vp
v
vo
vi
vi

Conclusão e Trabalhos Futuros

- Fez-se as provas geométricas e analíticas do sistema KB2D;
- Fez-se a verificação formal em PVS do sistema KB2D (Escape);
- Resta fazer a verificação formal em PVS do sistema KB2D (Recuperação);
- Desenvolvimento de estratégias de prova da teoria de reescrita no sistema PVS.

Conclusão e Trabalhos Futuros

- Fez-se as provas geométricas e analíticas do sistema KB2D;
- Fez-se a verificação formal em PVS do sistema KB2D (Escape);
- Resta fazer a verificação formal em PVS do sistema KB2D (Recuperação);
- Desenvolvimento de estratégias de prova da teoria de reescrita no sistema PVS.

Conclusão e Trabalhos Futuros

- Fez-se as provas geométricas e analíticas do sistema KB2D;
- Fez-se a verificação formal em PVS do sistema KB2D (Escape);
- Resta fazer a verificação formal em PVS do sistema KB2D (Recuperação);
- Desenvolvimento de estratégias de prova da teoria de reescrita no sistema PVS.

Conclusão e Trabalhos Futuros

- Fez-se as provas geométricas e analíticas do sistema KB2D;
- Fez-se a verificação formal em PVS do sistema KB2D (Escape);
- Resta fazer a verificação formal em PVS do sistema KB2D (Recuperação);
- Desenvolvimento de estratégias de prova da teoria de reescrita no sistema PVS.

Conclusão e Trabalhos Futuros

- Fez-se as provas geométricas e analíticas do sistema KB2D;
- Fez-se a verificação formal em PVS do sistema KB2D (Escape);
- Resta fazer a verificação formal em PVS do sistema KB2D (Recuperação);
- Desenvolvimento de estratégias de prova da teoria de reescrita no sistema PVS.

Referências

- V.A. Fernandes. *Detecção e Resolução Formal de Conflitos de Tráfego Aéreo*. Dissertação de Mestrado, Departamento de Matemática, Universidade de Brasília, 2004.
- A. Geser, C. Muñoz and G. Dowek and F. Kirchner. *Air Traffic Conflict Resolution and Recovery*. ICASE Report 2002-12, ICASE, NASA, Langley Research Center, Hampton, Virginia, 2002.
- A. Geser, C. Muñoz and G. Dowek. *Tatical Conflict Detection and Resolution in a 3-D Airspace*. ICASE Report 2001-7, ICASE, NASA, Langley Research Center, Hampton, Virginia, 2001.
- J. Maddalon, R. Butler, A. Geser and C. Muñoz. *Formal Verification of a Conflict Resolution and Recovery Algorithm*. NASA/TP-2004-213015, NASA Langley Research Center, Hampton, Virginia, 2004.
- S. Owre and N. Shankar. *The formal semantics of PVS*. Technical Report SRI-CSL-97-2, Computer Science Laboratory, SRI International, Menlo Park, CA, August 1997.
- N. Shankar, S. Owre, J. M. Rushby, and D. W. J. Stringer-Calvert. *PVS Prover Guide*. Computer Science Laboratory, SRI International, Menlo Park, CA, September 1999.