UNIVERSIDADE FEDERAL DE SANTA CATARINA
PROGRAMA DE PÓS-GRADUAÇÃO
EM ENGENHARIA ELÉTRICA

UMA METODOLOGIA FORMAL PARA O PLANEJAMENTO E CONTROLE DE MISSÕES DE AERONAVES NÃO-TRIPULADAS

Tese submetida à
Universidade Federal de Santa Catarina
como parte dos requisitos para a
obtenção do grau de Doutor em Engenharia Elétrica.

Conrado Werner Seibel

Florianópolis, novembro de 2000.

UMA METODOLOGIA FORMAL PARA O PLANEJAMENTO E CONTROLE DE MISSÕES DE AERONAVES NÃO-TRIPULADAS

Conrado Werner Seibel

'Esta Tese foi julgada adequada para obtenção do título de Doutor em Engenharia Elétrica, Área de Concentração em Sistemas de Informação, e aprovada em sua forma final pelo Programa de Pós-Graduação em Engenharia Elétrica da Universidade Federal de Santa Catarina.'

Prof. Jean-Marie Farines, Dr.

Orientador

Prof. Aguinaldo Silveira e Silva, PhD

Coordenador do Programa de Pós-Graduação em Engenharia Elétrica

Banca Examinadora:

Prof. Celso A. A. Kaestner, Dr.

Presidente

Prof. Alfredo Olivero, Dr.

Prof. José E. R. Cury, Dr.

Prof. Guilherme Bittencourt, Dr. Ing.

Eng. Edison Modesto Penna, MSc

Resumo da Tese apresentada à UFSC como parte dos requisitos necessários para a obtenção do grau de Doutor em Engenharia Elétrica.

UMA METODOLOGIA FORMAL PARA O PLANEJAMENTO E CONTROLE DE MISSÕES DE AERONAVES NÃO-TRIPULADAS

Conrado Werner Seibel

Novembro 2000

Orientador: Prof. Jean-Marie Farines, Dr.

Área de Concentração: Sistemas de Informação.

Palavras-chave: aeronaves não-tripuladas, veículos autônomos, planejamento de missões, controle de missões, sistemas híbridos, autômatos híbridos.

Número de páginas: 120.

Este trabalho descreve uma metodologia formal que objetiva garantir que aeronaves não-tripuladas, quando operando de forma autônoma, apresentem um comportamento condizente com os objetivos da missão durante toda a duração da missão e, se impedidas de exibir tal comportamento, minimizam as conseqüências desta falha. Na fase de *planejamento da missão*, autômatos híbridos lineares são usados para modelar a aeronave utilizada e os recursos necessários à execução de uma missão (condições internas), o ambiente no qual a missão será realizada (condições externas) e um plano de vôo condizente com os objetivos da missão. O modelo resultante é utilizado para a construção de um plano de vôo contendo uma estratégia primária para a consecução dos objetivos da missão e comportamentos alternativos para todas as situações passíveis de serem encontradas durante a realização da missão. Durante a *execução da missão*, um controlador de vôo reativo a bordo da aeronave é utilizado para selecionar um comportamento adequado com base no progresso da missão, no ambiente no qual a aeronave está operando e no estado interno da mesma.

Abstract of Thesis presented to UFSC as a partial fulfillment of the requirements for the degree of Doctor in Electrical Engineering.

A FORMAL METHODOLOGY FOR MISSION PLANNING AND CONTROL OF UNMANNED AERIAL VEHICLES

Conrado Werner Seibel

November 2000

Advisor: Prof. Jean-Marie Farines, Dr.

Area of Concentration: Information Systems.

Keywords: unmanned aerial vehicles, autonomous vehicles, mission planning, hybrid systems, hybrid automata

Number of pages: 120.

This work describes a formal methodology for mission planning and control for unmanned aerial vehicles. Aircraft executing flight plans developed with our methodology are guaranteed to comply with the mission objectives at all times. If, for any reason, the flight plan fails, it will fail in a controlled way. During *mission planning*, we use linear hybrid automata to model the chosen aircraft, the resources needed to perform a mission and the environment in which the aircraft will operate. We use the terms "internal conditions" for the first two and "external conditions" for the last one. We also model the flight plan itself with hybrid automata. The resulting model is used to construct *complete flight plans*. A complete flight plan contains a *primary flight plan*, aimed at achieving the mission objectives, and a set of *alternative flight plans* for all the possible situations that the aircraft could encounter during the execution of the mission. During *mission execution*, a reactive, on-board flight controller is used to select the most appropriate behavior based on mission progress, external events from the environment where the aircraft is operating and the aircraft's internal status.

Sumário

Lista de Figuras

Capítulo 1

Introdução

Este capítulo apresenta o contexto e a motivação para o desenvolvimento de uma metodologia para o planejamento e controle de missões para aeronaves não-tripuladas. O capítulo também descreve brevemente o problema a ser resolvido, bem como os objetivos e a proposta do presente trabalho. O capítulo encerra com uma descrição do conteúdos dos capítulos subseqüentes.

1.1 Contexto e motivação

Veículos aéreos não-tripulados (UAVs—*Unmanned Aerial Vehicles*) tem sido usados por forças militares para fins de reconhecimento há mais de trinta anos [1]. Mais recentemente, as vantagens inerentes a este tipo de aeronave, principalmente ausência de risco para vidas humanas e baixo custo operacional, atraíram a atenção de usuários civis. As aplicações desenvolvidas vão desde operações de segurança pública e monitoração ecológica [2] à pesquisa científica em alta altitude [3].

A grande maioria dos sistemas desenvolvidos até o presente é baseada em aeronaves de asas fixas (aviões). Isto, não apenas porque aplicações militares requerem alta velocidade à frente, grande raio operacional e baixa assinatura acústica, mas também porque aviões podem ser projetados de forma a se comportarem de forma inerentemente estável e são, portanto, comparativamente fáceis de pilotar a partir de uma estação de controle em terra.

Aplicações civis de UAVs, entretanto, apresentam requisitos diferentes. O mais importante deles é, certamente, a capacidade de decolagem, pouso e operação em áreas restritas e em baixa velocidade, incluindo o vôo pairado. Aeronaves não-tripuladas de asas rotativas (helicópteros), capazes de vôo pairado e decolagem e pouso verticais, adequam-se bem a estes requerimentos. Diferentes veículos e sistemas de controle foram amplamente descritos em, por exemplo, [2, 4, 5, 6, 7, 8].

Diversas ferramentas para o planejamento de missões de aeronaves tripuladas usadas para combate, patrulhamento e transporte foram desenvolvidas [9, 10, 11]. Tais ferramentas procuram maximizar a eficiência do uso da aeronave e, ao mesmo tempo, minimizar sua exposição a ações hostis. Algumas ferramentas, como a descrita em [11], objetivam ainda harmonizar a operação conjunta de aeronaves de diferentes características.

Ferramentas de análise de desempenho de UAVs [12] também foram desenvolvidas com o objetivo de examinar quais as características de uma aeronave que mais influenciam o seu desempenho na realização de certos tipos de missão. Estas ferramentas, por sua própria natureza, são utilizadas na fase de estudos que precede o desenvolvimento de novos veículos.

Estações de controle para aeronaves não-tripuladas como as descritas em [13, 14, 15] preocupam-se principalmente em apresentar informações ao operador, delegando a este a responsabilidade da tomada de decisões. O uso crescente de aeronaves não-tripuladas nas forças armadas dos Estados Unidos da América levou o Pentágono a financiar o desenvolvimento de uma ferramentas mais moderna, a *Tactical Unmanned Control Station*. Esta ferramenta apresenta recursos para construção de planos de vôo e permite a verificação de alguns parâmetros básicos como alcance e altitude.

A perda de aeronaves não-tripuladas em decorrência de erros de operação é um dos maiores problemas associados com este tipo de veículo, tendo mesmo causado o cancelamento de alguns programas de desenvolvimento [16]. O esgotamento de combustível durante a execução de uma missão é citado pelas forças armadas norte-americanas como causa bastante comum de acidentes envolvendo aeronaves UAVs. Este dado ilustra a complexidade da tarefa de balancear dois requisitos conflitantes: utilização eficiente da aeronave a fim de maximizar as possibilidades de sucesso da missão e operação conservadora da mesma a fim de maximizar sua vida útil.

1.2 Objetivo e proposta

Os fatores a serem levados em conta quando do planejamento e execução de missões por UAVs em aplicações civis são bastante distintos daqueles levados em consideração pelos sistemas referenciados na seção anterior: ferramentas de planejamento e controle de missões para usuários civis devem basicamente aumentar a segurança da utilização do equipamento e reduzir seu custo operacional ao facilitar sua operação, reduzindo assim os investimentos necessários ao treinamento e qualificação do operador, sem prejuízo da utilização eficiente do equipamento.

O objetivo deste trabalho é desenvolver uma metodologia que permita a construção de planos de vôo que, quando executados autonomamente por uma aeronave não-tripulada, satisfaçam critérios de *conformidade com os objetivos da missão* e *robustez*, critérios estes adaptados de [17] e comumente utilizados em sistemas de alta segurança. Uma aeronave não-tripulada que executa um plano de vôo com estas características, possui um comportamento condizente com os objetivos da missão durante toda a missão e, se impedida de exibir este comportamento, minimiza as conseqüências desta falha.

Neste trabalho propõe-se resolver o problema de planejamento e controle de missões para aeronaves não-tripuladas através da:

modelagem da aeronave, do seu ambiente de operações e dos recursos necessários à realização da missão;

verificação formal de planos de vôo de forma a garantir sua exeqüibilidade;

controle reativo da missão, selecionando planos de vôo alternativos adequados à situação encontrada pela aeronave durante a realização da missão.

A completa automatização do processo de planejamento e controle de missões de aeronaves não-tripuladas será, sem dúvida alguma, de grande utilidade prática. Apesar de não ser este o objetivo do presente trabalho, esta idéia esteve sempre presente durante a realização do mesmo e foi utilizada como critério para seleção de alternativas quando as mesmas se apresentaram.

Similarmente, a modelagem de aeronaves não-tripuladas concentrou-se em características típicas desta classe de aeronaves, sem ambição de ser completa. Acreditamos que as técnicas de modelagem apresentadas sejam suficientemente genéricas para permitir a modelagem de parâmetros e recursos além dos adotados neste trabalho.

Sem comprometimento do descrito no parágrafo anterior, deu-se maior ênfase no trabalho a aeronaves não-tripuladas de asas rotativas pois as mesmas apresentam maior número de graus de liberdade que aeronaves de asas fixas. Todo o trabalho desenvolvido, entretanto, independe desta característica e é aplicável a ambos os tipos de aeronave.

1.3 Organização do texto

O capítulo 2 introduz aspectos relevantes de aeronaves não-tripuladas de asas rotativas e descreve o problema de planejamento e controle de missões para esta classe de aeronaves.

O capítulo 3 apresenta a proposta deste trabalho: a construção e verificação de planos de vôo para aeronaves não-tripuladas com o auxílio de autômatos híbridos lineares, o controle de missão baseado em um sistema reativo e sua interação em tempo real com o sistema contínuo responsável pela pilotagem, guiagem e navegação da aeronave. Este capítulo também discute as hipóteses necessárias para a realização da metodologia proposta.

O capítulo 4 descreve a utilização de autômatos híbridos para a descrição e análise de sistemas híbridos, sistemas dinâmicos resultantes da interação de componentes contínuas e discretas.

A utilização de autômatos híbridos lineares para a modelagem da aeronave, do ambiente no qual a mesma será operada e dos recursos necessários à realização de uma missão é descrita em detalhes no capítulo 5.

O capítulo 6 descreve três diferentes técnicas para a elaboração de planos de vôo: verificação de exeqüibilidade, instanciação de planos de vôos parametrizados e construção incremental de planos de vôo.

O capítulo 7 é dedicado à interpretação de planos de vôo a bordo da aeronave durante a

execução da missão. Neste capítulo é descrito o controlador de vôo baseado em um sistema reativo, responsável pela seleção do plano de vôo alternativo mais apropriado à situação enfrentada pela aeronave.

O capítulo 8 apresenta conclusões e perspectivas derivadas do presente trabalho, bem como apresenta algumas sugestões para sua continuação.

Finalmente, o apêndice A contém material introdutório sobre autômatos e linguagens.

Capítulo 2

Aeronaves Não-Tripuladas de Asas Rotativas

Com o objetivo de descrever o problema a ser resolvido neste trabalho, este capítulo apresenta aeronaves de asas rotativas em geral e discute aspectos das mesmas relevantes ao planejamento e controle de missões.

O capítulo inicia com uma descrição dos princípios de funcionamento, manobras passíveis de serem efetuadas e comandos utilizados para controle desta classe de aeronaves (seção 2.1).

Os diferentes sistemas de coordenadas necessários para o planejamento de missões de aeronaves de asas rotativas são apresentados na seção 2.2.

Na seção 2.3 são introduzidos os conceitos de pilotagem (controle da atitude da aeronave em torno de seu centro de massa), guiagem (controle da posição do centro de massa em relação a um sistema de coordenadas) e navegação (obtenção da posição, velocidade e atitude da aeronave em relação a um sistema de coordenadas).

A seção 2.4 apresenta o problema de preparação e execução de missões para aeronaves não-tripuladas de asas rotativas, descrevendo objetivos e doutrina de missão, fases constituintes de uma missão, modos de operação da aeronave e planos de vôo associados à missão.

O contexto operacional da missão é discutido na seção 2.5. Neste contexto estão incluídas:

as características da aeronave utilizada, os recursos necessários à realização de uma missão, as condições meteorológicas prevalecentes durante a execução da missão, o relevo da região sobrevoada e zonas proibidas para operação da aeronave.

Finalmente, na seção 2.6 são descritos os requisitos de segurança obrigatórios e desejáveis que precisam ser satisfeitos por todo plano de vôo.

2.1 Princípio de funcionamento

Diversos tipos de aeronaves de asas rotativas existem. Nesta descrição será apresentado o mais comum deles, idealizado por Igor Sikorsky e conhecido universalmente como "helicóptero". A maior parte do material apresentado nesta seção é derivado de [18, 19].

O helicóptero é uma aeronave de pouso e decolagem vertical que utiliza um conjunto de aerofólios (asas, pás) rotativos para obtenção da força necessária à sua sustentação e controle. A figura 2.1 mostra uma aeronave não-tripulada de asas rotativas de pequeno porte.

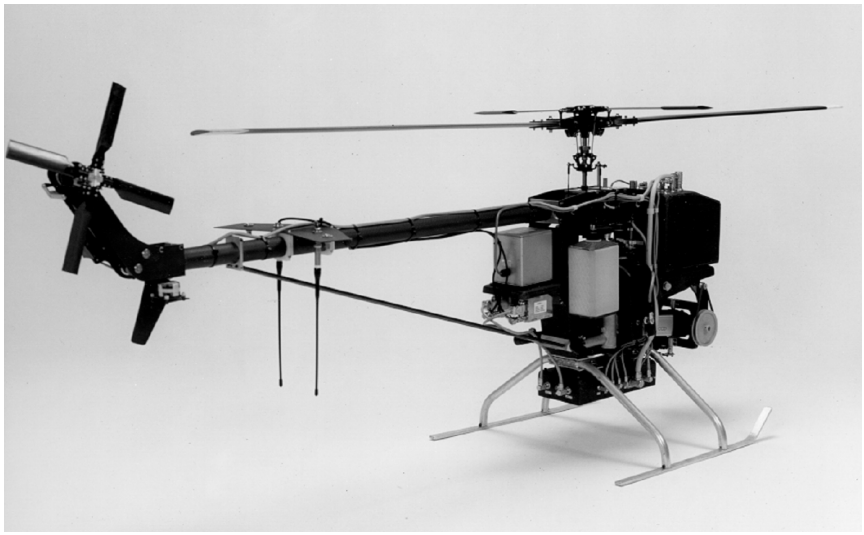


Figura 2.1: UAV de asas rotativas de pequeno porte

Um *rotor principal*, constituído de duas ou mais pás, é responsável por fornecer sustentação à aeronave, além de servir como principal forma de controle. Em todos os modelos mod-

ernos, o rotor principal é operado em regime de rotação constante e acionado diretamente pelo motor da aeronave.

Um *rotor de cauda* é utilizado para contrabalançar os efeitos de reação da fuselagem ao movimento de rotação das pás do rotor principal. O rotor de cauda geralmente é acionado através de um eixo ou correia dentada, derivada do acionamento do rotor principal.

Além deste rotores, estabilizadores vertical e horizontal provêem estabilidade adicional durante o vôo a frente.

Ao contrário de aeronaves de asas fixas, um helicóptero é capaz de voar não apenas à frente, mas permanecer imóvel no ar, voar lateralmente ou para trás, voar verticalmente e rotacionar em torno de seu eixo vertical.

Todo e qualquer movimento executado por um helicóptero resulta do balanceamento de forças e momentos. Um helicóptero apresenta seis graus de liberdade, referenciados ao sistema de coordenadas mostrado na figura 2.2:

- *movimentos longitudinais* são movimentos de translação *ao longo* do eixo X;
- *movimentos laterais* são movimentos de translação *ao longo* do eixo Y;
- *movimentos verticais* são movimentos de translação *ao longo* do eixo Z;
- *rolagem* são movimentos de rotação *em torno* do eixo X;
- *arfagem* são movimentos de rotação *em torno* do eixo Y;
- *guinada* são movimentos de rotação *em torno* do eixo Z.

Ao piloto interessa controlar apenas quatro graus de liberdade: translação ao longo dos eixos Z (controle vertical), X e Y (controle horizontal) e guinada. A descrição apresentada a seguir desconsidera os acoplamentos que existem entre os diferentes movimentos[1].

[1] O desacoplamento entre os movimentos pode ser realizado de diferentes formas, por exemplo [20, 21, 6].

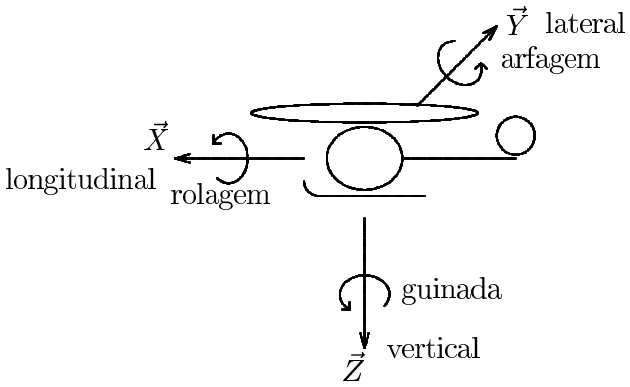


Figura 2.2: Eixos e momentos de rotação de um helicóptero

2.1.1 Controle vertical

Pouso e decolagem são manobras efetuadas ao longo do eixo vertical. Este movimento depende da relação entre peso da aeronave (atuante no centro de gravidade da mesma) e a força de sustentação (atuante no centro geométrico do disco do rotor). No projeto da aeronave contempla-se a concentricidade do centro de gravidade e centro geométrico do rotor.

A variação da força de sustentação é conseguido pela variação do ângulo de ataque das pás do rotor principal de forma simultânea, ou *coletiva*, (vide figura 2.3):

- se a força de sustentação gerada pelo rotor principal é maior que o peso da aeronave, a mesma acelera para cima;
- se a força de sustentação gerada pelo rotor principal é menor que o peso da aeronave, a mesma acelera para baixo;
- se a força de sustentação gerada pelo rotor principal é igual ao peso da aeronave, a mesma permanece a uma altitude constante.

2.1.2 Controle horizontal

O deslocamento no plano horizontal é conseguido pela variação do ângulo de ataque das pás do rotor principal de forma *cíclica* ao longo de uma rotação do rotor.

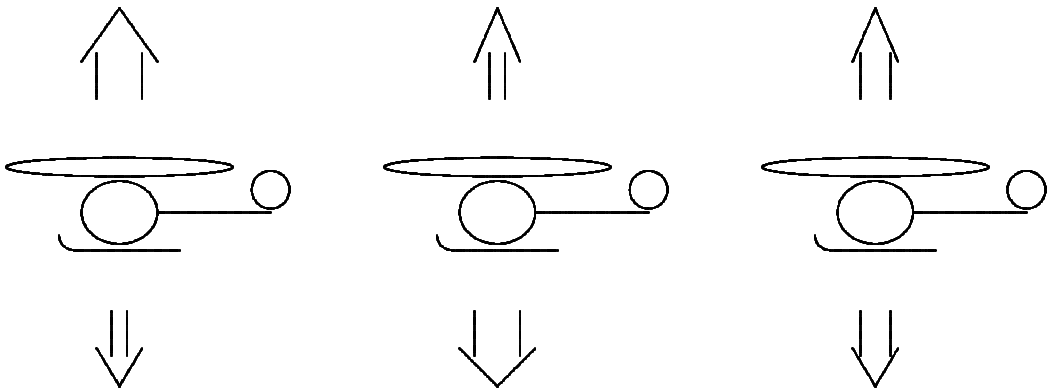


Figura 2.3: Controle de movimento vertical por variação da força de sustentação: (a) aceleração para cima, (b) aceleração para baixo e (c) altitude constante

De forma simplificada, isto equivale a inclinar o plano do rotor principal e, conseqüentemente, a direção da força por ele desenvolvida. A componente vertical da força desenvolvida pelo rotor principal continua sendo responsável pela sustentação do helicóptero, enquanto a componente horizontal é utilizada para deslocar a aeronave no sentido desejado, vide figura 2.4.

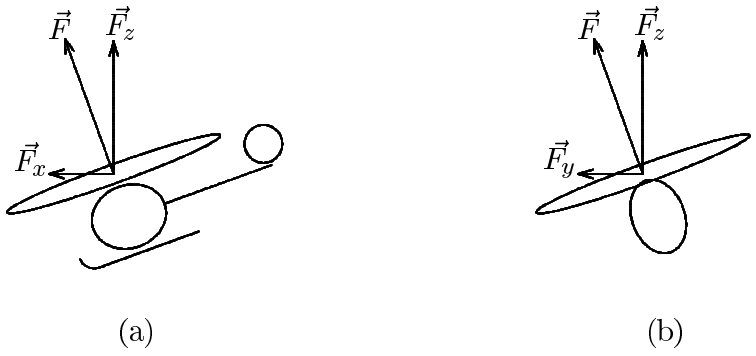


Figura 2.4: Controle de movimento horizontal por variação das componentes longitudinal (a) e lateral (b) de passo do rotor principal

Notar que a variação cíclica do ângulo de ataque das pás do rotor principal permite deslocar a aeronave em qualquer direção do plano horizontal, inclusive para trás.

2.1.3 Controle de guinada

O controle do movimento de guinada implica em controle do movimento de rotação ao redor do eixo vertical. Note-se que este movimento não necessariamente implica na alteração da direção de movimento da fuselagem.

O rotor principal gira em um sentido fixo e determinado: horário nos modelos europeus e anti-horário nos modelos de origem norte-americana. A fuselagem da aeronave reage a esta rotação, tendendo a girar no sentido oposto ao do rotor principal (contra-torque do rotor principal).

O rotor de cauda é utilizado para gerar um torque compensador. O ângulo de ataque do rotor de cauda pode ser variado e, por conseguinte, a intensidade deste torque (vide figura 2.5):

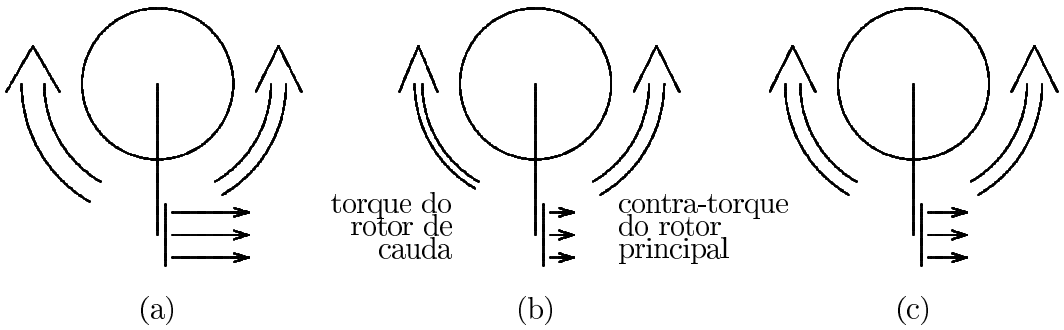


Figura 2.5: Controle de guinada por variação do contra-torque exercido pelo rotor de cauda

- se o torque gerado pelo rotor de cauda for inferior ao torque de rotação, a proa da aeronave girará no sentido oposto ao da rotação das pás do rotor principal;
- se o torque gerado pelo rotor de cauda for superior ao torque de rotação, a proa da aeronave girará no mesmo sentido ao da rotação das pás do rotor principal;
- se os torques forem iguais, a proa permanecerá imóvel.

2.2 Geometria do universo de operações

Três sistemas de coordenadas distintos serão usadas para descrever a posição e a dinâmica da aeronave e de objetos em seu universo de operações. O *sistema de coordenadas geodéticas* é usado para especificar a posição de objetos de interesse para o cumprimento dos objetivos da missão. Os problemas de navegação da aeronave são resolvidos usando um *sistema de coordenadas cartesiano plano tangente*, referenciado ao ponto de lançamento/recolhimento da aeronave. Finalmente, as velocidades desenvolvidas pela aeronave são especificadas usando um *sistema de coordenadas cartesiano rigidamente acoplado ao centro de gravidade da aeronave*.

Para fins de navegação, a superfície da Terra pode ser aproximada por um elipsóide cujo eixo de rotação coincide com o eixo de rotação do globo terrestre. O centro do elipsóide coincide com o centro de massa da Terra e sua forma é escolhida de forma a minimizar as diferenças entre o vetor gravidade e a normal ao elipsóide, diferenças estas integradas sobre toda a superfície terrestre.

Diversos elipsóides foram definidos [22], o mais usado deles sendo conhecido por WGS-84 (*World Geodetic System 1984*). É importante notar que qualquer elipsóide é aceitável para fins de navegação, desde que todos os pontos de interesse sejam referidos ao mesmo elipsóide.

2.2.1 Sistema de coordenadas geodéticas

O *sistema de coordenadas geodéticas* é um sistema de coordenadas que especifica um ponto usando as coordenadas esféricas da normal ao elipsóide de referência, vide figura 2.6.

A *latitude* Ψ de um ponto é o ângulo formado entre a normal ao elipsóide no ponto e o plano do equador. A *longitude* Θ é o ângulo formado entre o meridiano de Greeenwich e o meridiano que passa pelo ponto de interesse. A *altitude* z é medida em relação ao elipsóide de referência, geralmente WGS-84. A maioria dos objetos no universo de operação da aeronave, tais como rodovias, estradas e aeroportos, é especificada neste sistema de coordenadas.

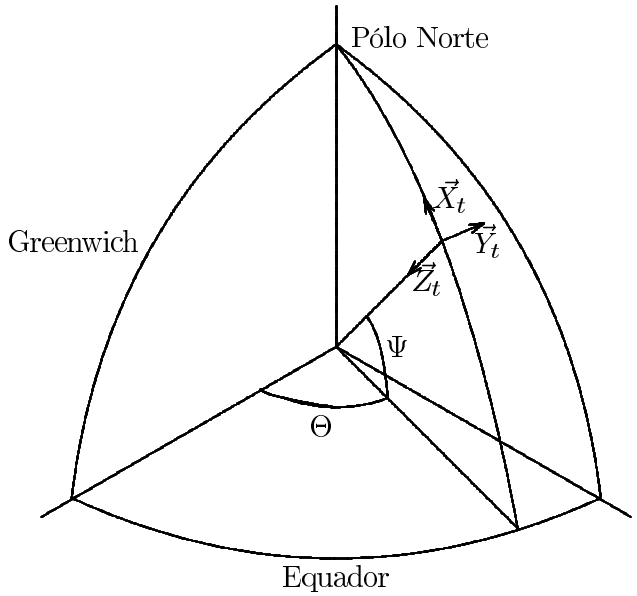


Figura 2.6: Sistemas de coordenadas geodéticas e plano tangente

2.2.2 Sistema de coordenadas plano tangente

O *sistema de coordenadas plano tangente* é um sistema de coordenadas cartesiano que utiliza distâncias lineares em relação a um ponto de referência (o ponto de lançamento/recolhimento da aeronave) para especificar a posição de um ponto de interesse.

O eixo $\vec{X}_t$ do sistema de coordenadas plano tangente é coincidente com o meridiano que passa pela origem do mesmo e é positivo na direção norte. O eixo $\vec{Y}_t$ é coincidente com o paralelo que passa pela origem do sistema de coordenadas e é positivo na direção leste. O eixo $\vec{Z}_t$ é perpendicular ao plano formado pelos eixos $\vec{X}_t$ e $\vec{Y}_t$ e é positivo para baixo, vide figura 2.6.

A utilização do sistema de coordenadas plano tangente permite resolver os problemas de navegação utilizando a geometria do plano ao invés da geometria esférica. A aproximação da superfície elipsoidal da terra por um plano tangente à superfície da mesma no ponto de lançamento/recolhimento é possível sempre que o raio operacional da aeronave é muito menor que o raio do globo terrestre [23].

2.2.3 Sistema de coordenadas rigidamente acoplado ao centro de gravidade da aeronave

As velocidades desenvolvidas pela aeronave são especificadas usando um sistema cartesiano de coordenadas *rigidamente acoplado ao centro de gravidade da aeronave.*

Neste sistema de coordenadas, o eixo $\vec{X_a}$ aponta para a frente da aeronave, o eixo $\vec{Y_a}$ aponta para a direita e o eixo $\vec{Z_a}$ é perpendicular ao plano formado pelos eixos $\vec{X_a}$ e $\vec{Y_a}$ e aponta para baixo, vide figura 2.7.

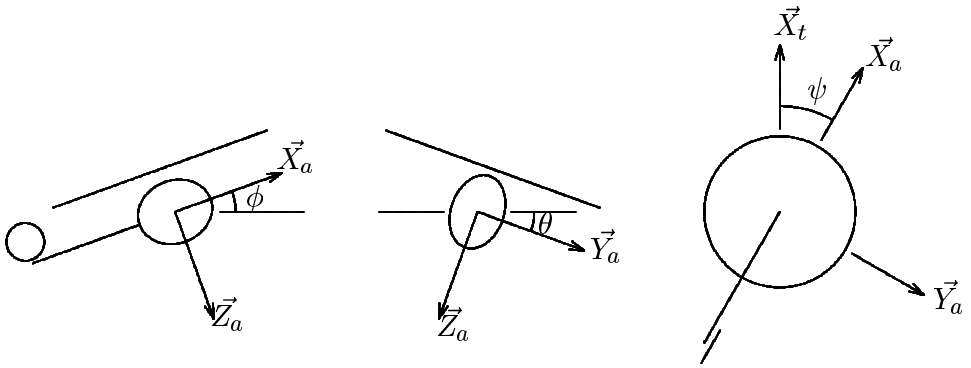


Figura 2.7: Sistema de coordenadas rigidamente acoplado à aeronave

O ângulo formado entre o eixo $\vec{X_a}$ e a horizontal é denominado *ângulo de arfagem*, ϕ. Similarmente, o ângulo formado entre o eixo $\vec{Y_a}$ e a horizontal é denominado *ângulo de rolagem*, θ. Denomina-se *curso* da aeronave, ψ, o ângulo formado entre o eixo longitudinal da aeronave, $\vec{X_a}$, e o norte geográfico, coincidente com o eixo $\vec{X_t}$.

2.2.4 Conversão entre os diferentes sistemas de coordenadas

Conversões entre o sistema de coordenadas geodéticas e o sistema de coordenadas plano tangente podem ser efetuadas com o auxílio das seguintes equações:

$$\begin{aligned} x_t &= (\Psi - \Psi_0)\mathcal{R} \\ y_t &= (\Theta - \Theta_0)\mathcal{R}\cos\left(\frac{\Psi + \Psi_0}{2}\right) \\ z_t &= z - z_0 \end{aligned}$$

onde $\mathcal{R}$ é o raio do globo terrestre, $\mathcal{R} \approx 6366707$ m e (Ψ_0, Θ_0, z_0) são as coordenadas da origem do sistema de coordenadas plano tangente, expressas no sistema de coordenadas geodéticas.

A transformada de Euler pode ser usada para definir a matriz $\mathcal{T}$ para conversões entre o sistema de coordenadas plano tangente e o sistema de coordenadas rigidamente acoplado ao corpo da aeronave [24, 20]:

$$\mathcal{T} = \begin{bmatrix} \cos\psi\cos\theta & -\sin\psi\cos\phi + \cos\psi\sin\theta\sin\phi & \sin\psi\sin\phi + \cos\psi\sin\theta\cos\phi \\ \sin\psi\cos\theta & \cos\psi\cos\phi + \sin\psi\sin\theta\sin\phi & -\cos\psi\sin\phi + \sin\psi\sin\theta\cos\phi \\ -\sin\theta & \cos\theta\sin\phi & \cos\theta\cos\phi \end{bmatrix}$$

2.3 Pilotagem, guiagem e navegação

O termo *navegação* é usado para descrever o conjunto de algoritmos capaz de prover posição, atitude e velocidades (lineares e angulares) do veículo com respeito a um sistema de coordenadas de referência [21].

Guiagem é a técnica de controle da posição do centro de massa de uma aeronave. *Pilotagem* é a técnica de controle da atitude da aeronave em torno de seu centro de massa [25]. A figura 2.8 mostra a inter-relação existente entre os blocos funcionais pilotagem, guiagem e navegação.

Em uma aeronave não-tripulada, um conjunto de controladores de baixo nível é responsável pelas funções combinadas de guiagem e pilotagem, agindo sobre as superfícies aerodinâmicas e sobre o motor da aeronave.

No caso específico de uma aeronave de asas rotativas, os seguintes controladores são necessários para implementar as funções descritas acima:

controladores longitudinal e lateral que atuam através da variação das componentes cíclicas do passo do rotor principal.

controlador de altitude que atua através da variação da componente coletiva do passo

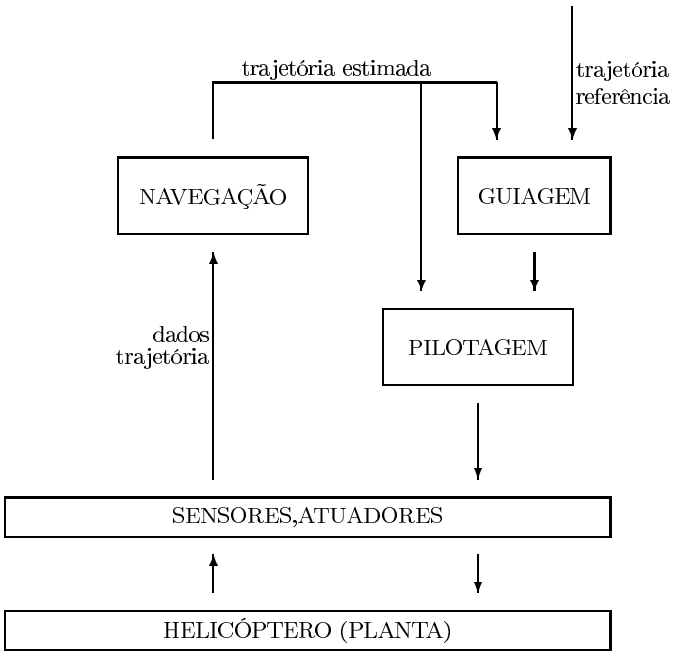


Figura 2.8: Pilotagem, guiagem e navegação

do rotor principal. O valor de referência para este controlador pode ser referenciado ao nível do mar ou ao solo diretamente abaixo da aeronave. O primeiro caso é geralmente utilizado durante a fase de cruzeiro de um vôo ou quando o vôo da aeronave precisa ser coordenado com outro tráfego aéreo (tripulado ou não) existente na região. O segundo caso é geralmente utilizado durante a fase útil da missão, principalmente se a missão envolve coleta de dados, inspeção ou vigilância.

controlador de azimute que atua através da variação do passo do rotor de cauda e do ângulo de rolagem da aeronave. Durante o vôo pairado e a baixas velocidades, o azimute é controlado pelo rotor de cauda. Quando desenvolvendo velocidade à frente é preciso, além de gerar comandos para o rotor de cauda, provocar uma atitude adequada ao longo do eixo de rolagem para a efetivação da assim chamada *curva coordenada*. O ângulo de rolagem ϕ necessário para tanto é dado por

$$\phi = \arctan(\dot{\psi} \cdot \dot{x}/g)$$

onde $\dot{\psi}$ é a taxa do movimento de guinagem, $\dot{x}$ é a velocidade à frente e g é a constante gravitacional.

controlador de rotação que comanda variações de torque no motor a fim de manter a rotação dos rotores principal e de cauda constantes, compensando as variações de carga mecânica impostas por estes durante os diferentes regimes de vôo.

Uma estratégia de guiagem bastante utilizada para o tipo de aeronave e missão aqui considerado é a assim chamada *line-of-sight strategy* (linha de visada direta) na qual o movimento do veículo é restrito a um plano horizontal e o mesmo desloca-se à frente com velocidade constante. Neste situação o papel do sistema de guiagem consiste em computar comandos de referência para o controlador de azimute de forma a manter o eixo longitudinal do veículo apontado para um ponto de referência imaginário, localizado sobre a trajetória de referência ou especificado na forma de um ponto de passagem.[2]

2.4 Preparação e execução de missões

O termo *missão* é usado para descrever a operação da aeronave em uma certa região durante um período restrito de tempo visando cumprir um objetivo específico, o *objetivo da missão*.

2.4.1 Objetivo da missão

Um vôo é sempre executado visando o cumprimento de um objetivo específico, denominado *objetivo da missão*. Exemplos de objetivos de missão são inspecionar um trecho de uma linha de alta tensão, monitorar o tráfego ao longo de uma rodovia ou medir a concentração de gases atmosféricos em um ou mais pontos pré-determinados.

Duas características podem ser associadas ao objetivo de uma missão:

- o *custo associado* ao cumprimento dos objetivos da missão. Tanto o custo operacional de uma aeronave não-tripulada como o custo de sua perda durante a execução de uma

[2]Esta estratégia não apresenta bom desempenho para missões de interceptação de outros veículos cuja velocidade seja da mesma ordem de grandeza ou maior que a velocidade da aeronave interceptante.

missão são quantificáveis.[3]

- o *benefício resultante* do cumprimento dos objetivos da missão. Devido à sua variedade e à conseqüente dificuldade em quantificá-los, os benefícios são normalmente melhor avaliados por um ser humano.

2.4.2 Doutrina da missão

O conjunto de regras que descreve a filosofia de operação da aeronave em uma determinada missão é denominado *doutrina da missão*.

Doutrinas são úteis para prescrever o comportamento a ser exibido pelo conjunto operador/aeronave. Uma doutrina de preservação do equipamento, por exemplo, optará sempre por abortar a missão em caso de anomalias, enquanto uma doutrina de sacrifício não se importará em esgotar o combustível remanescente a bordo da aeronave em uma última tentativa de atingir o objetivo da missão.

2.4.3 Fases constituintes de uma missão

Uma missão compreende todas as atividades necessárias à utilização da aeronave com o intuito de cumprir o objetivo associado. As atividades constituintes de uma missão podem ser agrupadas em diferentes *fases* [26], a saber:

- A fase de *inicialização* compreende todas as atividades executadas no solo, antes do vôo propriamente dito, incluindo inspeção inicial da aeronave, energização, verificação funcional dos diferentes subsistemas, partida e pré-aquecimento do motor.

- As atividades realizadas durante a fase de *decolagem e ascensão* objetivam levar a aeronave até a altitude de cruzeiro, necessária para a execução das fases seguintes. Esta fase compreende a manobra de decolagem propriamente dita e a ascensão à altitude de cruzeiro.

[3] O envolvimento de vidas humanas dificulta enormemente considerações relativas à perda de aeronaves tripuladas durante a execução de uma missão.

- A fase de *deslocamento* compreende a execução de atividades destinadas a conduzir a aeronave das proximidades do ponto de lançamento a um ponto determinado pelos objetivos da missão a ser executada.

- A fase de *execução* é constituída pelo conjunto de atividades necessárias ao cumprimento dos objetivos da missão. Esta é, geralmente, a fase mais complexa da missão pois compreende a operação da carga útil transportada pela aeronave (*payload*) e a execução de todo um conjunto de manobras de vôo destinado a posicionar a carga útil de acordo com os objetivos da missão.

- As atividades realizadas durante a fase de *retorno* destinam-se a conduzir a aeronave do ponto onde os objetivos da missão foram cumpridos (ou abandonados) às proximidades do ponto de recolhimento, geralmente coincidente com o ponto de lançamento.

- A fase de *descida e pouso* compreende as atividades destinadas ao recolhimento da aeronave. Esta fase compreende a manobra de perda de altitude e a manobra de pouso propriamente dita.

- A fase de *finalização* é executada no solo e compreende o desligamento do motor, de-energização dos diferentes subsistemas e inspeção visual da aeronave.

A figura 2.9 apresenta de forma esquemática as fases constituintes de uma missão realizada por uma aeronave não-tripulada de asas rotativas.

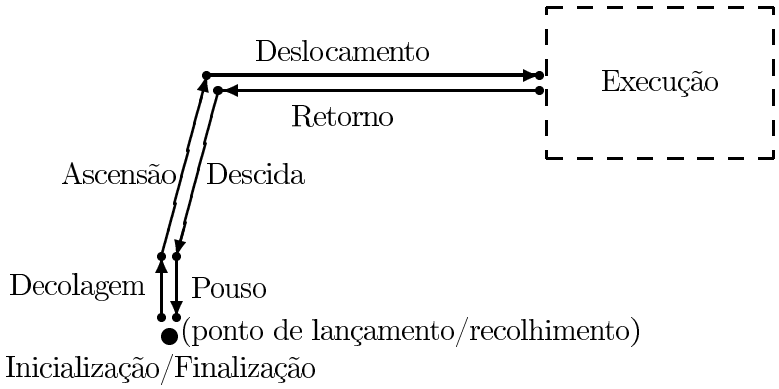


Figura 2.9: Exemplo de fases constituintes de uma missão

2.4.4 Modos de operação

Durante qualquer uma das fases acima, a aeronave pode ser operada de dois modos distintos:

- No *modo pré-programado* de operação a aeronave executa autonomamente um plano de vôo previamente estabelecido. O modo pré-programado é utilizado quando o plano de vôo da aeronave é ditado pelos objetivos da missão a ser cumprida. No controle de tráfego em rodovias, por exemplo, a rota a ser seguida é definida pelo traçado da rodovia a ser monitorada.

  Às vezes, principalmente durante missões de longa duração, um plano de vôo pode vir a ser alterado durante sua execução visando cumprir novos objetivos, mais atuais que os originalmente pretendidos para aquela missão. Chama-se a isto de *reprogramação da missão*. A reprogramação de uma missão implica no abandono do plano de vôo atual e na construção de um novo plano de vôo, plano este que substitui a parte ainda não executada do plano de vôo abandonado.

- No *modo interativo* de operação o operador define de forma interativa, em tempo-real, a trajetória a seguir. O modo interativo é utilizado quando as manobras a serem executadas durante o vôo dependem de informações coletadas *durante* a execução do mesmo.

Freqüentemente, aeronaves são operadas em um modo híbrido: um plano de vôo pré-programado é usado para levar a aeronave a uma área de interesse. A partir deste ponto o operador utiliza o modo interativo para cumprir os objetivos da missão.

A ocorrência de falhas em algum dos subsistemas da aeronave pode provocar a reprogramação da missão, ou o abandono do modo pré-programado em favor do modo de operação interativo com o objetivo de recuperar a aeronave.

2.4.5 Planos de vôo

A seqüência de manobras executada pela aeronave durante a missão é definida no *plano de vôo* associado à missão.

Um plano de vôo é constituído de várias *etapas*. Cada etapa do vôo pode ser especificada de duas maneiras distintas:

- pelas coordenadas de dois *pontos de passagem*[4] e pela velocidade com a qual a aeronave deve se deslocar entre estes pontos. Etapas especificadas desta forma são consideradas completas tão logo o segundo ponto de passagem seja atingido.
- por um ponto de passagem inicial, uma velocidade de deslocamento e uma duração. Etapas especificadas desta maneira são consideradas completas quando o tempo especificado na duração da mesma se expira.

Um *plano de vôo parametrizado* é um plano de vôo no qual as etapas e a seqüência em que as etapas serão executadas está especificada. Entretanto, as condições que determinam a transição de uma etapa para a próxima são especificadas por parâmetros a serem determinados.

Através da *instanciação de um plano de vôo*, os parâmetros de um plano de vôo parametrizado são substituídos para valores que satisfazem requisitos especificados.

2.5 Contexto operacional da missão

O contexto operacional da missão compreende:

condições internas: condições que dependem apenas da aeronave escolhida e não da missão realizada;

condições externas: independem da aeronave utilizada e dizem respeito ao local e momento em que será realizada a missão.

[4] *waypoints*

2.5.1 Condições internas: características da aeronave e recursos necessários à realização de uma missão

Cada aeronave possui um conjunto de características que precisa ser considerado quando do planejamento da missão. O conjunto varia de uma aeronave para outra, mas exemplos típicos são:

- as velocidades a que a aeronave pode ser operada;
- o consumo de combustível a cada uma destas velocidades;
- a capacidade de combustível armazenável a bordo;
- a fonte de energia elétrica usada pelos diferentes subsistemas existentes a bordo da aeronave e pela carga útil selecionada para a missão, bem como a potência consumida por estes equipamentos.

A execução de uma missão também implica na utilização de *recursos* limitados. Os recursos normalmente considerados são combustível e energia elétrica. Outro exemplo, menos comum, é o nitrogênio líquido necessário para refrigeração do plano focal de um sensor FLIR[5], utilizado para obtenção de imagens térmicas em vôos noturnos.

A seguir serão detalhadas a utilização de combustível e energia elétrica.

Combustível

O consumo específico de combustível, s, é medido em gramas/segundo e depende principalmente da velocidade desenvolvida[6] e da massa da aeronave. Em menor escala, o consumo de combustível depende também da altitude de operação e das condições de temperatura e pressão atmosférica. Aqui serão considerados apenas os dois primeiros fatores mencionados.

Considerando f_0 como a quantidade inicial de combustível a bordo da aeronave, a quantidade de combustível restante f, em gramas, a qualquer instante é dada por:

[5] *forward looking infra-red imaging sensor*
[6] Todas as velocidades mencionadas são relativas à massa de ar na qual a aeronave está imersa.

$$f = f_0 - \int_0^t s dt$$

A figura 2.10 mostra uma curva típica de variação de s em função da velocidade desenvolvida pela aeronave para uma dada massa [19]. É importante notar que a curva faz parte de uma família de curvas similares que expressam o consumo de combustível para as diferentes massas da aeronave.

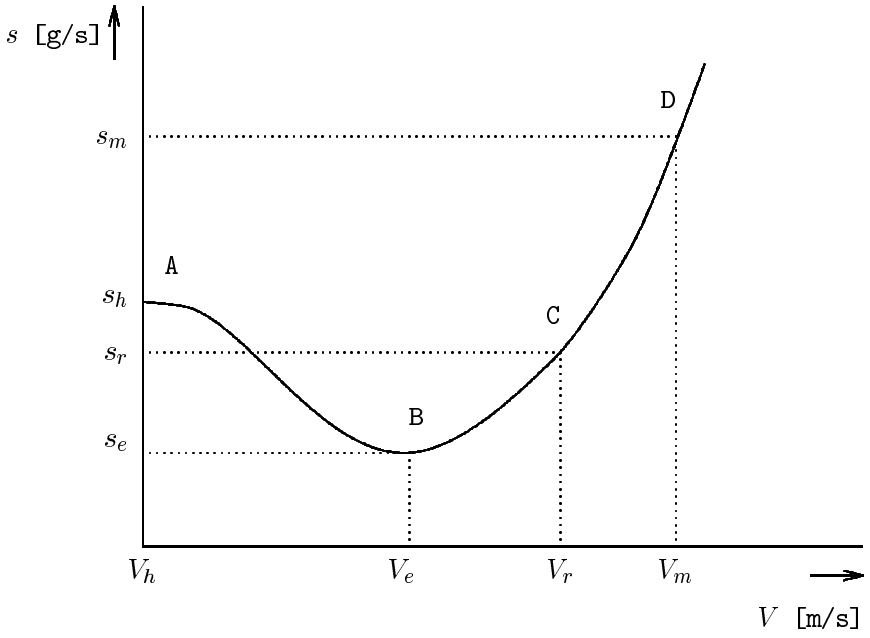


Figura 2.10: Consumo específico de combustível em função da velocidade da aeronave

Considerando que a aeronave pode ser operada de acordo com os objetivos da missão em um dos quatro pontos identificados na figura 2.10, temos [27, 28]:

- no *vôo pairado* (*hover*, ponto A da curva), a velocidade V_h é zero ou próxima de zero, visto que o vôo pairado inclui todas as manobras efetuadas à baixa velocidade. O consumo específico de combustível no vôo pairado será denotado por s_h.
- o deslocamento à frente à *velocidade mais econômica* (*endurance speed*, ponto B da curva), V_e, permite *maximizar o tempo* que a aeronave permanece no ar para uma dada quantidade de combustível. O consumo específico de combustível no vôo à

velocidade mais econômica será denotado por s_e.

- o deslocamento à frente à *velocidade mais eficiente* (*best range speed*, ponto C da curva), V_r, corresponde ao ponto de máxima derivada da curva de consumo específico em função da velocidade desenvolvida. Deslocamentos a esta velocidade permitem *maximizar a distância* percorrida ou a área coberta para uma dada quantidade de combustível. O consumo específico de combustível no vôo à velocidade mais eficiente será denotado por s_r.

- o deslocamento à frente à *velocidade máxima* definida pelo envelope operacional da aeronave, V_m, permite *minimizar o tempo* necessário para percorrer um dado trajeto. O consumo específico de combustível no vôo à velocidade máxima será denotado por s_m.

Para a maioria das aeronaves,

$$V_m > V_r > V_e > V_h$$

e

$$s_m > s_h > s_r > s_e$$

A variação de massa decorrente do consumo de combustível durante o vôo e sua influência no alcance da aeronave pode ser determinada computando o *alcance específico*, $\dot{W}_F$ (em metros/grama de combustível). O incremento de alcance dR devido à redução de massa resultante do consumo de combustível durante o vôo é dado por [27]:

$$dR = (V/\dot{W}_F)\, dW$$

onde V é a velocidade desenvolvida pela aeronave e dW é a diminuição incremental de peso devido à queima do combustível. Uma curva típica de alcance específico em função

do peso bruto da aeronave é mostrada na figura 2.11.

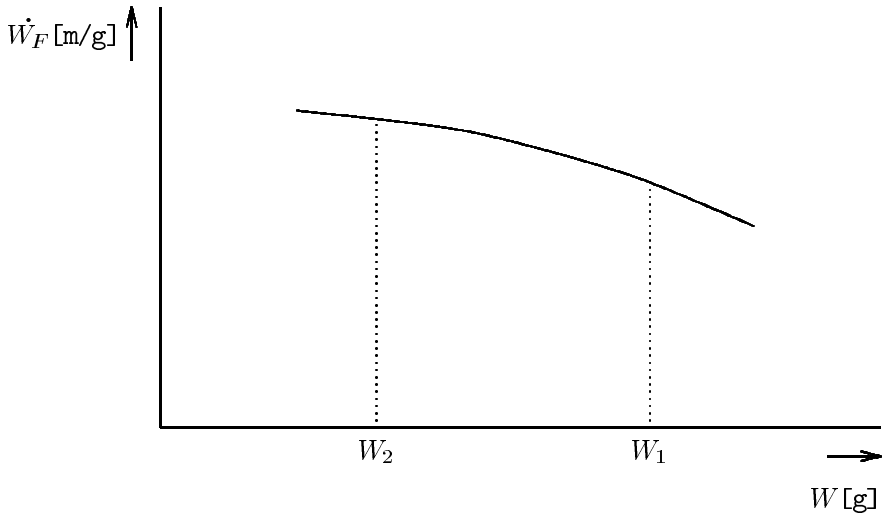


Figura 2.11: Alcance específico em função do peso bruto da aeronave

O *alcance total* R para uma dada quantidade de combustível é obtido integrando ambos os lados da equação anterior:

$$R = \int_{W_2}^{W_1} (V/\dot{W}_F)\, dW$$

onde W_1 é o peso bruto inicial da aeronave e W_2 é o peso bruto da aeronave após consumido o combustível.

Graficamente, o alcance corresponde à área sob a curva de alcance específico em função do peso bruto da aeronave entre os pontos de peso bruto inicial W_1 e final W_2, figura 2.11. Se a curva de alcance específico é razoavelmente linear entre W_1 e W_2, a área pode ser computada usando a média dos alcances específicos [27].

Energia elétrica

Os diferentes subsistemas existentes a bordo da aeronave necessitam de energia elétrica para seu funcionamento.

Tal energia é proveniente de uma de duas fontes distintas:

- um alternador acoplado ao motor de combustão da aeronave;
- um acumulador de emergência.

O alternador é capaz de prover energia elétrica somente quando o motor de combustão opera à rotação nominal e, nestas condições, parte da energia provida pelo mesmo é usada para carregar o acumulador de emergência com a corrente I_c, até sua carga máxima Q_{max}. Assumindo-se I_c como constante, tem-se:

$$Q = \min\left(Q_0 + I_c t, Q_{max}\right)$$

Quando o alternador não é capaz de fornecer energia elétrica para a aeronave (rotação do motor de combustão insuficiente ou falha do alternador ou do circuito controlador de carga), a energia elétrica necessária para a operação da mesma é obtida do acumulador de emergência. Nestas condições, a corrente (assumida como constante) I_d é drenada do acumulador de emergência e a carga do mesmo pode ser expressa por:

$$Q = \max\left(Q_0 - I_d t, 0\right)$$

Se a aeronave for dotada de um sistema de gerenciamento de energia que permita o desligamento seletivo de subsistemas não essenciais para o vôo, deve-se ainda considerar o consumo mínimo de energia elétrica I_{min} após o desligamento de parte dos equipamentos/sensores a bordo.

2.5.2 Condições externas: meteorologia, relevo e zonas de exclusão

As condições externas definem a parte do contexto operacional da missão que independe da aeronave utilizada. As condições externas compreendem: as condições meteorológicas prevalentes no momento do vôo, o relevo da região sobrevoada e a existência de zonas de

exclusão.

Condições meteorológicas

As condições meteorológicas esperadas durante a realização da missão precisam ser consideradas de duas formas distintas:

Não-execução da missão: é preciso, inicialmente, garantir que a aeronave não seja exposta à condições para as quais não foi construída, o que implica na não-execução da missão sob tais condições.

Execução da missão: a intensidade, a direção e o tipo de vento (constante ou em rajadas) influenciam a dinâmica da aeronave. Esta influência é mais evidente em UAVs de dimensões reduzidas que utilizam motores pouco potentes.

Relevo da região sobrevoada

As elevações do terreno sobrevoado precisam ser levadas em consideração durante o planejamento da missão a fim de que se possam garantir distâncias mínimas ao solo durante todas as fases do vôo, bem como uma altitude adequada à consecução dos objetivos da missão possa ser mantida.

O relevo da região sobrevoada também influencia a propagação das ondas de rádio utilizadas para comunicação entre a aeronave e sua estação de controle em terra.

Durante a execução de uma missão há necessidade de comunicação permanente entre a aeronave e a estação de controle em terra. Um canal de comunicação bidirecional é usado para a transmissão de comandos para a aeronave e para a recepção de dados telemétricos da mesma, bem como dados relativos à carga útil usada durante a missão.

Para uma operação confiável da aeronave, é preciso garantir uma intensidade mínima do sinal de rádio-freqüência usado para implementar o enlace de comando/telemetria. A intensidade do sinal de rádio-freqüência é função da potência do transmissor, do ganho das antenas de transmissão/recepção usadas para implementar o enlace, da freqüência de

operação do enlace e da topografia da região sobrevoada.

Zonas de exclusão

Para o planejamento de missões, é necessário também considerar as *zonas de exclusão*, regiões onde a operação da aeronave não é permitida ou somente o é durante certos períodos de tempo.

Exemplos de zonas de exclusão permanente são aeroportos, aerovias em geral e zonas de alta periculosidade como o espaço aéreo sobre reatores nucleares e refinarias de petróleo.

Zonas de exclusão temporária incluem áreas reservadas para exercícios militares ou outras áreas sob controle dos órgão responsáveis pelo controle de tráfego aéreo.

2.6 Requisitos de segurança

Todo plano de vôo precisa satisfazer um conjunto de *requisitos obrigatórios de segurança*. Dentre estes, destacam-se:

- o não esgotamento de recursos não-renováveis a bordo da aeronave, como o combustível;
- a operação dentro da área de cobertura do enlace de comunicação usado para comando e telemetria.

A violação dos requisitos de segurança obrigatórios implica em perda da aeronave.

A segurança da operação da aeronave pode ser aumentada se, além dos requisitos obrigatórios, um conjunto de *requisitos desejáveis de segurança* também for satisfeito. Dentre estes pode-se citar:

- a manutenção de distâncias mínimas em relação ao solo durante todas as fases da missão;

- o pouso com reserva de combustível;
- a garantia de retorno ao ponto de lançamento em caso de anomalias usando recursos de emergência.

Um exemplo da utilização de recursos emergenciais é o abandono dos objetivos da missão após a falha do alternador. Durante o retorno com alternador inoperante, a energia é fornecida pelo acumulador de emergência e certos subsistemas não-essenciais podem ser desativados temporariamente para reduzir o consumo de energia elétrica a bordo da aeronave.

2.7 O problema de planejamento e controle de missões

Pela diversidade de missões possíveis de serem executadas por aeronaves não-tripuladas e devido à dificuldade de se quantificar os benefícios advindos do cumprimento dos objetivos de uma missão, o planejamento de missões é, atualmente, uma tarefa reservada a seres humanos.

Entretanto, partes importantes do processo de planejamento de missões podem ser automatizadas. Tal automatização resulta em maior segurança de operação, melhor utilização de recursos e menor custo operacional, ao mesmo tempo que preserva o poder de decisão do operador referente aos benefícios e custos da missão.

Dados o objetivo e o contexto operacional da missão, o *planejamento de missões* tem por finalidade produzir um plano de vôo que conduza à consecução dos objetivos da missão, ao mesmo tempo que satisfaz um conjunto de requisitos de segurança. Observe-se que plano de vôo é um dos fatores a ser considerado durante o planejamento da missão e, simultaneamente, o resultado do planejamento efetuado.

O *controle de missões* tem por finalidade acompanhar o progresso do plano de vôo, ajustando-o às condições encontradas quando de sua execução em consonância com a doutrina de utilização da aeronave. Para tanto, o controle de missão precisa levar em consideração o estado da aeronave, a ocorrência de eventos externos e o possível sucesso prematuro na consecução do objetivo da missão.

Deseja-se que a combinação das ações de planejamento e controle da missão levem a aeronave, quando operando de forma autônoma, a exibir um comportamento caracterizado por:

conformidade com os objetivos da missão: a execução do plano de vôo contribui para a consecução dos objetivos da missão.

robustez: o plano de vôo é robusto se

- garantidamente não contém instruções que conduzem a aeronave a estados perigosos (segurança ativa);
- contém alternativas que permitem conduzir a aeronave a um estado seguro (falha controlada do plano de vôo) se é impossível cumprir os objetivos da missão (segurança passiva).

2.8 Resumo do capítulo

Este capítulo apresentou os princípios de funcionamento de aeronaves de asas rotativas e introduziu os conceitos de pilotagem, guiagem e navegação.

Os diferentes sistemas de coordenadas necessários para a descrição da geometria do universo de operações e da dinâmica de UAVs foram descritos.

Os conceitos de *missão*, *objetivo e doutrina da missão* e *plano de vôo* foram introduzidos. As fases constituintes de uma missão foram descritas bem como o foram os possíveis modos de operação de aeronaves não-tripuladas.

O contexto operacional de uma missão foi definido em termos de condições internas e externas e os requisitos de segurança a serem satisfeitos por um plano de vôo foram descritos.

Finalmente, o problema de planejamento e controle de missões de aeronaves não-tripuladas foi definido em termos de conformidade com os objetivos da missão e robustez do comportamento a ser exibido pela aeronave durante a realização da missão.

Capítulo 3

Uma Metodologia Formal para o Planejamento e Controle de Missões de Aeronaves Não-Tripuladas

Neste capítulo será apresentada, em linhas gerais, uma proposta de solução para o problema de planejamento e controle de missões de aeronaves não-tripuladas. Detalhes serão apresentados em capítulos posteriores. Também serão discutidas (seção 3.3) as hipóteses necessárias para a realização da metodologia.

O objetivo da metodologia a ser desenvolvida é produzir planos de vôo cuja conformidade com os objetivos da missão e robustez (segurança ativa e passiva)[1] possam ser formalmente garantidas.

Para tanto, serão utilizadas duas técnicas:

planejamento formal: A conformidade com os objetivos da missão e a segurança ativa serão garantidas durante o planejamento da missão utilizando um método formal (autômatos híbridos lineares) para verificar se um dado plano de vôo satisfaz um conjunto de requisitos de segurança comum a todos os planos de vôo. Um conjunto

[1] Vide definições na seção 2.7.

típico de requisitos de segurança inclui, por exemplo, garantias de não-esgotamento de combustível, não-invasão de zonas de exclusão e manutenção de distâncias mínimas ao solo durante todas as etapas do vôo.

controle reativo: A segurança passiva da aeronave será garantida pela inclusão no plano de vôo, durante a fase de planejamento, de comportamentos alternativos para todas as situações previsíveis passíveis de serem enfrentadas durante a missão. Novamente, autômatos híbridos lineares serão utilizados para garantir que cada uma destas alternativas satisfaça o conjunto de requisitos de segurança comum a todos os planos de vôo.

Durante a execução da missão, um *controlador de vôo* a bordo da aeronave selecionará o plano alternativo mais apropriado em função do progresso da missão, do ambiente no qual a aeronave está operando e do estado interno da mesma.

3.1 Modelagem utilizando autômatos híbridos lineares

Uma abordagem formal para o problema de planejamento e controle de missões exige a utilização de uma ferramenta matemática de modelagem e análise capaz de modelar uma aeronave não-tripulada, sua dinâmica e seu universo de operações.

Os fatores que precisam ser considerados no planejamento de missões de aeronaves não-tripuladas, tais como mencionados no capítulo 2, podem ser considerados da perspectiva de *sistemas híbridos*. Um sistema híbrido é um sistema dinâmico resultante da interação de componentes contínuas e discretas.

No caso de planejamento de missões para aeronaves não-tripuladas, a posição da aeronave, a quantidade de combustível restante a bordo da mesma e a carga do acumulador de emergência são exemplos de componentes contínuas de um sistema híbrido. As transições entre as diferentes etapas constituintes de um plano de vôo constituem componentes discretas do mesmo sistema híbrido.

Uma das maneiras de modelar sistemas híbridos, particularmente adequada à verificação simbólica baseia-se em *autômatos híbridos* [29, 30, 31], uma extensão de autômatos tem-

porizados [32].

O capítulo 4 descreve a utilização de autômatos híbridos para a modelagem e verificação de sistemas. Sua aplicação ao problema de modelagem de planos de vôo e modelagem do contexto operacional da missão é discutido no capítulo 5.

3.2 Elaboração e interpretação de planos de vôo

A metodologia aqui proposta consiste em duas fases distintas:

- *elaboração* de um plano de vôo, realizada antes da execução da missão;
- *interpretação* do plano de vôo elaborado, realizada em tempo real durante a execução da missão.

Durante a fase de elaboração do plano de vôo, autômatos híbridos são utilizados para modelar o plano de vôo a ser executado pela aeronave, o contexto operacional da missão e os requisitos de segurança aplicáveis para a missão. O resultado desta etapa é um *plano de vôo primário*. O plano de vôo primário contém um único encadeamento de etapas de vôo e reflete o plano inicial do operador para a consecução dos objetivos da missão.

O plano de vôo primário é então aumentado de um conjunto de planos de vôo alternativos destinados a contemplar faltas antecipadas, sucesso prematuro e diferentes doutrinas de missão. O plano de vôo resultante é denominado *plano de vôo completo* e contém múltiplas alternativas para pelo menos uma de suas etapas e, conseqüentemente, mais de um possível encadeamento das mesmas.

O plano de vôo completo é modelado por um autômato híbrido $\mathcal{M}$, denominado autômato modelador da missão. A figura 3.1 representa de forma esquemática a construção do plano de vôo completo.

O modelo resultante é utilizado para verificar a satisfação de requisitos de segurança previamente estabelecidos, permitindo assim validar o plano de vôo proposto para a missão.

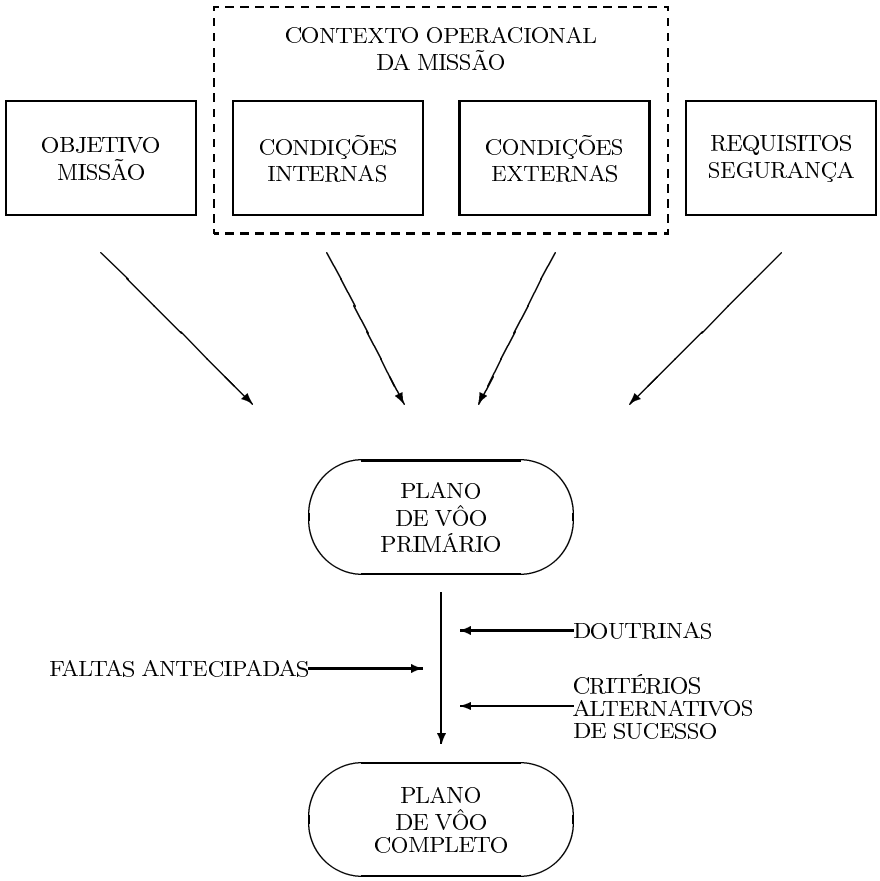


Figura 3.1: Elaboração de um plano de vôo completo

Precedendo a execução da missão, o autômato híbrido $\mathcal{M}$ é convertido em um autômato de estados finitos $\mathcal{C}$, apropriada para carga no controlador de vôo da aeronave e posterior interpretação pelo mesmo.

Durante a fase de execução da missão, o controlador de vôo interpreta o plano de vôo armazenado a bordo e produz eventos e valores de referência para os módulos de guiagem e pilotagem da aeronave em reação a eventos externos, mudanças no estado interno da aeronave e eventuais alterações de doutrina de missão ditadas pelo operador. A figura 3.2 representa de forma esquemática o exposto neste parágrafo.

A elaboração de planos de vôo será detalhado no capítulo 6, enquanto que a interpretação dos planos de vôo resultantes da elaboração será explorada em maiores detalhes no capítulo 7.

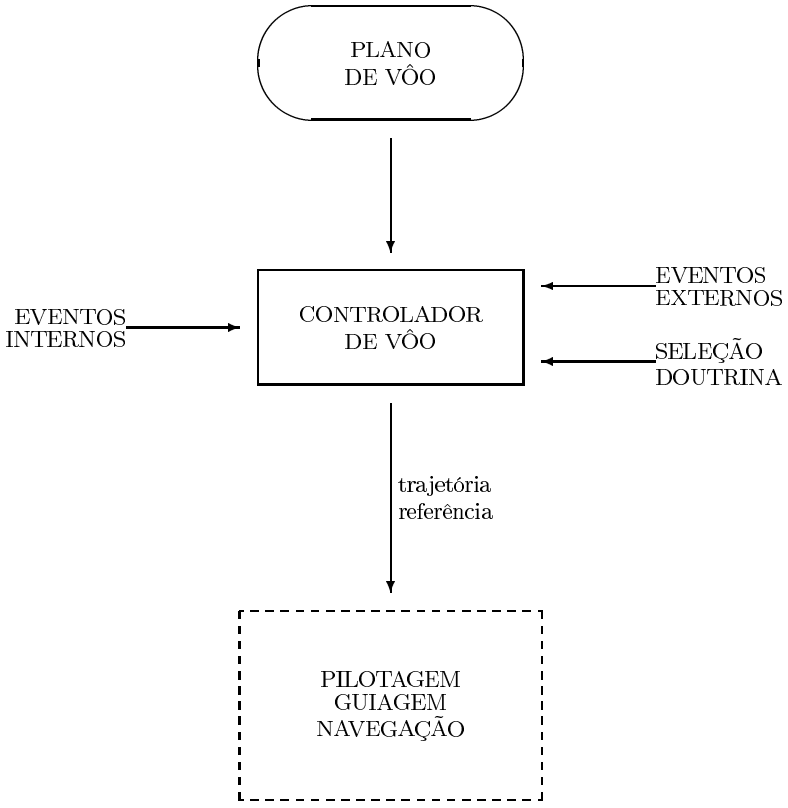


Figura 3.2: Interpretação de um plano de vôo a bordo da aeronave

3.3 Hipóteses para utilização da metodologia proposta

Os algoritmos hoje existentes permitem a verificação simbólica de *sistemas híbridos lineares*, ou seja sistemas onde a evolução das variáveis durante a fase contínua é descrita por equações diferenciais de primeiro ordem.[2]

A modelagem de um UAV, sua dinâmica e seu universo de operações por um conjunto de autômatos híbridos lineares torna-se possível através de:

- Utilização de um sistema de coordenadas plano tangente. O sistema de coordenadas plano tangente é um sistema cartesiano que permite resolver os problemas de navegação utilizando a geometria do plano ao invés da geometria esférica. O erro

[2]A definição formal de um sistema híbrido linear é apresentada na seção 4.1.4.

introduzido pela aproximação da superfície terrestre por um plano é negligenciável para o raio operacional de UAVs civis[3].

- Operação da aeronave apenas a velocidades pré-determinadas (velocidade mais eficiente, mais econômica, máxima e vôo pairado), o que permite que sua dinâmica seja descrita por equações diferenciais de primeira ordem.

- Operação da aeronave a altitudes comparativamente baixas (geralmente a menos de 500 metros acima do nível do solo), característica de aplicações civis. A operação a baixas altitudes permite desprezar a variação do consumo específico de combustível com a altitude e a não-linearidade associada com esta variação.

- Desconsideração dos períodos de transição entre uma etapa e outra, visto ser sua duração muito inferior à duração das etapas propriamente ditas.

- Aproximação das regiões de cobertura do enlace de comunicação, das zonas de exclusão e das elevações do terreno com resolução satisfatória pela união de regiões definidas por um conjunto de desigualdades de primeira ordem.

- Linearização da variação do consumo específico de combustível com a massa da aeronave[4] utilizando a técnica descrita em [33].

3.4 Resumo do capítulo

Este capítulo objetivou apresentar de forma sucinta a metodologia proposta para solucionar o problema de planejamento e controle de missões de aeronaves não-tripuladas. Maiores detalhes serão apresentados nos capítulos subseqüentes.

Também foram apresentadas neste capítulo as hipóteses necessárias para a realização da metodologia proposta.

[3] O erro também é negligenciável para a maioria dos UAVS militares.

[4] À medida que a missão progride a massa do combustível remanescente a bordo da aeronave diminui. Por esta razão, a massa da aeronave não é constante.

Capítulo 4

Modelagem e Verificação de Sistemas usando Autômatos Híbridos

A dinâmica e as características de aeronaves não-tripuladas descritas no capítulo 2 caracterizam um *sistema híbrido*. Um sistema híbrido é um sistema dinâmico resultante da interação de componentes contínuas (no caso de UAVs, posição, velocidade, combustível) e componentes discretas (por exemplo, as transições entre as diferentes etapas do plano de vôo executado pelo UAV).

Neste capítulo será apresentada uma técnica para a especificação formal e a análise algorítmica de sistemas híbridos.

A técnica aqui apresentada foi desenvolvida independentemente por [29] e [30] e utiliza autômatos finitos associados a variáveis que evoluem continuamente com o tempo, de acordo com as leis da dinâmica do sistema modelado.

A seção 4.1 apresenta autômatos e sistemas híbridos e introduz o caso particular de sistemas híbridos lineares. A seção 4.2 discute a análise e a verificação de sistemas híbridos lineares.

Material introdutório sobre autômatos, linguagens e autômatos temporizados pode ser encontrado no apêndice A.

4.1 Autômatos híbridos e sistemas híbridos

Em 1993, Alur et al. [29] e Nicollin et al. [30] independentemente desenvolveram um modelo para a descrição e análise de sistemas híbridos baseado em autômatos híbridos. A seguinte descrição é baseada principalmente em [31, 34].

Um autômato híbrido é construído pela generalização de um autômato de estados finitos equipado com um conjunto de variáveis contínuas. Um autômato híbrido é capaz de modelar não somente ações discretas (como os autômatos discutidos no apêndice A), mas também atividades contínuas governadas por um conjunto de equações diferenciais.

4.1.1 Um modelo para sistemas híbridos

Informalmente, um *autômato híbrido* é constituído por um conjunto finito de variáveis reais X e por um multigrafo etiquetado (V, E). O conjunto das derivadas primeiras de X será denotado por $\dot{X}$. Os arcos E representam ações discretas e são etiquetados com restrições sobre os valores de X *antes e após* a execução das ações correspondentes. Os vértices V representam atividades contínuas e são etiquetados com restrições sobre os valores de X e $\dot{X}$ *durante* a realização das atividades associadas. Desta forma, o estado de um autômato híbrido pode ser modificado tanto por ações discretas e instantâneas como pelo passar do tempo.

Um *sistema híbrido* é descrito por uma coleção de autômatos híbridos, um para cada componente do sistema. Os autômatos constituintes do sistema operam de forma concorrente e coordenada. A comunicação entre os diferentes autômatos se dá por meio de variáveis compartilhadas e por meio de etiquetas de sincronização.

Um autômato híbrido $H = (X, V, E, syn, act, inv)$ é constituído por seis componentes:

Variáveis Um conjunto finito $X = (x_1, x_2, \ldots, x_n)$ de *variáveis* contendo valores reais. O tamanho n de X é a *dimensão* de H. Uma *avaliação* de H é um ponto $s = (x_1 = a_1, x_2 = a_2, \ldots, x_n = a_n)$ no espaço n-dimensional real R^n e representa o estado das variáveis contínuas do autômato. S será usado para denotar o conjunto das avaliações

possíveis do autômato H.

Lugares Um conjunto finito V de vértices chamados *lugares de controle*.

Um *estado* do autômato H é um par (v, s) constituído de um lugar $v \in V$ e de uma avaliação $s \in R^n$. O termo *região* é usado para denotar um conjunto de estados. As avaliações *associadas com* um lugar v em uma região W são as avaliações s tais que $(v, s) \in W$. Σ será usado para denotar o conjunto dos possíveis estados do autômato H.[1]

Transições Um conjunto finito E de arcos chamados de *transições*. Cada transição $e = (v, a, \mu, v')$ é constituída por um lugar de *origem* $v \in V$, um lugar de *destino* $v' \in V$, um rótulo de sincronização $a \in syn$ e uma *relação de transição* $\mu \subseteq S^2$.

A transição e é dita *habilitada* em um estado (v, s) se para alguma avaliação $s' \in S$, $(s, s') \in \mu$. O estado (v', s') é dito um *sucessor transitivo* do estado (v, s).

Etiquetas de sincronização Um conjunto finito *syn* de *etiquetas de sincronização*, usadas para definir a composição paralela de dois autômatos: se dois autômatos partilham a etiqueta α, então cada α-transição de um dos autômatos é acompanhada de uma α-transição do outro autômato.

Atividades Uma função *act* que atribui a cada lugar $v \in V$ um conjunto de *atividades*. Cada atividade é uma função do conjunto de reais não-negativos $R^{\geq 0}$ para S. O modelo exige que as atividades de cada lugar sejam *invariantes no tempo*: para todos os lugares $v \in V$, atividades $f \in act(v)$, e reais não negativos $t \in R^{\geq 0}$, também $(f + t) \in act(v)$, onde $(f + t)(t') = f(t + t')$ para todo $t' \in R^{\geq 0}$.

Para todos os lugares $v \in V$, atividades $f \in act(v)$ e variáveis $x \in X$ denota-se f^x a função de $R^{\geq 0}$ para R tal que $f^x(t) = f(t)(x)$.

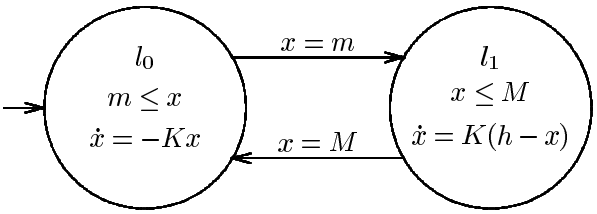
Invariantes Uma função *inv* que atribui a cada lugar $v \in V$ um *invariante* $inv(v) \subseteq S$. O autômato pode permanecer no estado v apenas enquanto o invariante do lugar for verdadeiro. Em outras palavras, invariantes podem ser usados para forçar a evolução de um autômato.

[1] O símbolo Σ será utilizado neste trabalho devido à sua ampla utilização em [31, 34, 29] e não deve ser confundido com o símbolo Σ definido na seção A.1 e representando um alfabeto.

O sistema híbrido H é dito *temporalmente determinístico* se, para cada lugar $v \in V$ e cada avaliação $s \in S$, existe no máximo uma atividade $f \in act(v)$ com $f(0) = s$. Neste caso, a atividade f é denotada por $\varphi_v[s]$.

Exemplo 4.1 Um termostato monitora constantemente a temperatura de uma sala, ligando ou desligando um aquecedor de modo a manter a temperatura dentro de limites pré-determinados. A temperatura é governada por equações diferenciais. Quando o aquecedor está desligado a temperatura, denotada por x, decresce de acordo com a função exponencial $x(t) = \theta e^{-Kt}$, onde t representa o tempo, θ é a temperatura inicial e K é uma constante que depende das características da sala. Quando o aquecedor está ligado, a temperatura evolui de acordo com a função $x(t) = \theta e^{-Kt} + h(1 - e^{Kt})$, onde h é uma constante que depende da potência do aquecedor. Deseja-se manter a temperatura da sala entre o valor mínimo m e o valor máximo M.

O sistema híbrido temporalmente determinístico que modela o sistema descrito no parágrafo anterior é mostrado abaixo. O sistema possui dois lugares: no lugar l_0 o aquecedor está desligado; no lugar l_1 o aquecedor está ligado. Os invariantes são, respectivamente, $m \leq x$ e $x \leq M$. As atividades são as equações diferenciais que representam a evolução da temperatura do modo descrito acima. As relações de transição são especificadas por comandos guardados correspondentes aos pontos de chaveamento do termostato.



□

4.1.2 As trajetórias de um sistema híbrido

A qualquer instante, o estado de um sistema híbrido é determinado por um lugar de controle e por valores para cada variável. Como já mencionado, o estado pode mudar de duas formas distintas:

- por uma *transição discreta* e instantânea que modifica tanto o lugar de controle como os valores das variáveis de acordo com a relação de transição μ.
- pelo *decorrer do tempo* que modifica apenas os valores das variáveis de acordo com as atividades do lugar de controle.

O sistema pode permanecer em um lugar apenas enquanto o invariante do lugar for verdadeiro. Isto implica em que alguma transição discreta deve ocorrer antes do invariante tornar-se falso, pois neste instante a mudança de lugar de controle torna-se obrigatória.

Uma *trajetória* do sistema híbrido H é uma seqüência finita ou infinita

$$\rho = \sigma_0 \mapsto^{t_0}_{f_0} \sigma_1 \mapsto^{t_1}_{f_1} \sigma_2 \mapsto^{t_2}_{f_2} \cdots$$

de estados $\sigma_i = (v_i, s_i) \in \Sigma$, reais não-negativos $t_i \in R^{\geq 0}$ e atividades $f_i \in act(v_i)$, tal que, para todo $i \geq 0$:

1. $f_i(0) = s_i$,
2. para todo $0 \leq t \leq t_i$, $f_i(t) \in inv(v_i)$,
3. o estado σ_{i+1} é um sucessor transitivo do estado $\sigma'_i = (v_i, f_i(t_i))$.

O estado σ'_i é dito um *sucessor temporal* do estado σ_i; o estado σ_{i+1} é dito um *sucessor transitivo* de σ_i. Denota-se por $[H]$ o conjunto de trajetórias do sistema híbrido H.

Observe-se que para sistemas temporalmente determinísticos, não é necessário especificar f_i na relação $\mapsto$.

4.1.3 Composição paralela de sistemas híbridos

Sejam dois sistemas híbridos $H_1 = (X_1, V_1, E_1, syn_1, act_1, inv_1)$ e $H_2 = (X_2, V_2, E_2, syn_2, act_2, inv_2)$ que sincronizam através do subconjunto comum de rótulos de sincronização $syn_1 \cap syn_2$.

O *produto* $H_1 \times H_2$ é o sistema híbrido $(X_1 \cup X_2, V_1 \times V_2, E, syn_1 \cup syn_2, act, inv)$, tal que:

- $((v_1, v_2), a, \mu, (v_1', v_2')) \in E$ se e somente se:
  1. $(v_1, a_1, \mu_1, v_1') \in E_1$ e $(v_2, a_2, \mu_2, v_2') \in E_2$,
  2. $a_1 = a_2 = a$ ou $a_1 \notin (syn_1 \cup syn_2)$ e $a_2 = \tau$, ou $a_1 = \tau$ e $a_2 \notin (syn_1 \cup syn_2)$,
  3. $\mu = \mu_1 \cap \mu_2$;
- $act(v_1, v_2) = act_1(v_1) \cap act_2(v_2)$;
- $inv(v_1, v_2) = inv_1(v_1) \cap inv_2(v_2)$.

Os lugares de controle do autômato resultante são pares de lugares da forma (v_1, v_2). O invariante do lugar (v_1, v_2) é a conjunção dos invariantes dos lugares v_1 e v_2.

Visto que os dois autômatos podem possuir variáveis em comum, a dimensão do autômato $H_1 \times H_2$ será um valor entre $\max(n_1, n_2)$ e $n_1 + n_2$.

Todas as trajetórias do sistema híbrido produto são trajetórias de ambos sistemas híbridos componentes:

$$[H_1 \times H_2]_{S_1} \subseteq [H_1] \text{ e } [H_1 \times H_2]_{S_2} \subseteq [H_2]$$

onde $[H_1 \times H_2]_{S_i}$ representa a projeção de $[H_1 \times H_2]$ sobre S_i.

O sistema híbrido resultante do produto de dois sistemas híbridos temporalmente determinísticos é também temporalmente determinístico.

4.1.4 Sistemas híbridos lineares

Um *termo linear* sobre um conjunto X de variáveis é uma combinação linear das variáveis em X com coeficientes inteiros. Uma *fórmula linear* sobre X é uma combinação booleana de desigualdades entre termos lineares sobre X.

O sistema híbrido temporalmente determinístico $H = (X, V, E, syn, act, inv)$ é dito *linear* se as atividades, invariantes e relações de transição de H podem ser definidas por expressões lineares sobre o conjunto X de variáveis:

1. Para todos os lugares $v \in V$, as atividades $act(v)$ são definidas por um conjunto de equações diferenciais da forma $\dot{a} = k_x$, uma para cada variável $x \in X$, onde $k_x \in Z$ é uma constante inteira: para todas as avaliações $s \in S$, variáveis $x \in X$ e reais não-negativos $t \in R^{\geq 0}$,

$$\varphi_v^x[s](t) = s(x) + k_x t.$$

   A notação $act(v, x) = k_x$ denota a *taxa* de variação da variável x no lugar v.

2. Para todos os lugares $v \in V$, o invariante $inv(v)$ é definido por uma fórmula linear ψ sobre X:

$$s \in inv(v) \text{ se e somente se } s(\psi).$$

3. Para todas as transições $e \in E$, a relação de transição μ é definida por um conjunto guardado de atribuições não-determinísticas

$$\psi \Rightarrow \{x := [\alpha_x, \beta_x] \mid x \in X\},$$

   onde a guarda ψ é uma fórmula linear e para cada variável $x \in X$, os limites α_x e β_x são termos lineares:

$$(s, s') \in \mu \text{ se e somente se } s(\psi) \wedge \forall x \in X \text{ e } v(\alpha_x) \leq v'(x) \leq v(\beta_x)$$

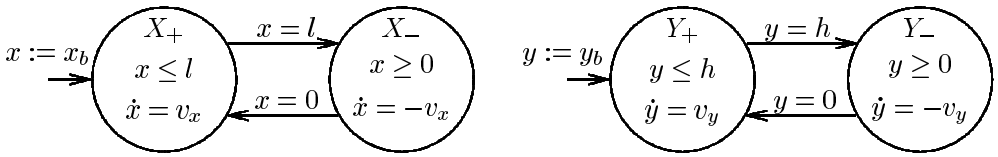
   Se $\alpha_x = \beta_x$, usa-se a notação $\mu(e, x) = \alpha_x$ para referenciar o valor atualizado da variável x após a transição e.

Exemplo 4.2 Seja uma mesa de bilhar de dimensões X e Y e uma bola de bilhar b.

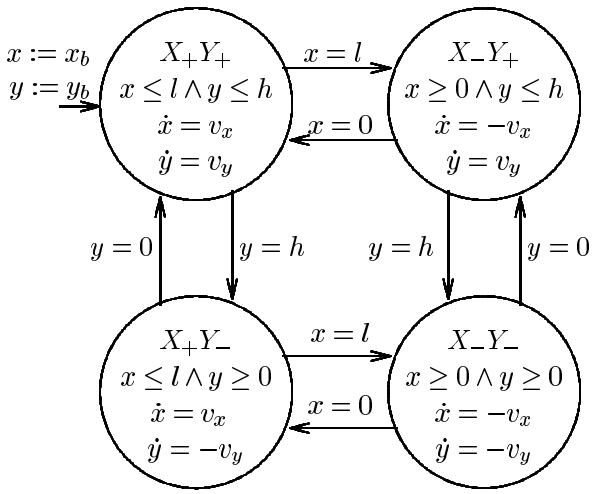
Consideremos que os choques da bola com a borda da mesa sejam perfeitamente elásticos e que não haja atrito entre a bola e a mesa.

Inicialmente a bola encontra-se na posição $b = (x_b, y_b)$ e desloca-se com velocidade v, cujas componentes ao longo das dimensões X e Y são, respectivamente, v_x e v_y. Se a bola atingir uma das bordas da mesa será rebatida, isto é, o sinal da velocidade correspondente será invertido.

Os autômatos híbridos lineares da figura abaixo representam os movimentos da bola ao longo das laterais da mesa. Os lugares X_+ e X_- descrevem o movimento da bola de bilhar ao longo da dimensão X da mesa, enquanto que Y_+ e Y_- descrevem o movimento ao longo da dimensão Y da mesa.



A composição paralela dos autômatos acima resulta no seguinte sistema híbrido:



□

4.1.5 Casos particulares de sistemas híbridos lineares

Existem diversos casos particulares de sistemas híbridos lineares:

- Se $act(v, x) = 0$ para todos os lugares $v \in V$, então x é uma *variável discreta*. Ou seja, o valor de uma variável discreta só é alterado quando o lugar de controle muda. Um *sistema discreto* é um sistema linear híbrido em que todas as variáveis são discretas.

- Uma variável discreta x é uma *proposição* se $\mu(e, x) \in \{0, 1\}$ para todas as transições $e \in E$. Um *sistema de estados finitos* é um sistema linear híbrido em que todas as variáveis são proposições.

- Se $act(v, x) = 1$ para todos os lugares v e $\mu(e, x) \in \{0, x\}$ para todas as transições e, então x é um *relógio*. Isto implica em que (1) o valor de um relógio é uniformemente crescente com o passar do tempo e (2) uma transição discreta reinicializa o relógio para zero ou não o altera. Um *autômato temporizado* [32] é um sistema híbrido linear em que todas as variáveis são proposições ou relógios e as expressões lineares são combinações booleanas de desigualdades da forma $x\#c$ ou $x - y\#c$, onde c é um inteiro não-negativo e $\# \in \{<, \leq, =, >, \geq\}$.

- Se existe uma constante inteira não-negativa $k \in Z$ tal que $act(v, x) = k$ para todos os lugares v e $\mu(e, x) \in \{0, x\}$ para todas as transições e, então x é um *relógio não-unitário*. Um relógio não-unitário é similar a um relógio ordinário exceção feita ao fato do mesmo avançar a uma taxa constante e diferente de 1. Um *sistema temporizado de múltiplas taxas* é um sistema linear híbrido cujas variáveis são proposições ou relógios não-unitários. Um *sistema temporizado de n-taxas* é um sistema temporizado de múltiplas taxas cujos relógios não-unitários avançam a n diferentes taxas.

- Se $act(v, x) \in \{0, 1\}$ para todos os lugares v e $\mu(e, x) \in \{0, x\}$ para todas as transições e, então x é um *integrador*. Um integrador é um relógio cujo progresso pode ser temporariamente suspenso, sendo geralmente utilizado para medir tempos cumulativos. Um *sistema integrador* é um sistema linear híbrido cujas variáveis são proposições ou integradores.

- Uma variável discreta x é um *parâmetro* se $\mu(e, x) = x$ para todas as transições $e \in E$. Em outras palavras, um parâmetro é uma constante simbólica. Para cada subclasse de sistemas híbridos lineares definida acima, podem-se obter versões parametrizadas dos mesmos ao admitir parâmetros em sua definição.

Sistemas lineares híbridos, incluindo todas as subclasses definidas acima, são fechados sob a operação de composição paralela.

4.2 Análise e verificação de sistemas híbridos lineares

Esta seção, baseada em [31, 34, 35], apresentará três algoritmos semi-decidíveis para a análise de sistemas híbridos lineares. Os algoritmos baseiam-se no cômputo de estados predecessores e sucessores e na minimização de um dado conjunto de estados (ou região).

Também se discutirá a verificação de um sistema híbrido linear H quanto à satisfação de um conjunto de requisitos especificado usando a lógica temporal de tempo real TCTL (*timed computation tree logic*).

4.2.1 Estados alcançáveis

Sejam σ e σ' dois estados de um sistema híbrido H. O estado σ' é dito *alcançável* a partir do estado σ, denotado $\sigma \mapsto^* \sigma'$, se existe uma trajetória de H que começa em σ e termina em σ'. O problema dos estados alcançáveis consiste então em verificar $\sigma \mapsto^* \sigma'$ para dois estados σ e σ' de um autômato híbrido H.

A resolução do problema dos estados alcançáveis é central para a verificação de sistemas híbridos. A verificação de propriedades invariantes de um sistema pode ser convertida em um problema de estados alcançáveis: uma região $W \subseteq \Sigma$ é um invariante do sistema híbrido H se e somente se nenhum estado de $\Sigma - W$ é alcançável de um estado inicial de H.

Um sistema híbrido linear é dito *simples* se todos os termos atômicos lineares dos invariantes e das guardas das transições são da forma $x \leq k$ ou $k \leq x$, para uma variável $x \in X$ e uma constante inteira $k \in Z$.

O problema dos estados alcançáveis é:

- decidível para sistemas temporizados de n-taxas simples;

- não-decidível para sistemas temporizados de 2 taxas;
- não-decidível para sistemas integradores simples.

4.2.2 Cômputo de estados sucessores

Dado um lugar $v \in V$ e um conjunto de avaliações $P \subseteq S$, define-se por *fechamento temporal progressivo* (*forward time closure*) $\langle P \rangle_v^{\nearrow}$ o conjunto de avaliações alcançáveis de alguma avaliação $s \in P$ por evolução temporal:

$$s' \in \langle P \rangle_v^{\nearrow} \text{ se e somente se } \exists s \in S, t \in R^{\geq 0} \text{ e } s \in P \wedge \mathrm{tcp}_v[s](t) \wedge s' = \varphi_v[s](t).$$

Ou seja, para todo $s' \in \langle P \rangle_s^{\nearrow}$, existe uma avaliação $s \in P$ e um real não negativo $t \in R^{\geq 0}$, tal que $(v, s) \mapsto^t (v, s')$.

Dada uma transição $e = (v, a, \mu, v')$ e um conjunto de avaliações $P \subseteq S$, a *pós-condição* $\mathrm{post}_e[P]$ de P com respeito a e é o conjunto de avaliações alcançáveis de alguma avaliação $s \in P$ pela execução da transição e.

$$s' \in \mathrm{post}_e[P] \text{ se e somente se } \exists s \in S \text{ e } \exists s \in P \wedge (s, s') \in \mu.$$

Portanto, para todas as avaliações $s \in \mathrm{post}_e[P]$, existe uma avaliação $s \in P$, tal que $(v, s) \mapsto^a (v', s')$.

Dado um conjunto de avaliações $P \subseteq S$, denota-se (v, P) a região $\{(v, s) \mid s \in P\}$; escreve-se $(v, s) \in (v, P)$ se e somente se $s \in P$. O fechamento temporal progressivo e a pós-condição podem ser estendidas a regiões: para $W = \bigcup_{v \in V} (v, W_v)$

$$\begin{aligned} \langle W \rangle^{\nearrow} &= \bigcup_{v \in V} (v, \langle W_v \rangle_v^{\nearrow}) \\ \mathrm{post}[W] &= \bigcup_{e=(v,v') \in E} (v', \mathrm{post}_e[W_v]). \end{aligned}$$

Uma *trajetória simbólica* do sistema híbrido linear H é uma seqüência finita ou infinita de regiões da forma

$$\varrho : \ (v_0, P_0)(v_1, P_1) \ldots (v_i, P_i) \ldots$$

tais que para todo $i \geq 0$, existe uma transição e_i de v_i para v_{i+1} e

$$P_{i+1} = \mathrm{post}_{e_i}[\langle P_i \rangle^{\nearrow}_{v_i}].$$

Isto é, a região (v_{i+1}, P_{i+1}) é o conjunto de estados alcançáveis de um estado $(v_0, s_0) \in (v_0, P_0)$ após execução da seqüência $e_0, \ldots, e_i$ de transições.

A trajetória simbólica ϱ representa o conjunto de todas as trajetórias da forma

$$(v_0, s_0) \mapsto^{t_0} (v_1, s_1) \mapsto^{t_1} \cdots$$

tais que $(v_i, s_i) \in (v_i, P_i)$ para todo $i \geq 0$.

Toda trajetória de H pode ser representada por alguma trajetória simbólica de H.

Dada uma região $I \subseteq \Sigma$ a *região alcançável* a partir de I, $(I \mapsto^*) \subseteq \Sigma$, é o conjunto de todos os estados alcançáveis de estados em I:

$$\sigma \in (I \mapsto^*) \text{ se e somente se } \exists \sigma' \in I \ \text{ e } \ \sigma' \mapsto^* \sigma.$$

Notar que $I \subseteq (I \mapsto^*)$.

A proposição a seguir sugere uma maneira de computar o conjunto de estados alcançáveis de I, $(I \mapsto^*)$.

Proposição 4.1 Seja $I = \bigcup_{v \in V}(v, I_v)$ uma região do sistema híbrido linear H. A região alcançável $(I \mapsto^*) = \bigcup_{v \in V}(v, W_v)$ é o menor ponto fixo da equação

$$X = \langle I \cup \mathrm{post}[X] \rangle^{\nearrow}$$

ou, de forma equivalente, para todos os lugares $v \in V$, o conjunto W_v de avaliações é o menor ponto fixo do conjunto de equações

$$X_v = \langle I_v \cup \bigcup_{e=(v,v') \in E} \mathrm{post}_e[X_{v'}] \rangle_v^{\nearrow}.$$

□

4.2.3 Cômputo de estados predecessores

Com auxílio do fechamento temporal progressivo e da pós-condição definiu-se na seção anterior o sucessor de uma região W. Dualmente, é possível definir o *predecessor* de W.

Dado um lugar $v \in V$ e um conjunto de avaliações $P \subseteq S$, define-se por *fechamento temporal regressivo* (*backward time closure*) $\langle P \rangle_v^{\swarrow}$ o conjunto de avaliações a partir das quais é possível alcançar alguma avaliação $s \in P$ por evolução temporal:

$$s' \in \langle P \rangle_v^{\swarrow} \text{ se e somente se } \exists s \in S, t \in R^{\geq 0} \text{ e } s = \varphi_v[s'](t) \wedge s \in P \wedge \mathrm{tcp}_v[s'](t).$$

Ou seja, para todo $s' \in \langle P \rangle_{\hat{s}}^{\swarrow}$, existe uma avaliação $s \in P$ e um real não negativo $t \in R^{\geq 0}$, tal que $(v, s') \mapsto^t (v, s)$.

Dada uma transição $e = (v, a, \mu, v')$ e um conjunto de avaliações $P \subseteq S$, a *pré-condição* $\mathrm{pre}_e[P]$ de P com respeito a e é o conjunto de avaliações a partir das quais é possível alcançar alguma avaliação $s \in P$ pela execução da transição e.

$$s' \in \mathrm{pre}_e[P] \text{ se e somente se } \exists s \in S. \exists s \in P \wedge (s', s) \in \mu.$$

Portanto, para todas as avaliações $s' \in \mathrm{pre}_e[P]$, existe uma avaliação $s \in P$, tal que $(v, s') \mapsto^a (v', s)$.

O fechamento temporal regressivo e a pré-condição também podem ser estendidas a regiões: para $W = \bigcup_{v \in V}(v, W_v)$

$$\begin{aligned} \langle W \rangle^{\swarrow} &= \bigcup_{v \in V} (v, \langle W_v \rangle_v^{\swarrow}) \\ \mathrm{pre}[W] &= \bigcup_{e=(v,v') \in E} (v', \mathrm{post}_e[W_v]). \end{aligned}$$

Dada uma região $W \subseteq \Sigma$ a *região inicial* de W, $(\mapsto^* W) \subseteq \Sigma$, é o conjunto de todos os estados a partir dos quais um estado de W é alcançável:

$$\sigma \in (\mapsto^* W) \text{ se e somente se } \exists \sigma' \in W \text{ e } \sigma \mapsto^* \sigma'.$$

Notar que $W \subseteq (\mapsto^* W)$.

A proposição apresentada abaixo sugere uma maneira de computar $(\mapsto^* W)$.

Proposição 4.2 Seja $W = \bigcup_{v \in V}(v, W_v)$ uma região do sistema híbrido linear H. A região inicial $I = \bigcup_{v \in V}(v, I_v)$ é o menor ponto fixo da equação

$$X = \langle W \cup \mathrm{pre}[X] \rangle^{\swarrow}$$

ou, de forma equivalente, para todos os lugares $v \in V$, o conjunto I_v de avaliações é o menor ponto fixo do conjunto de equações

$$X_v = \langle W_v \cup \bigcup_{e=(v,v')\in E} \mathrm{pre}_e[X_{v'}]\rangle_v^{\swarrow}.$$

□

4.2.4 Minimização de estados

A relação $\mapsto$ pode ser estendida para regiões: para todas as regiões W e W', escreve-se $W \mapsto W'$ se algum estado $\sigma' \in W'$ é um sucessor de algum estado $\sigma \in W$.

Seja π uma partição do espaço de estados Σ.

Uma região $W \in \pi$ é dita *estável* se para todo $W' \in \pi$,

$$W \mapsto W' \text{ implica em } \forall \sigma \in W \text{ e } \{\sigma\} \mapsto W'$$

ou, de forma equivalente,

$$W \cap \mathrm{pre}[\langle W'\rangle^{\swarrow}] \neq \emptyset \text{ implica em } W \subseteq \mathrm{pre}[\langle W'\rangle^{\swarrow}].$$

A partição π é uma *bissimulação* se toda região $W \in \pi$ é estável.

A partição π *respeita* a região W_F se para toda região $W \in \pi$, $W \subseteq W_F$ ou $W \cap W_F = \emptyset$.

Uma partição π que respeita uma região W_F e é uma bissimulação pode ser usada para computar a região inicial ($\mapsto^* W_F$): para todas as regiões $W \in \pi$, se $W \mapsto^* W_F$ então $W \subseteq (\mapsto^* W_F)$, em caso contrário $W \cap (\mapsto^* W_F) = \emptyset$. O objetivo é construir a bissimulação de maior granularidade que respeita uma dada região W_F, desde que exista uma bissimulação finita que respeite W_F.

Se, além da região W_F, parte-se de uma região I que restringe o interesse à região ($I \mapsto^*$), torna-se vantajosa a utilização de um algoritmo capaz de executar simultaneamente a

análise de alcançabilidade e minimização de um sistema de transições ([36, 37]), como o algoritmo descrito a seguir.

A partir de uma partição inicial $\{W_F, \Sigma - W_F\}$ que respeita W_F, o algoritmo seleciona uma região W e verifica se W é estável com respeito à partição atual; em caso negativo, W é particionado em subconjuntos menores.

No algoritmo cujo pseudocódigo é mostrado abaixo, π é a partição atual, $\alpha \subseteq \pi$ contém as regiões W alcançáveis a partir de I e $\beta \subseteq \pi$ contém as regiões W estáveis com respeito a π. A função split$[\pi](W)$ particiona a região $W \in \pi$ em subconjuntos que são "mais" estáveis com respeito a π:

$$\text{split}[\pi](W) := \begin{cases} \{W', W - W'\} & \text{se } \exists W'' \in \pi \text{ e } W' = \text{pre}[\langle W'' \rangle^{\swarrow}] \cap W \wedge W' \subset W \\ \{W\} & \text{em caso contrário} \end{cases}$$

$\pi := \{W_F, \Sigma - W_F\}$; $\alpha := \{W \mid W \cap I \neq \emptyset\}$; $\beta := \emptyset$
while $\alpha \neq \beta$ **do**
    selecione $W \in (\alpha - \beta)$
    $\alpha' := \text{split}[\pi](W)$
    if $\alpha' = \{W\}$ **then**
        $\beta := \beta \cup \{W\}$
        $\alpha := \alpha \cup \{W' \in \pi \mid W \mapsto W'\}$
    else
        $\alpha := \alpha - \{W\}$
        if $\exists W' \in \alpha'$ tal que $W' \cap I \neq \emptyset$ **then** $\alpha := \alpha \cup \{W'\}$ **fi**
        $\beta := \beta - \{W' \in \pi \mid W' \mapsto W\}$
        $\pi := (\pi - \{W\}) \cup \alpha'$
    fi
od
return existe $W \in \alpha$ tal que $W \subseteq W_F$.

4.2.5 Verificação de modelos

Nas seções anteriores foram descritos os algoritmos de cômputo de estados predecessores e sucessores e de minimização de estados e sua utilização para a resolução do problema dos estados alcançáveis de sistemas híbridos lineares. Nesta seção será abordado o problema mais genérico de verificar se um sistema híbrido linear H satisfaz um requisito expresso na lógica temporal de tempo real TCTL (*timed computation tree logic*) [38].

A lógica tempo real TCTL

Seja C um conjunto de relógios não contido em X, ou seja $C \cap X = \emptyset$. Um *predicado de estados* é uma fórmula linear sobre o conjunto de variáveis $X \cup C$.

As fórmulas de TCTL são construídas a partir dos predicados de estados usando operadores booleanos, os operadores temporais $\exists\mathcal{U}$ ("possivelmente") e $\forall\mathcal{U}$ ("forçosamente") e um quantificador de reinicialização dos relógios em C. Ou seja, as fórmulas de TCTL são definidas pela seguinte gramática:

$$\phi ::= \varphi \mid \neg\phi \mid \phi_1 \vee \phi_2 \mid z.\phi \mid \phi_1 \exists\mathcal{U} \phi_2 \mid \phi_1 \forall\mathcal{U} \phi_2$$

onde φ é um predicado de estados e $z \in C$. A fórmula ϕ é dita *fechada* se todas as ocorrências de um relógio $x \in C$ estão contidos no escopo de um quantificador de reinicialização z.

As fórmulas fechadas de TCTL são interpretadas sobre o espaço de estados Σ do sistema híbrido linear H.

Um estado σ satisfaz a fórmula $\phi_1 \exists\mathcal{U} \phi_2$ se existe *alguma* trajetória de H do estado σ a um estado σ' satisfazendo ϕ_2 de forma que $\phi_1 \vee \phi_2$ é satisfeito ao longo de toda a trajetória.

Um estado σ satisfaz a fórmula $\phi_1 \forall\mathcal{U} \phi_2$ se para *toda* trajetória de H do estado σ a um estado σ' satisfazendo ϕ_2, $\phi_1 \vee \phi_2$ é satisfeito ao longo de toda a trajetória.

Relógios podem ser usados para exprimir restrições temporais. Por exemplo, a fórmula

$z.(true\exists\mathcal{U}(\phi \wedge z \leq 5))$ expressa que existe uma trajetória na qual ϕ é satisfeita dentro de 5 unidades de tempo.

Interpretando $\Box$ como "sempre" e $\Diamond$ como "eventualmente", as seguintes abreviações são utilizadas:

- $\forall\Diamond\phi$ (*all diamond*) para $true\forall\mathcal{U}\phi$: ao longo de todas as trajetórias, ϕ eventualmente é satisfeita;
- $\exists\Diamond\phi$ (*exists diamond*) para $true\exists\mathcal{U}\phi$: ao longo de alguma trajetória, ϕ eventualmente é satisfeita;
- $\exists\Box\phi$ (*exists box*) para $\neg\forall\Diamond\neg\phi$: ao longo de alguma trajetória, ϕ é sempre satisfeita;
- $\forall\Box\phi$ (*all box*) para $\neg\exists\Diamond\neg\phi$: ao longo de todas as trajetórias, ϕ é sempre satisfeita.

Restrições temporais são indicadas por subscritos dos operadores temporais. Por exemplo, a fórmula $z.\exists\Diamond(\phi \wedge z < 5)$ é abreviada como $\exists\Diamond_{<5}\phi$.

Seja $\rho = \sigma_0 \mapsto^{t_0} \sigma_1 \mapsto^{t_1} \ldots$ uma trajetória do sistema híbrido linear H, com $\sigma_i = (v_i, s_i)$ para todo $i \geq 0$. Uma posição π de ρ é um par (i,t) constituído de um inteiro não-negativo i e um real não-negativo $t \leq t_i$. As posições de π são ordenadas lexicograficamente, isto é, $(i,t) \leq (j,t')$ se e somente se $i < j$ ou $i = j$ e $t \leq t'$. Para todas as posições $\pi = (i,t)$ de ρ:

- o estado $\rho(\pi)$ na posição π de ρ é $(v_i, \varphi_{v_i}[s_i](t))$ e
- o tempo $\delta_\rho(\pi)$ na posição π de ρ é $t + \sum_{j<i} t_j$.

Uma *avaliação dos relógios* ε é uma função de C para $R^{\geq 0}$. Para qualquer real não-negativo $t \in R^{\leq 0}$, denota-se por $\varepsilon + t$ a avaliação dos relógios ε', tal que $\varepsilon'(z) = \varepsilon(z) + t$ para todos os relógios $z \in C$. Para qualquer relógio $z \in C$, denota-se por $\varepsilon[z := 0]$ a avaliação ε' tal que $\varepsilon'(z) = 0$ e $\varepsilon'(z') = \varepsilon(z')$ para todos os relógios $z' \neq z$.

Um *estado estendido* (σ, ε) consiste de um estado $\sigma \in \Sigma$ e uma avaliação dos relógios ε. Diz-se que o estado estendido (σ, ε) *satisfaz* a fórmula ϕ (denotado por $(\sigma, \varepsilon) \models \phi$), se:

- $(\sigma, \varepsilon) \models \varphi$ se e somente se $(\sigma, \varepsilon)(\varphi)$;

- $(\sigma, \varepsilon) \models \neg\phi$ se e somente se $(\sigma, \varepsilon) \not\models \phi$;
- $(\sigma, \varepsilon) \models \phi_1 \vee \phi_2$ se e somente se $(\sigma, \varepsilon) \models \phi_1$ ou $(\sigma, \varepsilon) \models \phi_2$;
- $(\sigma, \varepsilon) \models z.\phi_1$ se e somente se $(\sigma, \varepsilon[z := 0]) \models \phi_1$;
- $(\sigma, \varepsilon) \models \phi_1 \exists\mathcal{U} \phi_2$ se e somente se existem uma trajetória ρ de H com $\rho(0,0) = \sigma$ e uma posição π de ρ tal que:
  1. $(\rho(\pi), \varepsilon + \delta_\rho(\pi)) \models \phi_2$ e
  2. para todas as posições $\pi' \leq \pi$ de ρ, $(\rho(\pi'), \varepsilon + \delta_\rho(\pi')) \models \phi_1 \vee \phi_2$;
- $(\sigma, \varepsilon) \models \phi_1 \forall\mathcal{U} \phi_2$ se e somente se para todas as trajetórias divergentes ρ de H com $\rho(0,0) = \sigma$, existe uma posição π de ρ tal que:
  1. $(\rho(\pi), \varepsilon + \delta_\rho(\pi)) \models \phi_2$ e
  2. para todas as posições $\pi' \leq \pi$ de ρ, $(\rho(\pi'), \varepsilon + \delta_\rho(\pi')) \models \phi_1 \vee \phi_2$.

Seja ϕ uma fórmula fechada de TCTL. Um estado $\sigma \in \Sigma$ satisfaz ϕ, denotado $\sigma \models \phi$, se $(\sigma, \varepsilon) \models \phi$ para todas as avaliações de relógios ε. O sistema híbrido linear H satisfaz ϕ, denotado $H \models \phi$, se todos os estados de H satisfazem ϕ. O *conjunto característico* $[[\phi]] \subseteq \Sigma$ de ϕ é o conjunto de estados que satisfaz ϕ.

Algoritmo de verificação

Dada uma fórmula fechada de TCTL, ϕ, um algoritmo de verificação computa o conjunto característico $[[\phi]]$. O algoritmo aqui apresentado foi desenvolvido em [39] e consiste em um procedimento semi-decidível para verificação de fórmulas TCTL sobre sistemas híbridos lineares.

O procedimento é baseado no operador binário $\rhd$. Dadas duas regiões $W, W' \subseteq \Sigma$, a região $W \rhd W'$ é o conjunto de estados σ que possuem um sucessor $\sigma' \in W'$ tal que todos os estados entre σ e σ' estejam contidos em $W \cup W'$: $(v, s) \in (W \rhd W')$ se e somente se

$$\exists (v', s') \in W', t \in R^{\geq 0} \text{ e } ((v, s) \mapsto^t (v', s') \wedge \forall 0 \leq t' \leq t \text{ e } (v, s + t') \in (W \cup W')).$$

Para definir o operador $\triangleright$ sintaticamente é necessário introduzir alguma notação adicional. Para uma fórmula linear φ, estende-se o operador tcp de forma a:

$$\text{tcp}_v[\varphi][s](t) \text{ se e somente se } \forall 0 \leq t' \leq t \text{ e } \varphi_v[s](t') \in (inv(v) \cap [[\varphi]]);$$

ou seja, todas as avaliações ao longo da evolução de um tempo t a partir do estado (v, s) satisfazem não somente o invariante do lugar v mas também φ. Para um estado $\sigma = (v, s) \in \Sigma$, denota-se por $\varphi[\sigma]$ a função $\varphi_v[s]$. Para uma região $W = \bigcup_{v \in V}(v, W_v)$, escreve-se:

$$\text{tcp}[W][\sigma](t) \text{ se e somente se } \text{tcp}_v[W_v][v](t).$$

Agora, dadas duas regiões $W, W' \subseteq \Sigma$, define-se a região $W \triangleright W'$ como

$$\sigma \in (W \triangleright W') \text{ se e somente se } \exists t \in R^{\geq 0} \text{ e } (\varphi[\sigma](t) \in pre[W'] \wedge \text{tcp}[W \cup W'][\sigma](t)).$$

A seguir discute-se a aplicação do método para algumas classes importantes de fórmulas TCTL:

- Sejam W e W' os conjuntos característicos de duas fórmulas TCTL, respectivamente ϕ e ϕ'. O conjunto característico da fórmula $\phi \exists \mathcal{U} \phi'$ pode ser computado iterativamente como $\bigcup_i W_i$, onde
  - $W_0 = W'$ e
  - para todo $i \geq 0$, $W_{i+1} = W_i \cup (W \triangleright W_i)$.
- Para verificar se a fórmula ϕ é um invariante de H, basta verificar se o conjunto dos estados iniciais está contido no conjunto característico da fórmula $\forall \Box \phi$. Este conjunto característico pode ser computado iterativamente como $\bigcap_i W_i$, onde
  - $W_0 = [[\phi]]$ e
  - para todo $i \geq 0$, $W_{i+1} = W_i \cap \neg(true \triangleright \neg W_i)$.

- A propriedade tempo real que assegura que um certo evento ocorre dentro de um certo limite temporal é expressa em TCTL por uma fórmula da forma $\forall\Diamond_{\leq c}\phi$, cujo conjunto característico pode ser iterativamente computado como $\neg\bigcup_i W_i[z := 0]$, onde

  - $W_0 = [[z > c]]$ e
  - para todo $i \geq 0$, $W_{i+1} = W_i \cup ((\neg W) \rhd W_i)$,

  onde $W = [[\phi]]$ e $z \in C$.

4.2.6 Utilização dos diferentes métodos de análise e verificação de sistemas híbridos lineares

Como descrito nas seções anteriores, a análise e verificação de sistemas híbridos lineares pode ser feita através de:

- cômputo dos estados sucessores;
- cômputo dos estados predecessores;
- minimização de estados;
- verificação quanto à satisfação de requisitos expressos na lógica TCTL.

Se o critério a ser verificado pode ser expresso em termos de um estado ou região que deve ser *sempre* alcançável (critério de *utilidade*) ou de um estado ou região que *nunca* deve ser alcançável (critério de *segurança*), pode-se usar o cômputo de estados sucessores a fim de verificar se o estado ou região em questão é ou não alcançável a partir de um estado inicial I.

O cômputo de estados predecessores pode ser usado para determinar a partir de quais estados um estado ou região de interesse é alcançável, enquanto a minimização de estados permite reduzir o número de estados a ser considerado durante a análise. A verificação quanto à satisfação de requisitos expressos na lógica TCTL permite examinar critérios lógicos e temporais de um sistema híbrido linear.

4.2.7 Ferramentas

Os autores do modelo para descrição e análise de sistemas híbridos baseado em autômatos híbridos descrito neste capítulo também dedicaram-se ao desenvolvimento de ferramentas computacionais para mecanização da análise de sistemas híbridos.

Kronos

Kronos, desenvolvido no VERIMAG (França), é "uma ferramenta destinada à *verificação simbólica de modelos* para sistemas tempo-real", [40].

As entradas da ferramenta são:

- a descrição de um sistema tempo real na forma de um *grafo temporizado*. Grafos temporizados são autômatos equipados com um conjunto finito de relógios utilizados para exprimir restrições temporais;
- uma fórmula TCTL especificando um requerimento a ser verificado.

A ferramenta produz como saída o conjunto de estados do sistema tempo real que satisfaz a fórmula TCTL especificada.

HyTech

HyTech, desenvolvido na Universidade de Cornell (EUA), é uma ferramenta destinada à "análise automática de sistemas híbridos", [41, 42].

A entrada da ferramenta é dividida em duas partes:

Descrição do sistema a ser analisado na forma de representação textual de autômatos híbridos lineares. A ferramenta assume que o sistema híbrido a ser analisado resulta da composição paralela de todos os autômatos especificados.

Comandos para análise que permitem:

- descrever regiões de interesse através de desigualdades lineares.

  Essas regiões podem ser armazenadas em variáveis e combinadas através das operações de complementação, intersecção, união e diferença de regiões.

  HyTech permite o cálculo de regiões sucessoras e antecessoras. Outros comandos permitem calcular estados sucessores (ou antecessores) iterativamente até a convergência, efetivamente computando a região alcançável (ou região inicial) de uma região.

- comparar regiões quanto à equivalência e inclusão e testar se regiões são vazias.

HyTech também suporta o uso de parâmetros simbólicos.

4.3 Resumo do capítulo

Autômatos híbridos, suas possíveis trajetórias e o conceito de região alcançável por um autômato híbrido foram descritos. A construção de sistemas híbridos complexos a partir da composição paralela de autômatos híbridos componentes também foi abordada.

Autômatos híbridos lineares foram apresentados como sendo um caso particular de autômatos híbridos nos quais a evolução das variáveis contínuas obedece a equações diferenciais de primeira ordem.

Três técnicas para análise de sistemas híbridos lineares foram apresentadas: cômputo de estados sucessores, cômputo de estados predecessores e minimização de estados. O capítulo foi encerrado com uma seção sobre a verificação de sistemas híbridos com respeito à requisitos expressos na lógica temporal TCTL.

O capítulo encerrou com uma breve descrição de duas ferramentas de análise e verificação de sistemas híbridos: Kronos e HyTech.

Capítulo 5

Modelagem de Missões

A abordagem aqui proposta para modelagem de missões de aeronaves não-tripuladas consiste em:

- Modelar a dinâmica da aeronave sob as condições meteorológicas prevalentes (ou esperadas/previstas) utilizando um autômato híbrido. Este autômato será denominado autômato $\mathcal{D}$.
- Modelar as condições internas à aeronave (consumo de combustível, carga do acumulador de emergência) com autômatos híbridos. Estes autômatos serão denominados, respectivamente, autômatos $\mathcal{F}$ e $\mathcal{Q}$.
- Modelar as condições externas (elevações do terreno, zonas de exclusão, comunicação), através de desigualdades no sistema de coordenadas plano tangente.

5.1 Dinâmica da aeronave

A dinâmica da aeronave, ou seja, sua posição e velocidade em função do tempo pode ser modelada por um autômato híbrido linear em que cada lugar corresponde a uma das etapas de vôo.

O conjunto de atividades de cada lugar contém funções que descrevem a evolução da

posição da aeronave no sistema de coordenadas plano tangente. Visto que cada etapa compreende deslocamentos à velocidade constante ao longo de uma trajetória retilínea, as funções mencionadas são de primeira ordem.

As transições que ligam os diferentes lugares são guardadas por testes pertencentes à uma das duas categorias abaixo:

- Testes sobre a *posição da aeronave*. Este tipo de teste é usado quando o final da n-ésima etapa de vôo é definido pela passagem pelo ponto de passagem $\mathrm{WP}_{n+1} = (x_{n+1}, y_{n+1}, z_{n+1})$, especificado em termos de coordenadas do sistema plano tangente.
- Testes sobre um *relógio*. Este tipo de teste é usado quando o final da n-ésima etapa de vôo é especificado em termos de duração da própria etapa, como no caso do vôo pairado. O relógio sobre o qual o teste é feito precisa ser reinicializado na transição que liga o lugar que descreve a etapa $n-1$ ao lugar que descreve a etapa n.

As transições do autômato que modela a dinâmica da aeronave usam rótulos de sincronização para permitir a evolução dos demais autômatos que descrevem o comportamento da aeronave e com os quais deve se sincronizar (por exemplo, o autômato que modela o consumo de combustível).

Os invariantes de cada lugar do autômato que modela a dinâmica da aeronave são desigualdades usadas para forçar a sua evolução. Conseqüentemente, os invariantes refletem os testes efetuados pelas guardas das transições originadas no lugar considerado.

Exemplo 5.1 Considere-se um plano de vôo parcial constituído de três etapas:

1. vôo à velocidade mais econômica à altitude de z metros, de um ponto $\mathrm{WP}_1 = (x_1, y_1, z)$ ao ponto $\mathrm{WP}_2 = (x_2, y_2, z)$.
2. vôo pairado no ponto $\mathrm{WP}_2 = (x_2, y_2, z)$ por t_2 segundos.
3. retorno ao ponto $\mathrm{WP}_1 = (x_1, y_1, z)$ à velocidade máxima.

A figura 5.1 mostra o autômato $\mathcal{D}$ para modelagem da dinâmica da aeronave quando executando o plano de vôo parcial descrito acima.

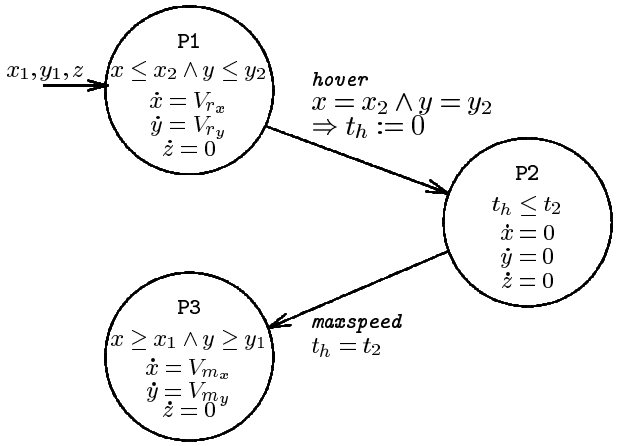


Figura 5.1: Exemplo de autômato para modelagem de um plano de vôo

O autômato inicia no lugar `P1`. Neste lugar, a posição da aeronave no sistema de coordenadas plano tangente é descrita pelas equações diferenciais $\dot{x} = V_{r_x}$ e $\dot{y} = V_{r_y}$. V_{r_x} e V_{r_y} são, respectivamente, as componentes norte e leste da velocidade mais econômica V_r, após considerar a influência do vento:

$$\begin{aligned} V_{r_x} &= V_r \cos\psi + V_w \cos\psi_w \\ V_{r_y} &= V_r \sin\psi + V_w \sin\psi_w \end{aligned}$$

onde $\psi = \arctan(\,(y_2 - y_1)/(x_2 - x_1)\,)$ é o curso que conduz de WP_1 a WP_2, ψ_w é a direção para onde o vento sopra e V_w é a velocidade do vento. Cabe ressaltar que o modelo aceita tanto valores constantes para a velocidade e direção do vento, como também faixas de valores mínimos e máximos.

Ao atingir o ponto $\mathrm{WP}_2 = (x_2, y_2, z)$, a transição para o lugar `P2` é habilitada e o invariante de `P1` força o disparo da mesma. O disparo da transição força a reinicialização do relógio $t_h := 0$ que será usado para medir a duração da etapa de vôo pairado. A etiqueta de sincronização *hover* será usada para sincronizar outros autômatos componentes da missão modelada.

O autômato permanece no lugar `P2` durante t_2 segundos. Notar que no vôo pairado, $\dot{x} = \dot{y} = 0$. Decorridos t_2 segundos, o autômato segue para o lugar `P3`, responsável pela modelagem da etapa de vôo de retorno ao ponto WP_1 à velocidade máxima V_m. □

5.2 Consumo específico de combustível

Dois modelos foram desenvolvidos para modelar o consumo específico de combustível:

- Um *modelo linear*, que despreza a variação do consumo específico de combustível com a massa da aeronave, que decresce à medida em que a missão progride e mais combustível foi consumido. Este modelo é conservador, pois o consumo específico de combustível decresce com a diminuição de massa da aeronave.

- Um *modelo linearizado*, que considera a variação de massa descrita no parágrafo acima, mas introduz um passo adicional na construção do autômato da missão.

5.2.1 Modelo linear

Se a variação do alcance específico da aeronave decorrente do consumo de combustível durante o vôo for assumida como linear, o consumo de combustível pode ser modelado por um autômato híbrido linear $\mathcal{F}$ de seis lugares (figura 5.2).

Os lugares `HOVER`, `BESTRANGE`, `ENDURANCE` e `MAXSPEED` são usados para modelar o consumo de combustível durante o vôo pairado e durante o deslocamento da aeronave respectivamente nas velocidades mais eficiente, mais econômica e máxima. O lugar `ENGINEOFF` é usado para modelar a situação em que o motor é desligado após o pouso e o lugar `NOFUEL` é usado para modelar o esgotamento do combustível.

O conjunto de atividades de cada lugar do autômato descreve o consumo de combustível para cada uma das situações em termos do consumo específico para a velocidade considerada. Os invariantes de cada lugar são constituídos por desigualdades sobre a quantidade de combustível restante.

A evolução do autômato é comandada por etiquetas de sincronização geradas pelo autômato que modela a dinâmica da aeronave e por transições guardadas por testes de combustível esgotado, $f = 0$. As etiquetas geradas pelo autômato modelador da dinâmica da aeronave correspondem a mudanças de estado (etapas do plano de vôo) deste.

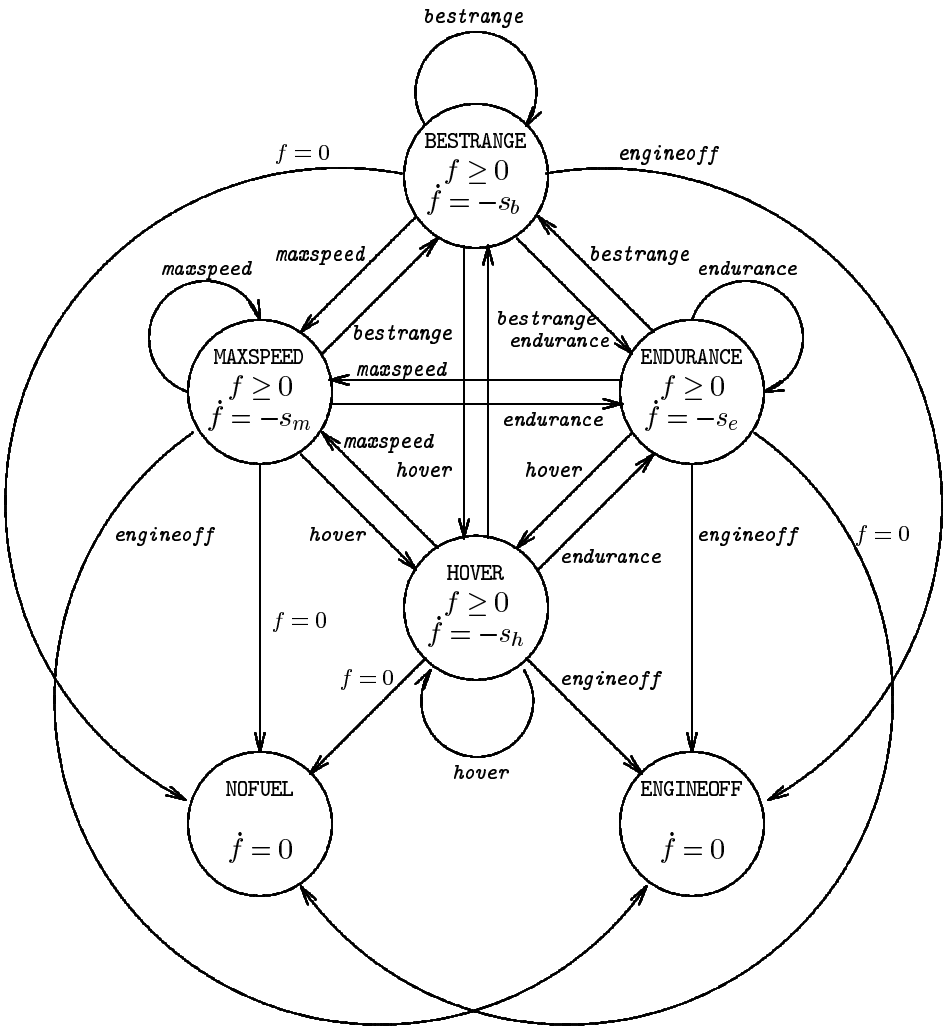


Figura 5.2: Autômato modelador do consumo de combustível

5.2.2 Modelo linearizado

O consumo específico de combustível de uma aeronave de asas rotativas não pode ser descrito por um sistema linear, já que o mesmo é função de uma série de variáveis e também das condições de vôo encontradas pela aeronave.

Com o objetivo de permitir sua análise no contexto deste trabalho, este sistema precisa ser modelado de forma aproximada por um autômato híbrido linear. Esta linearização será feita através da técnica de *translação de taxa* [33], que substitui cada variável não-linear x por uma variável parcialmente linear que aproxima x. Este método de translação é parcial para propriedades lineares podendo ser assintoticamente completo para propriedades de

segurança. Sua aplicação ao problema aqui apresentado foi inicialmente descrito em [43, 44].

Suponhamos, por exemplo, um modelo de consumo específico de combustível, s, que reflita a dependência da massa da aeronave e do regime de vôo (pairado, velocidade mais econômica, velocidade mais eficiente, velocidade máxima). De forma genérica temos

$$s = \dot{f} = g_u(m)$$

onde $m = m_e + f$ é a massa total da aeronave, com m_e sendo a massa da aeronave sem qualquer combustível a bordo, f a massa de combustível a bordo e $u \in \{hover, bestrange, endurance, maxspeed\}$ um parâmetro que determina o regime de vôo. Sob tais condições, g_u é obviamente uma função não-positiva que decresce à medida que m aumenta.

Suponhamos g_u aproximável por

$$g_u(m) = g_u(m_e) + h_u f$$

onde $g_u(m_e)$ é o consumo específico de combustível para o regime de vôo u e $h_u f$ seu incremento devido à quantidade de combustível f a bordo da aeronave; h_u é uma constante negativa.

Considerando que um plano de vôo é composto de diversas etapas, cada uma delas correspondente a um regime de vôo constante, pode-se modelar o consumo específico de combustível de uma aeronave não-tripulada de asas rotativas por um autômato híbrido não-linear onde cada lugar P_i modela uma etapa do vôo, com consumo específico de combustível dado por

$$s = k_{1_i} + k_{2_i} f$$

com k_{1_i}, k_{2_i} constantes não-positivas correspondentes a $g_u(m_e)$ e h_u para o lugar i e regime

de vôo u. Em cada lugar P_i, f está restrito ao intervalo $[0, F]$ onde F é a quantidade de combustível inicial a bordo da aeronave.

Um lugar `NO-FUEL` com dinâmica $\dot{f} = 0$ é usado para modelar a situação em que o combustível a bordo é esgotado. Transições no autômato são forçadas por etiquetas de sincronização que refletem mudanças no regime de vôo ou por transições guardadas pela condição $f = 0$ que testam o esgotamento de combustível e conduzem o autômato ao lugar `NO-FUEL`.

O autômato não-linear resultante é limitado [33] e pode ser convertido em um autômato híbrido linear através da aproximação da variável não-linear f por uma variável parcialmente linear que aproxima f. Uma possível aproximação é a que substitui o lugar P_i com um lugar que satisfaz

$$0 <= f <= F_i$$

e

$$\dot{f} \in [k_{1_i} + k_{2_i} F_i, k_{1_i}]$$

onde F_i é estimado a partir do limite inferior de combustível consumido na etapa anterior do vôo.

A figura 5.3 mostra um autômato linearizado que modela o consumo de combustível de uma aeronave executando o plano de vôo do exemplo 5.1.

5.3 Acumulador de emergência

A carga do acumulador de emergência pode ser modelada por um autômato híbrido linear $\mathcal{Q}$ de cinco lugares (figura 5.4). O lugar `CHARGE` é usado para modelar a situação de carga pelo alternador com corrente I_c. Supondo que a aeronave seja dotada de um mecanismo de gerenciamento de energia elétrica que permite desligar seletivamente cargas a bordo da mesma, a descarga do acumulador é modelada pelos lugares `DISCHARGE1` (corrente drenada

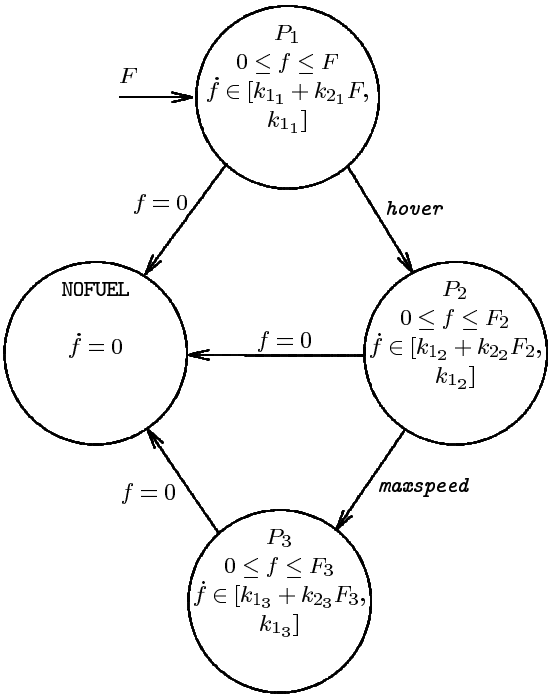


Figura 5.3: Um autômato híbrido linearizado para modelagem de consumo de combustível

I_d) e `DISCHARGE2` (corrente drenada $I_{min} < I_d$). Dois lugares adicionais (`FULL` e `EMPTY`) são usados para modelar os limites impostos pelo acumulador de emergência, visto sua carga não poder ser maior que Q_{max} ou negativa.

As etiquetas de sincronização *charge* e *discharge* permitem a sincronização com os autômatos $\mathcal{D}$, $\mathcal{F}$ e outros usados para modelar a missão.

5.4 Comunicação, topografia, zonas de exclusão

Zonas de cobertura do enlace de comunicação, a topografia (elevações do terreno) e zonas de exclusão são zonas geográficas com limites definidos no sistema de coordenadas geodéticas.

Estas zonas geográficas serão modeladas por regiões[1] definidas por desigualdades lineares no sistema de coordenadas plano tangente.

[1] O termo região é usado aqui para denotar um conjunto de estados de um sistema híbrido, vide seção 4.1.

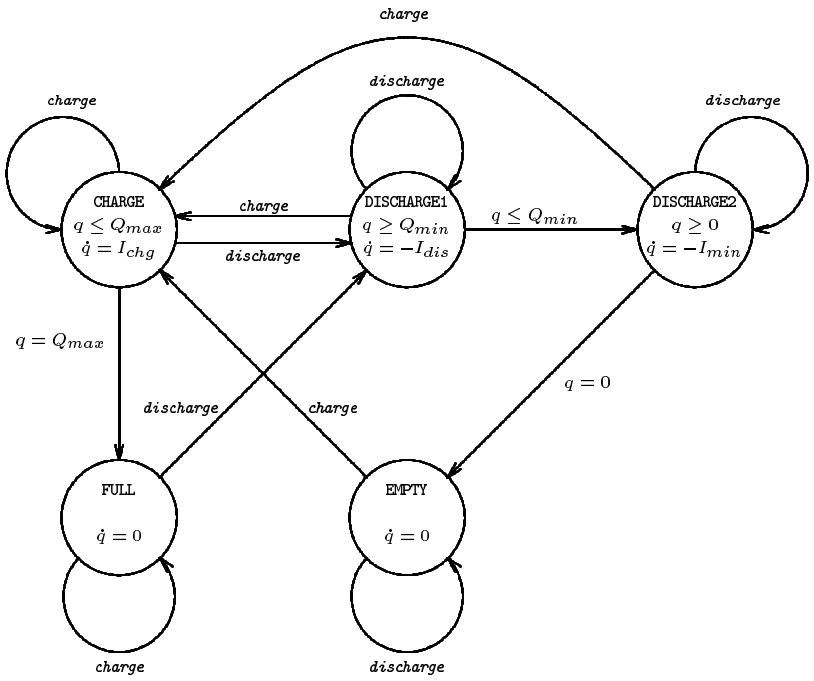


Figura 5.4: Autômato modelador da carga do acumulador de emergência

5.4.1 Enlace de comunicação

A cobertura do enlace de comunicação entre a aeronave e sua estação de controle em terra é modelada por uma região, descrita por uma desigualdade no sistema de coordenadas plano tangente, onde a intensidade do sinal de rádio-freqüência é suficientemente forte para garantir a comunicação. Esta região potencialmente não-linear pode então ser aproximada pela união de diversas regiões lineares.

Exemplo 5.2 Supondo uma antena omnidirecional e propagação homogênea das ondas de rádio em um certo terreno, a região de cobertura do enlace de comunicação pode ser descrita por um círculo de raio R_{max}. Se a antena esta localizada no ponto de lançamento (a origem do sistema de coordenadas plano tangente), a região de cobertura do enlace de rádio freqüência é dada por:

$$x^2 + y^2 \leq R_{max}^2$$

Esta região não-linear pode ser aproximada de forma conservadora pela união de diversas

regiões lineares:

$$
\begin{array}{lcll}
-x_1 \leq x \leq +x_1 & \wedge & -y_1 \leq y \leq +y_1 & \vee \\
-x_2 \leq x \leq +x_2 & \wedge & +y_1 \leq y \leq +y_2 & \vee \\
-x_2 \leq x \leq +x_2 & \wedge & -y_2 \leq y \leq -y_1 & \vee \\
-x_3 \leq x \leq +x_3 & \wedge & +y_2 \leq y \leq +y_3 & \vee \\
-x_3 \leq x \leq +x_3 & \wedge & -y_3 \leq y \leq +y_2 & \vee \\
 & & \vdots &
\end{array}
$$

A figura 5.5 ilustra graficamente a aproximação da região $x^2 + y^2 \leq R_{max}^2$ pelo conjunto de regiões acima.

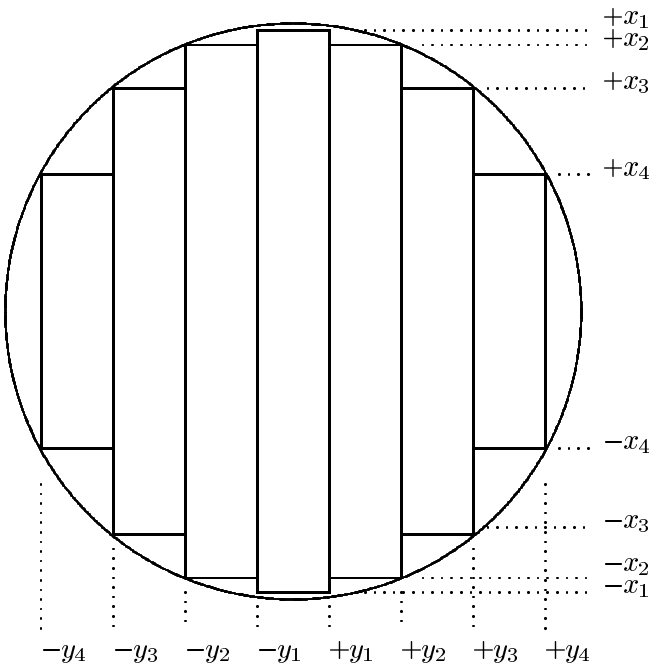


Figura 5.5: Modelagem da região de cobertura do enlace de comunicação

□

5.4.2 Topografia do terreno sobrevoado

A *topografia do terreno* pode ser modelada por uma função $\mathcal{E}$ que fornece a elevação z acima do elipsóide de referência em função das coordenadas plano tangente do ponto considerado:

$$z = \mathcal{E}(x, y)$$

Dados discretos para a construção de uma função deste tipo podem ser obtidos para qualquer parte do globo terrestre no formato DTED[2] na *Nacional Imagery and Mapping Agency*[3].

5.4.3 Zonas de exclusão

Zonas de exclusão são descritas por inequações no sistema de coordenadas geodéticas, de forma similar àquela utilizada para modelar zonas de cobertura do enlace de comunicação.

A região geograficamente equivalente à zona de exclusão é construída através da conversão das coordenadas dos vértices da zona de exclusão para o sistema de coordenadas plano tangente. Para zonas de exclusão temporária, é preciso levar em consideração a hora e/ou data em que se pretende realizar a missão.

5.5 Condições meteorológicas

A influência da direção, intensidade e tipo de vento (constante ou em rajadas) precisa ser considerada na construção do autômato modelador da dinâmica da aeronave.

Para tanto, o vetor velocidade do vento precisa ser somado vetorialmente ao vetor velocidade desenvolvida pela aeronave. Tal soma é feita no sistema de coordenadas plano tangente, como descrito na seção 5.1.

[2] *Digital Terrain Elevation Data*
[3] `http://www.nima.mil`

Existem três possibilidades de utilização de dados meteorológicos:

- Pode-se utilizar uma *previsão* das condições meteorológicas para a data e hora em que se pretende realizar a missão.
- Podem-se utilizar *séries estatísticas* a fim de determinar, com diferentes graus de confiabilidade, as intensidades máximas de vento a serem esperadas em função da época do ano e da região onde se pretende executar a missão.
- Pode-se parametrizar a intensidade e direção do vento no plano de vôo em construção e construir um plano de vôo parametrizado. Através do processo de instanciação de planos de vôo, a ser descrito na seção 6.2, pode-se então obter a máxima intensidade de vento sob a qual o plano ainda é exeqüível. Será preciso então esperar por um dia e hora em que as condições meteorológicas sejam aceitáveis para a execução da missão.

5.6 Conclusões

Este capítulo foi dedicado à modelagem de missões de aeronaves não-tripuladas utilizando autômatos híbridos e regiões definidas sobre seu espaço de estados.

Autômatos híbridos foram usados para modelar a dinâmica da aeronave (tal como prescrita no plano de vôo), a influência do vento, o consumo específico de combustível e o estado do acumulador de emergência. Visto que, atualmente, somente sistemas compostos de autômatos híbridos lineares podem ser verificados, descreveu-se uma técnica de linearização adequada à tarefa de modelagem aqui usada.

Também descreveu-se a utilização de desigualdades sobre o sistema de coordenadas plano tangente para modelar elevações de terreno, zonas de exclusão e regiões de cobertura do enlace de rádio-freqüência.

Como mencionado na introdução a este trabalho (capítulo 1), tratou-se de modelar as características mais comuns de aeronaves não-tripuladas. Um tratamento exaustivo e genérico seria impossível devido à grande variedade de aeronaves existentes.

Mesmo não se tratando de uma modelagem exaustiva, as técnicas aqui utilizadas são suficientemente expressivas para permitir a modelagem de outras características, internas ou externas. Por exemplo:

- A utilização de nitrogênio líquido para refrigeração do plano focal de um sensor infravermelho pode ser modelada por um autômato de forma bastante similar à utilizada para modelar o consumo de combustível.
- Em aplicações policiais, por exemplo monitoração de rebeliões em presídios, a aeronave está potencialmente exposta às ações de armas de fogo de pequeno calibre. Para missões deste tipo, pode-se definir regiões adicionais correspondentes ao alcance do armamento em questão, permitindo sua posterior consideração na elaboração do plano de vôo. Um raciocínio semelhante pode ser utilizado em missões de inspeção de linhas de alta tensão ou monitoração de incêndios florestais.

Capítulo 6

Elaboração de Planos de Vôo

Nas seções seguintes serão apresentadas três diferentes técnicas para elaboração de planos de vôo para aeronaves não-tripuladas com base na verificação formal de autômatos híbridos.

Algoritmos para a análise de autômatos híbridos lineares são apresentados em [31, 34, 35]. Os algoritmos baseiam-se no cômputo de estados predecessores e sucessores e na minimização de um dado conjunto de estados (ou região).

Utilizando aproximações sucessivas, os algoritmos permitem o cômputo de $post^*(W)$, a *região alcançável* a partir de uma região W, isto é, o conjunto de todos os estados alcançáveis a partir de estados em W. Similarmente, é possível computar $pre^*(W)$, a *região inicial* de W, o conjunto de todos os estados a partir dos quais um estado em W é alcançável.

Estes algoritmos também permitem verificar se um sistema híbrido linear H satisfaz um conjunto de requisitos especificado usando a lógica temporal de tempo real TCTL (*timed computation tree logic*), [31]. Usando os operadores *nunca*, *sempre* e *eventualmente*, é possível descrever o comportamento desejado do autômato a ser verificado, vide seção 4.2.5.

Outra maneira de se especificar requisitos de segurança é utilizando o conceito de regiões, conjuntos de estados do autômato híbrido sendo analisado. Todos os requisitos de segurança aplicáveis a planos de vôo para aeronaves não-tripuladas podem ser expressos em termos de inclusão em regiões "autorizadas" e intersecção com regiões "proibidas". Os ter-

mos serão adotados ao longo do restante do trabalho, seu significado será esclarecido mais adiante.

Este capítulo abordará três técnicas distintas para elaboração de planos de vôo:

- A exeqüibilidade de um plano de vôo pode ser *verificada*. O resultado de uma verificação pode ser "plano de vôo é exeqüível" ou "plano de vôo não é exeqüível". Esta abordagem será descrita na seção 6.1.
- Parâmetros simbólicos em um plano de vôo parametrizado podem ser *instanciados* de maneira a garantir que o plano de vôo resultante seja exeqüível. O resultado do processo de instanciação é "plano de vôo será exeqüível se ...". Esta abordagem será descrita na seção 6.2.
- Planos de vôo podem ser *construídos de forma incremental*, computando a região alcançável à medida que cada nova etapa é adicionada ao plano de vôo em construção. A exeqüibilidade de um plano de vôo construído desta maneira é, portanto, garantida *a priori*. Esta abordagem será descrita na seção 6.3.

6.1 Verificação de planos de vôo

A *verificação de um plano de vôo* aplica-se a situações em que um plano de vôo construído de acordo com critérios externos precisa ser verificado quanto à sua exeqüibilidade.

Usando regiões, a exeqüibilidade de um plano de vôo pode ser verificada pelo seguinte algoritmo:

1. Construir o autômato $\mathcal{M}$ modelador da missão. Este autômato resulta da composição paralela dos autômatos $\mathcal{D}$ (dinâmica da aeronave), $\mathcal{F}$ (consumo específico de combustível) e $\mathcal{Q}$ (acumulador de emergência). Outros autômatos, eventualmente utilizados para modelagem de características adicionais da missão, podem ser incluídos na composição do autômato $\mathcal{M}$ da mesma forma.
2. Computar $post^*(I)$, a região alcançável pelo autômato $\mathcal{M}$ a partir das condições iniciais da aeronave no ponto de decolagem, descritas pela região inicial I.

3. Computar a intersecção da região alcançável pelo autômato $\mathcal{M}$ com a região "proibida". A região "proibida" é definida pelas condições externas e resulta da união, no sistema de coordenadas plano tangente, das zonas de exclusão permanentes e temporárias e das elevações de terreno. Se a intersecção não for vazia, a exeqüibilidade do plano de vôo não pode ser garantida.

4. Verificar se a região alcançável pelo autômato $\mathcal{M}$ está completamente contida na região "autorizada", definida como sendo a região de cobertura do enlace de rádio-freqüência.

Exemplo 6.1

Consideremos a missão representada diagramaticamente na figura 6.1. A missão consiste em sobrevoar duas ilhas ao longo da costa de Santa Catarina, supostamente investigando atividades pesqueiras ilícitas nas referidas ilhas.

As coordenadas geodéticas do ponto de lançamento/decolagem são $27°40.9'$ S, $48°33.8'$ W, as coordenadas geodéticas da Ilha Francisca são $27°42.2'$ S, $48°33.9'$ W e da Ilha do Largo $27°42.4'$ S, $48°35.6'$ W. No sistema de coordenadas plano tangente, as coordenadas geodéticas acima são, respectivamente, $(0,0)$, $(-2247,-118)$ e $(-3051,-3080)$[1]. A aeronave será operada à sua velocidade mais eficiente, 15 m/s. O consumo específico de combustível nestas condições é menor que 0.56 g/s.

Nosso objetivo é verificar se a quantidade inicial de combustível, $F = 1000$ g, é suficiente para cumprir a missão e, ao mesmo tempo, garantir que o corredor de aproximação do aeroporto Hercílio Luz, localizado nas proximidades, não seja invadido em nenhum momento. No sistema de coordenadas plano tangente o corredor de aproximação é descrito pela região

$$-2/5y + 700 < x < -2/5y + 3700$$

Utilizando HyTech, computamos a região alcançável pelo autômato $\mathcal{M}$:

$$post^*(I) \quad = \quad 0 = x + 15t \wedge 4x = 75y \wedge 27f = x + 27000 \wedge$$

[1] coordenadas no sistema plano tangente são expressas em metros

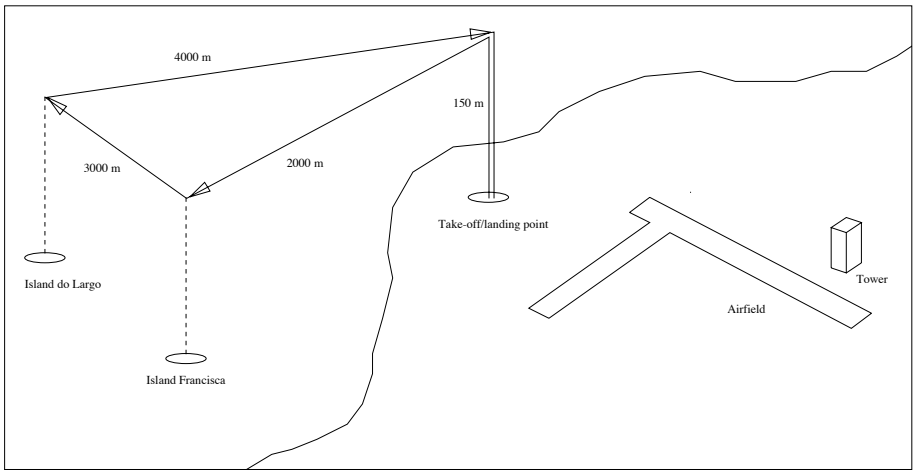


Figura 6.1: Missão usada para exemplificar a verificação de planos de vôo

$$
\begin{aligned}
& 0 >= x \ \wedge \ x + 2250 >= 0 \\
\vee \quad & 0 = x + 4t + 1650 \ \wedge \ 8y = 29x + 64290 \ \wedge \ 36f = 5x + 44250 \ \wedge \\
& 0 >= x + 2250 \ \wedge \ x + 3045 >= 0 \\
\vee \quad & 32t = 3x + 20295 \ \wedge \ 63x = 64y + 285 \ \wedge \ 5x + 96f = 62175 \ \wedge \\
& x + 3045 >= 0 \ \wedge \ 0 >= x \\
\vee \quad & x = 0 \ \wedge \ 64y + 285 = 0 \ \wedge \ 32f = 20725 \ \wedge \ 32t >= 20295
\end{aligned}
$$

O resultado acima mostra que a aeronave consumirá $f = \frac{20725}{32}$ g de combustível, valor este inferior a $F = 1000$ g.

Usando HyTech, também é possível verificar que a região resultante da intersecção da região $post^*(I)$ e da zona de exclusão definida anteriormente é vazia.

Podemos, portanto, concluir que missão proposta é exeqüível. □

6.2 Instanciação de planos de vôo

A metodologia apresentada em [31] é capaz não apenas de manipular quantidades numéricas, mas também *parâmetros simbólicos*.

A utilização de parâmetros simbólicos em um um plano de vôo é útil quando se deseja maximizar o aproveitamento da aeronave para a execução de uma certa missão. Um exemplo consiste em maximizar a capacidade de carga útil da aeronave no que a mesma é abastecida com o volume mínimo de combustível necessário, volume este obtido através do dimensionamento para a missão planejada. A utilização de acumuladores de emergência de diferentes capacidades (e pesos) também pode ser considerada.

Um *plano de vôo parametrizado* é um plano de vôo onde as etapas e a seqüência em que as etapas serão executadas está especificada. Entretanto, as condições que determinam a transição de uma etapa para a próxima, sejam elas posição ou tempo decorrido, são especificadas por *parâmetros* a serem determinados.

Neste trabalho, denominamos *instanciação de um plano de vôo parametrizado* a determinação de para quais valores dos parâmetros simbólicos as condições de segurança são satisfeitas. O algoritmo para tanto é:

1. Construir o autômato $\mathcal{M}$ modelador da missão.
2. Computar a região inicial do autômato $\mathcal{M}$ a partir da região "proibida". A região assim computada é aquela a partir da qual a região "proibida" é alcançável.
3. Computar a intersecção da região determinada no passo anterior com a região inicial I e instanciar todos os parâmetros simbólicos. Os valores obtidos para os parâmetros simbólicos neste passo são aqueles que conduzem da região inicial à região "proibida".
4. Complementar os valores obtidos no passo anterior. Estes são os valores para os quais a missão é exeqüível.

Exemplo 6.2 Considere-se o plano de vôo representado na figura 6.2[2].

O vôo compreende cinco etapas:

1. decolagem e ascensão a uma velocidade de 5 m/s até uma altitude de 300 metros, $\mathrm{WP}_1 = (0, 0, -300)$;

[2]Originalmente apresentado em [45].

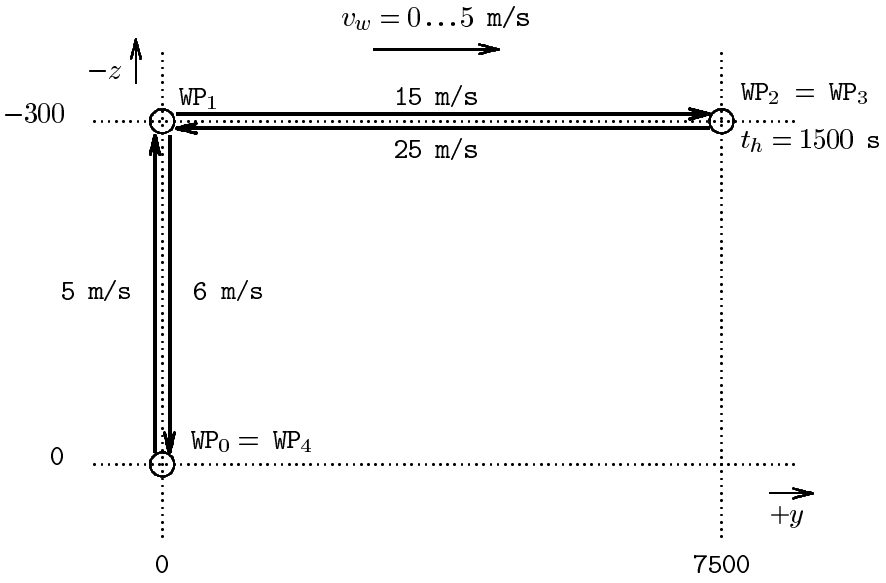


Figura 6.2: Missão usada para exemplificar a instanciação de planos de vôo

2. vôo à velocidade mais eficiente $V_r = 15$ m/s para leste até o ponto $\mathrm{WP}_2 = (0, 7500, -300)$;

3. vôo pairado por um período de 1500 s no ponto $\mathrm{WP}_2 = (0, 7500, -300)$;

4. retorno ao ponto $\mathrm{WP}_1 = (0, 0, -300)$ à velocidade máxima $V_m = 25$ m/s;

5. descida a uma velocidade de 6 m/s e pouso.

O vôo é efetuado em presença de um vento leste com intensidade variável entre $0 \ldots 5$ m/s. Assumam-se consumos específicos de combustível para o vôo pairado e para as velocidades mais eficiente e máxima iguais a $s_h = 4$ g/s, $s_r = 2$ g/s e $s_m = 3$ g/s, respectivamente.[3]

Deseja-se saber qual a quantidade mínima de combustível necessária para a execução do plano de vôo proposto.

Somando vetorialmente as velocidades da aeronave e do vento para cada etapa do plano de vôo, obtém-se o autômato híbrido mostrado na figura 6.3.

Relembrando, deseja-se saber qual a quantidade mínima de combustível necessária para a execução do plano de vôo proposto. Para tanto, basta computar a intersecção da região

[3]Este exemplo desconsidera a variação do consumo específico de combustível com a massa da aeronave.

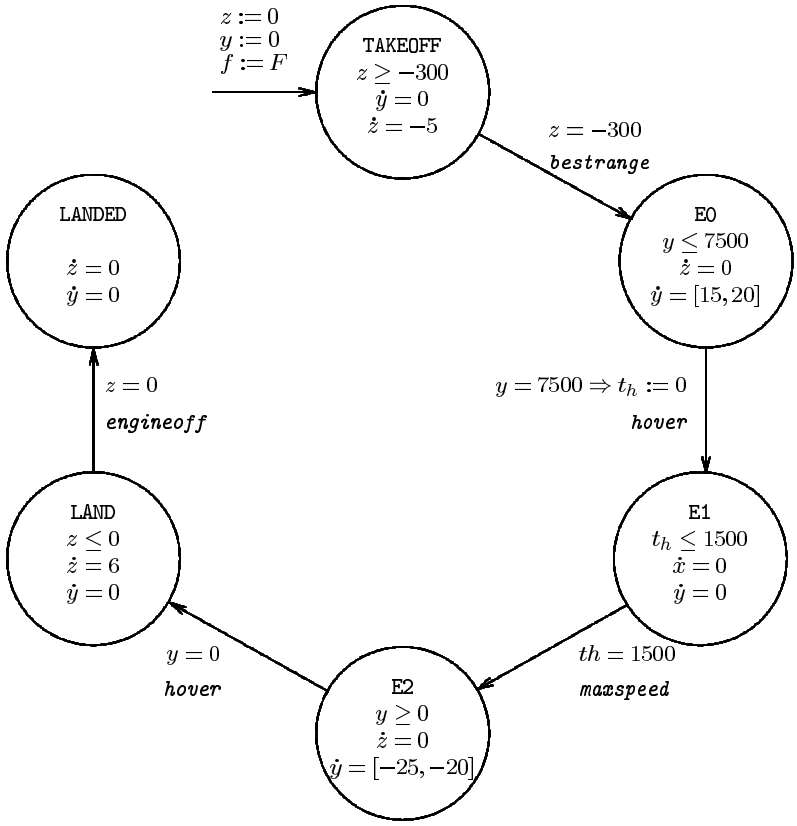


Figura 6.3: Autômato híbrido modelador do plano de vôo

inicial I com a região a partir da qual o estado $(f = 0 \wedge z < 0)$ é alcançável e instanciar F. A região desejada será o complemento da região assim obtida.

Usando HyTech, obtém-se:

$$\begin{aligned} pre^*(f = 0 \wedge z < 0) \cap I \quad &= \quad F \geq 0 \ \wedge \ 240 \geq F \\ &\vee \quad F \geq 240 \ \wedge \ 1240 \geq F \\ &\vee \quad F \geq 990 \ \wedge \ 7240 \geq F \\ &\vee \quad F \geq 6990 \ \wedge \ 8365 \geq F \\ &\vee \quad 8565 \geq F \ \wedge \ F \geq 7890 \end{aligned}$$

cujo complemento é a região:

$$F > 8565$$

Ou seja, a missão é exeqüível se a aeronave for abastecida com mais de 8565 g de combustível. □

6.3 Construção incremental de planos de vôo

Planos de vôo podem ser *construídos de forma incremental*, computando a região alcançável à medida que cada nova etapa é adicionada ao plano de vôo em construção. Isto permite a geração de planos de vôo de forma eficiente, visto que a execução destes pode ser garantida *a priori*.

Usando a metodologia de modelagem e verificação aqui propostos, a construção incremental de um plano de vôo consiste em, ciclicamente:

1. Partindo de um plano de vôo parcial, construir o autômato modelador de missão parcial $\mathcal{M}$.

2. Computar a região alcançável pelo autômato $\mathcal{M}$.

3. Converter a região alcançável, computada no sistema de coordenadas plano tangente, para o sistema de coordenadas geodéticas e representá-la graficamente sobre um mapa da região onde será realizada a missão.

As conseqüências da adição ou remoção de um ponto de passagem são imediatamente refletidas na forma da região alcançável, assistindo o operador na determinação da próxima etapa do plano de vôo sendo construído, vide figura 6.4.

Em [46] foi desenvolvida uma biblioteca de funções para representação gráfica de regiões descritas por desigualdades no sistema de coordenadas plano tangente. As bibliotecas foram escritas na linguagem C e requerem ambiente gráfico X-Windows e sistema operacional

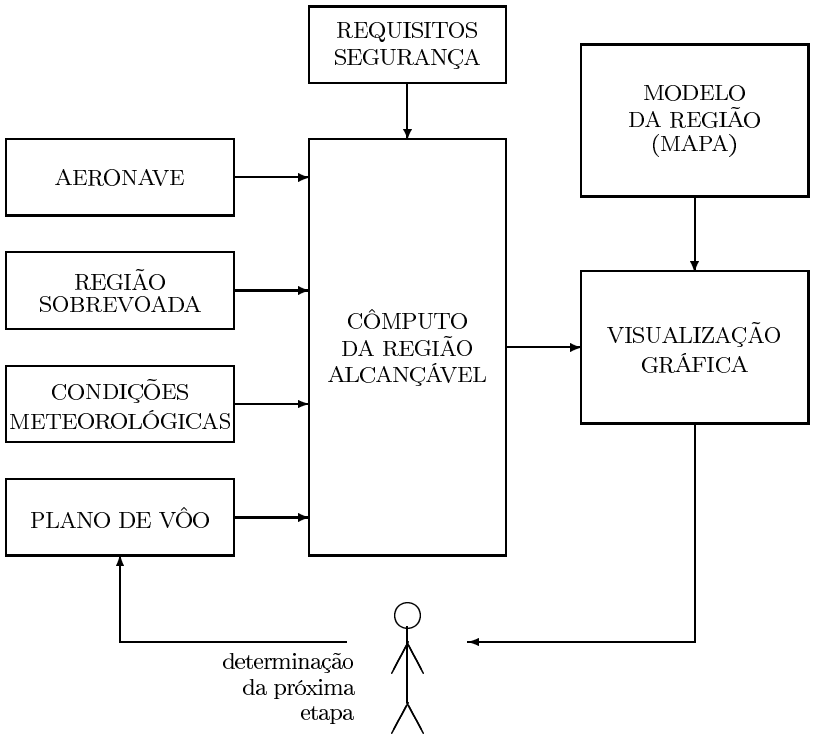


Figura 6.4: Construção incremental de planos de vôo

Unix. A figura 6.5 mostra a utilização das funções de visualização para auxiliar a construção de um plano de vôo, com as regiões "proibidas" hachuradas.

6.4 Conclusões

Com base no modelo apresentado no capítulo anterior, este capítulo apresentou três técnicas para elaboração de planos de vôo: verificação de planos de vôo previamente elaborados, instanciação de parâmetros simbólicos em planos de vôo parametrizados e construção incremental de planos de vôo com apoio de uma ferramenta de visualização de regiões "autorizadas" e "proibidas".

Todas as três técnicas são passíveis de serem incorporadas a uma solução automatizada de planejamento e controle de missões.

A ferramenta HyTech mostrou-se de grande utilidade ao facilitar as operações de composição de autômatos, cômputo de regiões alcançáveis e manipulação de regiões.

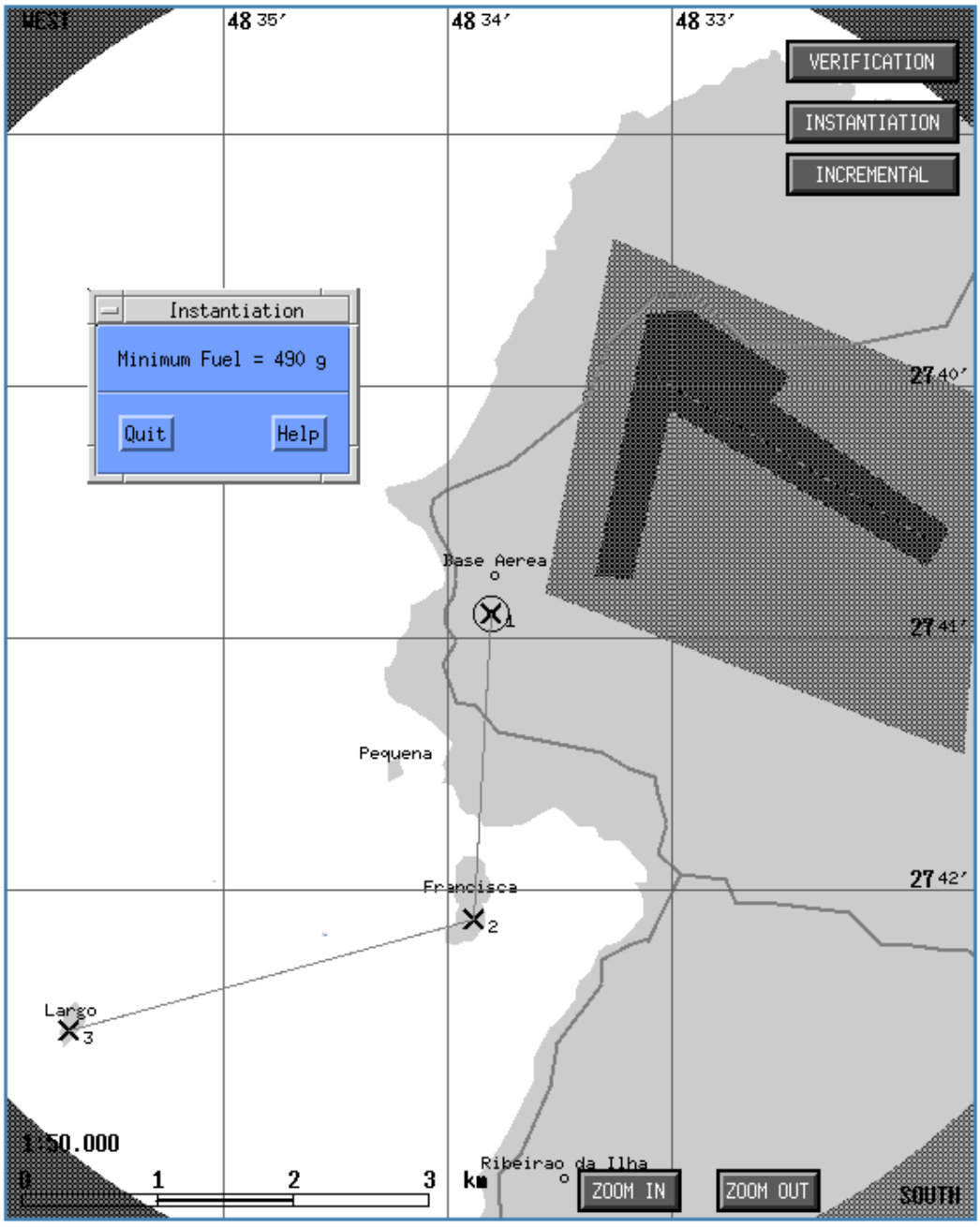


Figura 6.5: Exemplo de visualização de regiões no sistema de coordenadas geodéticas

Um problema encontrado durante a utilização de HyTech diz respeito à ocorrência de erros de saturação (*overflow*)[4]. O problema é conhecido pelos autores da ferramenta e, aparentemente, tem sua origem na maneira como foi implementada a biblioteca de manipulação de poliedros de Halbwachs [47, 48]. A versão atual de HyTech representa e manipula regiões geometricamente utilizando a referida biblioteca.

A implementação original, implementada em Mathematica [49], utilizava uma representação diferente para regiões e não exibia problema descrito. Infelizmente, tal versão foi descartada e irrecuperavelmente perdida pelos autores antes do surgimento dos problemas de saturação da versão atual.

[4]Versão utilizada datada de outubro 1996.

Capítulo 7

Interpretação de Planos de Vôo

Este capítulo descreve a *interpretação de planos de vôo* a bordo da aeronave *durante* a execução da missão.

Para tanto, as características de planos de vôo completos são brevemente discutidos na seção 7.1.

Na seção 7.2 descreve-se a construção do autômato de controle $\mathcal{C}$ a partir do autômato de missão $\mathcal{M}$. O autômato $\mathcal{C}$ é adequado para carga no controlador de vôo e é interpretado pelo mesmo durante a execução da missão, vide figuras 3.1 e 3.2 (capítulo 3).

Um *controlador de vôo*, responsável pela interpretação de planos de vôo em tempo real a bordo da aeronave é descrito na seção 7.3. Diferentes alternativas para sua implementação também são discutidas.

7.1 Planos de vôo primários e planos de vôo completos

Como já mencionado no capítulo 3, o plano de vôo primário para uma missão contém um único encadeamento de etapas de vôo e reflete o plano inicial do operador para a consecução dos objetivos da missão.

Um *plano de vôo completo* contém:

- um *plano de vôo primário* constituído das etapas que conduzem à consecução dos objetivos da missão.
- um conjunto de *planos de vôo alternativos* que refletem a ocorrência prevista de falhas (por exemplo, pane no sistema gerador de energia, nível de combustível excessivamente baixo) e doutrinas alternativas de missão.

Observe-se que um plano de vôo completo contém múltiplas alternativas para pelo menos uma de suas etapas e, conseqüentemente, mais de um possível encadeamento das mesmas.

Exemplo 7.1 Para exemplificar o exposto acima, consideremos o plano de vôo primário representado na figura 6.2 (capítulo 6). Considere-se ainda o requerimento adicional de que a detecção de um nível de combustível abaixo de 100 g (provavelmente devido a um vazamento do tanque de combustível durante a missão) deve, de acordo com uma doutrina de preservação do equipamento, conduzir à execução de uma manobra de descida e pouso à baixa velocidade (1 m/s), independente da localização atual da aeronave.

A figura 7.1 mostra o autômato de missão $\mathcal{M}$ para o plano de vôo completo descrito no parágrafo anterior. □

7.2 Construção do autômato de controle

Nesta seção será descrito um algoritmo para geração do autômato $\mathcal{C}$ a partir do autômato híbrido $\mathcal{M}$ modelador da missão. O autômato $\mathcal{C}$ corresponde à parte discreta do autômato $\mathcal{M}$ e será usado pelo controlador de vôo durante a execução da missão. Vale lembrar que o autômato $\mathcal{M}$ modelador da missão contém não somente o plano de vôo primário, como também os planos de vôos alternativos.

O autômato $\mathcal{C}$ associado à missão modelada pelo autômato $\mathcal{M}$ pode ser construída a partir das seguintes observações:

1. A cada lugar de controle do autômato $\mathcal{M}$ corresponde um estado no autômato $\mathcal{C}$.
2. A cada transição do autômato $\mathcal{M}$ corresponde uma transição do autômato $\mathcal{C}$.

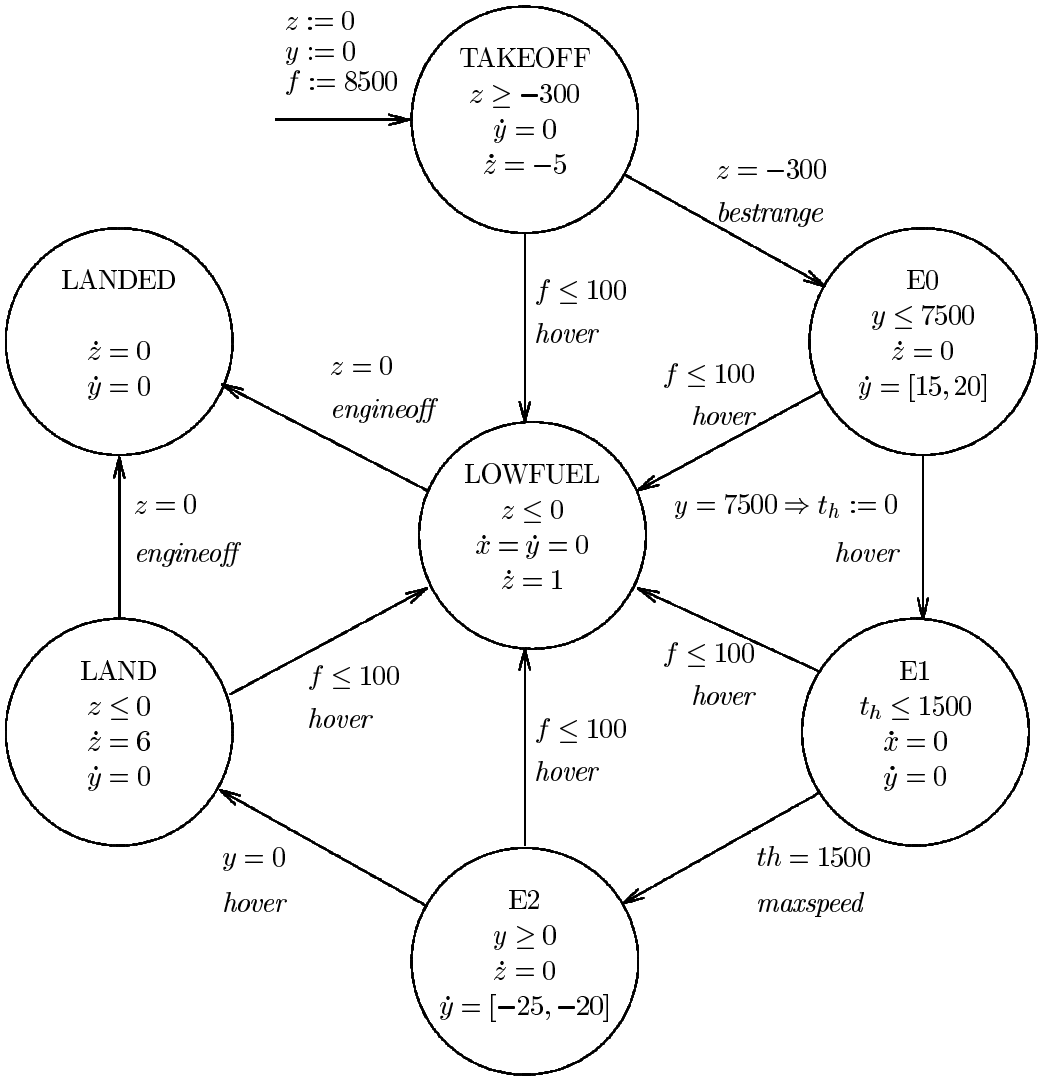


Figura 7.1: Autômato híbrido modelador do plano de vôo completo

3. Os testes que guardam as transições do autômato $\mathcal{M}$ são símbolos do alfabeto reconhecido por $\mathcal{C}$ e guardam as transições correspondentes.

4. As ações associadas às transições do autômato $\mathcal{C}$ produzem valores de referência para os controladores de baixo nível localizados nos módulos de guiagem e pilotagem. Os valores a serem produzidos como resultado das ações associadas a cada transição podem ser obtidos no plano de vôo usado para construir o autômato $\mathcal{M}$.

Como os autômatos $\mathcal{M}$ e $\mathcal{C}$ possuem o mesmo número de lugares e transições, os grafos usados para representação de ambos são similares.

Exemplo 7.2 Considere-se o plano de vôo completo apresentado no exemplo anterior. O autômato modelador de missão $\mathcal{M}$ para o referido exemplo pode ser visto na figura 7.1. O grafo do autômato de controle $\mathcal{C}$ associado ao autômato de missão $\mathcal{M}$ é apresentado na figura 7.2 abaixo:

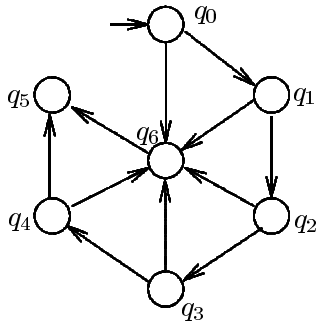


Figura 7.2: Autômato de controle associado ao autômato modelador da missão

□

7.3 Controlador de vôo

Como já mencionado anteriormente, o *controlador de vôo* a bordo da aeronave é utilizado para *executar* o plano de vôo em tempo real. Por execução de um plano de vôo compreende-se:

1. manter registro da etapa na qual o plano se encontra;
2. prover valores de referência apropriados para o módulos de guiagem e pilotagem da aeronave;
3. avaliar permanentemente o progresso da missão e o estado interno dos diferentes subsistemas constituintes da aeronave;
4. reagir a eventos externos;
5. refletir mudanças de doutrina selecionadas pelo operador da aeronave;
6. selecionar a próxima etapa a ser executada com base nos critérios anteriores, bem como o momento em que a próxima etapa deve ser executada.

O controlador de vôo instalado a bordo da aeronave opera de forma *reativa* [50], emitindo valores de referência para os controladores de baixo nível responsáveis pela implementação das funções de pilotagem e guiagem em resposta a eventos derivados da realização da missão. A figura 7.3 é um diagrama do controlador de vôo e sua interligação com os controladores de baixo nível. Para maior clareza, destacou-se a funcionalidade *supervisor*, responsável pela geração de eventos para o sistema reativo em função do estado interno do veículo. reativo.

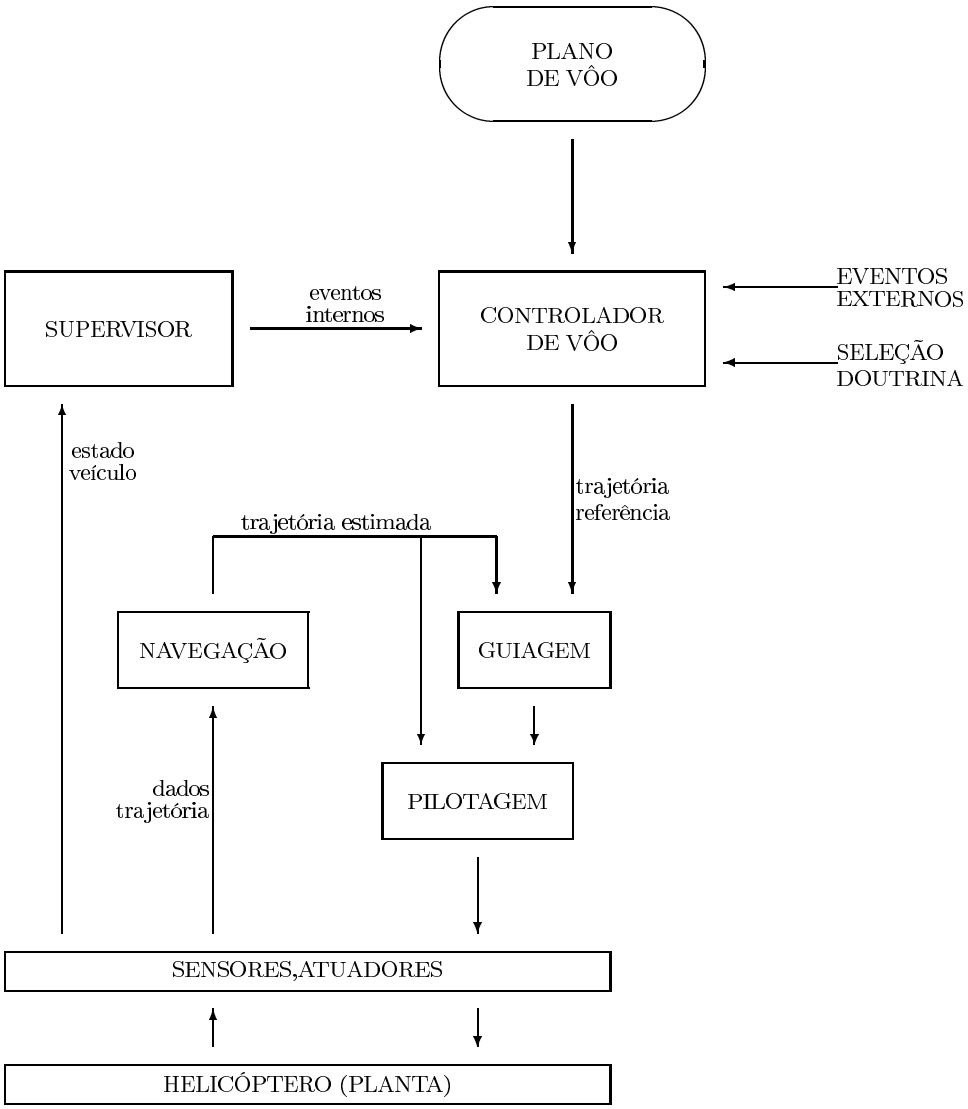


Figura 7.3: Arquitetura do controlador de vôo

O controlador de vôo opera em tempo real durante a realização da missão. Sua implementação precisa, conseqüentemente, preocupar-se com aspectos práticos referentes a capacidade de processamento e armazenamento necessárias a bordo da aeronave.

Diversas técnicas podem ser utilizadas para implementar o controlador de vôo a bordo da aeronave. Três delas (redes de Petri [51], sistemas de produção [52] e autômatos [50]) serão descritas a seguir. As primeiras duas abordagens podem ser classificadas como sendo *interpretativas*, a outra como *compilativa*.

7.3.1 Abordagens Interpretativas

Rede de Petri

Cada plano de vôo pode ser representado por uma *rede de Petri interpretada associada ao plano de vôo* ou simplesmente rede de Petri associada, cuja semântica é:

- Cada *lugar* da rede de Petri associada corresponde a uma das etapas do plano de vôo. O progresso da missão é representado pela marcação da rede de Petri associada, com uma única ficha sendo usada para tanto.
- As *transições* da rede de Petri são defendidas por *testes* sobre o estado do veículo. A cada transição também está associada uma *ação*, responsável por definir valores de referência para os controladores de baixo nível encarregados das funções de guiagem e pilotagem.

A transição de uma etapa para a próxima ocorre quando a marcação da rede de Petri sensibiliza a transição e quando o estado do veículo corresponde à condição especificada na transição.

Todos os arcos das redes de Petri utilizadas para representar planos de vôo possuem peso unitário.

Utilizando-se uma abordagem declarativa para a rede de Petri associada à missão, o controlador de vôo pode ser implementado através de um *jogador de redes de Petri*. O resultado

é uma clara separação entre a representação do plano de vôo e o mecanismo de execução do mesmo.

Sistema de produção

Um sistema de produção consiste de (1) uma base de dados, (2) um conjunto de regras que modifica a base de dados e (3) um motor de inferência que determina a aplicabilidade de regras e seleciona uma delas para execução. O mecanismo de controle também é responsável pela resolução de conflitos quando duas ou mais regras são simultaneamente aplicáveis.

Um controlador de vôo baseado em um sistema de produção usa o conjunto de regras para representar o plano de vôo, enquanto a base de dados contém o estado do veículo. O resultado é bastante similar ao obtido pelo uso de um jogador para redes de Petri.

A maior sofisticação do motor de inferência de um sistema de produção permite a utilização de heurísticas para determinar a aplicabilidade de regras. Esta característica, entretanto, não necessariamente se traduz em uma vantagem pois todas as possíveis combinações de regras já devem ter sido previstas no plano de vôo e formalmente verificadas.

7.3.2 Abordagem compilativa

Esterel [53, 50] é uma linguagem de programação síncrona e imperativa adequada à programação tempo real. A linguagem foi especificamente construída para tratar sistemas reativos determinísticos.

O resultado final da compilação de um programa em Esterel (vide figura 7.4, adaptada de [54]) produz um autômato de estados finito semanticamente equivalente ao programa inicial. O autômato resultante é especificado no código intermediário "`oc`" (*output code*).[1]

O código `oc` é bem documentado e pode ser convertido para diversas linguagens (C, Ada, Lisp, FORTH). Um compilador apropriado pode então ser utilizado para gerar código objeto para o processador desejado. O código gerado inclui um núcleo de execução para o

[1] Além do formato oc, Esterel v5 suporta dois outros formatos de geração de código intermediário.

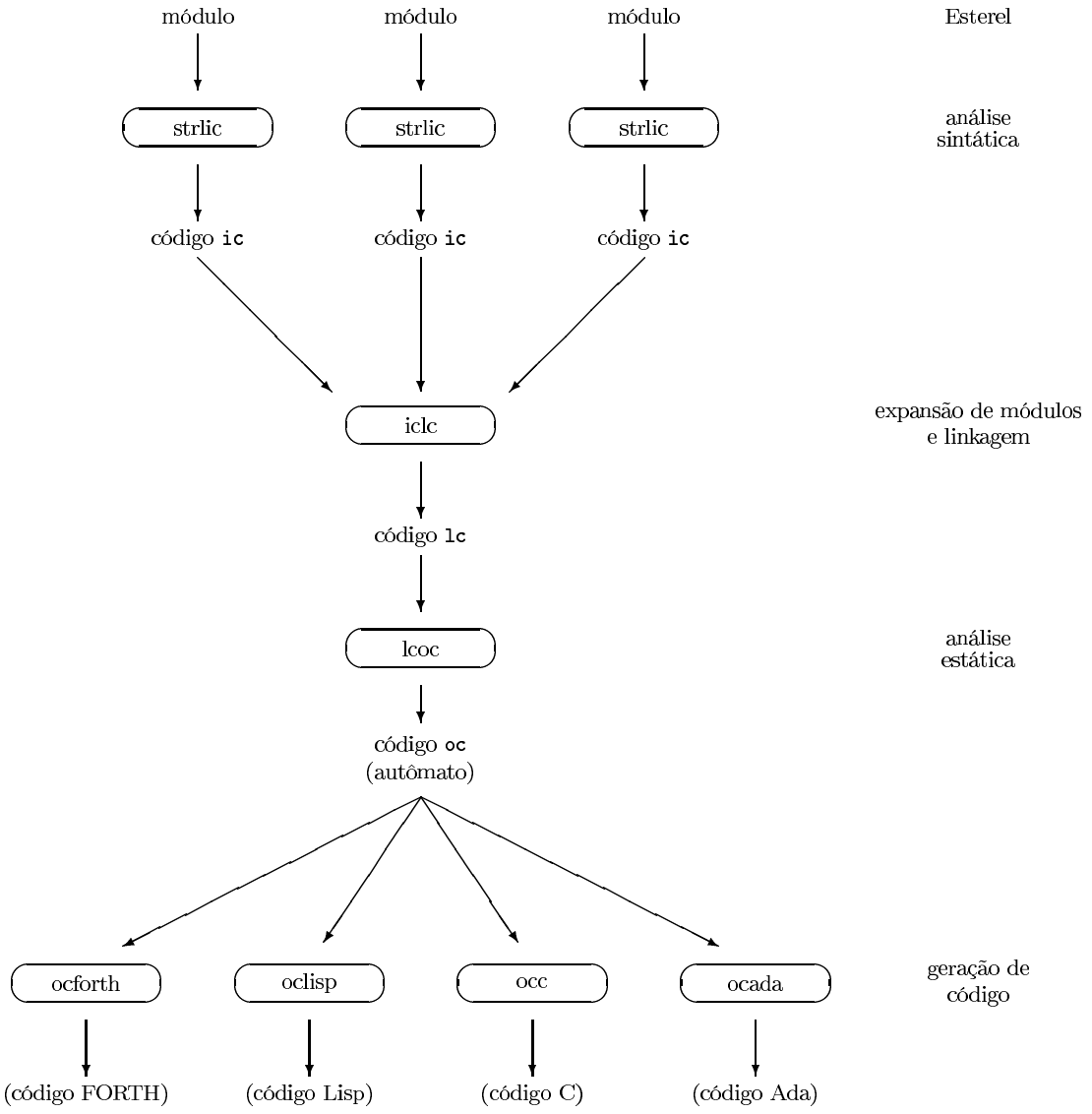


Figura 7.4: Compilação em Esterel

autômato produzido.

Uma opção para implementação do controlador de vôo é a geração de código `oc` representativo do autômato de controle a partir do autômato $\mathcal{M}$ modelador da missão. O código `oc` resultante poderia então ser compilado para o processador utilizado no controlador de vôo.

Note-se que o descrito nos parágrafos anteriores não implica em nenhum momento na utilização da *linguagem de programação* Esterel. Apenas a representação de um autômato no formato do código intermediário `oc` está sendo considerada.

Esta alternativa é interessante quando se considera a interação do controlador de vôo com os demais componentes de software existentes a bordo da aeronave. Uma característica adicional é que não existe mais uma clara separação entre o plano de vôo e o mecanismo de execução usado para processá-lo.

7.4 Conclusões

Este capítulo descreveu a interpretação de planos de vôo usando um controlador de vôo a bordo da aeronave e descreveu o algoritmo pelo qual o autômato de controle pode ser construído a partir do autômato modelador da missão.

Três alternativas foram propostas para implementação do controlador de vôo:

- a utilização de *redes de Petri* é provavelmente a mais facilmente implementável;
- uma implementação baseada em *sistemas de produção* que permite a utilização de heurísticas para seleção de comportamentos da aeronave. Uma abordagem deste tipo seria útil em um *controlador de missões* capaz de exibir comportamentos não puramente reativos;
- a implementação em código `oc` que facilita potencialmente a integração com os demais componentes de software existentes a bordo da aeronave.

Capítulo 8

Conclusões e Perspectivas

Neste capítulo serão apresentados um resumo do trabalho desenvolvido e suas principais contribuições e conclusões, bem como serão feitas algumas sugestões para continuação do presente trabalho.

8.1 Trabalho desenvolvido e resultados atingidos

Este trabalho apresentou uma metodologia que permite a construção e execução de planos de vôo para aeronaves não-tripuladas cuja *conformidade* com os objetivos da missão e cuja *robustez* podem ser formalmente garantidas.

Para tanto, este trabalho concentrou-se no desenvolvimento de:

- *modelos* capazes de representar a dinâmica de aeronaves não-tripuladas, suas características, os recursos necessários para a realização de uma missão e o terreno sobre o qual a missão será realizada;
- *algoritmos para verificação* dos modelos quanto à satisfação de requisitos de segurança;
- um *controlador de vôo* capaz de acompanhar o progresso da missão e de reagir a mudanças no estado interno da aeronave, a eventos externos e a alterações da doutrina

da missão, impostas pelo operador do sistema.

Para a tarefa de modelagem e verificação foram utilizados *autômatos híbridos*. Atualmente, somente autômatos híbridos lineares podem ser formalmente verificados, o que exigiu a aplicação de técnicas de linearização para as grandezas não lineares envolvidas.

A verificação utilizou amplamente o conceito de *regiões* e as operações de intersecção e inclusão de regiões. Especificamente, a verificação consiste em verificar se a região alcançável pelo autômato híbrido modelador da missão está completamente contida em uma região "autorizada" (onde a operação da aeronave é conhecidamente segura) e se a intersecção da região alcançável pelo mesmo autômato e a região "proibida" é vazia.

Duas técnicas adicionais foram desenvolvidas a partir da técnica básica de verificação: a utilização de parâmetros simbólicos em *planos de vôo parametrizados* e sua instanciação de modo a garantir a exeqüibilidade dos planos de vôo resultantes, bem como a *construção incremental de planos de vôo* utilizando um conjunto de rotinas para visualização gráfica de regiões alcançáveis, regiões "autorizadas" e regiões "proibidas" sobre um mapa do terreno a ser sobrevoado durante a realização da missão.

Os planos de vôo assim construídos podem ser convertidos em um autômato de controle, passível de armazenamento no controlador de vôo a bordo da aeronave. O controlador de vôo seleciona, através de um comportamento puramente reativo, o encadeamento de etapas de vôo apropriado durante a realização da missão.

Três possíveis implementações do controlador de vôo foram apresentadas e suas características discutidas.

8.2 Conclusões

Autômatos híbridos mostraram-se extremamente adequados para modelar aeronaves não-tripuladas e seu ambiente operacional. A utilização de regiões no sistema de coordenadas plano tangente mostrou-se igualmente apropriada para a especificação de requisitos de segurança.

O uso de um controlador de vôo reativo provê a aeronave de um comportamento suficientemente sofisticado para garantir compliância com os requisitos de segurança impostos e com a doutrina de missão previamente estabelecida.

Finalmente, o trabalho mostrou que aeronaves não-tripuladas podem ser providas de um grau de autonomia relativamente elevado sem enfrentar o maior dos problemas tradicionalmente associados com veículos autônomos: a complexidade do mundo real, sua representação interna no veículo e um mecanismo de inferência que permita a tomada de decisões apropriadas por parte do veículo. Isto deve-se em grande parte ao fato de que UAVs, ao contrário de muitos outros robôs, não estão propriamente "imersos" em seu ambiente de operações. Em conseqüência, o mundo real, tal como percebido por UAVs, apresenta-se suficientemente estruturado para ser tratado com as ferramentas atualmente disponíveis.

8.3 Perspectivas

Apresentaremos aqui três sugestões para continuação do presente trabalho: verificação de requisitos temporais, planejamento de missões envolvendo vários veículos e desenvolvimento de uma ferramenta comercial para o planejamento e controle de missões de aeronaves não-tripuladas.

8.3.1 Verificação de requisitos temporais

Certas missões, em especial aquelas que envolvem operações de busca ou interceptação, apresentam "janelas" de oportunidade para a consecução dos objetivos da missão. Esta classe de missões se beneficiaria da verificação formal de satisfação de *requisitos temporais* associados aos objetivos da missão.

De forma semelhante aos requisitos de segurança, é possível utilizar regiões para exprimir requisitos temporais. Entretanto, tais regiões não poderão mais ser representadas no sistema de coordenadas plano tangente, impedindo sua visualização no processo de construção incremental de planos de vôo.

Uma alternativa consiste em especificar os requisitos temporais a serem verificados em uma

lógica temporal tempo-real como TCTL (*timed computation tree logic*).

As fórmulas de TCTL são construídas a partir dos predicados de estados usando os operadores booleanos, os operadores temporais $\exists\mathcal{U}$ ("possivelmente") e $\forall\mathcal{U}$ ("forçosamente") e um quantificador de reinicialização para um conjunto de relógios.

Relógios podem ser usados para exprimir restrições temporais. Por exemplo, a fórmula

$$z.(true\exists\mathcal{U}(\phi \wedge z \leq 5))$$

expressa a existência de uma trajetória do sistema híbrido na qual a condição ϕ é satisfeita dentro de 5 unidades de tempo.

Existem ferramentas para a verificação de sistemas híbridos a partir de fórmulas expressas em TCTL, por exemplo Kronos [40]. Como é praticamente inconcebível que o operador de uma aeronave não-tripulada aprenda TCTL, torna-se necessário encontrar uma maneira mecanizável para traduzir requisitos temporais do domínio do operador da aeronave para o domínio TCTL.

8.3.2 Planejamento de missões envolvendo vários veículos

Missões complexas possuem o potencial de exigir a utilização coordenada de diversas aeronaves não-tripuladas ou mesmo destas com outros classes de veículos, tripulados ou não.

Reconhecendo a complexidade deste tipo de tarefa, a *Association for Unmanned vehicles International* realiza anualmente uma *International Aerial Robotic Competition* entre alunos de graduação de cursos universitários de engenharia. As regras para a competição de 2001[1] foram explicitamente formuladas para exigir a utilização de mais de um veículo. Requisitos conflitantes com respeito a alcance/velocidade e capacidade de evitar obstáculos tem sido usados para forçar a utilização de sub-veículos lançados a partir de uma aeronave principal.

[1] `http://avdil.gtri.gatech.edu/AUVS/IARCLaunchPoint.html`

Um possível ponto de partida para o planejamento de missões envolvendo mais de um veículo é a construção, através da composição paralela, de um único autômato híbrido modelador de missão a partir dos autômatos híbridos que descrevem a sub-missão realizada por cada um dos sub-veículos. Como a verificação de um plano de vôo precede sua execução, a potencial complexidade do autômato modelador de missão não deverá ser um obstáculo.

O controle de uma missão envolvendo mais de um veículo exigiria a difusão de eventos reconhecidos em cada controlador de vôo para os demais veículos, tarefa esta que exige a resolução de problemas relacionados a erros e atrasos de comunicação. Idealmente, o controlador de vôo de cada sub-veículo deveria preocupar-se apenas com seu próprio plano de vôo. Um ponto de partida poderia ser o trabalho descrito em [55].

8.3.3 Desenvolvimento de uma ferramenta comercial para o planejamento de missões de aeronaves não-tripuladas

Durante a concepção da metodologia de planejamento e controle de missões proposta neste trabalho, esteve sempre presente preocupação de que os passos de modelagem, verificação e controle fossem mecanizáveis.

O objetivo da mecanização é permitir a construção de uma *ferramenta para planejamento de missões de aeronaves não-tripuladas*, a ser possivelmente integrada na estação de controle da aeronave. Tal ferramenta isolaria completamente o operador da aeronave dos detalhes de modelagem e verificação formal.

A visualização de regiões já foi abordada em [46] enquanto que a utilização de modelos numéricos de terreno (DTED – *Digital Terrain Elevation Data* e DFAD – Digital Feature Analysis Data) no sistema de coordenadas plano tangente chegou a ser codificada no contexto do trabalho desenvolvido em [56].

Infelizmente, os problemas de saturação encontrados quando da utilização de HyTech impediram a construção de um protótipo completo da referida ferramenta. Entretanto, versões intermediárias foram apresentadas em congressos da comunidade aeronáutica [57, 56], tendo inclusive despertado a consulta de uma empresa americana sobre sua possível comercialização.

O maior volume de trabalho no desenvolvimento de uma ferramenta comercial encontrar-se-ia, sem dúvida, na re-codificação dos algoritmos de verificação baseados na biblioteca de Halbwachs, responsável pela manipulação de poliedros usados para representar regiões em HyTech.

Alternativamente, poder-se-ia basear a verificação na utilização de TCTL para especificação de requisitos temporais, baseando-a, por exemplo, no trabalho desenvolvido em [35]. A utilização de TCTL também permitiria a adição futura da capacidade de verificação de critérios temporais.

Em ambos os casos, aspectos legais de licenciamento dos respectivos algoritmos de verificação precisariam ser considerados.

Apêndice A

Revisão de Autômatos e Linguagens

A seção A.1 revisa autômatos e linguagens e introduz a terminologia usada nas seções subseqüentes.

Diferentes formas de modelar o tempo e sua aplicação a autômatos e linguagens temporizados são introduzidas na seção A.2.

A.1 Revisão de autômatos e linguagens

Nesta seção, baseada principalmente em [58, 51, 59] serão revisados conceitos básicos de autômatos e linguagens e apresentadas algumas definições necessárias para o desenvolvimento das seções subseqüentes.

Uma das maneiras formais de descrever e estudar sistemas a eventos discretos é baseada na teoria de linguagens e autômatos. É possível pensar no conjunto de eventos associado a um sistema a eventos discretos como o alfabeto de uma linguagem e interpretar as seqüências de eventos como palavras sobre esta mesma linguagem. Nesta interpretação, um autômato é um dispositivo capaz de gerar uma linguagem através da manipulação do alfabeto de eventos de acordo com um conjunto de regras pré-especificadas.

Autômatos e linguagens são conceitos duais. Linguagens são geralmente utilizadas para descrever o comportamento externo de um sistema como uma seqüência de eventos ad-

missíveis. Já autômatos prestam-se melhor à descrição do comportamento interno de um sistema como uma seqüência de estados admissíveis.

A.1.1 Linguagens

Linguagens permitem especificar de maneira formal todas as seqüências possíveis de eventos que um sistema a eventos discretos é capaz de manipular.

Define-se por *alfabeto* Σ um conjunto finito, não vazio de símbolos, σ, δ, ...

Denota-se por Σ^* o conjunto de *todas as cadeias finitas* de símbolos da forma $\sigma_1\sigma_2\sigma_3\ldots\sigma_k \mid \sigma_i \in \Sigma$. A cadeia vazia é representada por $\epsilon \in \Sigma^*$.

Uma *palavra* sobre um alfabeto Σ é um elemento qualquer de Σ^*.

Dadas duas palavras $u, v \in \Sigma^*$, a *concatenação* de u e v, uv é a palavra formada pela cadeia de símbolos em u, seguida da cadeia de símbolos em v.

Uma *linguagem* L definida sobre o alfabeto Σ é um subconjunto qualquer de Σ^*. Notar que $\emptyset$ e Σ^* são linguagens e que $\emptyset \neq \{\epsilon\}$.

Diz-se que $u \in \Sigma^*$ é um *prefixo* de $v \in \Sigma^*$ se $\exists w \in \Sigma^*$ tal que $uw = v$.

O *prefixo fechamento* de uma linguagem L, denotado por $\overline{L}$ é a linguagem formada pelos prefixos das palavras em L, ou $\overline{L} \triangleq \{u \mid uv \in L \text{ para algum } v \in \Sigma^*\}$

Uma linguagem $L \subseteq \Sigma^*$ é dita *prefixo-fechada* se $L = \overline{L}$. Ou, se $l \in L$ e u é prefixo de l, então $u \in L$.

O operador *Kleene fechamento* de um conjunto A é denotado por A^* e definido como

$$A^* \triangleq \bigcup_{n=0}^{\infty} A^n$$

onde $A^0 = \{\epsilon\}$ e $A^n = AA^{n-1}$ para todo $n \geq 1$.

Se $u, v \in \Sigma^*$, então $(u + v) \triangleq \{u\} \cup \{v\} \cup \{u, v\}$.

Uma *expressão regular* é definida recursivamente da seguinte maneira:

1. (a) $\emptyset$ é uma expressão regular e representa a linguagem vazia.
   (b) ϵ é uma expressão regular e representa a linguagem formada pela palavra vazia ϵ.
   (c) u é uma expressão regular e representa a linguagem $\{u\} \in \Sigma^*$ para todo $u \in \Sigma$.
2. Se r e s são expressões regulares então rs, $r + s$, r^* e s^* são expressões regulares.
3. Não existem expressões regulares que não sejam construídas pela aplicação das regras 1 e 2 um número finito de vezes.

Expressões regulares fornecem uma representação finita e compacta para descrever linguagens. Uma *linguagem regular* é qualquer linguagem que pode ser representada por uma expressão regular.

Exemplo A.1 A expressão regular $(\alpha\beta)^* + \gamma$ representa a linguagem

$$L = \{\epsilon, \gamma, \alpha\beta, \alpha\beta\alpha\beta, \alpha\beta\alpha\beta\alpha\beta, \alpha\beta\alpha\beta\alpha\beta\alpha\beta, \ldots\}$$

□

A.1.2 Autômatos a estados finitos

Um autômato é uma quíntupla $\mathcal{A} = (\Sigma, Q, \delta, q_0, Q_m)$ onde:

Σ é um alfabeto

Q é um conjunto não vazio de estados

$\delta : \Sigma \times Q \to Q$ é uma função de transição de estados

$q_0 \in Q$ é um estado inicial

$Q_m \subseteq Q$ é um conjunto de estados marcados

Observar que a função δ permite a aplicação de apenas um evento de cada vez, visto que seu domínio é o alfabeto Σ. Pode-se estender δ a uma função $\hat{\delta} : \Sigma^* \times Q \to Q$ como segue:

$$\begin{aligned} \hat{\delta}(\epsilon, q) &= q & \forall q \in Q \\ \hat{\delta}(\sigma, q) &= \delta(\sigma, q) & \forall \sigma \in \Sigma, q \in Q \\ \hat{\delta}(s\sigma, q) &= \delta(\sigma, \hat{\delta}(s, q)) & \forall \sigma \in \Sigma, s \in \Sigma^*, q \in Q \end{aligned}$$

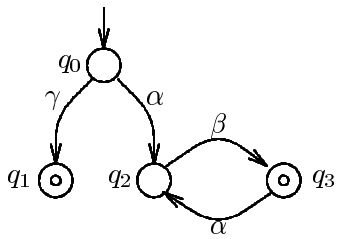
Com o auxílio de $\hat{\delta}$ é possível definir a linguagem $L \subseteq \Sigma^*$ reconhecida por um autômato $\mathcal{A}$ como sendo:

$$L \triangleq \{s \in \Sigma^* | \hat{\delta}(s, q_0) \in Q_m\}$$

Diz-se também que $\mathcal{A}$ é um reconhecedor de L.

Muitas vezes é conveniente representar um autômato graficamente através de um *diagrama de transição de estados* usando um grafo constituído de círculos e arcos. Os círculos são usados para representar estados enquanto os arcos são usados para representar eventos. Um arco etiquetado por σ conectando dois círculos etiquetados respectivamente por q e q' representa a transição do estado atual q para o próximo estado q' como resultado da ocorrência do evento σ. Usam-se dois círculos concêntricos para diferenciar os estados marcados dos demais. Uma seta apontando para um círculo indica o estado inicial.

Exemplo A.2 Seja L a linguagem definida pela expressão regular $(\alpha\beta)^* + \gamma$. Um autômato reconhecedor de L é $\mathcal{A} = (\Sigma, Q, \delta, q_0, Q_m)$, onde o alfabeto é $\Sigma = \{\alpha, \beta, \gamma\}$, o conjunto de estados é $Q = \{q_0, q_1, q_2, q_3\}$, q_0 é o estado inicial, o conjunto de estados marcados é $Q_m = \{q_1, q_3\}$ e a função de transferência δ é definida por $\delta(\gamma, q_0) = q_1$, $\delta(\alpha, q_0) = q_2$, $\delta(\beta, q_2) = q_3$ e $\delta(\alpha, q_3) = q_2$. Uma representação gráfica de $\mathcal{A}$ é mostrada abaixo:



□

Se L é a linguagem reconhecida por algum autômato com número finito de estados, então L é regular, sendo esta condição necessária e suficiente.

A.1.3 Uso de linguagens para modelagem

O comportamento lógico de um sistema a eventos discretos pode ser modelado por um par (Σ, L) onde:

Σ é um alfabeto cujos elementos são símbolos que representam os eventos que afetam o sistema a eventos discretos. Os elementos $\sigma \in \Sigma$ são chamados de eventos.

$L \subset \Sigma^*$ é uma linguagem prefixo-fechada cujas palavras representam seqüências parciais admissíveis de eventos. "Admissíveis" significa que os eventos são fisicamente possíveis, "parciais" indica que podem ocorrer outros eventos após o último evento da seqüência parcial. A condição de prefixo-fechamento de L implica que passos intermediários (prefixos) também devem ser passíveis de representação.

Exemplo A.3 Sistema a eventos discretos com dois eventos possíveis (α e β) que ocorrem sempre alternadamente, qualquer um deles podendo ocorrer primeiro.

$$\begin{aligned} \Sigma &= \{\alpha, \beta\} \\ L &= \{\epsilon, \alpha, \beta, \alpha\beta, \beta\alpha, \alpha\beta\alpha, \beta\alpha\beta, \alpha\beta\alpha\beta, \beta\alpha\beta\alpha, \ldots\} \\ L &= (\beta + \epsilon)(\alpha\beta)^*(\alpha + \epsilon) \end{aligned}$$

□

A.2 Autômatos temporizados

O modelo apresentado na seção anterior é capaz unicamente de descrever aspectos de seqüenciamento (ou lógicos) do sistema considerado, não sendo capaz de descrever aspectos temporais do mesmo.

Nesta seção será apresentado o trabalho de Alur e Dill [32], que expandiu os conceitos

de autômatos e linguagens de modo a incluir um conjunto de relógios. Transições de um estado para outro são habilitadas por condições impostas sobre os relógios e os relógios podem ser reinicializados quando da ocorrência de transições.

Alur e Dill também demonstraram que a verificação de sistemas modelados por autômatos temporizados só é decidível se as relações entre as velocidades dos relógios constituintes do sistema forem números racionais [29, 60].

A.2.1 Tempo

Quando se decide associar tempos a cada evento, é preciso decidir acerca da natureza do tempo a ser utilizado. Existem três abordagens distintas.

- A primeira alternativa considera o tempo como uma seqüência de inteiros monotônicos crescentes e é bastante apropriada para a modelagem de sistemas digitais síncronos em que mudanças de sinal ocorrem quando da chegada de um sinal de sincronismo. Este modelo é conhecido como *modelo a tempo discreto*.

  Uma das vantagens deste modelo é que o mesmo pode ser facilmente transformado em uma linguagem formal ordinária. Uma palavra temporizada pode ser convertida em uma palavra ordinária pela inserção de um *evento silencioso* tantas vezes quanto necessário entre os eventos da palavra original. Desta forma, o tempo de cada evento coincide com sua posição na palavra, permitindo a desconsideração da informação temporal e conduzindo a uma palavra de uma linguagem ordinária.

- A segunda alternativa requer que o tempo seja modelado por uma seqüência não-decrescente de inteiros. Este modelo considera que eventos ocorrem em uma determinada seqüência a qualquer tempo, mas são registrados apenas com referência a um relógio digital fictício.

  Este modelo, conhecido como *modelo de relógio fictício*, também pode ser facilmente convertido em uma linguagem formal convencional pela adição de um evento *tick* ao conjunto de eventos existentes. A palavra não-temporizada correspondente incluirá todos os eventos da palavra temporizada na seqüência original com $t_{i+1} - t_i$ *ticks* inseridos entre o i-ésimo e o $(i+1)$-ésimo elementos.

- A terceira alternativa, usada nas seções subseqüentes, considera o tempo como sendo *denso* ou contínuo. Neste modelo, os tempos associados a eventos são número reais monotonicamente crescentes e não-limitados.

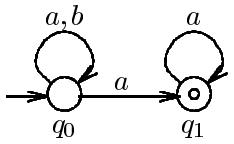
  Ao contrário dos dois primeiros modelos, o tratamento do tempo denso em autômatos finitos não é trivial, visto que não existe uma maneira óbvia de transformar um conjunto de palavras densamente temporizadas em uma linguagem formal ordinária.

A.2.2 w-Autômatos

Uma linguagem *formal* consiste em um conjunto de palavras finitas sobre um alfabeto. Já uma w-linguagem é constituída de um conjunto de palavras infinitas sobre o mesmo alfabeto. Ou seja, uma w-linguagem sobre um alfabeto Σ é um subconjunto de Σ^w, o conjunto de todas as palavras infinitas sobre Σ.

Um w-autômato fornece uma representação finita para certos tipos de w-linguagens e consiste essencialmente em um autômato de estados finitos determinístico ou não cuja condição de aceitação foi modificada para manipular palavras infinitas.

Exemplo A.4 Considere-se o autômato de dois estados sobre o alfabeto $\{a, b\}$ da figura abaixo. O estado q_0 é o estado inicial e q_1 é o estado marcado. O autômato reconhece todas as palavras contendo um número finito de bs; ou seja, a linguagem $L = (a + b)^* a^w$.



□

A.2.3 Linguagens temporizadas

Linguagens temporizadas permitem a descrição do comportamento de sistemas tempo-real por uma palavra temporizada sobre um alfabeto de eventos. O domínio do tempo é

formado pelo conjunto de números reais não-negativos, R. Uma palavra σ é acoplada a uma seqüência temporal τ definida como segue:

Uma *seqüência temporal* $\tau = \tau_1\tau_2\cdots$ é uma seqüência infinita de valores de tempo $\tau \in R$ com $\tau_i > 0$, satisfazendo as seguintes restrições:

1. *Monotonicidade*: τ cresce de maneira estritamente monotônica, ou seja, $\tau_i < \tau_{i+1}$ para todo $i \geq 1$.

2. *Progresso*: Para todo $t \in R$, existe um $i \geq 1$ tal que $\tau_i > t$.

Uma palavra temporizada sobre um alfabeto Σ é um par (σ, τ) onde $\sigma = \sigma_1\sigma_2\ldots$ é uma palavra infinita sobre Σ e τ é uma seqüência temporal. Uma linguagem temporizada sobre Σ é um conjunto de palavras temporizadas sobre Σ.

Uma palavra temporizada (σ, τ) apresentada como entrada para um autômato, produz o símbolo σ_i no instante τ_i. Se cada símbolo σ_i for interpretado como denotando a ocorrência de um evento, então a componente τ_i é interpretada como sendo o momento da ocorrência de σ_i.

Exemplo A.5 Seja o alfabeto $\{a, b\}$. Uma linguagem temporizada L_1 que consiste de todas as palavras temporizadas (σ, τ) em que b não ocorre após o instante de tempo 5.6 pode ser definida por:

$$L_1 = \{(\sigma, \tau) \mid \forall i \text{ e } ((\tau_i > 5.6) \rightarrow (\sigma_i = a))\}.$$

Outro exemplo é a linguagem L_2 constituída pelas palavras em que a e b se alternam e a diferença de tempo entre os sucessivos pares de a e b é crescente:

$$L_2 = \{((ab)^w, \tau) \mid \forall \text{ e } ((\tau_{2i} - \tau_{2i-1}) < (\tau_{2i+2} - \tau_{2i+1}))\}.$$

□

A.2.4 Autômatos temporizados

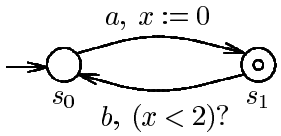
Funções de transição temporizadas podem ser construídas a partir de funções de transição convencionais pela adição de um conjunto finito de relógios. Um relógio pode ser reinicializado no momento do disparo de uma transição. O valor de um relógio a qualquer instante é igual ao tempo decorrido desde a última vez que o mesmo foi reinicializado. À cada transição é associada uma restrição temporal. A transição só pode ser disparada se o valor do relógio satisfizer a restrição a ele imposta.

Exemplo A.6 Considere-se o autômato temporizado da figura abaixo. O estado inicial é s_0 e um único relógio x é utilizado. A notação $x := 0$ em um arco corresponde à ação de reinicializar o relógio x quando a transição associada ao arco é disparada. A notação $(x < 2)?$ representa a restrição temporal associada ao arco.

O autômato inicia no estado s_0. O evento a leva-o ao estado s_1, reinicializando o relógio x. Enquanto no estado s_1, o relógio x contém o tempo transcorrido desde o último evento a. A transição de s_1 para s_0 só é habilitada se o valor deste tempo for inferior a 2. Desta forma, o tempo decorrido entre um evento a e o subseqüente evento b é sempre inferior a duas unidade de tempo. Formalmente, a linguagem é:

$$L = \{((ab)^w, \tau) \mid \forall i \text{ e } (\tau_{2i} < \tau_{2i-1} + 2)\}$$

.



□

Um autômato temporizado é dito *determinístico* se e somente se:

1. possui apenas um estado inicial, $|S_0| = 1$ e

2. para todo $s \in S$, para todo $a \in \Sigma$, para todo par de vértices da forma $\langle s, -, a, -, \delta_1 \rangle$

e $\langle s, -, a, -, \delta_2 \rangle$, as restrições temporais δ_1 e δ_2 são mutuamente exclusivas, isto é não é possível satisfazer $\delta_1 \wedge \delta_2$.

A.3 Resumo

O material apresentado neste apêndice serve de base para o material do capítulo 4.

Inicialmente foi feita uma revisão de autômatos e linguagens e introduzida a terminologia necessária às seções subseqüentes. A seguir foram apresentados autômatos temporizados e brevemente discutidas diferentes formas de modelar o tempo e as vantagens e desvantagens de cada abordagem.

Referências Bibliográficas

[1] J. Unitt. A bright future for RPVs after Vietnam? *Unmanned Systems*, 11(2), 1993.

[2] S. Kandebo. CYPHER moves toward autonomous flight. *Aviation Week & Space Techology*, March 7 1994.

[3] NASA. Extending the vision. *Unmanned Systems*, 11(1), 1993.

[4] Gyron Sistemas Autônomos Ltda. Projeto HELIX: Definição e descrição geral. Internal document, unpublished, 1992.

[5] M. Sugeno. Development of an intelligent unmanned helicopter. Technical report, Tokyo Institute of Technology, Tokyo, 1992.

[6] M. F. Weilenmann. *Robuste Mehrgrössen-Regelung eines Helikopters*. PhD thesis, Eidgenössische Technische Hochschule Zürich, 1994. Diss. ETH Nr. 10890.

[7] Col. B. M. Brown, C. H. Jacobus, and P. G. Hall. Tiltrotor UAV: The next generation unmanned system. *Vertiflite*, 38(3):18–24, May/June 1992.

[8] J. P. Cycon. Sikorsky aircraft UAV program. *Vertiflite*, 38(3):26–30, May/June 1992.

[9] T. Capaccio. Basic change in mission planning. *Air Force Magazin*, pages 58–62, December 1994.

[10] C. Roche. Les systèmes de préparation de mission des armements aéroportés tirés à distance de sécurité. *Nouvelle Revue d'Aéronautique et d'Astronautique*, pages 44–50, Janvier/Février 1996.

[11] D. Hughes. Advanced USAF mission planning system will serve fighters, bombers and transporters. *Aviation Week & Space Technology*, pages 52–57, June 10 1991.

[12] R. E. Sheffield. An analysis tool for UAV effectiveness evaluation. *Vertiflite*, 38(3):31–37, May/June 1992.

[13] D. Weiler, T. Wong, V. Vila, and R. Chesney. A general purpose control station for unmanned vehicles. White paper from CDL Systems, Calgary, and Defence Research Establishment Suffield, Canada.

[14] R. Watts. A mobile command unit for DEMO II — requirements and specification. In *AUVS-93 Proceedings Manual*, Washington, DC, June 1993.

[15] S. Falik. IAI mission control unit. In *AUVS-93 Proceedings Manual*, Washington, DC, June 1993.

[16] David A. Fulghum. Outrider UAV tackles army, navy requirements. *Aviation Week & Space Techology*, July 22 1996.

[17] I-Ling Yen, Raymond Paul, and Kinji Mori. Towards integrated methods for high-assurance systems. *Computer*, pages 32–34, April 1998.

[18] D. Schlüter. *Helicopter Manual*. Argus Books, 1981.

[19] R. W. Prouty. *Helicopter Performance, Stability, and Control*. Robert E. Krieger Publishing Company, Malabar, Florida, 1990.

[20] J. R. Kelly and F. R. Niessen. Navigation, guidance, and control for helicopter automatic landing. NASA Technical Paper 1649, NASA, 1969.

[21] C. Lin. *Modern Navigation, Guidance, and Control Processing*. Prentice-Hall, 1991.

[22] C. de Oliveira. *Curso de Cartografia Moderna*. Fundação Instituto Brasileiro de Geografia e Estatística, Rio de Janeiro, 2nd edition, 1993.

[23] M. Kayton and W. R. Fried, editors. *Avionics Navigation Systems*. John Wiley & Sons, New York, 1969.

[24] J. L. Farrel. *Integrated Aircraft Navigation*. Academic Press, Inc., Orlando, Florida, 1976.

[25] W. C. Leite Filho. PAS — Plataforma de Atitude Solidária. In *Segundo Simpósio Brasileiro de Engenharia Inercial*, IPqM, Rio de Janeiro, 1998.

[26] Department of the Army. *Engineering Design Handbook — Helicopter, Part One, Preliminary Design*. United States Army Materiel Command, Alexandria, VA, August 1974.

[27] C. N. Keys and W. Z. Stepniewsky. *Rotary-Wing Aerodynamics*, volume II — Performance Prediction of Helicopters. Dover Publications, Inc., New York, 3rd. edition, 1979.

[28] R. W. Prouty. *Helicopter Aerodynamics*. Phillips Publishing, Inc., Potomac, MD, 1985.

[29] R. Alur, C. Courcoubetis, T. Henzinger, and P. Ho. Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems. In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*, pages 209–229. Springer Verlag, 1993.

[30] X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. An approach to the description and analysis of hybrid systems. In R. L. Grossman, A. Nerode, A. P. Ravn, and H. Rischel, editors, *Hybrid Systems*, volume 736 of *Lecture Notes in Computer Science*, pages 149–178. Springer Verlag, 1993.

[31] R. Alur, C. Courcoubetis, T. Henzinger, P. Ho, X. Nicollin, A. Olivero, and S. Yovine. The algorithmic analysis of hybrid systems. In *Proceedings of the 11th International Conference on Analysis and Optimization of Discrete Event Systems*, pages 331–351. Springer Verlag, 1994.

[32] R. Alur and D. Dill. The theory of timed automata. *Theoretical Computer Science*, 126, 1994.

[33] Pei-Hsin Ho. *Automatic Analysis of Hybrid Systems*. PhD thesis, Cornell University, Department of Computer Science, 1995.

[34] R. Alur, T. Henzinger, and P. Ho. Automatic symbolic verification of embedded systems. *IEEE Transactions on Software Engineering*, 22(3), March 1996.

[35] S. Yovine. *Méthodes et Outils pour la Vérification Symbolique de Systèmes Temporisés*. PhD thesis, Institut National Polytechnique de Grenoble, 1993.

[36] A. Bouajjani, J. Fernandez, and N. Halbwachs. Minimal model generation. In E. M. Clarke and R. P. Kurshan, editors, *Proceedings of the 2nd Workshop on Computer-Aided Verification*, volume 531 of *Lecture Notes in Computer Science*. Springer Verlag, 1990.

[37] D. Lee and M. Yannakakis. Online minimization of transition systems. *ACM Symposium on Theory of Computing*, 1992.

[38] R. Alur, C. Courcoubetis, and D. Dill. Model-checking for real-time systems. In *Proceedings of the 5th Symposium on Logics in Computer Science*, pages 414–425. IEEE Computer Society Press, 1990.

[39] T. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. In *IEEE Proceedings of the 7th Symposium on Logic in Computer Science*, California, June 1992.

[40] A. Olivero and S. Yovine. Kronos: A tool for verifying real-time systems. User's guide and reference manual. Technical Report Draft 0.0, VERIMAG, August 1993.

[41] T. Henzinger and P. Ho. HyTech: The Cornell HYbrid TECHnology tool. In *Proceedings of 1994 Workshop on Hybrid Systems and Autonomous Control*. Springer Verlag, 1995.

[42] T. Henzinger, P. Ho, and H. Wong-Toi. A user guide to HyTech. In *TACAS 95: Tools and Algorithms for the Construction and Analysis of Systems*. Springer Verlag, 1995.

[43] A. Cunha. Aspectos de verificação de sistemas híbridos utilizando a ferramenta HYTECH. Master's thesis, Universidade Federal de Santa Catarina, 1997.

[44] C. Seibel, J.M. Farines, and José E. R. Cury. Towards using hybrid automata for the mission planning of unmanned aerial vehicles. In *Hybrid Systems V*, Lecture Notes in Computer Science. Springer Verlag, 1998.

[45] C. Seibel and J.M. Farines. O uso de autômatos híbridos para modelagem e verificação formal de planos de vôo de aeronaves não-tripuladas. In *III Simpósio Brasileiro de Automação Inteligente*, Vitória, ES, Setembro 1997.

[46] G. C. Dallagnolo. Ferramenta para auxílio ao planejamento de vôo de aeronaves não tripuladas. Projeto de Fim de Curso, 1998. Orientador: C. Seibel, Universidade Federal de Santa Catarina, Curso de Engenharia de Controle e Automação Industrial.

[47] N. Halbwachs. Delay analysis in synchronous programs. In C. Courcoubetis, editor, *CAV 93: Computer-aided Verification*, volume 697 of *Lecture Notes in Computer Science*. Springer Verlag, 1993.

[48] N. Halbwachs, P. Raymond, and Y.-E. Proy. Verification of linear hybrid systems by means of convex approximation. In B. LeCharlier, editor, *International Symposium on Static Analysis, SAS 94*, volume 864 of *Lecture Notes in Computer Science*. Springer Verlag, 1994.

[49] Wolfram Research Inc. *Mathematica 3.0 User's Guide*. Champaign, IL, 1995.

[50] G. Berry and L. Cosserat. The synchronous programming language esterel and its mathematical semantics. In S. Brookes and G. Winskel, editors, *Seminar on concurrency*, volume 197 of *Lecture Notes in Computer Science*. Springer Verlag, 1984.

[51] C. G. Cassandras. *Discrete Event Systems: Modeling and Performance Analysis*. Richard D. Irwin, Inc., and Aksen Associates, Inc., Boston, MA, 1993.

[52] Nils J. Nilsson. *Principles of Artificial Intelligence*. Springer-Verlag, 1982.

[53] G. Berry. The esterel v5 language primer. Technical Report Version 5.10, release 2.0, Centre de Mathématiques Appliquées, Ecole des Mines and INRIA, Sophia-Antipolis, March 1998.

[54] C. Andre and M-A. Peraldi. Synchronous approach to industrial process control. Technical Report I3S TR-93-10, Laboratoire Informatique, Signaux, Systémes (I3S), Université de Nice-Sophia Antipolis, April 1993.

[55] P. Caspi, A. Girault, and D. Pilaud. Automatic distribution of reactive systems for asynchronous networks of processors. *IEEE Transactions on Software Engineering*, 25(3), May/June 1999.

[56] C. Seibel, J.M. Farines, L. C. Corrêa, and G. C. Dallagnolo. Generating executable flight plans for unmanned aircraft: A formal mission planning tool. In *Proceedings of the 13th Bristol International Conference on RPVs/UAVs*, Bristol, UK, March 1998.

[57] C. Seibel and J.M. Farines. Formal verification and dimensioning of flight plans for rotary-wing unmanned aerial vehicles. In *Proceedings of the 24th Annual Technical Symposium of the Association for Unmanned Vehicle Systems International*, Baltimore, MD, June 1997.

[58] P. J. G. Ramadge and W. M. Wonham. The control of discrete event systems. *Proceedings of the IEEE*, 77(1), January 1989.

[59] J. E. Cury. Modelagem, análise e controle de sistemas a eventos discretos. Notas de aula, 1993. Universidade Federal de Santa Catarina, Laboratório de Controle e Microinformática.

[60] *Discrete Events and Hybrid Systems in Process Control*, Tahoe City, California, January 1996. Chemical Process Control (CPC-V).