JOURNAL OF GUIDANCE, CONTROL, AND DYNAMICS
Vol. 30, No. 1, January–February 2007

Aircraft Autolander Safety Analysis Through Optimal Control-Based Reach Set Computation

Alexandre M. Bayen*
University of California at Berkeley, Berkeley, California 94720-1710
Ian M. Mitchell† and Meeko M. K. Oishi‡
University of British Columbia, Vancouver, British Columbia V6T 1Z4, Canada
and
Claire J. Tomlin§
Stanford University, Stanford, California 94305-4035

DOI: 10.2514/1.21562

A method for the numerical computation of reachable sets for hybrid systems is presented and applied to the design and safety analysis of autoland systems. It is shown to be applicable to specific phases of landing: descent, flare, and touchdown. The method is based on optimal control and level set methods; it simultaneously computes a maximal controlled invariant set and a set-valued control law guaranteed to keep the aircraft within a safe set of states under autopilot mode switching. The method is applied to the sequenced flap and slat deflections of a simplified model of a DC9-30. The paper concludes with a demonstration of the method on higher dimensional aircraft models.

Nomenclature

b	=	wingspan, m
C_L, C_D	=	lift and drag coefficients
$D(\alpha, V)$	=	drag of the aircraft, N
e	=	efficiency factor
$f(x, u)$	=	continuous system's dynamics
$H(x, p)$	=	Hamiltonian of the system
h_{alt}	=	missed approach altitude, m
h_δ	=	parameter of C_L depending on flap deflection
$J(x, t)$	=	solution of the Hamilton–Jacobi equation
$J_0(x)$	=	implicit surface function representing the unsafe set $\mathcal{V}_0$
K	=	modeling constant
$L(\alpha, V)$	=	lift of the aircraft, N
m	=	mass of the aircraft, kg
p	=	costate of the system
S	=	wing area
T	=	thrust of the aircraft $T \in [0, T_{\max}]$, N
u	=	input thrust and angle of attack or its derivative
u^*	=	optimal input
V	=	velocity of the aircraft, m/s
$\mathcal{V}(t)$	=	reachable set
$\mathcal{V}_0$	=	a priori unsafe set
$\mathcal{W}$	=	maximal controllable set or set of controllable states
$\mathcal{W}_0$	=	safe flight envelope in a mode
$\mathbb{X}$	=	state space, $\mathbb{R}^3$ or $\mathbb{R}^4$
x	=	state vector of the aircraft, $\boldsymbol{x} = [V, \gamma, z]$
z	=	altitude of the aircraft, m
$\dot{z}_0$	=	maximal touchdown vertical velocity, m/s
α	=	angle of attack of the aircraft, $\alpha \in [\alpha_{\min}, \alpha_{\max}]$, deg
γ	=	flight-path angle of the aircraft, $\gamma \in [\gamma_{\min}, \gamma_{\max}]$, deg
δ	=	flap setting, deg
θ	=	pitch of the aircraft, deg
ρ	=	air density, kg/m^3

Received 4 December 2005; revision received 19 June 2006; accepted for publication 22 August 2006.

*Assistant Professor, Department of Civil and Environmental Engineering, Davis Hall 711; bayen@berkeley.edu. Member AIAA (corresponding author).

†Assistant Professor, Department of Computer Science; mitchell@cs.ubc.ca.

‡Assistant Professor, Department of Electrical and Computer Engineering; moishi@ece.ubc.ca. Member AIAA.

§Associate Professor, Department of Aeronautics and Astronautics; and Associate Professor, Department of Electrical Engineering and Computer Sciences, University of California at Berkeley, Berkeley, CA; tomlin@stanford.edu. Member AIAA.

Introduction

ONE of the key technologies for design and analysis of safety critical and human-in-the-loop systems is *verification*, which allows for heightened confidence that the system will perform as desired. In the context of the present work, verification consists of proving that, from an initial set of states (for example, aircraft configurations), a system can reach another desired set of states (*target*) while remaining in an acceptable range of states (*envelope*). The subset of states that can reach the target while remaining in the envelope is called the set of *controllable states* or the *maximal controllable set*. For example, if an aircraft is landing, the initial set of states is the set of acceptable aircraft configurations, or states, such as position, velocity, flight-path angle, and angle of attack, of the aircraft a few hundred feet before landing; the target is the set of acceptable aircraft states at touchdown; and the envelope is the range of states in which it is safe to operate the aircraft. A safe landing trajectory is one that starts from the set of initial states, is contained in the envelope, and reaches the target in finite time.

Although the verification of discrete state systems is a relatively well-explored field for which efficient tools have been successfully developed [1,2], algorithms for verification of continuous state systems have been developed relatively recently [3,4]; verifying an uncountable (infinite) set of states represented by continuous variables requires a numerical treatment that is theoretically more difficult than for discrete systems and harder to implement in practice. A possible approach is to use the *Hamilton–Jacobi partial differential equation* (HJ PDE). The HJ PDE framework models the envelope as the zero sublevel sets of a user defined function. This function is used as a terminal condition for a HJ PDE that is integrated backward in time. The result of the integration provides a new function, the zero sublevel sets of which can be shown to be the set of points that can reach the target while staying in the envelope, i.e., the maximal controllable set. The HJ PDE framework also provides a set-valued control law, which indicates the range of

allowable control inputs that can be applied as a function of the continuous state, to keep the system inside the maximal controllable set.

The benefit of this approach, sometimes called *reachability analysis*, is that it provides a proof (for the mathematical models used) that the system will remain inside the envelope and reach the target. This is to be contrasted with Monte Carlo methods, which do not provide any guarantee for trajectories that are not part of the simulation. Monte Carlo methods have historically been used to explore the possible trajectories a system might follow. The more finely gridded the state space, the more information the Monte Carlo simulations will provide. However, this class of methods is fundamentally limited in that it provides no information about initial conditions in between the grid points. A second benefit of reachability analysis is that it complements the traditional gain-scheduled linear control design methods used for commercial flight systems [5]. As will be seen in this paper, reachability analysis can be applied to analyze the behavior of the aircraft over the full flight envelope and can generate a *least restrictive control filter* that is only applied if the aircraft state gets close to the boundary of the maximal controllable set. Inside the maximal controllable set, traditional controllers designed to optimize, for example, performance or passenger comfort would be applied. Finally, the reachable set framework encompasses systems with inputs; thus, control problems with cooperating inputs or differential game problems with competing inputs (from different players) can be treated effectively.

The validity of this proof goes back to the discovery of the *viscosity solution* [6,7] of the HJ PDE. Before this, methods based on differential games [8] (or optimal control, for only one player) provided, at best, certificates that specific trajectories of the system stayed inside of the envelope but did not provide guarantees on sets. The advent of level set methods [9–11] enabled numerical computation of the viscosity solution, with a theoretical proof of convergence of the numerical result to the viscosity solution. In parallel, *viability theory* [12] provided engineers with an equivalent approach to solve the same problems, leading to a new suite of numerical schemes [13] developed to solve differential game problems [14]. These numerical schemes have also been proved to converge to the viscosity solution of the HJ PDE, providing the same guarantees as level set methods. These methods have now been extended to treat hybrid systems, which combine continuous state and discrete state dynamics [15–18].

When the actual implementations of these methods became operational in the late 1990s, the computational power limited such computations to two dimensional systems [13,15]. Algorithmic improvements and the increase in computing power now enable computations for systems with continuous state dimension up to four or five depending on the mathematical characteristics of the dynamics considered. This is a major technological breakthrough that now allows the treatment of problems involving realistic models of physical systems. This gives aerospace engineers an unprecedented ability to use these methods for analysis and safety verification of aircraft control systems, which are inherently hybrid, i.e., their evolution exhibits continuous behavior (position and velocity change) as well as discrete behavior (autopilot mode switches). For example, the motion of a landing aircraft is described by continuous variables, but it undergoes different discrete flap settings during landing, which have distinct dynamics and can be viewed as discrete *modes* that the pilot selects by pushing a lever or button with the corresponding setting. Interestingly, landing is one of the few portions of the flight that is not fully automated; in particular, flap deflection is still operated manually by pilots.

Aerospace engineering offers a long list of examples of algorithms or methods that slowly made their way from research to implementation onboard physical aircraft. The most famous example is probably Bryson's minimum time to climb control history computation for a supersonic jet fighter (the F4) [19]. Reachability analysis is one such example, and it is now at a stage where system implementations have become possible. It has been used in research on air traffic control, for *enhanced traffic management system* data classification [20], for soft wall analysis [21], and in conflict resolution and analysis [22]. It has also been used for underwater technology: five-dimensional reachability computations have been implemented on a glider submarine at the French Department of Defense [23]. Hardware implementation of reachable set computations has led to successful demonstrations of automated *unmanned aerial vehicles* conflict avoidance [24]. This technology was implemented in a T33 aircraft and a F15 aircraft, and a successful conflict resolution maneuver was realized, demonstrating the feasibility of the method for manned aircraft [24,25]. This provides evidence that an actual implementation on a civilian airliner of the schemes presented in this paper is feasible and realistic, which is the motivation for this paper.

This paper presents several contributions. First, a model of aircraft longitudinal dynamics is presented and analyzed. The model is written in such a way that it is possible to find an analytical expression of the optimal input to apply in the reachability computation of interest. This is a remarkable property given the model; in general, optimal Hamiltonians in HJ PDEs have to be computed numerically. The second contribution is the application of the technique to successive phases of landing. The novelty of this result lies in the hybrid reachability computation, a field for which few nonacademic examples (such as this one) exist. The hybrid nature of the model makes it possible to compute the maximal controllable set, despite the fact that the system switches dynamics several times through the landing. Finally, these results are extended to higher dimensional models, which incorporate flap dynamics in the form of a more realistic description of the evolution of the angle of attack.

This paper is organized as follows: The first section of this paper presents the model of the longitudinal dynamics of the aircraft, as well as the definition of the safety envelopes in the different modes of the aircraft (e.g., descent, flare, go-around) with corresponding slat and flap deflections. The following section presents the method used to do the verification and the corresponding input to apply to keep the aircraft inside the flight envelope. This method is then generalized to hybrid systems and applied to the successive flap and slat deflections of a DC9-30 in final approach. Finally, current research directions with higher dimensional models are shown. The model of the aircraft is refined, and the numerical technique is adapted accordingly. The appendix presents the proof of optimality, which is necessary for the solution of the HJ PDE.

Physical Model

This section presents the equations of motion used to model the aircraft's longitudinal dynamics. The aerodynamic properties of the aircraft are derived from empirical data as well as fundamental principles. The aircraft envelopes are derived using the aircraft characteristics as well as regulations.

Equations of Motion

The longitudinal dynamics of an aircraft are modeled using the frame of reference shown in Fig. 1. The state variables are the velocity, the flight-path angle, and the altitude. The state of the system is called $\boldsymbol{x}^T = [V, \gamma, z]$. A point mass model is considered in which the aircraft is subjected to forces of thrust, lift, drag, and mg

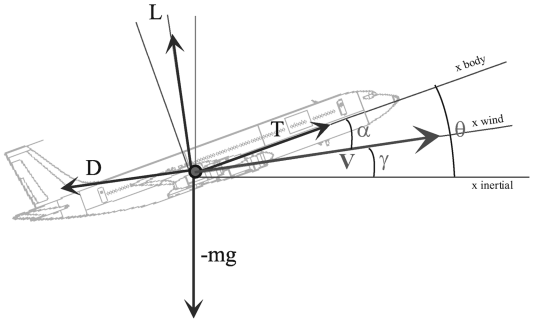

Fig. 1 Point mass force diagram for the longitudinal dynamics of the aircraft.

due to gravity. The equations of motion for this system read

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} V \\ \gamma \\ z \end{bmatrix} = \begin{bmatrix} \frac{1}{m}[T\cos\alpha - D(\alpha, V) - mg\sin\gamma] \\ \frac{1}{mV}[T\sin\alpha + L(\alpha, V) - mg\cos\gamma] \\ V\sin\gamma \end{bmatrix} \quad (1)$$

In Eq. (1), T and α are the inputs. In some modes (i.e., portions of landing), T might be fixed at nominal values T_{idle} or $T_{\max}$, where $T_{\text{idle}} = 0.2 \cdot T_{\max}$ and $T_{\max}$ is the maximal thrust. Although the pilot has control over elevator deflection, the model assumes that it can control α directly. A realistic model would assume that the pilot has control over $\ddot{\alpha}$. This is unfortunately not possible given the currently available computing resources. The validity as well as limitations of these assumptions will be discussed in the last section of this paper.

Aerodynamic Properties of the Aircraft

In a commonly accepted approximation (see, for example, [26,27]), lift and drag depend on the two flight parameters α and V as well as on numerous characteristics of the aircraft. The model of these characteristics is expressed by the dimensionless lift and drag coefficients defined by

$$C_D = \frac{D}{(1/2)\rho S V^2} \quad \text{and} \quad C_L = \frac{L}{(1/2)\rho S V^2} \quad (2)$$

The coefficient C_L can be computed for an ideal lift using thin airfoil theory. C_L is a linear function of α given by

$$C_L(\alpha) = C_{L_o} + C_{L_\alpha}\alpha \quad (3)$$

where C_{L_o} is the lift coefficient at zero angle of attack and C_{L_α} is the lift coefficient slope. Figure 2 shows a typical affine model of $C_L(\alpha)$ for different flap and slat deflections as well as the corresponding stall angles $\alpha_{\max}$, above which Eq. (3) is not valid and the aircraft might become uncontrollable. As seen, C_L increases with flap deflection, but the stall angle $\alpha_{\max}$ decreases. The stall angle $\alpha_{\max}$ increases with slat deflection. The terminology used in this figure and the deflection angle values correspond to a DC9-30 aircraft. For drag, because coefficients are not available, estimates have to be used. A procedure advocated by Kroo [27] is followed. From lifting line theory [28], the drag coefficient C_D can be computed using the drag polar:

$$C_D = C_{D_\circ} + \frac{C_L^2}{\pi \cdot \mathrm{AR} \cdot 0.95 \cdot e} = C_{D_\circ} + K \cdot C_L^2 \quad (4)$$

where $C_{D_\circ}$ accounts for the drag of the body of the aircraft, the slats, the flaps, and the landing gear. The second term accounts for drag induced by lift $K = 1/(\pi \cdot \mathrm{AR} \cdot 0.95 \cdot e)$ and is a constant (its numerical value will be given later for a specific aircraft). AR is the aspect ratio of the aircraft defined by $\mathrm{AR} = b^2/S$. The efficiency

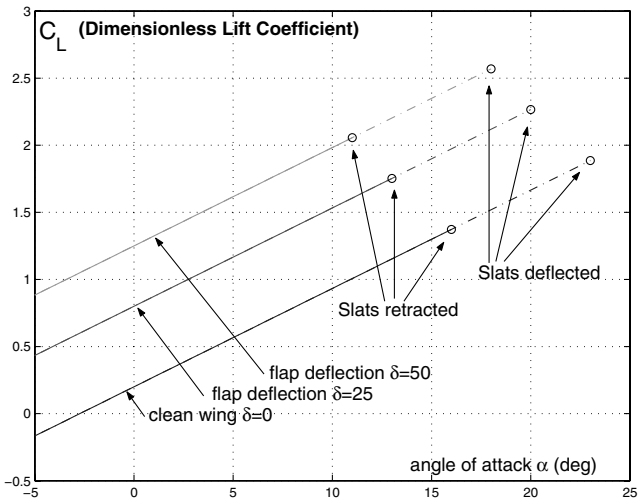

Fig. 2 Lift coefficient model for three different flap settings ($\delta = 0$, 25, and 50 deg) and for deflected/retracted slats.

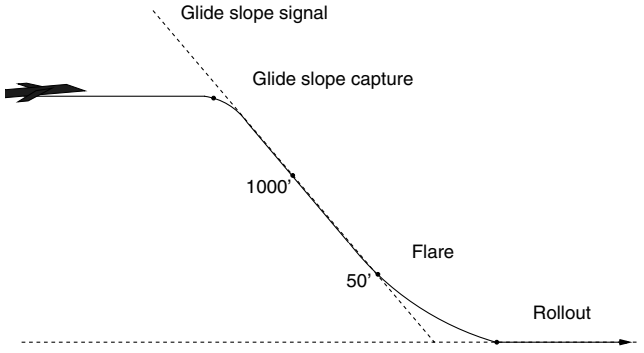

Fig. 3 Typical landing profile.

factor is corrected by 0.95 for the landing configuration. The efficiency factor quantifies the difference in performance between idealized lift (available from lifting line theory [28]) and actual lift (which accounts for the assumptions made in the idealized case).

In a typical autoland maneuver (Fig. 3), the aircraft begins its approach approximately 10 n mile from the touchdown point. The aircraft descends towards the glide slope, an inertial beam that the aircraft can track. The landing gear is down, and the pilot sets the flaps at the first high-lift configuration in the landing sequence. The autopilot captures the glide slope signal around 5 n mile from the touchdown point. The pilot increases flap deflection to effect a descent without increasing speed (indicated by larger δ in the flap settings). The pilot steps the flaps through the different flap settings, reaching the highest deflection when the aircraft reaches 1000 ft in altitude. At approximately 50 ft, the aircraft leaves the glide slope and begins the flare maneuver, which allows the aircraft to touch down smoothly on the runway with an appropriate descent rate. The deflection of the slats is correlated with the deflection of the flaps in an automated way.

Flight operating conditions are defined by the limits of aircraft performance, as well as by airport and FAA regulations [29]. The aerodynamic envelope for each discrete mode is the set of states in which the aircraft should remain. The envelope is associated with a set of operating conditions, which are allowed ranges of input signals for each discrete state. Given this set of operating conditions, the controllable subset of the envelope is defined as that subset from which it is possible to maintain the aircraft in the envelope. States not in the controllable subset are such that no matter what input the pilot chooses, the pilot will not be able to prevent the state from exiting the envelope.

During descent and flare, the aircraft proceeds through successive flap and slat settings. In each of these settings, the safe set is defined by bounds on the state variables. The maximal allowed speed $V_{\max}$ is dictated by regulations. The minimal speed is related to the stall speed by $V_{\min} = 1.3 \cdot V_{\text{stall}}$. The minimal speed is an FAA safety recommendation; the aircraft might become uncontrollable below V_{stall}. The stall speed is given by the formula

$$V_{\text{stall}} = \sqrt{\frac{2mg}{\rho S C_{L_{\max}}}} \quad (5)$$

Here, $C_{L_{\max}} := C_{L_o} + C_{L_\alpha}\alpha_{\max}$ is the maximal lift coefficient (denoted by a dot in Fig. 2) obtained at the stall angle $\alpha_{\max}$.

During descent, the aircraft tracks the glide slope (GS) and must remain within $\pm d\gamma$ of the glide-slope angle γ_{GS}. As a result, the flight-path angle in flare mode can range from $\gamma_{\min} = \gamma_{\text{GS}} - d\gamma$ to $\gamma_{\max} = \gamma_{\text{GS}} + d\gamma$. As the aircraft reduces its descent rate to land smoothly (in the last 50 ft before touchdown), this range becomes $[\gamma_{\text{GS}} - d\gamma, 0 \text{ deg}]$. By regulation, the flight-path angle γ is thus restricted to lie in the interval $[\gamma_{\min}, 0 \text{ deg}]$. (Typical values for landing are $d\gamma = -0.7$ deg, $\gamma_{\text{GS}} = -3.0$ deg; thus, $\gamma_{\min} = -3.7$ deg. Note that this is a conservative approximation. Other studies have suggested to extend this range to $[-6 \text{ deg}, 0 \text{ deg}]$.[¶])

[¶]Charlie Hynes, private communication.

During descent and flare, thrust should be at idle, but the pilot can use the full range of the angle of attack. In the following computations, we will thus use $[\gamma_{\min}, 0]$ as the set for γ, which encompasses flare and approach. A more detailed analysis of the sets $[\gamma_{GS} - d\gamma, \gamma_{GS} + d\gamma]$ and $[\gamma_{\min}, 0]$ and the corresponding switches is provided in [30].

$$\text{Parameters: } \begin{cases} V \geq V_{\min} & \text{faster than stall speed} \\ V \leq V_{\max} & \text{slower than limit speed} \\ \gamma \geq \gamma_{\min} & \text{limited descent flight path} \\ \gamma < 0 & \text{monotonic descent} \end{cases} \quad (6)$$

$$\text{Inputs: } \begin{cases} T = T_{\text{idle}} & \text{thrust at idle} \\ \alpha \in [\alpha_{\min}, \alpha_{\max}] & \text{full range available} \end{cases}$$

At touchdown (for $z = 0$ and with a negative descent velocity $\dot{z}(0) < 0$), the restrictions on the parameters are the same as in the previous paragraph for the state space except for the descent velocity. This last requirement becomes $\dot{z}(0) > \dot{z}_0$, where $\dot{z}_0$ is a constant and represents the maximal touchdown velocity (to avoid damage to the landing gear). The subscript 0 in $\dot{z}_0$ denotes $z = 0$ (ground). This condition thus reads $V \sin\gamma \geq \dot{z}_0$. In summary,

$$\text{Parameters: } \begin{cases} V \geq V_{\min} & \text{faster than stall speed} \\ V \leq V_{\max} & \text{slower than limit speed} \\ V \sin\gamma \geq \dot{z}_0 & \text{limited touchdown velocity} \\ \gamma < 0 & \text{monotonic descent} \end{cases} \quad (7)$$

$$\text{Inputs: } \begin{cases} T = T_{\text{idle}} & \text{thrust at idle} \\ \alpha \in [\alpha_{\min}, \alpha_{\max}] & \text{full range available} \end{cases}$$

Safety Analysis

The state bounds described in the previous section define safe flight envelopes for the different types of flight conditions in which the aircraft operates. The states in these envelopes are not necessarily controllable, i.e., it might not be possible to maintain the aircraft in the flight envelope from any of these states. (Note that the word *controllable* is used in a nontraditional way here and throughout the article. By saying that a state is controllable, it is understood that it is possible to keep it inside the safety set. This property is sometimes referred to as *viable* [12] or *control invariant* [15,30].) For example, an aircraft traveling just above stall speed and already at a steep negative flight-path angle might inevitably stall or start to descend too quickly. Thus, it is necessary to determine what subsets of these envelopes are actually controllable given the input authority available to the pilot or autopilot. Because the nonlinear dynamics of the model (1) make analytic determination of the controllable subsets impossible, a previously developed computational algorithm for finding controlled invariant sets for this problem is used [3].

Computation of the Reachable Set

Given some dynamically evolving system and some set of a priori unsafe states, the (backward) reachable set is defined as the set of all system states that reach $\mathcal{V}_0$ in time t. For the autoland system, in which the model is extended to several modes with different envelopes and dynamics, $\mathcal{V}_0$ will represent, in each discrete mode, the region outside the aerodynamic flight envelope. If a system's dynamics are influenced by inputs, these inputs may either try to drive the state toward or away from the unsafe set; for the airplane autopilot the inputs (α and T) will do the latter.

Computing the reachable set in a discrete system with a finite number of states, and hence a finite number of possible transitions, is a straightforward but possibly time consuming task of enumerating all the states that have a path to the target set. Computing reachability for a continuous system is a much more difficult undertaking, for example, how should the uncountably many states in any nontrivial unsafe set be represented?

An algorithm for computing the reachable sets of continuous systems with nonlinear dynamics was developed based on a time-dependent HJ PDE [3]. Let $\mathbb{X}$ be the continuous system's state space, and let $\dot{x} = f(x, u)$ be the system's dynamics, where the input $u \in \mathcal{U}$ tries to keep the system from reaching the unsafe set. Define a continuous function (sometimes called an implicit surface function) $J_0: \mathbb{X} \to \mathbb{R}$ such that

$$\mathcal{V}_0 = \{x \in \mathbb{X} | J_0(x) \leq 0\}$$

$\mathcal{V}_0$ is the zero sublevel set of the level set function $J_0(x)$. In earlier work [3] it is shown that, by solving the terminal value HJ PDE,

$$\begin{aligned} D_t J(x,t) + \min[0, H(x, D_x J(x,t))] = 0 \qquad & \text{for } x \in \mathbb{X}, \quad t < 0 \\ J(x,0) = J_0(x) \qquad & \text{for } x \in \mathbb{X}, \quad t = 0 \end{aligned} \quad (8)$$

where

$$H(x,p) = \max_{u \in \mathcal{U}} p^T \cdot f(x,u)$$

for the function $J: \mathbb{X} \times (-\infty, 0] \to \mathbb{R}$. An implicit representation of the reachable set is obtained:

$$\mathcal{V}(t) = \{x \in \mathbb{X} | J(x, -t) \leq 0\}$$

The set-valued control synthesized from this calculation is

$$u^*(x,p) = \arg\max_{u \in \mathcal{U}} p^T \cdot f(x,u) \quad (9)$$

It is "set valued" because the argument maximum (argmax) is not necessarily unique.

Analytically solving (8) for a general $J_0(x)$ and $f(x, u)$ is likely to be impossible. Computational algorithms are complicated by the fact that, even for smooth $J_0(x)$ and $f(x, u)$, the solution $J(x, t)$ can develop discontinuities in its derivatives after finite time and hence cease to solve (8) in a classical sense. The appropriate weak solution of (8) in this case turns out to be the viscosity solution [7], and level set algorithms [9] are numerical techniques developed to compute such solutions. A set of high-resolution schemes [3] has been developed based on novel numerical techniques [10,11] to compute $J(x, t)$, and hence the reachable set, very accurately.

Computation of the Optimal Input

The optimal input $u^*(x)$ at a given state x represents a choice of u that will maximize the Hamiltonian at that point x. The physical interpretation of $u^*(x)$ is thus as follows: For a point inside the reachable set, it is known from reachability analysis [3] that a trajectory starting inside the reachable set will lead to the target set (7) while maintaining the state x inside the envelope (6) provided the optimal control $u^*(x)$ is applied to the system along the trajectory. Note, however, that it is sufficient to apply the optimal control to the system on the boundary of the reachable set, which therefore enables the synthesis of less restrictive controllers (thus leaving flexibility for optimization of other flight parameters inside the reachable set). The word "optimal" thus refers only to the maximality of the Hamiltonian. Note that no cost functional is optimized explicitly in the present case, though an interpretation of optimality can be given in terms of maximization of the distance between the state and the boundary of the envelope at any given time (see [3] for more detail).

The computation of the optimal input $u^*(x)$ is, in general, extremely expensive because it is a nonconvex optimization problem, which therefore requires exhaustive search on the domain of interest. In the present case it would require maximizing H over the (α, T) space. However, for this particular model, the optimization problem can be reduced to checking six points, which is computationally tractable. The case in which the input is restricted to $[0, \alpha_{\max}] \times [0, T_{\max}]$ is investigated. The case in which negative angles of attack are considered is obtained by slight modifications of the method shown next [31].

Proposition 1: The optimal input $u^*(x) \triangleq (\alpha^*, T^*) = \arg\max_{u \in \mathcal{U}} p^T \cdot f(x,u)$ is never in the range $(\alpha, T) \in]\alpha_{\min}, \alpha_{\max}[\times]0,$

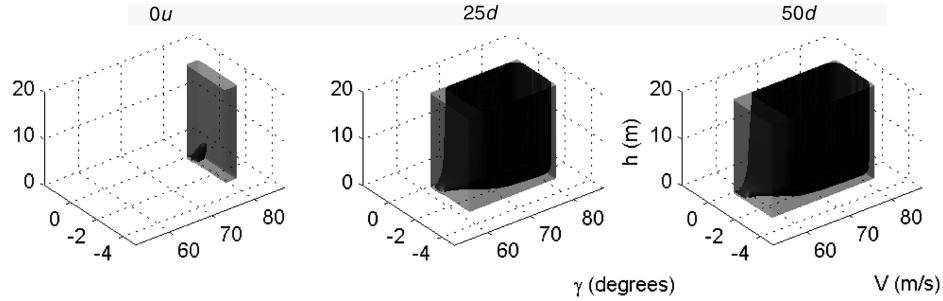

Fig. 4 Flight envelope $\mathcal{W}_0$ in each mode (gray). Controlled set $\mathcal{W}$ within each mode (dark), with no switching allowed.

$T_{\max}[$. In other words, one of the two inputs (α, T) is always extremal. (The notation $]a, b[\triangleq\overset{\circ}{[}a, b]$ denotes the open interval between a and b. This is sometimes denoted (a, b), but this would lead to confusion with other notation of this paper. Note that in the formula defining u^*, the dependency of the costate on variables has been omitted for simplicity of the definition.)

Proposition 2: The optimal input (α^*, T^*) is found among the six following values: $(0, 0)$, $(0, T_{\max})$, $(\alpha_{\max}, 0)$, $(\alpha_{\max}, T_{\max})$, $(\alpha_1, T_{\max})$, and $(\alpha_2, T_{\max})$, where α_1 and α_2 solve a quadratic and a transcendental equation, respectively, shown in the Appendix.

The proofs are presented in the Appendix.

Computation of the Controlled Envelopes

Consider the aircraft in a given mode (e.g., in a given portion of the landing). The numerical values of the parameters in the dynamics (1) can be computed. Let $\mathcal{W}_0$ be the safe flight envelope in this mode, and let $\mathcal{W}_0^c$ be its complement. To determine the maximal controllable subset $\mathcal{W}$ of $\mathcal{W}_0$, set $\mathcal{V}_0 = \mathcal{W}_0^c$, and run a reachability computation in which the inputs attempt to keep the system away from $\mathcal{V}_0$ (or equivalently, within $\mathcal{W}_0$). The reachable set typically converges to a fixed point: $\mathcal{V}(t) \to \mathcal{V}$ as $t \to +\infty$. In that case, the largest controllable subset of the envelope is the complement of the fixed point $\mathcal{W} = \mathcal{V}^c$. An example is shown in Fig. 4. In this figure, the dark set is $\mathcal{W}$ for each of the corresponding modes, and the gray set is $\mathcal{W}_0$. The controlled set is the set of points which can touch the ground safely without flying out the box while staying in that mode. As can be seen on the left subplot, in the mode $0u$ (undeflected flap and slats), this set is bounded in height, which means that it is not possible to land safely in this mode. Only three modes are represented here; the two transition modes are omitted because the pilot has no switching control while the system is in these modes.

Flap Deflection: Hybrid Reachability

In the preceding section, continuous reachable set computations for each discrete state were described; in this section, a discussion is presented to understand how mode switches should be incorporated into the design. The difficulty here is to compute the maximal controllable sets given that the switches (and corresponding dynamics and envelope changes) can occur at arbitrary times. This type of computation would be needed for automating flap deflection, as one needs to know when it is safe to switch mode. A general algorithm has been developed in [15,18] to solve such problems. A variation of this algorithm suitable for successive deflections of flaps for a landing DC9-30 is now presented.

Physical Problem and Hybrid Model

In the process of landing described in the preceding sections, the aircraft successively deflects the flaps and slats from 0 deg (clean wing) to the maximal deflection. The 0 deg modes are alternatively labeled $0u$ (for undeflected) or $0r$ (for retracted). Each of these deflection angles as well as the transitions between them is associated with different envelopes as well as operating conditions. Thus, transitioning from one configuration to another might drive the system into an unsafe state. The following question is now of interest: starting from a given position in space (altitude) with given flight conditions (speed, flight-path angle, and flap deflection) and with fixed thrust, is there a switching policy (i.e., a set of successive flap deflections/retractions) for which there exists an input (angle of attack) able to bring the aircraft safely to the ground?

The usual landing procedure requires the deflection of the flaps to be increasing in angle. This is modeled with a hybrid automaton, shown in Fig. 5. The intermediate flap deflection is 25 deg. The (slat) retracted state is denoted with r; the (slat) deflected state is denoted with d. There are three possible wing configurations: 0, 25, and 50 deg deflection. The lift coefficients for these modes are represented in Fig. 2. The safe set for these three modes is generated according to the preceding section. For the transition from one mode to another, the lift is approximated by the mean of the two values of the lift (in the two corresponding modes) and the stall angle is chosen to be the one that is the most restrictive (to have a conservative approximation). For example, in mode $25d \to 50d$, the coefficient $C_L(\alpha)$ at a given α is the mean of $C_L(\alpha)$ for $\delta = 25$ deg and $C_L(\alpha)$ for $\delta = 50$ deg. The $\alpha_{\max}$ for this mode is the minimum of the $\alpha_{\max}$ in mode $25d$ and $\alpha_{\max}$ in mode $50d$, i.e., 16 deg (see Table 1 or Fig. 2). The stall speed can then be computed using Eq. (5). It is assumed that the time the system has to remain in mode $0r \to 25d$ or $25d \to 50d$ is 10 s, which is the order of magnitude it takes to achieve half the maximal deflection of the flaps on a DC9-30. This implies that in the hybrid automaton of Fig. 5 the switches from mode $0r \to 25d$ to mode $25d$ and from $25d \to 50d$ to mode $50d$ happen automatically 10 s after the switch to mode $0r \to 25d$ and mode $25d \to 50d$, respectively. Most of the parameters for the DC9-30 can be found in the literature [26,27,32,33]. The previously derived model enables the computation of the lift and drag. The values of the numerical parameters used for the DC9-30 are $m = 60,000$ kg, $T_{\max} = 160,000$ N, $g = 9.8$ m/s^2, $e = 0.84$, $S = 112$ m^2, and

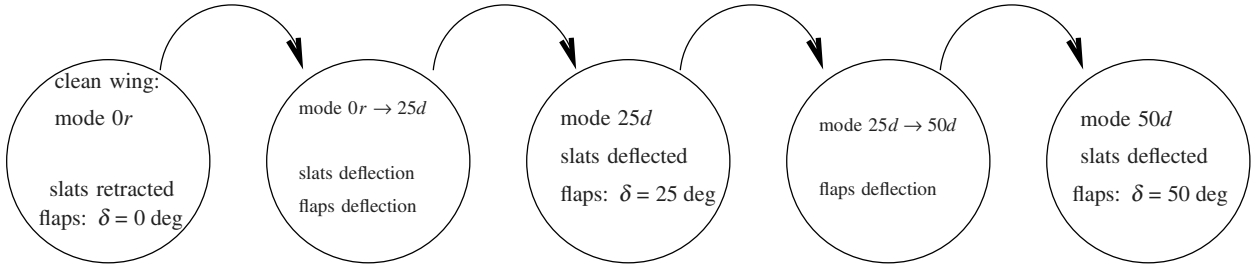

Fig. 5 Transition diagram from clean wing, no flap/slat deflection ($0r$), to fully deflected wing ($50d$).

Table 1 Summary of flap/slat deflection specific numerical parameter values for the DC9-30

Mode	V_{stall}	$V_{\max}$	$\alpha_{\max}$	h_δ	$\gamma_{\min}$	$\gamma_{\max}$
$0r$	79.01 m/s	83 m/s	16 deg	0.2	−3 deg	0 deg
$0r \to 25d$	71.58 m/s	83 m/s	16 deg	0.5	−3 deg	0 deg
$25d$	61.50 m/s	83 m/s	20 deg	0.8	−3 deg	0 deg
$25d \to 50d$	60.46 m/s	83 m/s	18 deg	1.025	−3 deg	0 deg
$50d$	57.75 m/s	83 m/s	18 deg	1.25	−3 deg	0 deg

$\rho = 1.225$ kg/m^3. The lift and drag forces are thus (in dimensional form)

$$L(\alpha, V) = 68.6(h_\delta + 4.2\alpha)V^2 \text{ N}$$
$$D(\alpha, V) = [2.7 + 3.08(h_\delta + 4.2\alpha)^2]V^2 \text{ N} \tag{10}$$

where $h_\delta = C_L(0 \text{ deg})$ depends on the flap setting. The letter N indicates that the units are Newtons (if V is taken in m/s). A summary of all constants for the DC9-30 is shown in Table 1.

Hybrid Algorithm

The modes in Fig. 5 can be divided into three classes according to the type of their outgoing transition. The simplest is mode $50d$, which has no outgoing transition and hence is treated by solving (8) without switches enabled. The controllable subset of the envelope is computed by solving (8) until it converges (after about 15 s of simulated time). A similar procedure can be run on the other two main modes ($0r$ and $25d$) to determine what subsets of their envelopes are controllable without mode switches. To determine the controllable subsets with mode switches enabled, the remaining modes are split into two classes depending on whether the switch to the subsequent mode in the sequence is controlled by the pilot (modes $0r$ and $25d$) or timed (the two transition modes).

A timed mode is a mode from which the system automatically switches at $t = t_f$. A state (V, γ, z) in a timed mode is safe if both of two conditions hold: First, it must give rise to a trajectory that remains within the flight envelope of the timed mode for all $t \in [0, t_f]$; otherwise, the trajectory becomes unsafe before the mode switch. Second, the state of the trajectory at $t = t_f$ must be within the controllable envelope of the subsequent mode; otherwise, the trajectory will become unsafe at some time after the mode switch. Let $\mathcal{W}_0$ be the safe flight envelope in the timed mode, and let $\mathcal{W}^{\text{next}}$ be the controllable envelope for the subsequent mode, which has already been computed numerically. The reachability computation for the timed mode then uses $\mathcal{V}_0 = (\mathcal{W}_0 \cap \mathcal{W}^{\text{next}})^c$ as initial conditions. Inputs are used to steer the system away from $\mathcal{V}_0$, and the computation is run backwards only to $-t_f$, which is typically short of convergence. The controllable envelope for the timed mode is then $\mathcal{W} = \mathcal{V}(t_f)^c$.

A controlled mode is a mode from which the system may switch at any time to avoid becoming unsafe. A state (V, γ, z) in a controlled mode is safe if any one of three conditions hold: First, it may give rise to a trajectory that always remains within the safe envelope of the controlled mode in which case it is safe without switching. Second, it may be within the controllable envelope of the subsequent mode in which case it is safe due to an instantaneous switch. Third, it may give rise to a trajectory that remains within the safe envelope of the controlled mode until it reaches a state that lies within the controllable envelope of the subsequent mode in which case it is safe due to a delayed switch. Note that a state may satisfy more than one of these conditions.

The controllable subset of a controlled mode's envelope is computed using a slight modification of the reach–avoid procedure outlined in previous work [15]. Let $\mathcal{W}_0$ be the safe flight envelope of the controlled mode, and let $\mathcal{W}^{\text{next}}$ be the controllable envelope of the subsequent mode. The first condition for safety is represented in the reach–avoid computation by setting $\mathcal{V}_0 = \mathcal{W}_0^c$, as would normally be done. The difference in a reach–avoid computation lies in the "avoid" or "escape" set $\mathcal{A}$, which represents the other two safety conditions that become available due to the controlled mode switch. Any trajectories that enter this set may safely switch to the subsequent mode and hence are deemed safe in the controlled mode. In this case, $\mathcal{A}$ is set to $\mathcal{A} = \mathcal{W}^{\text{next}} \cap \mathcal{W}_0$. For the reach–avoid computation, it is assumed that $J_{\mathcal{A}}(x)$ such that $\mathcal{A} = \{x \in \mathbb{X} | J_{\mathcal{A}}(x) \le 0\}$. Then $\mathcal{V}(t)$ is computed according to (8) subject to the additional constraint that $J(x, t) \ge -J_{\mathcal{A}}(x)$ for all t. In the two modes of interest ($0r$ and $25d$), the reach–avoid computation achieves a fixed point $\mathcal{V}$, and the controllable envelope for these modes is the complement of this fixed point $\mathcal{W} = \mathcal{V}^c$. For the particular sets and dynamics of these two modes, it turns out that $\mathcal{V} = \mathcal{A}^c$, for all safe states there exists a safe instantaneous switch to the subsequent mode, but that need not be true in general.

Results

The results of the reachability computation are shown in Figs. 4, 6, and 7.

Figure 4 shows the set of controllable states in modes $0u$, $25d$, and $50d$ without switching (dark), as well as the corresponding flight envelopes (gray). This figure shows the boundary of the flight envelope as well as the computational result for $\mathcal{W}$, which is the largest set contained in $\mathcal{W}_0$ such that the pilot can touch down safely. As can be seen from Fig. 4, portions of $\mathcal{W}_0$ are excluded from $\mathcal{W}$. There are three reasons for this fact.

1) For low speeds, there is not enough lift/thrust to prevent the aircraft from stalling almost immediately: In the state space (V, γ, z) a point too close to the face $V = V_{\min}$ in $\mathcal{W}_0$ will not be able to stay in $\mathcal{W}_0$ and will exit this box through the $V = V_{\min}$ face.

2) For steep flight-path angles (close to the $\gamma = \gamma_{\min}$ face in the $\mathcal{W}_0$ box), the aircraft has too steep of a flight-path angle to maintain it in the box: The state space exits the box through the $\gamma = \gamma_{\min}$ face.

3) Too close to the ground, with steep flight-path angle, the aircraft is not able to reach the $V \sin\gamma \ge \dot{z}_0$ subset of the box and touches the ground with too high a vertical velocity.

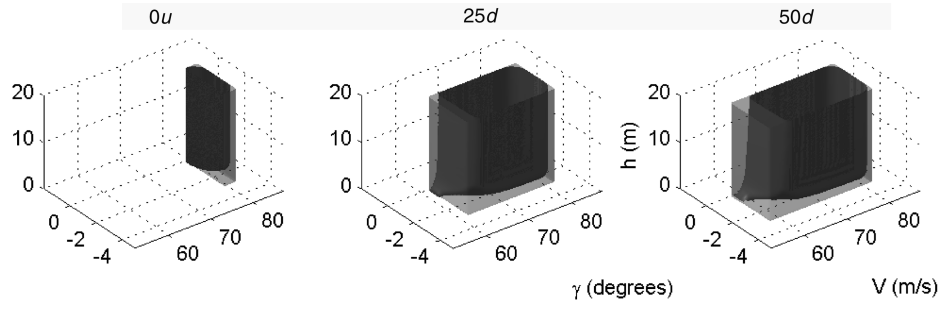

Fig. 6 Flight envelope $\mathcal{W}_0$ in each mode (gray). Controlled set $\mathcal{W}$ within each mode (dark), with switching allowed.

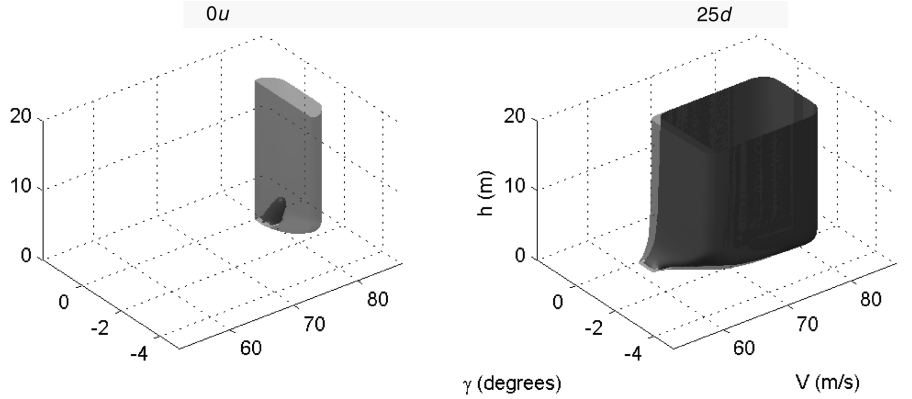

Fig. 7 Comparison between the set of controllable states without switching (dark) and with switching (gray), from Figs. 4 and 6.

As can be seen, the only sets that are controllable in mode $0u$ are close to the ground (the dark set does not extend higher than a few meters). This means that states too far from the ground are not controllable in mode $0u$: It is not possible to touch the ground safely in that mode from these states. For the other modes, some portions of the flight envelope are excluded from the set of controllable states.

The benefit of switching thus appears in Fig. 6. Mode $0u$ becomes controllable by switching to mode $25d$ through the transition mode $0r \rightarrow 25d$. The dark set now extends vertically to the top of the computational domain. Figure 7 compares the maximal controllable set without switching with the maximal controllable set when switching is enabled. The difference between the two sets in mode $25d$ is relatively small: switching from mode $25d$ leads to mode $50d$ through mode $25d \rightarrow 50d$. Because this transition mode has to last for at least 10 s, the system might still exit the envelope before achieving mode $50d$ in which it becomes controllable. The envelope is not shown here. The benefit of switching is obvious from the left subplot (the set of controllable states is bigger and allows safe landing). The set of controllable states for the $25d$ mode becomes slightly bigger as well. The mode $50d$ is not shown here because no switching from that mode is available (Fig. 5) and therefore the only relevant set in that mode is the set shown in Figs. 4 or 6 (right-hand part).

This type of computation can be used as a design mechanism for autopilots, to determine the times at which switches can be initiated. For example, reducing the speed in mode $0u$ requires switching; otherwise, the aircraft will most likely stall.

Current Work: Toward More Realistic Models

The model of the preceding sections assumes that the control inputs of the aircraft are α and T. In reality the pilot has control over $\ddot{\alpha}$ and T. The currently available computational resources enable fast computations of reachable sets for dimensions up to four. This section shows how such computation could be used. It is therefore assumed that the pilot has control over $\dot{\alpha}$. $\dot{\alpha}$ is the input and ranges in an interval that is known a priori and represents realistic rates of change of α, given known acceptable values of $\ddot{\alpha}$:

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{bmatrix} V \\ \gamma \\ z \\ \alpha \end{bmatrix} = \begin{bmatrix} \frac{1}{m}[T\cos\alpha - D(\alpha, V) - mg\sin\gamma] \\ \frac{1}{mV}[T\sin\alpha + L(\alpha, V) - mg\cos\gamma] \\ V\sin\gamma \\ u \end{bmatrix} \tag{11}$$

The method presented in preceding sections applies to this new model. In this case, the computation of the optimal input is easier: the Hamiltonian is given by

$$H(x, p) = \frac{p_1}{m}[T\cos\alpha - D(\alpha, V) - mg\sin\gamma] + \frac{p_2}{mV}[T\sin\alpha + L(\alpha, V) - mg\cos\gamma] + p_3 V\sin\gamma + p_4 u \tag{12}$$

Therefore, the optimal input T^* can be determined as before, and the optimal input u^* is $\mathrm{sgn}(p_4)$. For the four-dimensional system (11) the envelope is now a four-dimensional set in the (V, γ, h, α) space. Equations (6) and (7) mathematically define a three-dimensional flight envelope in flare mode. Let us call this set $\mathcal{E}$. With α now a state variable, the flight envelope becomes $\mathcal{E} \times [\alpha_{\min}, \alpha_{\max}]$, and the task of a controller is to maintain the state in this set. The problem can be solved as previously, and the result is a four-dimensional set such that if the state of the system (V, γ, h, α) is initially inside the set, there exists a control that will keep it inside the four-dimensional envelope $\mathcal{E} \times [\alpha_{\min}, \alpha_{\max}]$.

Figures 8 and 9 show three-dimensional slices of the four-dimensional controllable set. The four-dimensional maximal controllable set for a single mode (mode $50d$) is computed. The numerical values are the same as in the preceding section, with $\dot{\alpha} \in [-0.35, 0.35]$ rad/s and $T = 0.7 \cdot T_{\max}$.

Figure 8 shows the slices for different α. These sets can be compared with the sets of Figs. 4 for a single mode. For any given α slice, the sets of Fig. 8 would be enclosed in their counterpart with (1) instead of (11). Equation (1) implies that the angle of attack can be changed instantaneously, whereas (11) takes into account the rotational inertia of the aircraft; therefore, it is harder to control the system through (11). These subplots provide the set of (V, γ, z) that are controllable when the dynamics (1) includes α as a state variable. As can be seen, starting from a very small α ($\alpha = 1$ deg) or a very large α ($\alpha = 17$ deg) restricts the set of (V, γ, z) for which the aircraft can ultimately touch down. As can be seen for $\alpha = 1$ deg, the set does not connect to the ground: The angle of attack (and, therefore, the lift) is too small, causing the flight-path angle to become too steep. For $\alpha = 17$ deg, the set does not connect to the ground either because the angle of attack is too high, causing either stall at low speed or causing the flight-path angle to become positive at high speeds (because of the high lift). Between these two values of α landing is possible, which seems intuitive: If α is initially set to a reasonable value, it is possible to reach the ground safely with the appropriate control.

Figure 9 should be interpreted as slices from a "reachability tube" in the four-dimensional space. For a given altitude, a three-dimensional slice gives the set of parameters for which the aircraft is controllable. As expected, the set decreases with altitude. As the aircraft approaches the ground, the set of states from which it is possible to control the aircraft becomes smaller because there is less time to rectify an approach leading to a touchdown outside the safe set (7). As in Fig. 8, one can see that very large or very small values of α become uncontrollable close to the ground (see the slice at $z = 2$ m) because they lead to a touchdown outside the safe set (7).

Figure 9 illustrates how these results could be used for autopilot design. The method allows checking for all z if (V, γ, z, α) is in the set of controllable parameters. This method could thus at every z provide the appropriate input to apply to keep (V, γ, z, α) inside the maximal controllable set as z further decreases.

Conclusion

The model of the longitudinal dynamics of a commercial jet aircraft that was presented in this paper was used to compute safety

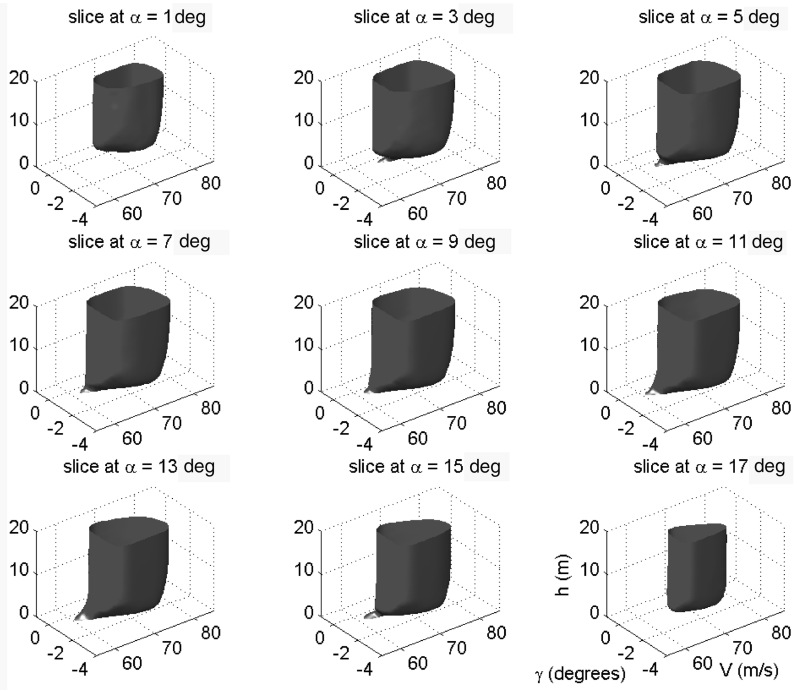

Fig. 8 Three-dimensional slices of the four-dimensional control invariant set corresponding to (11), for various values of α.

envelopes of the aircraft in the different modes of landing. The main outcome of this paper is the construction of an input to apply to keep the aircraft inside a user-prescribed flight envelope. The simulations shown demonstrate the possibility of generating such a control for an actual aircraft. The method presented used concepts from hybrid systems theory and was successfully applied to the successive flap and slat deflection of a DC9-30 aircraft in final approach. Finally, higher dimensional reachability computations were displayed, which show the potential of the method for applications to more accurate models.

In the future, computational resources will allow the treatment of higher dimensional models (which would incorporate more parameters and features of the systems). Therefore, the proofs of safety provided by our model are valid only within the limits of this model. They are relevant for current autopilots, as confirmed by recent experiments realized on conflict avoidance maneuvers. Another approach currently under investigation is the possibility of computing guaranteed approximations of the controllable set in higher dimension.

Appendix

Proof of Proposition 1: The Hamiltonian associated with Eq. (1) reads

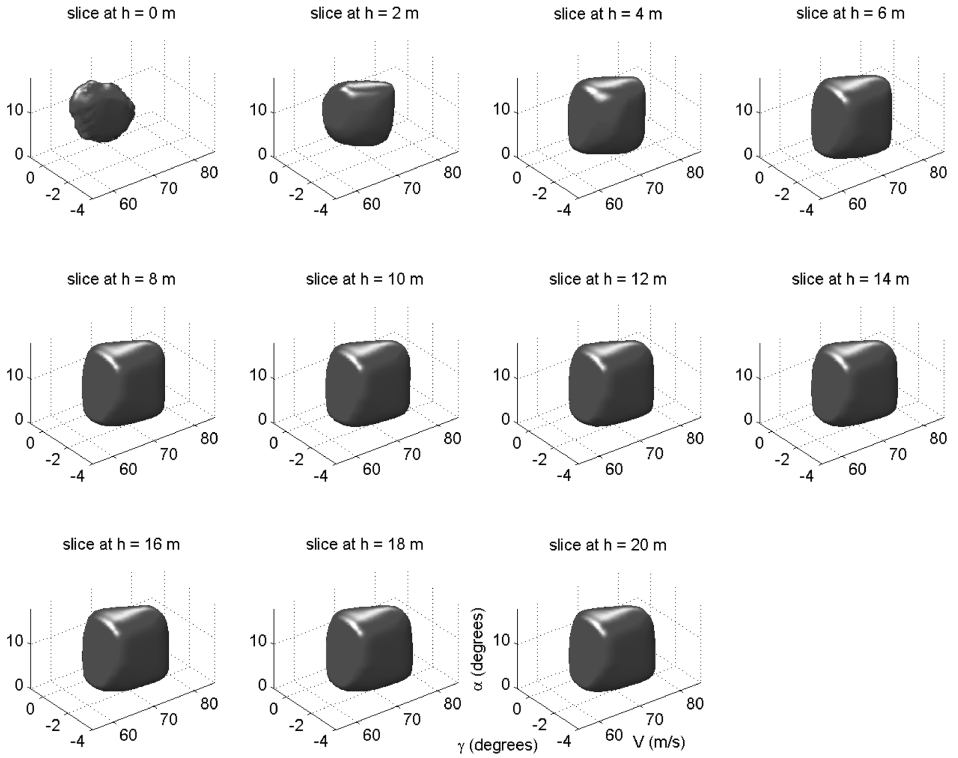

Fig. 9 Three-dimensional slices of the four-dimensional control invariant set corresponding to (11), for various values of z.

Table A1 Optimal input (α^*, T^*) given as a function of the costate (p_1, p_2)

α	T	Condition	(α^*, T^*)
0	$[0, T_{\max}]$	$p_1 > 0$	$(0, T_{\max})$
		$p_1 < 0$	$(0, 0)$
$\alpha_{\max}$	$[0, T_{\max}]$	$p_1 \cos\alpha_{\max} + (p_2/V)\sin\alpha_{\max} > 0$	$(\alpha_{\max}, T_{\max})$
		$p_1 \cos\alpha_{\max} + (p_2/V)\sin\alpha_{\max} < 0$	$(\alpha_{\max}, 0)$
$[0, \alpha_{\max}]$	0	$p_1 > 0$	
		if $\tilde{\alpha}_1 \in [0, \alpha_{\max}]$	$(\tilde{\alpha}_1, 0)$
		if $\tilde{\alpha}_1 > \alpha_{\max}$	$(\alpha_{\max}, 0)$
		if $\tilde{\alpha}_1 < \alpha_{\max}$	$(0, 0)$
		$p_1 < 0$	$(\alpha_{\max}, 0)$ or $(0, 0)$
$[0, \alpha_{\max}]$	$T_{\max}$	$p_1 < 0$ $p_2 > 0$	$(\alpha_{\max}, T_{\max})$
		$p_1 > 0$ $p_2 < 0$	$(0, T_{\max})$
		$p_1 < 0$ $p_2 < 0$	$(\alpha_{\max}, T_{\max})$ or $(0, T_{\max})$
		$p_1 > 0$ $p_2 > 0$	
		if $\partial H/\partial\alpha|_{(0,T_{\max})} < 0$	$(0, T_{\max})$
		if $\partial H/\partial\alpha|_{(\alpha_{\max},T_{\max})} > 0$	$(0, T_{\max})$
		if $\partial H/\partial\alpha|_{(0,T_{\max})} \cdot \partial H/\partial\alpha|_{(\alpha_{\max},T_{\max})} < 0$	$(\tilde{\alpha}_2, T_{\max})$

$$p^T \cdot f(x,u) = \frac{p_1}{m}[T\cos\alpha - D(\alpha,V) - mg\sin\gamma] + \frac{p_2}{mV}[T\sin\alpha + L(\alpha,V) - mg\cos\gamma] + p_3 V\sin\gamma \tag{A1}$$

where $u = [\alpha, T]$. The optimality condition reads

$$\frac{\partial[p^T\cdot f(x,u)]}{\partial u_1} = \frac{\partial[p^T\cdot f(x,u)]}{\partial\alpha} = \frac{p_1\cos\alpha}{m} + \frac{p_2\sin\alpha}{mV} = 0$$
$$\frac{\partial[p^T\cdot f(x,u)]}{\partial u_2} = \frac{\partial[p^T\cdot f(x,u)]}{\partial T} = -\frac{Tp_1\sin\alpha}{m} - \frac{p_1}{m}\frac{\partial D(\alpha,V)}{\partial\alpha} + \frac{p_2 T\cos\alpha}{mV} + \frac{p_2}{mV}\frac{\partial L(\alpha,V)}{\partial\alpha} = 0 \tag{A2}$$

From (A2), the necessary conditions on the domain interior can be computed:

$$\alpha^* = -\tan^{-1}\left(\frac{p_1 V}{p_2}\right),$$
$$T^* = \frac{1}{\sqrt{1+(p_1V/p_2)^2}}\left[\frac{p_1 V}{p_2}\frac{\partial D}{\partial\alpha}\left(\tan^{-1}\left(-\frac{p_1V}{p_2}\right), V\right) - \frac{\partial L}{\partial\alpha}\left(\tan^{-1}\left(-\frac{p_1V}{p_2}\right), V\right)\right] \tag{A3}$$

Using the fact that, for this particular model of lift and drag, $L(\alpha, V)$ is a linear function of α and $D(\alpha, V)$ is a quadratic function of α, it can be checked quite easily that the eigenvalues of the Hessian matrix are given by

$$\lambda = -\frac{p_1}{2m}\left\{\frac{\partial^2 D}{\partial\alpha^2}(V) \pm \sqrt{\left[\frac{\partial^2 D}{\partial\alpha^2}(V)\right]^2 + \left[\frac{2}{\sin(\alpha^*)}\right]^2}\right\} \tag{A4}$$

where the dependence on α has been omitted when α disappears in the differentiation. It can be easily checked that the two eigenvalues are of opposite sign and that therefore $p^T\cdot f(x,u)$ can never be extremal at (α^*, T^*). The extremum of $p^T\cdot f(x,u)$ is thus on the boundary of the domain.

Proof of Proposition 2: In Eq. (A1),

$$h(x,p) := \frac{p_1}{m}[T\cos\alpha - D(\alpha,V) - mg\sin\gamma] + \frac{p_2}{mV}[T\sin\alpha + L(\alpha,V) - mg\cos\gamma]$$

is the only part of $H(x, p)$ that depends on the input. To find (α^*, T^*), one needs to use h instead of H. Table A1 summarizes the possible situations and corresponding optimal inputs. The justification for these results is as follows.

For the cases where α is fixed (the first and second rows of Table A1), the only term of interest in h is given by $[p_1\cos\alpha + (p_2/V)\sin\alpha](T/m)$. Clearly, for $\alpha = \alpha_{\max}$ as well as for $\alpha = 0$, if $[p_1\cos\alpha + (p_2/V)\sin\alpha](T/m) > 0$, $T^* = T_{\max}$; otherwise, $T^* = 0$.

For $T = 0$, one can rewrite $h(x, p)$ as

$$h(x,p) = \frac{p_2}{mV}L_0(h_\delta + c\alpha)V^2 - [D_0 + \kappa(h_\delta + c\alpha)^2]V^2$$

which is a quadratic in α. The constants L_0, D_0, κ, c, and h_δ can be easily related to the model through Eqs. (2–4). If $p_1 > 0$, the maximum occurs between the two zeros of the quadratic:

$$\alpha_1 = \frac{1}{c}\left(\frac{L_0 p_2}{V p_1 \kappa} - h_\delta\right) \tag{A5}$$

Because the parabola is upside down, if $\alpha_1 < 0$, $\alpha^* = 0$; if $\alpha_1 \in [0, \alpha_{\max}]$, $\alpha^* = \alpha_1$; and if $\alpha_1 > \alpha_{\max}$, $\alpha^* = \alpha_{\max}$. If $p_1 < 0$, the situation is much simpler because the parabola is right-side up, and so depending on the location of α_1 in $[0, \alpha_{\max}]$, $\alpha^* = 0$ or $\alpha^* = \alpha_{\max}$.

For $T = T_{\max}$, one wants to solve for

$$\frac{\partial h}{\partial\alpha} = -\frac{p_1}{m}\left(T\sin\alpha + \frac{\partial D}{\partial\alpha}\right) + \frac{p_2}{mV}\left(T\cos\alpha + \frac{\partial L}{\partial\alpha}\right) = 0 \tag{A6}$$

There are four cases: The first case is $p_1 > 0$ and $p_2 < 0$. It is easy to see that $\partial h/\partial\alpha \geq 0$, which means that $\alpha^* = \alpha_{\max}$. Conversely, if $p_2 < 0$ and $p_1 > 0$, $\alpha^* = 0$. For the two remaining cases, it is needed to compute

$$\frac{\partial^2 h}{\partial\alpha^2} = -\frac{1}{m}\left(T\cos\alpha + \frac{\partial^2 D}{\partial\alpha^2}\right)p_1 - \frac{p_2}{mV}T\sin\alpha$$

from which it can be seen that if $p_1 < 0$ and $p_2 < 0$, then $h(x, p)$ cannot have a local maximum; therefore, $\alpha^* = 0$, or $\alpha^* = \alpha_{\max}$. The last case, $p_1 > 0$ and $p_2 > 0$, is more difficult: $h(x, p)$ can eventually have a local maximum because $\partial^2 h/\partial\alpha^2 < 0$. In that case, $\partial h/\partial\alpha$ is a decreasing function of α. Thus if $\partial h/\partial\alpha|_{\alpha=0} < 0$, $\alpha^* = 0$; if $\partial h/\partial\alpha|_{\alpha=\alpha_{\max}} > 0$, $\alpha^* = 0$ as well. The remaining case is when they have opposite sign: $\partial h/\partial\alpha|_{\alpha=0}\partial h/\partial\alpha|_{\alpha=\alpha_{\max}} < 0$. In that case, one needs to solve the transcendental Eq. (A6) numerically, and the solution is called α_2.

Corollary 1: Call $p = [p_1, p_2, p_3]$ the costate of the system. To solve efficiently for the optimal input, if $p_1 > 0$ and $p_2 > 0$, solve Eq. (A6) numerically for α_2 and compare the six possible cases of Proposition 2. Otherwise, compare only the five possible cases of Proposition 2 (no α_2).

Acknowledgments

This research was supported by NASA under Grant NCC 2-5422, by the Office of Naval Research (ONR) under MURI Contract N00014-02-1-0720, by Defense Advanced Research Projects Agency (DARPA) under the Software Enabled Control Program (AFRL Contract F33615-99-C-3014), and by a graduate fellowship of the Délégation Générale pour l'Armement (France). We are very grateful to Ilan Kroo for his initial suggestions for the model of the aircraft as well as for his help in computing the numerical value of the parameters.

References

[1] Bryant, R. E., "Graph-Based Algorithms for Boolean Function Manipulation," *IEEE Transactions on Computers*, Vol. C-35, No. 8, Aug. 1986, pp. 677–691.

[2] Hu, A. J., Dill, D. L., Drexler, A. J., and Yang, C. H., "Higher-Level Specification and Verification With BDDs," *Computer Aided Verification*, edited by G. v. Bochmann and D. K. Probst, Vol. 663, Lecture Notes in Computer Science, Springer–Verlag, Berlin, 1993, pp. 82–95.

[3] Mitchell, I., Bayen, A. M., and Tomlin, C. J., "Computing Reachable Sets for Continuous Dynamic Games Using Level Set Methods," *IEEE Transactions on Automatic Control*, Vol. 50, No. 7, 2005, pp. 986–1001.

[4] Lygeros, J., "On Reachability and Minimum Cost Optimal Control," *Automatica*, Vol. 40, No. 6, June 2004, pp. 917–927.

[5] Bryson, A. E., *Control of Spacecraft and Aircraft*, Princeton Univ. Press, Princeton, NJ, 1994, pp. 28–49.

[6] Crandall, M. G., and Lions, P.-L., "Viscosity Solutions of Hamilton-Jacobi Equations," *Transactions of the American Mathematical Society*, Vol. 277, No. 1, 1983, pp. 1–42.

[7] Crandall, M., Evans, L., and Lions, P.-L., "Some Properties of Viscosity Solutions of Hamilton-Jacobi Equations," *Transactions of the American Mathematical Society*, Vol. 282, No. 2, 1984, pp. 487–502.

[8] Isaacs, R., *Differential Games*, Wiley, New York, 1965; reprint Dover, New York, 1999, pp. 200–335.

[9] Osher, S., and Sethian, J., "Fronts propagating with Curvature-Dependent Speed: Algorithms Based on Hamilton-Jacobi Formulations," *Journal of Computational Physics*, Vol. 79, No. 1, 1988, pp. 12–49.

[10] Sethian, J. A., *Level Set Methods and Fast Marching Methods*, Cambridge Univ. Press, New York, 1999, pp. 305–308.

[11] Osher, S., and Fedkiw, R., *Level Set Methods and Dynamic Implicit Surfaces*, Springer–Verlag, New York, 2002, pp. 23–37.

[12] Aubin, J.-P., *Viability Theory, Systems and Control: Foundations and Applications*, Birkhäuser Boston, Cambridge, MA, 1991, pp. 77–195.

[13] Saint-Pierre, P., "Approximation of the Viability Kernel," *Applied Mathematics and Optimization*, Vol. 29, 1994, pp. 187–209.

[14] Cardaliaguet, P., Quincampoix, M., and Saint-Pierre, P., "Set-Valued Numerical Analysis for Optimal Control and Differential Games," *Stochastic and Differential Games: Theory and Numerical Methods*, edited by M. Bardi, T. Raghavan, and T. Parthasarathy, Annals of the International Society of Dynamic Games, Birkhäuser Boston, Cambridge, MA, 1999, pp. 177–248.

[15] Tomlin, C., Lygeros, J., and Sastry, S., "A Game Theoretic Approach to Controller Design for Hybrid Systems," *Proceedings of the IEEE*, Vol. 88, No. 7, 2000, pp. 949–970.

[16] Tomlin, C. J., Mitchell, I., Bayen, A. M., and Oishi, M. K., "Computational Techniques for the Verification and Control of Hybrid Systems," *Proceedings of the IEEE*, Vol. 91, No. 7, July 2003, pp. 986–1001.

[17] Bayen, A. M., Crück, E., and Tomlin, C. J., "Guaranteed Overapproximations of Unsafe Sets for continuous and Hybrid Systems: Solving the Hamilton-Jacobi Equation Using Viability Techniques," *Hybrid Systems: Computation and Control*, edited by C. J. Tomlin, and M. Greenstreet, Vol. 2289, Lecture Notes in Computer Science, Springer–Verlag, New York, 2002, pp. 90–104.

[18] Mitchell, I. M., "Application of Level Set Methods to Control and Reachability Problems in Continuous and Hybrid Systems," Ph.D. Thesis, Scientific Computing and Computational Mathematics Program, Stanford University, Stanford, CA, Dec. 2003.

[19] Bryson, A. E., and Denham, W. F., "A Steepest-Ascent Method for Solving Optimum Programming Problems," *Transactions of the American Society of Mechanical Engineers*, Vol. 29, No. E, 1962, pp. 247–257.

[20] Bayen, A. M., Santhanam, S., Mitchell, I., and Tomlin, C. J., "A Differential Games Formulation of Alert Levels in ETMS Data for High Altitude Traffic," *AIAA Conference on Guidance, Navigation and Control*, AIAA Paper 2003-5341, Aug. 2003.

[21] Lee, E. A., "Soft Walls: Frequently Asked Questions," University of California, Technical Memorandum UCB/ERL M03/31, Berkeley, CA, 2003.

[22] McGuire, B., and Neogi, N., "Verifying Correctness of Conflict Detection Devices in the Presence of Uncertainties," *AIAA 1st Intelligent Systems Technical Conference*, AIAA Paper 2004-6548.

[23] Rigal, S., "Guidage d'un Véhicule Sous Marin de Type Glider par des Méthodes de Viabilité, Rapport de DEA AIA," Ecole Centrale de Nantes, Technical Rept., Nantes, France, 2001.

[24] Teo, R., Jang, J. S., and Tomlin, C. J., "Flight Demonstration of Provably Safe Closely Spaced Parallel Approaches," *AIAA Conference on Guidance Navigation and Control*, AIAA Paper 2005-6197.

[25] Eklund, J. M., Sprinkle, J., and Sastry, S., "Template Based Planning and Distributed Control for Networks of Unmanned Underwater Vehicles," *IEEE Conference on Decision and Control*, (in preparation).

[26] Shevell, R., *Fundamentals of Flight*, Prentice–Hall, New York, 1989, pp. 158–176.

[27] Kroo, I., *Applied Aerodynamics—A Digital Textbook* [online textbook], Desktop Aeronautics, Stanford, 2006, http://www.desktopaero.com. (This textbook is online only.)

[28] Prandtl, L., and Tietjens, O., "*Fundamentals of Hydro- and Aeromechanics*, Eng. Societies Monographs, 1934, pp. 189–221; reprint Dover, New York, 1957.

[29] Sharma, V., Voulgaris, P. G., and Frazzoli, E., "Aircraft Autopilot Analysis and Envelope Protection for Operation under Icing Conditions," *Journal of Guidance, Control, and Dynamics*, Vol. 27, No. 3, pp. 454–465.

[30] Oishi, M. K., Mitchell, I., Bayen, A. M., and Tomlin, C. J., "Invariance-preserving abstractions of Hybrid Systems: Application to User Interface Design," *IEEE Transactions on Control Systems Technology*, 2005 (submitted for publication).

[31] Oishi, M. K., Mitchell, I., Bayen, A. M., Tomlin, C. J., and Degani, A., "Hybrid Verification of an Interface for an Automatic Landing," *Proceedings of the 41th IEEE Conference on Decision and Control*, Vol. 2, IEEE Publications, Piscataway, NJ, Dec. 2002, pp. 1607–1613.

[32] Roskam, J., and Lan, C.-T., *Airplane Aerodynamics and Performance*, Design, Analysis, and Research Corp., Lawrence, KS, 1997, pp. 1–547.

[33] "Gas Turbine Engines Specifications," *Aviation Week and Space Technology* [online journal], 17 Jan. 1999, http://www.aviationnow.-com [retreived Dec. 2005].