GENERAL SAFETY INDEX SYNTHESIS

Weiye Zhao
Robotics Institute
Carnegie Mellon University
Pittsburgh, PA 15213, USA

ABSTRACT

In this paper we discuss the safety index synthesis rule for the general dynamics system.

1 FLYING PENDULUM DYNAMICS

In this paper, we are consider a continuous-time system, the state space and control space for the flying pendulum are summarized as following:

$$q = \begin{bmatrix} x \\ y \\ z \\ \dot{x} \\ \dot{y} \\ \dot{z} \\ \gamma \\ \beta \\ \alpha \\ \dot{\gamma} \\ \dot{\beta} \\ \dot{\alpha} \\ \psi \\ \theta \\ \dot{\psi} \\ \dot{\theta} \end{bmatrix} \quad , \quad u = \begin{bmatrix} F \\ \tau_\gamma \\ \tau_\beta \\ \tau_\alpha \end{bmatrix} \tag{1}$$

The dynamics of the system is summarized as following:

$$\begin{bmatrix} \ddot{\gamma} \\ \ddot{\beta} \\ \ddot{\alpha} \end{bmatrix} = R_V^O(\gamma, \beta, \alpha) J^{-1} \begin{bmatrix} \tau_\gamma \\ \tau_\beta \\ \tau_\alpha \end{bmatrix} \tag{2}$$

$$\begin{bmatrix} \ddot{\psi} \\ \ddot{\theta} \end{bmatrix} = \begin{bmatrix} \frac{3}{2ML_p \cos\theta}(k_y(\gamma,\beta,\alpha)\cos\psi + k_z(\gamma,\beta,\alpha)\sin\psi) \\ \frac{3}{2ML_p}(-k_x(\gamma,\beta,\alpha)\cos\theta - k_y(\gamma,\beta,\alpha)\sin\psi\sin\theta + k_z(\gamma,\beta,\alpha)\cos\psi\sin\theta) \end{bmatrix} F + \begin{bmatrix} 2\dot{\theta}\dot{\psi}\tan\theta \\ -\dot{\psi}^2\sin\theta\cos\theta \end{bmatrix} \tag{3}$$

where M, L_p are the mass and length of the pendulum, respectively. The thrust $F \in [0, 4k_1]$, where k_1 is the thrust coefficient. $k_x(\gamma,\beta,\alpha) = \cos\alpha\sin\beta\cos\gamma + \sin\alpha\sin\gamma$; $k_y(\gamma,\beta,\alpha) = \sin\alpha\sin\beta\cos\gamma - \cos\alpha\sin\gamma$; $k_z(\gamma,\beta,\alpha) = \cos\beta\cos\gamma$.

2 SAFE INDEX DESIGN

The safety problem will be to keep the pendulum from falling past a certain angle (measured from the vertical), where δ denotes the angle from the world vertical.

We have ψ, θ, which specify the pendulum's rotation about the x and y world axes, respectively. Therefore, δ can be computed with the following equation:

$$\delta = \cos^{-1}(\cos(\theta)\cos(\phi)) \tag{4}$$

where $\cos^{-1}(\cdot) : [-1, 1] \to [0, \pi]$.

Therefore, the user defined safety index ϕ_0 is defined as following:

$$\phi_0(x) = \delta - \delta_{max} \tag{5}$$

Since the relative degree from ϕ_0 to control is 2, and thus the safety index ϕ follows the following structure:

$$\phi(x) = \delta^{c_1} - \delta_m^{c_1} + c_2\dot{\delta} + c_3 \tag{6}$$

3 Safety Index Synthesis Rule

3.1 Fundamental Condition

In this paper, we mainly discuss *Forward-Invariance* of system safety. Since we are considering the continuous-time system, the ultimate goal for the safety index synthesis rule is to ensure the existence of safe control, such that $\dot{\phi} < 0$, for all possible states when $\phi = 0$.

Mathematically, the fundamental condition to ensure there exists non-empty set of safe control for all possible states when $\phi = 0$ is:

$$\forall_{\phi=0,\theta,\psi,\dot{\theta},\dot{\psi},\alpha,\beta,\gamma}, \exists \ddot{\delta}, \text{ s.t. } \dot{\phi} = c_1\delta^{c_1-1}\dot{\delta} + c_2\ddot{\delta} < 0 \tag{7}$$

Alternatively, equation 7 can be verified by the following condition:

$$\forall_{\phi=0,\theta,\psi,\dot{\theta},\dot{\psi},\alpha,\beta,\gamma}, \ddot{\delta}_{min} < \frac{-(c_1\delta^{c_1-1}\dot{\delta})}{c_2} \tag{8}$$

Remark 1. *As you may notice the fundamental condition for nonempty set of safe control for flying pendulum system is very similar to 2D collision avoidance system (ISSA) equation 7 due to the fact that 1) δ is always positive in flying pendulum, and 2) d (relative distance between car and obstacle) is also always positive in 2D collision avoidance.*

*However, in this flying pendulum case, we cannot adopt the similar non-empty set of safe control proof strategy from ISSA, which is to ensure equation 8 is satisfied in the **worst case**:*

$$\ddot{\delta}_{min} < \min_{\phi=0,\theta,\psi,\dot{\theta},\dot{\psi},\alpha,\beta,\gamma} \frac{-(c_1\delta^{c_1-1}\dot{\delta})}{c_2} \tag{9}$$

*The main reason is that: **General degree-2 dynamics system doesn't have the assumption that the relative acceleration are bounded and both can achieve zeros, e.g.,** $\delta \in [\delta_{min}, \delta_{max}]$ **for** $\delta_{min} \leq 0 \leq \delta_{max}$.*

In fact, the bounds of $\ddot{\delta}$ varies for different states, and thus $\ddot{\delta}_{min}$ varies for different states. Consider the state where $\ddot{\delta}_{min} > 0$. Since RHS of equation 9 is negative (when $\dot{\delta} < 0$), equation 9 doesn't hold at that state regardless of c_1, c_2 design.

Therefore, using equation 9 as non-empty set of safe control condition is non-proper for general dynamics system.

3.2 Solve the Fundamental Condition

To find the condition for the c_1, c_2 to ensure equation 8 is satisfied, it is crucial to understand the relationship between $\ddot{\delta}_{min}$ and system states. Next, we summarize the $\dot{\delta}$ and $\ddot{\delta}$ as following:

$$\dot{\delta} = \frac{c\theta s\psi\dot{\psi} + c\psi s\theta\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{1/2}} \tag{10}$$

$$\begin{aligned}\ddot{\delta} &= \frac{c\psi c\theta\dot{\psi}^2 + c\psi c\theta\dot{\theta}^2 + c\theta s\psi\ddot{\psi} + c\psi s\theta\ddot{\theta} - 2s\psi s\theta\dot{\psi}\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{(2c\theta^2 c\psi s\psi\dot{\psi} + 2c\psi^2 c\theta s\theta\dot{\theta})(c\theta s\psi\dot{\psi} + c\psi s\theta\dot{\theta})}{2(1 - c\psi^2 c\theta^2)^{\frac{3}{2}}} \\ &= \frac{c\psi c\theta\dot{\psi}^2 + c\psi c\theta\dot{\theta}^2 + c\theta s\psi\ddot{\psi} + c\psi s\theta\ddot{\theta} - 2s\psi s\theta\dot{\psi}\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{(2c\theta^2 c\psi s\psi\dot{\psi} + 2c\psi^2 c\theta s\theta\dot{\theta})}{2(1 - c\psi^2 c\theta^2)}\dot{\delta}\end{aligned} \tag{11}$$

where $c\theta = \cos(\theta)$, $s\theta = \sin(\theta)$, $c\psi = \cos(\psi)$, $s\psi = \sin(\psi)$.

According to equation 11, we have that $\ddot{\delta}$ is impacted by $\ddot{\psi}, \ddot{\phi}$. However, the bounds on $\ddot{\psi}, \ddot{\phi}$ also vary at different states. Therefore, by substituting $\ddot{\psi}, \ddot{\phi}$ with thrust F in equation 11 according to equation 3, we have the following condition holds:

$$\begin{aligned}\ddot{\delta} = &\frac{c\theta s\psi\ddot{\psi}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{c\psi s\theta\ddot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} \\ &+ \frac{c\psi c\theta\dot{\psi}^2 + c\psi c\theta\dot{\theta}^2 - 2s\psi s\theta\dot{\psi}\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{(2c\theta^2 c\psi s\psi\dot{\psi} + 2c\psi^2 c\theta s\theta\dot{\theta})}{2(1 - c\psi^2 c\theta^2)}\dot{\delta} \\ = &\frac{c\theta s\psi(\frac{A}{c\theta}(k_y c\psi + k_z s\psi)F + 2\dot{\theta}\dot{\psi}\tan\theta)}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} \\ &+ \frac{c\psi s\theta(A(-k_x c\theta - k_y s\psi s\theta + k_z c\psi s\theta)F - \dot{\psi}^2 s\theta c\theta)}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} \\ &+ \frac{c\psi c\theta\dot{\psi}^2 + c\psi c\theta\dot{\theta}^2 - 2s\psi s\theta\dot{\psi}\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{(2c\theta^2 c\psi s\psi\dot{\psi} + 2c\psi^2 c\theta s\theta\dot{\theta})}{2(1 - c\psi^2 c\theta^2)}\dot{\delta} \\ = &\frac{(Ak_y s\psi c\psi + Ak_z s\psi^2)F + 2\dot{\theta}\dot{\psi}s\theta s\psi}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} \\ &+ \frac{c\psi s\theta(A(-k_x c\theta - k_y s\psi s\theta + k_z c\psi s\theta)F - \dot{\psi}^2 s\theta c\theta)}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} \\ &+ \frac{c\psi c\theta\dot{\psi}^2 + c\psi c\theta\dot{\theta}^2 - 2s\psi s\theta\dot{\psi}\dot{\theta}}{(1 - c\psi^2 c\theta^2)^{\frac{1}{2}}} + \frac{(2c\theta^2 c\psi s\psi\dot{\psi} + 2c\psi^2 c\theta s\theta\dot{\theta})}{2(1 - c\psi^2 c\theta^2)}\dot{\delta}\end{aligned} \tag{12}$$

where $A = \frac{3}{2ML_p} > 0$, $k_x = k_x(\gamma, \beta, \alpha)$, $k_y = k_y(\gamma, \beta, \alpha)$, $k_z = k_z(\gamma, \beta, \alpha)$.

Denote $f(F, \theta, \psi, \dot{\theta}, \dot{\psi}, \alpha, \beta, \gamma) =$ RHS of equation 12. Then by substituting equation 12 into equation 8, the condition for nonempty set of safe control becomes:

$$\forall_{\phi=0,\theta,\psi,\dot{\theta},\dot{\psi},\alpha,\beta,\gamma}, \min_{F\in[0,4k_1]} f(F, \theta, \psi, \dot{\theta}, \dot{\psi}, \alpha, \beta, \gamma) < \frac{-(c_1\delta^{c_1-1}\dot{\delta})}{c_2} \tag{13}$$

In fact, $\arg\min_{F\in[0,4k_1]} f(F, \theta, \psi, \dot{\theta}, \dot{\psi}, \alpha, \beta, \gamma)$ is quite simple. There are only two cases, 1) if $Ak_y s\psi c\psi + Ak_z s\psi^2 + c\psi s\theta A(-k_x c\theta - k_y s\psi s\theta + k_z c\psi s\theta) > 0$, then $\arg\min_{F\in[0,4k_1]} f = 0$; 2) if $Ak_y s\psi c\psi + Ak_z s\psi^2 + c\psi s\theta A(-k_x c\theta - k_y s\psi s\theta + k_z c\psi s\theta) < 0$, then $\arg\min_{F\in[0,4k_1]} f = 4k_1$.

By plugging the analytical solution of $\arg\min_{F\in[0,4k_1]} f$ into equation 13, and treat $c\psi, s\psi, c\theta, s\theta, \dot{\theta}, \dot{\psi}, k_x, k_y, k_z$ as bounded variables, equation 13 becomes a **local-positiveness con-**

straints, where $\min_{F\in[0,4k_1]} f(F,\theta,\psi,\dot{\theta},\dot{\psi},\alpha,\beta,\gamma) < \frac{-(c_1\delta^{c_1-1}\dot{\delta})}{c_2}$ can be expressed as $g(x) > 0$, and $g(x)$ is a polynomial.

Therefore, the original safety index synthesis problem becomes that we should optimize c_1, c_2, such that the prescribed **local-positiveness constraints** are satisfied. This could be treated as a natural extension of JTE toolbox.

4 Differential Drive Dynamics

In this section, we first introduce the dynamics of differential drive 2D robot to verify JTE toolbox on general safety index design.

The state space and control space for the differential drive are summarized as following:

$$x = \begin{bmatrix} x \\ y \\ \theta \end{bmatrix} \quad , \quad u = \begin{bmatrix} v \\ w \end{bmatrix} \tag{14}$$

Note that $v \in [0,1], w \in [0,1]$.

The dynamics of differential drive is summarized as following:

$$x_{t+1} = x_t + \begin{bmatrix} \cos(\theta) & 0 \\ \sin(\theta) & 0 \\ 0 & dt \end{bmatrix} \begin{bmatrix} v \\ w \end{bmatrix} \tag{15}$$

5 Differential Drive Dynamics (similar to ISSA version)

5.1 Dynamics

In this section, we first introduce the dynamics of differential drive 2D robot to verify JTE toolbox on general safety index design.

The state space and control space for the differential drive are summarized as following:

$$x = \begin{bmatrix} d \\ v \\ \alpha \end{bmatrix} \quad , \quad u = \begin{bmatrix} a \\ w \end{bmatrix} \tag{16}$$

Note that d is the distance from robot to obstacle. And we denote v as the velocity of robot in the obstacle frame and α as the hitting angle from robot to obstacle. As for the control u, we denote the acceleration of robot as a and the angular velocity of α as w.

The dynamics of differential drive is summarized as following:

$$x_{t+1} = f(x_t, u_t) \tag{17}$$

$$= \begin{bmatrix} d - v\cdot\cos(\alpha)\cdot dt \\ v \\ \alpha \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ dt & 0 \\ 0 & dt \end{bmatrix} \begin{bmatrix} a \\ w \end{bmatrix} \tag{18}$$

5.2 Safety Index

The safety problem will be to keep the robot from crashing into the obstacle (measured by d_{min}).

Therefore, the user-defined safety index ϕ_0 is defined as following:

$$\phi_0(x) = d_{min} - d \tag{19}$$

Since the relative degree from ϕ_0 to control is 2, and thus the safety index ϕ follows the following structure:

$$\phi(x) = d_{min}^{c_1} - d^{c_1} - c_2\dot{d} + c_3 \tag{20}$$

5.3 Fundamental Condition

In this paper, we mainly discuss *Forward-Invariance* of system safety. Since we are considering the continuous-time system, the ultimate goal for the safety index synthesis rule is to ensure the existence of safe control, such that $\dot{\phi} < 0$, for all possible states when $\phi = 0$.

Mathematically, the fundamental condition to ensure there exists non-empty set of safe control for all possible states when $\phi = 0$ is:

$$\forall_{\phi=0,d,v,\alpha}, \exists(a,w), \text{ s.t. } \dot{\phi} = -c_1 d^{c_1-1}\dot{d} - c_2\ddot{d} < 0 \tag{21}$$

Alternatively, equation 21 can be verified by the following condition:

$$\forall_{\phi=0,d,v,\alpha}, \ddot{d}_{max} > \frac{-c_1 d^{c_1-1}\dot{d}}{c_2} \tag{22}$$

Instead using worst case analysis, we aim to solve the fundamental condition in equation 22 directly. To find the condition for the c_1, c_2 to ensure equation 22 is satisfied, it is crucial to understand the relationship between $\ddot{d}_{max}$ and system states. Next, we summarize the $\dot{d}$ and $\ddot{d}$ as following:

$$\dot{d} = -v\cos(\alpha) \tag{23}$$

$$\ddot{d} = -a\cos(\alpha) + v\sin(\alpha)w \tag{24}$$

Denote $f(a,w,v,\alpha) =$ RHS of equation 24. Then by substituting equation 24 into equation 22, the condition for nonempty set of safe control becomes:

$$\forall_{\phi=0,d,v,\alpha}, \max_{(a,w)\in W} f(a,w,v,\alpha) > \frac{-c_1 d^{c_1-1}\dot{d}}{c_2}\ , \tag{25}$$

where we denote $(a,w) \in W := \{(a,w) \mid a_{min} \leq a \leq a_{max}, w_{min} \leq w \leq w_{max}\}$.

Note that $\alpha \in [0,\pi]$ and $v \in [0, v_{max}]$. Therefore, $\arg\max_{(a,w)} f(a,w,v,\alpha)$ is quite simple. There are only two cases: 1) $\alpha \in [0, \frac{\phi}{2}]$, then $\arg\max_{(a,w)} f(a,w,v,\alpha)$ = (a_{min}, w_{max}); 2) $\alpha \in [\frac{\phi}{2}, \pi]$, then $\arg\max_{(a,w)} f(a,w,v,\alpha)$ = (a_{max}, w_{max}).

By plugging the analytical solution of $\arg\max_{(a,w)} f(a,w,v,\alpha)$ into equation 25, and treat d, v, α as bounded variables, equation 25 becomes a **local-positiveness constraints**, where $\max_{(a,w)\in W} f(a,w,v,\alpha) > \frac{-c_1 d^{c_1-1}\dot{d}}{c_2}$ can be expressed as $g(x) > 0$, and $g(x)$ is a polynomial.

Therefore, the original safety index synthesis problem becomes that we should optimize c_1, c_2, such that the prescribed **local-positiveness constraints** are satisfied. This could be treated as a natural extension of JTE toolbox.

5.4 From Fundamental Condition to SOS Formulation

Constructing the refute set and showing it is empty to ensure global positiveness is the core idea behind Sum-of-Squares Programming (SOSP). We now construct the refute set of equation **??** as following:

$$\begin{cases} \gamma_0^* = \frac{-c_1 d^{c_1-1}\dot{d}}{c_2} - \max_{(a,w)\in W} f(a,w,v,\alpha) \geq 0 \\ \gamma_5^* = d \geq 0 \\ \gamma_6^* = v \geq 0 \\ \gamma_7^* = v_{max} - v \geq 0 \\ \gamma_8^* = \alpha \geq 0 \\ \gamma_9^* = \pi - \alpha \geq 0 \\ \phi_0^* = \phi = 0 \end{cases} \tag{26}$$

When By substituting $\dot{d} = -v\cos(\alpha)$ and $\max_{(a,w)\in W} f(a, w, v, \alpha) = -a_{min}\cos(\alpha) + v\sin(\alpha)w_{max}$ when $\alpha \in [0, \frac{\pi}{2}]$, we have:

$$\begin{cases} \gamma_0^* = \frac{c_1 d^{c_1-1} v\cos(\alpha)}{c_2} - (-a_{min}\cos(\alpha) + v\sin(\alpha)w_{max}) \geq 0 \\ \gamma_1^* = d \geq 0 \\ \gamma_2^* = v \geq 0 \\ \gamma_3^* = v_{max} - v \geq 0 \\ \gamma_4^* = \alpha \geq 0 \\ \gamma_5^* = \frac{\pi}{2} - \alpha \geq 0 \\ \phi_0^* = \phi = 0 \end{cases} \tag{27}$$

When $\alpha \in [\frac{\pi}{2}, \pi]$, we have:

$$\begin{cases} \gamma_0^* = \frac{c_1 d^{c_1-1} v\cos(\alpha)}{c_2} - (-a_{max}\cos(\alpha) + v\sin(\alpha)w_{max}) \geq 0 \\ \gamma_1^* = d \geq 0 \\ \gamma_2^* = v \geq 0 \\ \gamma_3^* = v_{max} - v \geq 0 \\ \gamma_4^* = \alpha - \frac{\pi}{2} \geq 0 \\ \gamma_5^* = \pi - \alpha \geq 0 \\ \phi_0^* = \phi = 0 \end{cases} \tag{28}$$

Then we can use Positivstellensatz theorem to turn the emptiness problem to a feasibility problem similar to (7). Finally, the problem (8) can be turned into the following optimization problem:

$$\begin{aligned} &\min \quad 0, \\ \text{s.t. } &\exists t \in \mathbb{R}, \exists p_i \in \text{SOS}, i = 0, 1, 2, \dots, 12, \text{ such that} \\ &p_0 + p_1\gamma_0^* + \dots + p_s\gamma_{12}^* + \dots + p_{01}\gamma_0^*\gamma_1^* + \dots + p_{012}\gamma_0^*\gamma_1^*\gamma_2^* + \dots \\ &+ p_{012\dots n}\gamma_0^* \dots \gamma_{12}^* + 1 + t(d_{min}^{c_1} - d^{c_1} - c_2\dot{d} + c_3) = 0 \end{aligned} \tag{29}$$

We set p_i to be a positive scalar β_i for all $i \geq 1$. A simplified problem of equation 29 can be defined:

$$\begin{aligned} &\min \quad 0, \\ \text{s.t. } &p_0 = -\beta_1\gamma_0^* - \dots - \beta_s\gamma_{12}^* - \beta_{01}\gamma_0^*\gamma_1^* - \dots - \beta_{012}\gamma_0^*\gamma_1^*\gamma_2^* + \dots \\ &- \beta_{012\dots n}\gamma_0^* \dots \gamma_{12}^* - 1 - t(d_{min}^{c_1} - d^{c_1} - c_2\dot{d} + c_3) \in SOS, \\ &\beta_i \geq 0, i = 1, 2, \dots \\ &t \in \mathbb{R} \end{aligned} \tag{30}$$

Mathematically, suppose the degree of p_0 is $2d$, we first do a sum-of-squares decomposition of p_0 such that $p_0 = Y^T Q^*(\beta_1, \beta_2, \dots, \beta_{012\dots n})Y$, where Q^* is symmetric and $Y = [y_1, y_2, \dots, y_{12}, y_1y_2, \dots, y_{12}^d]$. Specifically, for off-diagonal terms Q_{ij}^* as the element of Q^* at i-th row and j-th column ($i \neq j$), assuming the the coefficient of the term Y_iY_j in p_0 is w_{ij}, we set $Q_{ij}^* = \frac{w_{ij}}{2}$.

With the decomposed Q^*, we can formulate the equivalent nonlinear programming problem of equation 30:

$$\begin{aligned} &\min \quad 0, \\ \text{s.t. } &det(Q^*(\beta_1, \beta_2, \dots, \beta_{012\dots n})_k) \geq 0, k = 1, 2, \dots \end{aligned} \tag{31}$$