7/18/2018

A Risk-Sensitive Reachability Problem for Safety of Stochastic Dynamic Systems in Discrete Time

- stochastic dyn in discrete-time
- non-ad disturbances
- degree of safety is quantified
- obtain prob. safety guarantee
- appreciate the reality that rare events can occur that are detrimental to safety

- A classic reachability analysis problem for safety of dynamic systems is to compute the set of initial states from which the state trajectory is guaranteed to stay inside a given constraint set, K, under the assumption of unknown but bounded disturbances.

- Bertsekas (2000) provides the discrete-time version of this problem (p.190, p.46, Ex. 1.5), which follows.

  $x_k \in S$ state, $u_k \in C$ control, $w_k \in W_k(x_k, u_k)$ disturbance

- Given a system, $x_{k+1} = f_k(x_k, u_k, w_k)$, one may compute a value function that specifies the safety of the state trajectory emanating from any initial condition, $x_0 \in S$,

$$J^*(x_0) := \inf_{\pi} \max_{\substack{w_k \in W_k \\ k=0,1,\dots,N-1}} \left\{ \sum_{k=0}^{N} g_k(x_k) \right\}, \quad \text{where} \quad g_k(x_k) = \begin{cases} 0 & \text{if } x_k \in K \\ 1 & \text{if } x_k \notin K \end{cases}, \quad \text{and} \qquad (1)$$

$\pi \in \widetilde{\Pi} := \{(\mu_0, \dots, \mu_{N-1}),\ \mu_k : S \to C\}$ is an admissible policy.

- $J^*(x_0)$ specifies safety because $J^*(x_0) = 0 \iff \exists\, \pi \in \widetilde{\Pi}$ such that $x_0 \in K, \dots, x_N \in K$ for all $w_0 \in W_0, \dots, w_{N-1} \in W_{N-1}$.

- In particular, the above min-max formulation assumes that (1) the disturbance is adversarial and and (2) safety is well-described solely as a binary notion according to set membership. (inside K is good, outside K is bad, being far inside/outside K is equally good/bad)

- More generally, one can define the safe set as follows:

$$\{x_0 \in S \mid \exists\, \pi \in \widetilde{\Pi} \text{ s.t. } x_0 \in K, \dots, x_N \in K \text{ for all } w_0 \in W_0, \dots, w_{N-1} \in W_{N-1}\},$$

which can be computed via $\{x_0 \in S \mid J^*(x_0) = 0\}$. (2)

- But, in practice, disturbances do not usually behave adversarially.
  - Most storms do not cause major floods.
  - Most drivers are never involved in car chases.
  - Most drones (outside of war) are not intending to collide with each other.

Indeed, min-max formulations, such as (1), may produce overly conservative control policies with limited practical utility; the set of control policies that satisfies (1) or the safe set (2) may be artifically small.

- In applications where min-max formulations are not useful, one may consider a stochastic formulation, where the disturbance is assumed to be drawn from some known probability distribution, $w_k \sim \mathbb{P}_k$. (Techniques for estimating such distributions from data is active research - refs?)

- Abate et al. (2008) formulized the probabilistic reachability problem for safety of stochastic dynamic systems in discrete time* as follows.
  - The probabilistic safe set with level $\varepsilon \in [0,1]$ is $\{x_0 \in S \mid \exists \pi \in \Pi \text{ s.t. } x_0 \in K, \dots, x_N \in K \text{ with probability at least } 1-\varepsilon\}$,

    which equals $\left\{x_0 \in S \;\middle|\; \sup_{\pi \in \Pi} \mathbb{E}\left[\prod_{k=0}^{N} \mathbb{1}_K(x_k)\right] \geq 1-\varepsilon\right\}$, (3)

    which is equivalent to $\left\{x_0 \in S \;\middle|\; \inf_{\pi \in \Pi} \mathbb{E}\left[\max_{k \in [0,N]} \mathbb{1}_{K^c}(x_k)\right] \leq \varepsilon\right\}$, (4)

    where $\mathbb{1}_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$ is the indicator function.
  - Abate et al. 2008 proved that (3), (4) can be computed via dynamic programming algorithms.

- Similar to the min-max formulation, the stochastic formulation above also assumes that safety is well-described solely as a binary notion according to set membership.

* Abate did the analysis for hybrid systems.

- However, this may not be an appropriate description for safety, especially when the system at hand is hard to control.
  - Water may occassionally overflow the banks of a stormwater detention pond.

    - boundary of K hard to define. Lidar map/perception has uncertainty

  - During a course of cancer treatment, some healthy cells may die in addition to cancer cells.

- In addition to quantifying set membership (does traj ever leave K?), we may also want to quantify <u>the degree of constraint violation (or satisfaction)</u> exhibited by a given state trajectory.

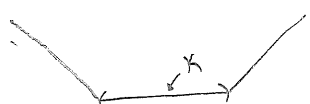
  We abbreviate " as <u>the degree of safety</u>.

- A natural way to quantify the degree of safety <u>at a given state</u> is to define a surface function that represents distance in some sense with respect to the boundary of K such that $x \in K \iff g(x) < 0$.

  E.g. $K = (0, 10)$. $g(x) = x(x-10)$, $g(x) = |x-5| - 5$.

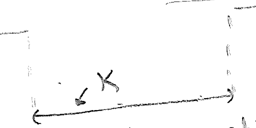
  (This technique is used in HJ Reachability Analysis for dynamics in continuous-time w/ unknown but bounded disturbances.)

  - Note that choosing $g(x)$



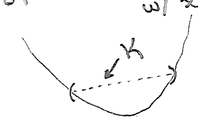
does not quantify the degree of constraint satisfaction

or



does not quantify the degree of constraint satisfaction or violation.

, so we will consider $g(x)$ of the form, w/ $x \in K \iff g(x) < 0$.



- However, it is not immediately clear how to quantify the degree of safety of a given state trajectory.

  Candidates include:

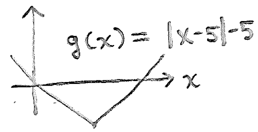
  $$\sum_{k=0}^{N} g(x_k) \quad (5)$$ (adopted from (1) - Bertsekas)

  $$\prod_{k=0}^{N} g(x_k) \quad (6)$$ (adopted from (3) - Abate)

  $$\max_{k \in \{0, \dots, N\}} g(x_k) \quad (7)$$ (" (4) - Abate)

- We will argue that (5) and (6) are likely not suitable for safety using examples of realizations of the state trajectory.

$K = (0, 10)$



- Ex. 1a $(x_0, x_1, x_2) = (1, -1, 1)$. Realized traj exited K. $\sum_{k=0}^{2} g(x_k) = -1$

  realized traj

- Ex. 1b $(x_0, x_1, x_2) = (1/3, 1/3, 1/3)$. Realized traj did not exit K. $\sum_{k=0}^{2} g(x_k) = -1$.

  The realized value of $\sum g(x_k)$ does not indicate whether the traj left K.

- Ex. 2a $(x_0, x_1, x_2) = (1, -1, -2)$. Realized traj left K. $\prod_{k=0}^{2} g(x_k) = -1 \cdot 1 \cdot 2 = -2$

- Ex. 2b $(x_0, x_1, x_2) = (1, 1, 2)$. Realized traj did not leave K. $\prod_{k=0}^{2} g(x_k) = -1 \cdot -1 \cdot -2 = -2$

  The realized value of $\prod g(x_k)$ does not indicate whether traj left K.

- However, (7) is a suitable metric. Let g be such that $x \in K \iff g(x) < 0$.

  Let $(x_0, x_1, \ldots, x_N)$ be any realized state trajectory.

  <u>Fact</u> $\max_{k \in \{0,\ldots,N\}} g(x_k) < 0 \iff \forall k,\ g(x_k) < 0 \iff \forall k,\ x_k \in K$.

  - (7) is an appropriate metric for the degree of safety of a state trajectory b/c (7) indicates
    - (i) whether the traj stays in K
    - (ii) the degree of constraint satisfaction if traj $\in K$
    - (iii) " " violation if traj $\notin K$

    via minimum distance to boundary of K.

- Recall that our system is stochastic, $x_{k+1} = f_k(x_k, u_k, w_k)$ $w_k \sim \mathbb{P}_k$, so

$$\max_{k \in \{0,\dots,N\}} g(x_k) \text{ is a random variable.}$$

- A natural way to evaluate a random variable is via expectation.

- We might consider the following value function, $V^*(x_0) := \min_{\pi \in \Pi} \mathbb{E}\left[\max_{k \in \{0,\dots,N\}} g(x_k)\right]$ (8), to quantify the degree of safety of the trajectory emanating from $x_0 \in S$.

- Key limitations of (8) include: $V^*(x_0)$ being sufficiently small does not
  - ⓐ provide a probabilistic safety guarantee
  - ⓑ appreciate the reality that rare events may occur and be detrimental to safety

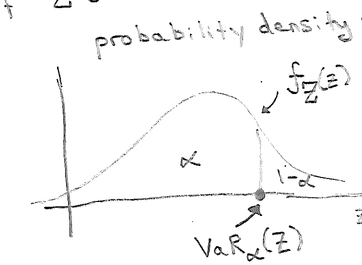
- There is another metric similar in spirit to expectation that does satisfy ⓐ and ⓑ, called <u>Conditional Value at Risk</u> (or Expected Shortfall) "CVaR"

- Intuitively, CVaR is a function from the space of random variables to $\mathbb{R}$ that penalizes the outcomes that hurt the most (cite Shapiro encyclopedia).

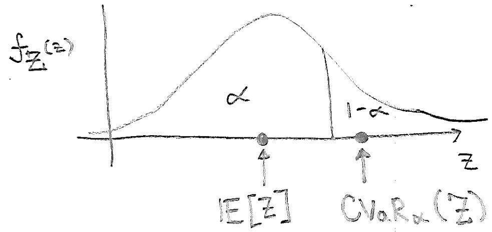
- A related function from the space of random variables to $\mathbb{R}$ is Value-at-Risk. (VaR)

VaR of r.v Z at confidence level $\alpha \in (0,1)$ is the α-quantile of the distribution of Z.

if Z continuous r.v.



- For continuous r.v. Z, CVaR of Z at confidence level $\alpha \in (0,1)$ is $\mathbb{E}[Z \mid Z \geq \mathrm{VaR}_\alpha(Z)]$.



- Why is CVaR a good option?

a "risk-sensitive" optimal control problem:

$$W^*(x_0) := \min_{\pi \in \Pi} \mathrm{CVaR}_\alpha\left[\max_{k \in \{0,\dots,N\}} g(x_k)\right]$$

vs.

a "risk-neutral" optimal control problem

$$V^*(x_0) := \min_{\pi \in \Pi} \mathbb{E}\left[\max_{k \in \{0,\dots,N\}} g(x_k)\right]$$

$$W^*(x_0) < 0 \Rightarrow \exists \pi \text{ s.t. } \mathrm{CVaR}_\alpha\left[\max_k g(x_k)\right] < 0$$

$$\Downarrow$$

$$\exists \pi \text{ s.t. } \underbrace{\mathbb{P}\left[\max_k g(x_k) \geq 0\right]}_{\shortparallel} < 1-\alpha$$

$$\mathbb{P}[\exists k \text{ s.t. } g(x_k) \geq 0]$$

$$\shortparallel$$

$$\mathbb{P}[\exists k \text{ s.t. } x_k \notin K]$$

- there is a probabilistic safety guarantee for $\underline{\underline{\text{any}}}$ g such that $g(x) < 0 \Leftrightarrow x \in K$

- does penalize more harmful outcomes

$$V^*(x_0) < 0 \Rightarrow \exists \pi \text{ s.t. } \mathbb{E}\left[\max_k g(x_k)\right] < 0.$$

$$\mathbb{E}[Z] = \sum_i z_i \, \mathbb{P}[Z = z_i]$$

- no known probabilistic safety guarantee for $g(x) \neq$ indicator function

- does not penalize the more harmful outcomes

- Recall the classic reachability analysis problem for safety:

  to compute the set of initial conditions from which the state trajectory is "guaranteed" to stay inside K.

- We can apply this concept to our risk-sensitive optimal control problem and define a risk-sensitive r-sublevel set,

$$S^{\alpha}_{(r)} := \left\{ x_0 \mid \min_{\pi} \mathrm{CVaR}_{\alpha}\left(\max_{k} g(x_k) \right) < r \right\}.$$

- In particular, if $r = 0$, then the states in $S(0)$ also satisfy a probabilistic safety guarantee.

  Further, as r decreases, the states in $S(r)$ can be considered more safe.

- Our problem is to compute S^{α}_{r} for various values of (α, r).

  set of initial conditions from which there is a control policy that can make the risk of "large" constraint violations" small".

- What are the features of S^{α}_{r}?
  - stochastic dynamics in discrete-time w/ non-adversarial disturbances
  - quantifies the degree of safety (constraint violation or satisfaction); appreciates situations where safety cannot be well-described solely as a binary notion in terms of set membership.
  - provides a probabilistic safety guarantee for $r=0$
  - appreciates the reality that rare harmful outcomes can occur by explicitly penalizing these outcomes as opposed to penalizing average outcomes.