Collision Probabilities for Continuous-Time Systems Without Sampling

Citation	2020. "Collision Probabilities for Continuous-Time Systems Without Sampling." Robotics: Science and Systems XVI.
As Published	10.15607/RSS.2020.XVI.019
Publisher	Robotics: Science and Systems Foundation
Version	Author's final manuscript
Citable link	https://hdl.handle.net/1721.1/137189
Terms of Use	Creative Commons Attribution-Noncommercial-Share Alike
Detailed Terms	http://creativecommons.org/licenses/by-nc-sa/4.0/

Collision Probabilities for Continuous-Time Systems Without Sampling

[with Appendices]

Kristoffer M. Frey[*][†], Ted J. Steiner[†], and Jonathan P. How[*]
[*]Department of Aeronautics and Astronautics, MIT
[†]The Charles Stark Draper Laboratory, Inc.
Cambridge, MA 02139
Email: kfrey@mit.edu

***Abstract*—Demand for high-performance, robust, and safe autonomous systems has grown substantially in recent years. Fulfillment of these objectives requires accurate and efficient risk estimation that can be embedded in core decision-making tasks such as motion planning. On one hand, Monte-Carlo (MC) and other sampling-based techniques can provide accurate solutions for a wide variety of motion models but are cumbersome to apply in the context of continuous optimization. On the other hand, "direct" approximations aim to compute (or upper-bound) the failure probability as a smooth function of the decision variables, and thus are widely applicable. However, existing approaches fundamentally assume discrete-time dynamics and can perform unpredictably when applied to continuous-time systems operating in the real world, often manifesting as severe conservatism. State-of-the-art attempts to address this within a conventional discrete-time framework require additional Gaussianity approximations that ultimately produce inconsistency of their own. In this paper we take a fundamentally different approach, deriving a risk approximation framework directly in continuous time and producing a lightweight estimate that actually improves as the discretization is refined. Our approximation is shown to significantly outperform state-of-the-art techniques in replicating the MC estimate while maintaining the functional and computational benefits of a direct method. This enables robust, risk-aware, continuous motion-planning for a broad class of nonlinear, partially-observable systems.**

I. Introduction

Robotic motion planning is a decision-making problem that must balance optimality and safety. In the real world, these decisions are complicated by the presence of uncertainty due to imperfect sensing, partial observability, and stochastic dynamics. This uncertainty is often difficult or impossible to explicitly bound, and safety cannot be guaranteed against all realizations of noise and disturbance.

This motivates the replacement of deterministic safety constraints with *risk constraints* [11] that seek to compute or bound the probability of failure. Unfortunately, exact evaluation of this probabilistic risk is challenging and computationally intractable for generic nonlinear systems. While Monte-Carlo (MC) estimation techniques [5, 3, 8] provide a general and powerful workaround, they are still computationally-demanding and difficult to embed within a continuous motion planner. A number of "directly-computable" risk approximations have been proposed [11, 2, 19, 18], but all fundamentally assume the system evolves in discrete time. Many systems we care to control in practice evolve continuously, and while application of discrete-time methods is possible in these settings, the ensuing risk estimates will be highly sensitive to the chosen time discretization. As recognized by Ariu et al. [1], Janson et al. [8], and others, they may be either too lax (allowing "corner-cutting"), too conservative (leading to severe sub-optimality or artificial infeasibility), or both simultaneously.

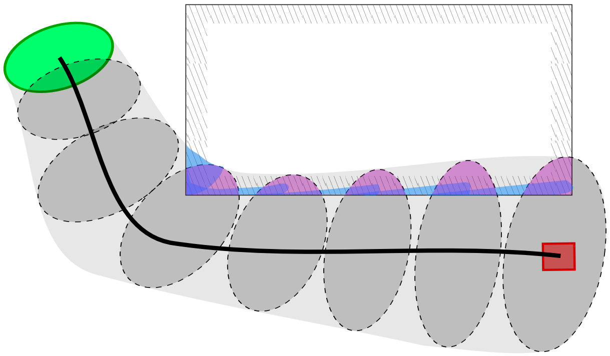

Fig. 1. Consider a planar system maneuvering from the green initial distribution to the red goal position in the presence of a rectangular obstacle. Shaded ellipses represent the state distribution at a set of discrete timesteps, $\mathcal{T} = \{t_0, t_1, \ldots, t_k\}$, and reflect uncertainty under closed-loop execution. A common technique for computing the total collision probability leverages Boole's inequality to simply sum the violation probabilities at each step (magenta). However, the resulting estimate will be sensitive to the choice of $\mathcal{T}$ – too coarse, and it will underestimate; too fine, and it will "double-count" probability mass corresponding to trajectories that remain in collision across multiple timesteps. This leads to over-conservatism, artificial infeasibility, and ultimately brittle planning. In this paper we introduce a *continuous*-time approximation (cyan) that instead aggregates probability mass *entering* collision over each *interval*. As $\mathcal{T}$ is refined, our result actually improves, eventually converging to the true failure probability.

This paper addresses this problem at its source, taking a rigorous look at the evolution of failure probability directly in continuous time. Our approximation is general, applying to partially-observable[1] stochastic systems $\boldsymbol{x}(t)$ in $X = \mathbb{R}^{n_x}$

[1] Note that under partial-observability, the process $\boldsymbol{x}(t)$ can only be considered Markov if it is "augmented" with the internal state of the estimator/controller. For the purposes of this paper we leave this implicit – because constraints are assumed to involve only on the state of the physical plant, augmentation will contribute no analytic or computational cost.

with nonlinear Itô dynamics

$$\mathrm{d}\boldsymbol{x}(t) = \boldsymbol{f}\big(t, \boldsymbol{x}(t), \boldsymbol{u}(t)\big)\,\mathrm{d}t + G\big(t, \boldsymbol{x}(t), \boldsymbol{u}(t)\big)\,\mathrm{d}\boldsymbol{w}(t) \quad (1)$$

where $\boldsymbol{u}(t)$ and $\boldsymbol{w}(t)$ represent a vector-valued control process and Brownian motion, respectively. Under partial observability, $\boldsymbol{x}(t)$ is not directly available to the controller, and feedback must be accomplished via a parallel observation process represented by the filtration $\mathcal{Y}_t$ (the information available at time t). The special case of fully-observable systems is easily captured here as well. In order to simplify presentation, our main results impose some additional restrictions between the dynamics (1) and the constraints that define the *safe set* $X_{\text{safe}} \subset X$. Even so, they accommodate a wide variety of nonlinear systems and constraints, including the ubiquitous case of second-order systems with position constraints. Moreover, relaxation of some of these requirements will be straightforward, though beyond the scope of this paper.

The types of planning problems we address take the form

$$\min_{\boldsymbol{u}(\cdot)} \quad \mathrm{E}\int_0^T l\big(t, \boldsymbol{u}(t), \boldsymbol{x}(t)\big)\,\mathrm{d}t \qquad (2)$$

$$\text{subject to: } P\Bigg(\bigvee_{t\in[0,T]} \boldsymbol{x}(t) \notin X_{\text{safe}}\Bigg) \leq \Delta \qquad (3)$$

where the $\bigvee$ symbol is a logical OR, implying existence of a satisfying event among a (possibly uncountable) collection, and $\Delta \in (0, 1)$ represents a given risk tolerance over the finite horizon $[0, T]$. The constraint (3) upper-bounds the probability of failure at *any* time in the planning horizon. This *risk* is challenging to evaluate and optimize against because it couples states across the planning horizon as a whole. As pointed out by Ono et al. [18] and others, joint constraints of this nature can be approached via Lagrangian relaxation; that is, converting the risk-*constrained* problem to a risk-*minimizing* one with objective

$$\mathrm{E}\int_0^T l\big(t, \boldsymbol{u}(t), \boldsymbol{x}(t)\big)\,\mathrm{d}t + \lambda\Big[P\big(\bigvee_{t\in[0,T]} \boldsymbol{x}(t) \notin X_{\text{safe}}\big) - \Delta\Big] \quad (4)$$

for some $\lambda \geq 0$. However, the augmented objective in (4) does not possess the time-additive *Bellman* structure of (2), precluding the application of many optimal control techniques such as dynamic programming [21, 23, 18]. Like [2, 18] and other direct approximations, the approximation presented in this paper restores this time-additive structure while achieving superior accuracy for continuous-time systems.

This paper takes a fresh look at the time-evolution of the failure probability in (3), specifically in continuous-time. Related work is outlined in Section II. Section III leverages the language of first-exit times to produce a time-additive framework for continuous-time risk estimation. The classic theory is rich and well-explored, but to the best of the authors' knowledge no techniques yet exist to enable computation in the context of generic nonlinear systems and nonlinear constraints. To address this, we propose a piecewise-continuous approximation in Sections IV and V that provably converges as the time discretization is refined – this allows us to losslessly extend classic results for constant-coefficient systems. As a second contribution, we identify a lightweight method to account for "safety-thus-far" that avoids attempting to approximate an explicit posterior and ensures conservatism without being excessively so. Finally, we identify a large class of systems for which the requisite numerical quadratures can be computed exactly at significantly-reduced dimension, which is critical to ensure computational feasibility. The resulting risk approximation is empirically demonstrated in Section VI to well-approximate MC estimates while retaining the computational simplicity and general applicability of direct methods, paving the way for risk-aware, continuous motion planning onboard real-world systems.

II. Related Work

Risk-aware motion planning is far from a new problem and has received much attention over the years. For example, when probabilistic constraints $P\big(\boldsymbol{x}(t) \notin X_{\text{safe}}\big) \leq \Delta$ are enforced *independently* for each t, suitable extensions of classic algorithms such as RRT [13, 4, 22] and differential dynamic programming (DDP) [23] have been proposed. Alternatively, for problems with discrete time and action spaces, risk-constrained search methods such as RAO* [20, 7] have shown promise.

This paper considers problems continuous in time and action, where safety is most naturally expressed by the joint constraint (3). The field of robust control provides some solutions against *worst-case* (i.e., bounded) disturbances, for example Majumdar and Tedrake [15] and Lopez et al. [12]. However, these approaches are generally restricted to fully-observable systems. Furthermore, their performance may be severely conservative in the average case, motivating a quantification of *probabilistic* risk to allow explicit trade-off between safety and expedience during planning.

A. Sampling-Based Methods

MC techniques provide a general and powerful method for estimating failure probabilities, at the cost of having to run a potentially large number of simulation rollouts. As closed-loop partially-observable systems require simulation of plant, estimator, and controller, this can represent non-negligible amounts of computation. Aside from the issue of sample-complexity, which has been partially addressed by Calafiore and Campi [5] and Janson et al. [8], sample-based estimates are discontinuous and therefore fundamentally cumbersome to incorporate into a continuous optimization framework. For example, [5] proposes enforcement of a deterministic constraint for each sample, [8] resorts to iterative obstacle inflation in RRT, and Blackmore et al. [3] apply Mixed-Integer techniques. This limitation of MC motivates the search for efficient, "direct" risk approximations amenable to online, *continuous* optimization over motion plans.

B. Direct Risk Estimates (in Discrete Time)

A number of direct techniques have been developed in a discrete-time setting, where (3) simplifies to

$$P\big(\vee_{i=0}^{k}\, \boldsymbol{x}(t_i) \notin X_{\text{safe}}\big) \le \Delta. \tag{5}$$

Early work by Li et al. [11] recognized that, under Linear-Time-Varying (LTV) dynamics, dispersions will be distributed as an $n_x(k+1)$-dimensioned normal distribution. The joint probability in (5) can then evaluated as a high-dimensional integral via quadrature methods or sampling, both of which have complexity exponential in dimension. To avoid this unfavorable scaling with k, Blackmore and Ono [2] use Boole's inequality (a.k.a. the union bound) to decompose the probability in (5) over time as

$$P\big(\vee_{i=0}^{k}\, \boldsymbol{x}(t_i) \notin X_{\text{safe}}\big) \le \sum_{i=0}^{k} P(\boldsymbol{x}(t_i) \notin X_{\text{safe}}). \tag{6}$$

This decoupling over timesteps is highly convenient. As pointed out by Ono et al. [18], the right-hand side of (6) is time-additive, allowing the use of dynamic programming to minimize (4). Alternatively, Ono and Williams [17] introduce the *risk-allocation* formulation

$$P(\boldsymbol{x}(t_i) \notin X_{\text{safe}}) \le \Delta_i \;\forall i \le k \quad \text{and} \quad \sum_{i=0}^{k} \Delta_i = \Delta \tag{7}$$

which explicitly allocates a risk "budget" between timesteps. This framework has inspired a series of other works including [24, 14, 6], all fundamentally dependent on decomposition (6).

Despite its popularity, the use of Boole's inequality to decompose joint constraints over time can be severely conservative, as illustrated in Fig. 1. By ignoring correlations between states at adjacent timesteps, the sum in (6) will "double-count" violation probabilities, particularly as the time discretization is refined. This problem is addressed by Patil et al. [19], who recognize that the state distributions should be *conditioned* on the safety of prior timesteps. Because capturing this conditioning exactly is challenging, they approximate the projected and truncated distribution corresponding to each constraint as a single-dimensional Gaussian, allowing closed-form update of the state distribution parameters. However, Gaussianity here is inexact and the resulting estimate may not remain statistically consistent or result in a conservative (upper-bounding) risk estimate.

When addressing continuous-time systems, a standard numeric approach to risk-aware optimization approximates the original system as discrete-time under a given time partition $\mathcal{T} = \{t_0 = 0, t_1, \ldots, t_k = T\}$ and then substitutes constraint (5) for (3). This allows well-studied discrete-time techniques to be applied, but, as mentioned earlier, the results will be highly sensitive to the choice of discretization. Depending on the complexity and movement speed of the robot, these effects can lead to unsafe or overly-cautious behavior, or both. This motivates the fundamental contribution of this paper – a direct risk approximation derived fundamentally in continuous time.

C. Stochastic Processes in Continuous-Time

In an effort to explicitly address the continuous-time constraint (3) and avoid "corner-cutting," Ariu et al. [1] apply Boole's inequality over *intervals* rather than instantaneous states as

$$P\Big(\bigvee_{s\in[0,T]} \boldsymbol{x}(s) \notin X_{\text{safe}}\Big) \le \sum_{i=0}^{k-1} P\Big(\bigvee_{s\in[t_i,t_{i+1})} \boldsymbol{x}(s) \notin X_{\text{safe}}\Big). \tag{8}$$

Note that continuity allows the endpoint $\boldsymbol{x}(T)$ to be dropped. As with (6), this "interval Boole's" neglects correlations between events. In particular, their method assumes the state process itself follows a Brownian motion, ultimately resulting in a *doubly*-conservative estimate compared to its discrete-time counterpart. In contrast, the approximation proposed in this paper also operates on intervals, but it addresses the nonlinear dynamics directly and avoids the use of Boole's inequality in this way, producing a much tighter risk bound.

This paper leans heavily on the classical notion of first-passage times, a well-studied topic in the field of continuous stochastic processes. Indeed, the piecewise approximation presented in Section IV of this paper is similar in spirit to that of Jin and Wang [9], although we consider the case where the process (rather than purely the boundary) is nonlinear.

III. How Risk Evolves in Time

Consider a càdlàg[2], Markov process $\boldsymbol{z}(t) \in \mathbb{R}^m$ with associated probability space $(\Omega, \mathcal{F}, P)$. Here, Ω represents the *outcome* space, $\mathcal{F}$ is a *sigma-algebra* over Ω (a collection of events $E \subseteq \Omega$) such that $\boldsymbol{z}(t)$ is measurable for all t, and P is a probability measure over $\mathcal{F}$. Note that for now we do *not* assume $\boldsymbol{z}(t)$ has continuous sample paths. We begin by exploring the "nearly" time-additive evolution of the *exit cumulant*

$$F_{\boldsymbol{z}}(t) \triangleq P\Big(\bigvee_{s\in[0,t]} \boldsymbol{z}(s) \notin D\Big) \tag{9}$$

for some closed set $D \subset \mathbb{R}^m$.

For clarity in the following discussion, we adopt the language of *passage times*, also known as *hitting* or *exit times* [10, 25]. Define a parameterized family of exit times with respect to process $\boldsymbol{z}(t)$ as

$$^{\boldsymbol{z}}\tau_t \triangleq \inf\big\{s \in [t,T] \,\big|\, \boldsymbol{z}(s) \notin D\big\} \tag{10}$$

where the infinum of the empty set is assigned to ∞. That is, $^{\boldsymbol{z}}\tau_t$ refers to the first time (after t) that $\boldsymbol{z}(s)$ "exits" D. For both $F_{\boldsymbol{z}}$ and $^{\boldsymbol{z}}\tau_t$ we will drop the explicit $\boldsymbol{z}$ specification when the corresponding process is unambiguous.

The following useful properties can be identified.

Lemma 1. *For any $0 \le t_1 < t_2 \le T$, the following hold:*

- $\tau_{t_1} \ge t_2 \iff \boldsymbol{z}(s) \in D \quad \forall s \in [t_1, t_2)$.
- $\tau_0 \in [t_1, t_2) \iff \tau_0 \ge t_1, \tau_{t_1} < t_2$.
- *For each outcome $\omega \in \Omega$, either*
    1) $\tau_0 = \infty$ *("no exit"), or*

[2] a.k.a. right-continuous with left limits.

2) $\boldsymbol{z}(\tau_0) \in \partial D \cup D^c$ *("smooth exit" or a "jump out"). where ∂D and D^c are the boundary and complement of D, respectively.*

It is straightforward to verify that the total exit probability can be written as $F(T) = P(\tau_0 \leq T)$, and thus τ_0 offers a means by which to analyze the time-evolution of $F(t)$. In some cases $F(t)$ is known to be time-differentiable [9], and thus computing this derivative (called the *first-passage density*) would seem to be a natural goal. However, this computation is challenging for generic nonlinear processes, and instead we will settle for an interval-based "integration" scheme that reflects how $F(T)$ can be approximated in practice. In later sections, through both analysis and experiment we demonstrate that this approximation indeed converges to the true value as the time discretization is refined.

Proceeding, assume a given partition $\mathcal{T} = \{t_0 = 0, t_1, t_2, \ldots, t_k = T\}$ of the fixed horizon $[0, T]$. A crucial advantage of the language of the *first*-exit time is that it provides a natural disjointness between events, and in particular

$$F(T) = \sum_{i=0}^{k-1} P\big(\tau_0 \in [t_i, t_{i+1})\big) + P(\tau_0 = T). \tag{11}$$

Note that, in contrast to (8), the relation (11) holds with equality. Proceeding from here and adopting the shorthand $\boldsymbol{z}_i \triangleq \boldsymbol{z}(t_i)$, $\tau_i \triangleq \tau_{t_i}$, and so on, the above can be written

$$\sum_{i=0}^{k-1} \Big(P\big(\tau_0 \in [t_i, t_{i+1}), \boldsymbol{z}_i \in D\big) + P\big(\tau_0 = t_i, \boldsymbol{z}_i \notin D\big) \Big) + P(\tau_0 = T, \boldsymbol{z}(T) \in D^c) \tag{12}$$

$$= \sum_{i=0}^{k-1} P\big(\tau_0 \in [t_i, t_{i+1}), \boldsymbol{z}_i \in D\big) + \sum_{i=0}^{k} P(\tau_0 = t_i, \boldsymbol{z}_i \in D^c) \tag{13}$$

where in (12) we split the probability over the event that $\boldsymbol{z}_i \in D$. Note that the right-hand summation in (13) involves the probabilities that discontinuous sample paths "jump out" of D at each of the partition points t_i. Examining the first set of terms, Lemma 1 allows

$$\begin{aligned} &P\big(\tau_0 \in [t_i, t_{i+1}), \boldsymbol{z}_i \in D\big) \\ &\quad = P\big(\tau_i < t_{i+1} \,|\, \tau_0 \geq t_i, \boldsymbol{z}_i \in D\big) P(\tau_0 \geq t_i, \boldsymbol{z}_i \in D). \end{aligned} \tag{14}$$

The conditioning on $\tau_0 \geq t_i$ and $\boldsymbol{z}_i \in D$ in (14) implies that the process has not exited "yet," imposing a specific posterior over $\boldsymbol{z}_i$ that we will call the *anthropic* distribution[3]

$$\bar{\pi}_t(\mathrm{d}\boldsymbol{z}) \triangleq P(\boldsymbol{z}(t) \in \mathrm{d}\boldsymbol{z} \,|\, \tau_0 \geq t, \boldsymbol{z}(t) \in D). \tag{15}$$

Before proceeding further, define the function

$$\Phi_{\boldsymbol{z}}(t_i, t_{i+1}; \mu_i) \triangleq P(\tau_i < t_{i+1} \,|\, \boldsymbol{z}_i \sim \mu_i) \tag{16}$$

for any (not necessarily normalized) measure μ_i over $\mathbb{R}^m$. (16) captures the probability of an exit (not necessarily the first) in the interval $[t_i, t_{i+1})$, given that $\boldsymbol{z}_i$ is distributed according to μ_i. As before, the $\boldsymbol{z}$ subscript will be left implicit where possible. Because the process $\boldsymbol{z}(t)$ is assumed Markov and applying (14), sum (13) can be re-written in terms of Φ and $\bar{\pi}_t$ as

$$\begin{aligned} F(T) = &\sum_{i=0}^{k-1} \Phi(t_i, t_{i+1}; \bar{\pi}_i) P(\tau_0 \geq t_i, \boldsymbol{z}_i \in D) \\ &+ \sum_{i=0}^{k} P(\tau_0 = t_i, \boldsymbol{z}_i \in D^c). \end{aligned} \tag{17}$$

A key challenge in evaluation of (17) is computation of $\bar{\pi}_i$. For one thing, its support is clearly limited to D, which is sufficient to ensure non-Gaussianity. This motivates us to avoid attempting to approximate or bound $\bar{\pi}_t$ directly and instead decompose it via Baye's rule, producing

$$\begin{aligned} \bar{\pi}_t(\mathrm{d}\boldsymbol{z}) &= \frac{P\big(\tau_0 \geq t, \boldsymbol{z}(t) \in D \,|\, \boldsymbol{z}(t) = \boldsymbol{z}\big) P\big(\boldsymbol{z}(t) \in \mathrm{d}\boldsymbol{z}\big)}{P(\tau_0 \geq t, \boldsymbol{z}(t) \in D)} \\ &\triangleq \frac{\bar{\Psi}_t(\boldsymbol{z}) \bar{b}_t(\mathrm{d}\boldsymbol{z})}{P(\tau_0 \geq t, \boldsymbol{z}(t) \in D).} \end{aligned} \tag{18}$$

where $\bar{b}_t$ is the *a priori* distribution of $\boldsymbol{z}(t)$, and we refer to $\bar{\Psi}_t : \mathbb{R}^m \mapsto [0, 1]$ as the *anthropic likelihood*. It is straightforward to show

$$\Phi(t_i, t_{i+1}; \bar{\pi}_i) P(\tau_0 \geq t_i, \boldsymbol{z}_i \in D) = \Phi(t_i, t_{i+1}; \bar{\Psi}_i \bar{b}_i), \tag{19}$$

and therefore (17) can be written

$$F(T) = \sum_{i=0}^{k-1} \Phi(t_i, t_{i+1}; \bar{\Psi}_i \bar{b}_i) + \sum_{i=0}^{k} P(\tau_0 = t_i, \boldsymbol{z}_i \in D^c). \tag{20}$$

As discussed in Section V-B, and in contrast to the case of $\bar{\pi}_t$, identifying conservative approximations for $\bar{\Psi}_t$ will be both straightforward and effective.

A. Analogous Development Under Filtration $\mathcal{F}_t$

Though not the primary focus of this paper, we note that the preceding development can be applied analogously in the context on a filtration $\mathcal{F}_t$ representing information that becomes available *during* execution as opposed to *a priori*. For example, in the context of $\boldsymbol{x}(t)$ as defined in (1), we might consider the observation filtration $\mathcal{F}_t = \mathcal{Y}_t$.

Though the information generated by $\mathcal{F}_t$ itself evolves randomly, modification of the above discussion is straightforward and we simply provide some analogous definitions here for clarity. As in (15), we can define the *anthropic belief* $\pi_t(\mathrm{d}\boldsymbol{z}) \triangleq P\big(\boldsymbol{z}(t) \in \mathrm{d}\boldsymbol{z} \,|\, \tau_0 \geq t, \boldsymbol{z}(t) \in D, \mathcal{F}_t\big)$, and like (15) it has the structure

$$\pi_t(\mathrm{d}\boldsymbol{z}) = \frac{\Psi_t(\boldsymbol{z}) b_t(\mathrm{d}\boldsymbol{z})}{P\big(\tau_0 \geq t, \boldsymbol{z}(t) \in D \,|\, \mathcal{F}_t\big)} \tag{21}$$

where the familiar estimation belief b_t and anthropic likelihood Ψ_t are adapted to $\mathcal{F}_t$. An analogous identity to (19) can be

[3] In cosmology, the *anthropic principle* remarks that life can only observe universes that themselves allow for the existence of life.

established, yielding

$$F(T) = \mathrm{E}\Big[\sum_{i=0}^{k-1} \Phi(t_i, t_{i+1}; \Psi_i b_i)\Big] + \sum_{i=0}^{k} P(\tau_0 = t_i, \boldsymbol{z}_i \in D^c). \tag{22}$$

where the expectation is taken over $\mathcal{F}_t$.

IV. A Piecewise-Continuous Approximation

The preceding section introduced a framework for computing the failure probability based on a helper function Φ defined in (16). Rather than attempting to evaluate $\Phi_{\boldsymbol{x}}$ directly for the nonlinear process $\boldsymbol{x}(t)$, this section introduces an approximating process *in the constraint space*, for which computation is made tractable. This simplified process is piecewise-continuous according to the given time discretization $\mathcal{T}$, which controls the "accuracy" of the approximation. Though $\mathcal{T}$ in practice will likely be dictated by the computational resources available, we prove that as it is refined the corresponding failure probability estimate converges to $F_{\boldsymbol{x}}(T)$. That is to say, the approximation is asymptotically lossless.

Assume the feasible set $X_{\text{safe}} \subset X$ is defined by the sublevel sets $g_j(\boldsymbol{x}) \leq 0$ for a set of m twice-differentiable, real-valued functions $\{g_j\}$. Let $\boldsymbol{g}(\boldsymbol{x})$ refer to the stacked vector in $\mathbb{R}^m$, and let $\boldsymbol{a}_j(\boldsymbol{x})$ and $H_j(\boldsymbol{x})$ refer to the gradient vector and Hessian of each g_j, respectively. Note that $\boldsymbol{x} \in X_{\text{safe}}$ is equivalent to the statement that $g_j(\boldsymbol{x}) \leq 0$ for all j. This naturally motivates a consideration of $\boldsymbol{y}(t) \triangleq \boldsymbol{g}\big(\boldsymbol{x}(t)\big)$ as a process with respect to the non-positive orthant $\mathcal{O}^- \subset \mathbb{R}^m$.

Before we proceed, however, computation and analysis will require some regularity conditions on the control process $\boldsymbol{u}(t)$, which evolves according to $\mathcal{Y}_t$ and some (potentially non-deterministic) policy. Rather than complicate the discussion by attempting to account for all such possibilities, we make the following simplifying assumption.

Assumption 1 ($\boldsymbol{y}(t)$ Locally Independent of Control)**.** *We require that either*

1) *we have state-feedback $\boldsymbol{u}(t) = \kappa\big(t, \boldsymbol{x}(t)\big)$, with κ deterministic and Lipschitz, or*
2) *$\boldsymbol{a}_j^{\mathrm{T}}(\boldsymbol{x})\boldsymbol{f}(t, \boldsymbol{x}, \boldsymbol{u})$ and $\boldsymbol{a}_j^{\mathrm{T}}(\boldsymbol{x})G(t, \boldsymbol{x}, \boldsymbol{u})$ are independent of $\boldsymbol{u}$ for all constraints j.*

Assumption 1 ensures that the dynamics of process $\boldsymbol{y}(t)$ depend on the control only via the state $\boldsymbol{x}(t)$, and notably accommodates second-order systems under workspace constraints (i.e., obstacle avoidance). Partial relaxation of this assumption will in many cases require only minor modifications of the analysis and computations presented in this paper.

Proceeding, we consider a piecewise approximation of this process constructed from the time discretization $\mathcal{T}$. Using the shortcuts $\boldsymbol{f}_t \triangleq \boldsymbol{f}\big(t, \boldsymbol{x}(t), \boldsymbol{u}(t)\big)$, $G_t \triangleq G\big(t, \boldsymbol{x}(t), \boldsymbol{u}(t)\big)$, and so on, define the process $\hat{\boldsymbol{y}}(s)$ such that

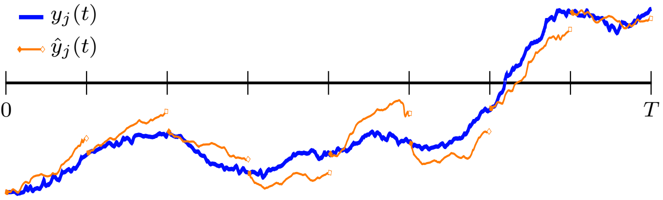

Fig. 2. An illustration of the continuous process $y_j(t) = g_j(\boldsymbol{x}(t))$ and our approximation $\hat{y}_j(t)$. The two processes coincide at each discrete timestep $t_i \in \mathcal{T}$, and as $\mathcal{T}$ is refined, Prop. 1 establishes that the two converge pathwise-uniformly. Zero-crossings of $y_j(t)$ imply constraint violations, and therefore exit-times of $\hat{\boldsymbol{y}}(t)$ from the non-positive orthant approximate those of $\boldsymbol{x}(t)$ from X_{safe}.

$$\hat{\boldsymbol{y}}(s) \triangleq \boldsymbol{g}\big(\boldsymbol{x}(t)\big) + \int_t^s \boldsymbol{h}_t \, \mathrm{d}s' + \int_t^s \Sigma_t \, \mathrm{d}\boldsymbol{w}(s') \tag{23}$$

$$h_{t,j} \triangleq \boldsymbol{a}_j\big(\boldsymbol{x}(t)\big)^{\mathrm{T}} \boldsymbol{f}_t + \frac{1}{2}\mathrm{tr}\left(G_t^{\mathrm{T}} H_j\big(\boldsymbol{x}(t)\big) G_t\right) \tag{24}$$

$$\Sigma_t \triangleq \begin{bmatrix} \boldsymbol{a}_1^{\mathrm{T}}\big(\boldsymbol{x}(t)\big) \\ \vdots \\ \boldsymbol{a}_m^{\mathrm{T}}\big(\boldsymbol{x}(t)\big) \end{bmatrix} G_t \triangleq \begin{bmatrix} \boldsymbol{\sigma}_1\big(t, \boldsymbol{x}(t)\big) \\ \vdots \\ \boldsymbol{\sigma}_m\big(t, \boldsymbol{x}(t)\big)\big) \end{bmatrix} \tag{25}$$

where $t = \max\{t_i \in \mathcal{T} \,|\, t_i \leq s\}$ corresponds to the start point of the interval $[t_i, t_{i+1})$ containing s. Here $\boldsymbol{h}_s$ and Σ_s can be identified as the drift and diffusion coefficients of $\boldsymbol{y}(s)$ as prescribed by Itô's formula [25, Thm. 5.5]. Thus, the piecewise-continuous $\hat{\boldsymbol{y}}(s)$ has constant coefficients over each interval and coincides with $\boldsymbol{y}(s)$ for every $s = t \in \mathcal{T}$.

Approximating $F_{\hat{\boldsymbol{y}}}$ will be much easier than working directly with $F_{\boldsymbol{x}}$, and in the following we show that, under mild conditions, the substitution of $\hat{\boldsymbol{y}}(s)$ for $\boldsymbol{y}(s)$ can be considered asymptotically lossless.

A. Convergence Analysis

Consider evaluating $F_{\hat{\boldsymbol{y}}}(T)$ for the process $\hat{\boldsymbol{y}}(t)$ – the result will, of course, depend on $\hat{\boldsymbol{y}}(t)$ and therefore the underlying time discretization $\mathcal{T}$. We show that as $\mathcal{T}$ is refined, $\hat{\boldsymbol{y}}(t)$ converges to $\boldsymbol{y}(t)$ in a specific sense, and that $F_{\hat{\boldsymbol{y}}}(T)$ converges to $F_{\boldsymbol{y}}(T) = F_{\boldsymbol{x}}(T)$. Proofs are left to Appendix A.

Definition 1 (Pathwise-Uniform Convergence)**.** *For a sequence of processes $\boldsymbol{z}^{(n)}(t)$ and an associated real-valued sequence $\varepsilon_n \to 0$, we say $\boldsymbol{z}^{(n)}(t)$ converges ε_n-*pathwise-uniformly *to process $\boldsymbol{z}(t)$ if there exists for each $\omega \in \Omega$ an $0 < M_\omega < \infty$ almost surely such that*

$$P\Big(\sup_{s\in[0,T]} \Big\|\boldsymbol{z}^{(n)}(s) - \boldsymbol{z}(s)\Big\|_2 > \varepsilon_n M_\omega\Big) \to 0.$$

Note that pathwise-uniform convergence (PUC) does not imply that $\boldsymbol{z}^{(n)}(\cdot;\omega)$ converges to $\boldsymbol{z}(\cdot;\omega)$ for any fixed outcome $\omega \in \Omega$. Additionally, it is specific to the given sequence ε_n. Nonetheless, we will see that this condition is sufficient to ensure a non-trivial convergence-of-probabilities result.

Definition 2 (Supremum Process)**.** *For a process $z(t)$, the corresponding* supremum process *is $z^\star(t) \triangleq \sup_{s\in[0,t]} z(s)$.*

Theorem 1. *If a given sequence of $\mathbb{R}^m$-valued processes $\boldsymbol{z}^{(n)}(t)$ converges ε_n-pathwise-uniformly to $\boldsymbol{z}(t)$, and we have that $P(z_j^\star(T)=0)=0$ for all j, then*

$$P\Big(\bigvee_{s\in[0,T]}\boldsymbol{z}^{(n)}(s)\notin\mathcal{O}^-\Big)\to P\Big(\bigvee_{s\in[0,T]}\boldsymbol{z}(s)\notin\mathcal{O}^-\Big).$$

For technical reasons, we will be required to make the following additional assumption relating the diffusion matrix G and the constraint gradients $\{\boldsymbol{a}_j\}$.

Assumption 2 (Paired Lipschitz:)**.** *With respect to a given function $g: X\mapsto\mathbb{R}$ and diffusion matrix $G(t,\boldsymbol{x},\boldsymbol{u})$, either*

1) *G is constant and the function gradient, $\boldsymbol{a}$, is Lipschitz,*
2) *$\boldsymbol{a}$ is constant (i.e., g is linear) and G is Lipschitz, or*
3) *both $\boldsymbol{a}$ and G are bounded and Lipschitz.*

Remark 1. *The requirements that Assumption 2 imposes on G in no way imply that disturbances are bounded. Furthermore, when constraints are linear G is only required to be Lipschitz, so cases of multiplicative noise can be handled here as well.*

This leads to our main result.

Proposition 1. *Let Assumptions 1 and 2 hold for the m constraint functions $\{g_j\}$. Additionally, assume:*

1) *$\boldsymbol{f}_t$ is pathwise-bounded a.s., and $\mathrm{E}\int_0^T\|\boldsymbol{f}_t\|_2^2\,\mathrm{d}t<\infty$.*
2) *$\mathrm{E}\,\|G_t\|_2^2$ bounded over $[0,T]$, and $\mathrm{E}\int_0^T\|G_t\|_2^2\,\mathrm{d}t<\infty$.*

Then, for a sequence of partitions $\mathcal{T}_n=\{0=t_0,t_1,\dots,t_{k_n}=T\}$ over the compact interval $[0,T]$ with mesh $\delta_n\to 0$ and $k_n\delta_n\le cT$ for fixed $c>0$, there exists a sequence $\varepsilon_n\to 0$ such that the sequence of processes $\hat{\boldsymbol{y}}^{(n)}(s)$ converges ε_n-pathwise-uniformly to $\boldsymbol{y}(s)$.

From Thm. 1 and the definition of $\boldsymbol{y}(t)$ the following corollary immediately follows.

Corollary 1. *If the assumptions of Prop. 1 hold and $P\big(y^\star(T)=0\big)=0$ for all j then $F_{\hat{\boldsymbol{y}}^{(n)}}(T)\to F_{\boldsymbol{x}}(T)$.*

Remark 2. *The condition $P\big(y_j^\star(T)=0\big)=0$ is somewhat difficult to verify; while conditions over which the variable $y_j(t)$ admits a density have been somewhat examined, the case of the supremum process is less explored. For the purposes of the paper we consider this, as well as the regularity conditions required by Prop. 1, to be fairly mild.*

Corollary 1 makes clear that the substitution of $\hat{\boldsymbol{y}}(s)$ for $\boldsymbol{y}(s)$ is (asymptotically) loss-less for the purposes of computing the risk probability $F_x(T)$. It is worth noting that this result does not anywhere assume that the dynamics or observation model are Gaussian or LTV, although practical computation of b_t may still require this assumption.

V. Computation

The results of Section IV indicate that we can perform computation with the simplified process $\hat{\boldsymbol{y}}(t)$ and the result will approximate the true $F_{\boldsymbol{x}}(T)$ in an asymptotic sense. While $\hat{\boldsymbol{y}}(t)$ is only piecewise-continuous and thus "jump out" probabilities in (22) may be non-zero, our empirical results indicate that they can be safely ignored. Identifying a rigorous proof is left as a topic for future work. Additionally, for the sake of presentation we make the simplifying assumption that $P(\boldsymbol{x}_0\notin X_{\text{safe}})=0$. In light of these considerations, we focus on computing

$$\hat{F}(T)\triangleq\sum_{i=0}^{k-1}\Phi_{\hat{\boldsymbol{y}}}(t_i,t_{i+1};\bar{\Psi}_i\bar{b}_i).\tag{26}$$

In order to compute (26), we require both a means of computing the quantity $\Phi_{\hat{\boldsymbol{y}}}(t_i,t_{i+1};\mu_i)$ for arbitrary measure μ_i and a means of approximating $\bar{\Psi}_i\bar{b}_i$. The former is the subject of V-A and the latter of V-B.

A. Bounding $\Phi_{\hat{\boldsymbol{y}}}$

The constant-coefficient approximation $\hat{\boldsymbol{y}}(t)$ allows us to leverage classic results in the study of first-exit times. First, recalling (16) we apply the union bound to decouple individual constraints, producing a sum over element-wise diffusions $\hat{y}_j$

$$\Phi_{\hat{\boldsymbol{y}}}(t_i,t_{i+1};\mu_i)\le\sum_{j=1}^{m}\Phi_{\hat{y}_j}(t_i,t_{i+1};\mu_i).\tag{27}$$

Letting ∂X_{safe} refer to the boundary of X_{safe}, a classic result (see Karatzsas and Shreve [10, Ch. 3, Eq. 5.12]) provides the following lemma.

Lemma 2. *Under Assumption 1, for any (not-necessarily normalized) measure μ_i over X_{safe}, and such that $\mu_i(\partial X_{safe})=0$,*

$$\begin{aligned}\Phi\hat{y}_j(t_i,t_{i+1};\mu_i)&=P\Big(\sup_{s\in[t_i,t_{i+1})}\hat{y}_j(s)>0\,\Big|\,\hat{y}_j(t_i)\sim g_j(\mu_i)\Big)\\&=\int_{X_{safe}}\psi\Big(g_j(\boldsymbol{x}),h_j(t_i,\boldsymbol{x}),\|\boldsymbol{\sigma}_j(t_i,\boldsymbol{x})\|_2,\Delta_i\Big)\,\mathrm{d}\mu_i(\boldsymbol{x})\end{aligned}\tag{28}$$

where $\Delta_i=t_{i+1}-t_i$ and we define $\psi(z,h,\sigma,\Delta t)\triangleq$

$$1-\phi\Big(\frac{-h\Delta t-z}{\sigma\sqrt{\Delta t}}\Big)+\exp\Big\{-\frac{2hz}{\sigma^2}\Big\}\phi\Big(\frac{-h\Delta t+z}{\sigma\sqrt{\Delta t}}\Big)\tag{29}$$

and ϕ refers to the CDF of the standard normal distribution.

Note that the condition $\mu_i(\partial X_{\text{safe}})=0$ is satisfied for all measures which admit a density (a mild assumption).

Like the instantaneous probability $P\big(x(t_i)\notin X_{\text{safe}}\big)$, computing (28) in general requires evaluating a multi-dimensional integral over the state space $X=\mathbb{R}^{n_x}$. Numerical quadrature techniques have exponential complexity in dimension (the curse of dimensionality). Fortunately, depending on the structure of the dynamics and constraints, significant dimensionality reductions can often be found. In particular, consider Gaussian-distributed second-order systems with workspace constraints (such as obstacle avoidance). If system noise is injected only in the velocity and acceleration dynamics (corresponding to $\boldsymbol{\sigma}_j=0$ for all j), then the integral in (28) reduces to workspace dimension n_p (commonly 2 or 3). This ensures that $\Phi_{\hat{\boldsymbol{y}}}$ can be evaluated efficiently for a large class of dynamics. Details are provided in Appendix B.

B. Approximating Anthropic Belief

Given we can compute (27), we still require some means of estimating the anthropic state distribution via $\bar{\pi}_t$ or $\bar{\Psi}_t \bar{b}_t$. Though inexact, Gaussian approximations for $\bar{b}_i$ are applicable and widely-used whenever the state dynamics are sufficiently smooth and, as can be seen in our experimental results, accurately model the dispersion of even nonlinear MC trajectories. However, modeling the anthropic information represented by $\bar{\Psi}_i$ or $\bar{\pi}_i$ is not so straightforward.

1) Approximating $\bar{\pi}_i$ as a Gaussian: In existing work, Patil et al. [19] propose a Gaussian approximation for the anthropic distribution $\bar{\pi}_i$ (or analogously, anthropic belief π_i) at each timestep t_i. This is attractive because it implies $\bar{\pi}_i$ can be propagated in parallel with $\bar{b}_i$. Likewise, we can consider approximating $\bar{\pi}_i$ by conditioning on safety (via a recursive Gaussian approximation) at each prior timestep

$$\hat{\bar{\pi}}_i(\mathrm{d}\boldsymbol{x}) \approx P\big(\boldsymbol{x}_i \in \mathrm{d}\boldsymbol{x} \,|\, \boldsymbol{x}_l \in X_{\text{safe}} \,\forall l \leq i\big). \tag{30}$$

We refer the interested reader to their paper for implementation details.

Again considering (26), we can apply identity (19) and directly produce an upper-bound in terms of $\bar{\pi}_i$

$$\hat{F}(T) \leq \sum_{i=0}^{k-1} \Phi_{\hat{\boldsymbol{y}}}(t_i, t_{i+1}; \bar{\pi}_i). \tag{31}$$

Together with our Gaussian approximation $\hat{\bar{\pi}}_i$ from (30), we refer to the resulting estimate as `ival_gauss`.

While the independence and Gaussianity assumptions involved here are convenient, they are also heuristic. This can lead to inconsistent $\bar{\pi}_t$ estimates and ultimately unpredictable risk estimation, as will be seen in Section VI.

2) A Simple Alternative: Rather than attempting to estimate $\bar{\pi}_t$, we propose a simple, yet surprisingly powerful alternative based on the anthropic likelihood $\bar{\Psi}_t$. A clear upper-bound follows directly from the definition as

$$\bar{\Psi}_t(\boldsymbol{x}) = P\big({}^{\boldsymbol{x}}\tau_0 \geq t, \boldsymbol{x}(t) \in X_{\text{safe}} \,|\, \boldsymbol{x}(t) = \boldsymbol{x}\big) \leq \mathbb{1}_{X_{\text{safe}}}(\boldsymbol{x}). \tag{32}$$

Applying (32) to (26) yields a conservative estimate

$$\hat{F}(T) \leq \sum_{i=0}^{k-1} \Phi_{\hat{\boldsymbol{y}}}(t_i, t_{i+1}; \mathbb{1}_{X_{\text{safe}}} \bar{b}_i) \tag{33}$$

which accumulates "new" exits over each interval – note the contrast with the naive "interval Boole's" approximation given by (8). Because it restricts exit flow to probability mass which is "safe" at the start of each interval, we refer to approximation (33) as `ival_safe`.

In principle, (33) shares one of the same weaknesses of the discrete-time Boole's approximation in (6) – it is not bounded above, and indeed may diverge as $\mathcal{T}$ is refined. However, it avoids "locally" double-counting by counting only probability mass *leaving* X_{safe} over each interval. This interpretation is illustrated in Fig. 1, and our empirical results suggest `ival_safe` does very well in practice. Furthermore, compared to [19] or (31) it requires no "extra" belief propagation at all, making this approximation particularly lightweight.

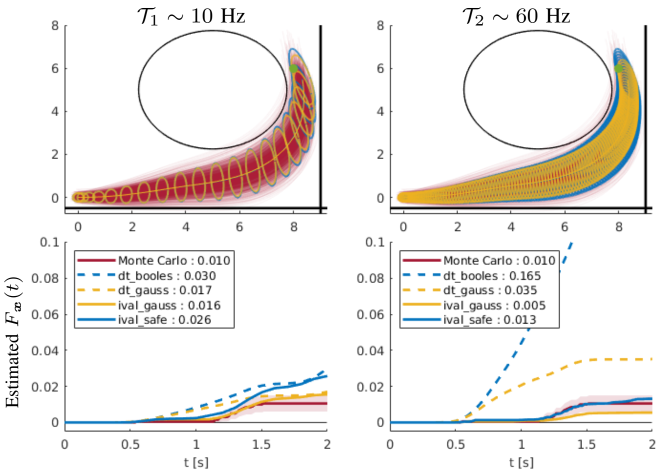

Fig. 3. We simulate a noisy Dubin's car system navigating in a narrow passageway, computing collision probabilities under coarse (left) and fine (right) time discretizations, $\mathcal{T}_1$ and $\mathcal{T}_2$. MC trajectories (red) simulate a fixed 60Hz feedback control rate, and a corresponding *a priori* state distribution $\bar{b}_i$ (blue) is propagated via an LTV-Gaussian assumption. The anthropic estimates $\{\hat{\bar{\pi}}_i\}_j$ (yellow) are computed according to each $\mathcal{T}_j$. The underlying plots confirm the divergence of `dt_booles` under fine discretizations, and illustrate the susceptibility of `dt_gauss` and `ival_gauss` to inconsistency in the Gaussian $\hat{\bar{\pi}}_i$ estimates. In contrast, our method `ival_safe` avoids estimating $\bar{\pi}$ entirely, producing a lightweight and consistent risk estimate.

VI. Results

To evaluate the accuracy of our approximation, we simulate a second-order Dubin's car system in the plane. System details are provided in Appendix C. Noise in dynamics and observations render the system partially-observable, and an LQG-style feedback control policy stabilizes around a nominal trajectory. We evaluate four principle approximations. Discrete-time methods `dt_booles` and `dt_gauss` refer to the naive Boole's approximation (6) and the conditioned variant proposed by [19], respectively. Our methods `ival_gauss` and `ival_safe` are described in the preceding section.

First, we successfully use our `ival_safe` estimate to optimize a risk-constrained ($\Delta = 2\%$) plan in a tight environment, shown in Fig. 3. We then computed risk estimates for this plan under multiple time discretizations. As predicted, `dt_booles` diverges severely as $\mathcal{T}$ is refined while `ival_safe` converges correctly. Interestingly, `dt_gauss` and `ival_gauss` converge to incorrect values, likely due to inconsistency in the underlying Gaussian $\hat{\bar{\pi}}_t$ estimate.

Next, we perform a larger statistical evaluation over random, programmatically-generated environments. We consider two different regimes: *nominally*-safe trajectories, which ensure only that the nominal trajectory is collision-free, and *risk*-constrained trajectories optimized using `ival_safe` with $\Delta = 10\%$. This segregation allows us to identify potentially distinct statistical performance in scenarios representing the full range of risk values $[0, 1]$ and over the smaller range of "planning-relevant" values in $[0, \Delta]$. These environments are non-convex, and the locally-optimal trajectories were generated via MATLAB's `fmincon` routine [16]. To ensure that the batch of experiments is not dominated by "uninteresting"

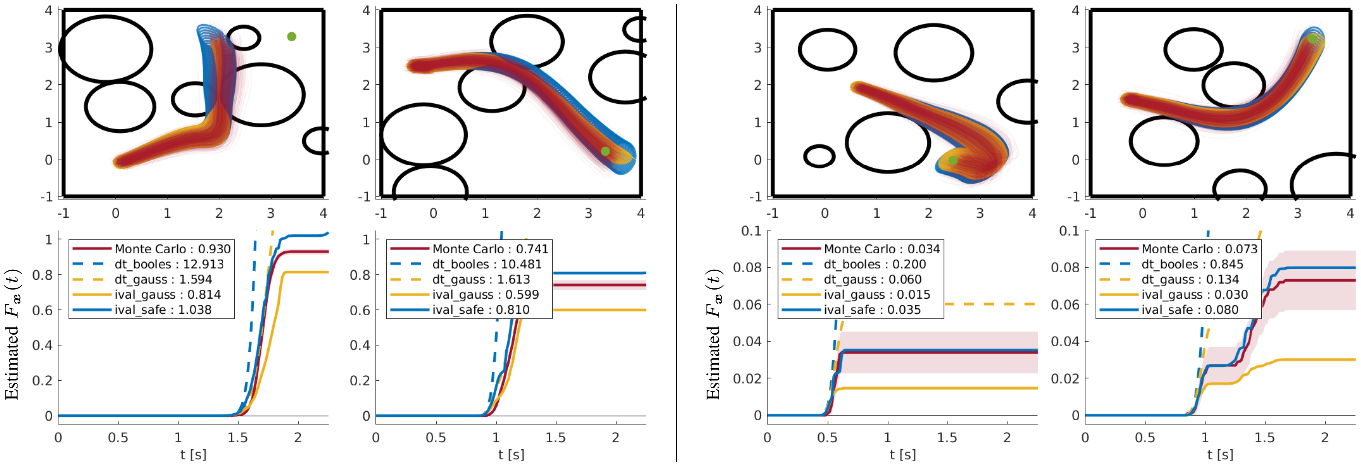

Fig. 4. Sample Dubin's car trajectories in randomly-generated environments over a $T = 2.5$ [s] horizon under 60 Hz LQG feedback control towards the (green) goal. The two scenarios on the left demonstrate *nominally*-safe plans, which can experience significant risk upon stochastic execution. On the right are risk-constrained plans (generated using our `ival_safe` approximation with $\Delta = 10\%$). MC trajectories are shown in red, and dispersions are well-approximated by the *a priori* distributions $\{\bar{b}_i\}$ shown in blue. The Gaussian anthropic belief estimates $\{\hat{\bar{\pi}}_i\}$ are shown in yellow. The lower plots show $F_{\boldsymbol{x}}(t)$ estimates as compared to MC (estimated standard error is indicated by the shaded region). Note that `dt_booles` is prone to extreme over-estimation, while the two $\{\hat{\bar{\pi}}_i\}$-dependent methods `dt_gauss` and `ival_gauss` suffer from the inconsistency of the underlying Gaussianity assumption. In contrast, our proposed method `ival_safe` achieves the best approximation performance and avoids explicit $\bar{\pi}_i$ approximation.

TABLE I
COMPUTE TIMES FOR DUBIN'S CAR MATLAB IMPLEMENTATION ON CONSUMER LAPTOP. QD REFERS TO QUADRATURE DIMENSION.

Monte Carlo $(N = 1000)$	LTV-Gaussian $\bar{b}_i$	Gaussian $\hat{\bar{\pi}}_i$	$\sum_{i=0}^{k} P(x(t_i) \notin X_{\text{safe}})$ QD: $(n_p - 1) = 1$	$\sum_{i=0}^{k-1} \Phi(t_i, t_{i+1}; \mathbb{1}_{X_{\text{safe}}} \bar{b}_i)$ QD: $n_p = 2$
39.1 [s]	0.034 [s]	0.054 [s]	0.034 [s]	0.316 [s]

cases, we specifically reject scenarios where the *unconstrained* optimal has negligible failure probability (i.e., when the obstacles are not relevant). Computation times for our MATLAB implementation of various methods are shown in Table I – as predicted, our method is significantly faster than MC while representing some additional complexity compared to discrete-time methods. A more detailed discussion is presented in Appendix B.

Some representative scenarios are shown in Fig. 4, and statistics are reported in Table II over 100 nominally-safe and 50 risk-constrained scenarios. For reference, the average MC-evaluated risk in each of the two test batches is listed in the top of the column. The **Bias** column lists the mean (signed) difference between the estimate and a 1000-sample MC estimate, and P(**Conservative**) reports the percentage of cases where the estimate was greater than (or within 5%) of the MC "truth." The proposed method `ival_safe` outperforms or matches all others in bias, root-mean-squared error (**RMSE**), and median relative error (**MRE**), while remaining conservative (i.e., safe) in a significant majority of trials. Both `dt_gauss` and `ival_gauss` outperform `dt_booles` but suffer from inconsistency of the Gaussian $\hat{\bar{\pi}}_i$ estimate.

VII. CONCLUSION

This paper addresses the challenging problem of efficiently and accurately estimating failure probabilities to enable risk-aware, continuous motion planning. By developing a rigorous framework directly in continuous-time and leaning heavily on

TABLE II
$F_{\boldsymbol{x}}(T)$ ESTIMATION STATISTICS FOR DUBIN'S CAR SYSTEM.

Batch / Method	**Bias**	**RMSE**	**MRE**	P(**Conservative**)
Nominally-safe	MC : 0.2649			
`dt_booles`	+2.9780	4.908	948 %	**100** %
`dt_gauss`	+0.3156	0.923	70 %	89 %
`ival_gauss`	**+0.0073**	0.257	49 %	46 %
`ival_safe`	+0.0915	**0.173**	**32 %**	92 %
Risk-constrained	MC : 0.0321			
`dt_booles`	+0.4849	0.957	1162 %	**100** %
`dt_gauss`	+0.0510	0.067	224 %	96 %
`ival_gauss`	-0.0138	0.025	**39** %	30 %
`ival_safe`	**+0.0057**	**0.019**	**41** %	86 %

the classic study of first-exit times, it becomes straightforward to identify a lightweight approximation (`ival_safe`) that dramatically outperforms existing methods. Furthermore, our approximation restores a convenient Bellman structure required for optimal control, enabling practical application for a wide variety of nonlinear systems.

Ultimately, the framework and concepts introduced in this paper (particularly Section III) motivate a number of future investigations. Of particular interest are robust methods of estimating anthropic belief via π_t or Ψ_t, as "survival-thus-far" may represent a useful and yet-uncaptured source of information for aspects of autonomous decision-making not limited to risk estimation. Also, fusing MC and Gaussian-based risk-approximations in a hybrid approach may provide the best of both worlds: high accuracy in the face of nonlinearity and compatibility with continuous optimization.

Acknowledgments

This work was supported by the Education Office at The Charles Stark Draper Laboratory, Inc. and by ARL DCIST under Cooperative Agreement Number W911NF-17-2-0181.

References

[1] Kaito Ariu, Cheng Fang, Marcio Arantes, Claudio Toledo, and Brian Williams. Chance-constrained path planning with continuous time safety guarantees. In *Workshops at the Thirty-First AAAI Conference on Artificial Intelligence*, 2017.

[2] Lars Blackmore and Masahiro Ono. Convex chance constrained predictive control without sampling. In *AIAA Guidance, Navigation, and Control Conference*, page 5876, 2009.

[3] Lars Blackmore, Masahiro Ono, Askar Bektassov, and Brian C Williams. A probabilistic particle-control approximation of chance-constrained stochastic predictive control. *IEEE Transactions on Robotics*, 26(3):502–517, 2010.

[4] Adam Bry and Nicholas Roy. Rapidly-exploring random belief trees for motion planning under uncertainty. In *Proc. IEEE Conf. Robot. Autom. (ICRA)*, pages 723–730. IEEE, 2011.

[5] Giuseppe C Calafiore and Marco C Campi. The scenario approach to robust control design. *IEEE Trans. Automat. Contr.*, 51(5):742–753, 2006.

[6] Siyu Dai, Shawn Schaffert, Ashkan Jasour, Andreas Hofmann, and Brian Williams. Chance constrained motion planning for high-dimensional robots. In *Proc. IEEE Conf. Robot. Autom. (ICRA)*, pages 8805–8811. IEEE, 2019.

[7] Xin Huang, Ashkan Jasour, Matthew Deyo, Andreas Hofmann, and Brian C Williams. Hybrid risk-aware conditional planning with applications in autonomous vehicles. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 3608–3614. IEEE, 2018.

[8] Lucas Janson, Edward Schmerling, and Marco Pavone. Monte Carlo motion planning for robot trajectory optimization under uncertainty. In *Robotics Research*, pages 343–361. Springer, 2018.

[9] Zhiyong Jin and Liqun Wang. First passage time for Brownian motion and piecewise linear boundaries. *Methodology and Computing in Applied Probability*, 19 (1):237–253, 2017.

[10] Ioannis Karatzsas and Steven E Shreve. *Brownian motion and stochastic calculus*, volume 113 of *Graduate Texts in Mathematics*. Springer, 1988.

[11] Pu Li, Moritz Wendt, and Günter Wozny. A probabilistically constrained model predictive controller. *Automatica*, 38(7):1171–1176, 2002.

[12] Brett T Lopez, Jonathan P How, and Jean-Jacques E Slotine. Dynamic tube MPC for nonlinear systems. In *American Control Conference (ACC)*, pages 1655–1662. IEEE, 2019.

[13] Brandon Luders, Mangal Kothari, and Jonathan How. Chance constrained RRT for probabilistic robustness to environmental uncertainty. In *AIAA guidance, navigation, and control conference*, page 8160, 2010.

[14] Yudong Ma, Sergey Vichik, and Francesco Borrelli. Fast stochastic MPC with optimal risk allocation applied to building control systems. In *Conf. on Dec. and Control (CDC)*, pages 7559–7564. IEEE, 2012.

[15] Anirudha Majumdar and Russ Tedrake. Robust online motion planning with regions of finite time invariance. In *Algorithmic Foundations of Robotics X*, pages 543–558. Springer, 2013.

[16] MATLAB Optimization Toolbox. MATLAB optimization toolbox, 2019b. The MathWorks Inc., Natick, MA, USA.

[17] Masahiro Ono and Brian C Williams. Iterative risk allocation: A new approach to robust model predictive control with a joint chance constraint. In *Conf. on Dec. and Control (CDC)*, pages 3427–3432. IEEE, 2008.

[18] Masahiro Ono, Marco Pavone, Yoshiaki Kuwata, and J Balaram. Chance-constrained dynamic programming with application to risk-aware robotic space exploration. *Autonomous Robots*, 39(4):555–571, 2015.

[19] Sachin Patil, Jur Van Den Berg, and Ron Alterovitz. Estimating probability of collision for safe motion planning under Gaussian motion and sensing uncertainty. In *Proc. IEEE Conf. Robot. Autom. (ICRA)*, pages 3238–3244. IEEE, 2012.

[20] Pedro Santana, Sylvie Thiébaux, and Brian Williams. RAO*: an algorithm for chance-constrained POMDP's. In *Thirtieth AAAI Conference on Artificial Intelligence*, 2016.

[21] Emanuel Todorov and Weiwei Li. A generalized iterative LQG method for locally-optimal feedback control of constrained nonlinear stochastic systems. In *Proceedings of the 2005, American Control Conference, 2005.*, pages 300–306. IEEE, 2005.

[22] Jur Van Den Berg, Pieter Abbeel, and Ken Goldberg. LQG-MP: Optimized path planning for robots with motion uncertainty and imperfect state information. *Int. J. of Robotics Research*, 30(7):895–913, 2011.

[23] Jur Van Den Berg, Sachin Patil, and Ron Alterovitz. Motion planning under uncertainty using iterative local optimization in belief space. *Int. J. of Robotics Research*, 31(11):1263–1278, 2012.

[24] Michael P Vitus and Claire J Tomlin. On feedback design and risk allocation in chance constrained control. In *Conf. on Dec. and Control (CDC)*, pages 734–739. IEEE, 2011.

[25] Jiongmin Yong and Xun Yu Zhou. *Stochastic controls: Hamiltonian systems and HJB equations*, volume 43. Springer Science & Business Media, 1999.

Appendix

A. Proofs of Stated Results

Lemma 1

Proof: The claims follow almost directly from the definitions; the proof here simply makes this explicit.

Let $S_{t_1} \triangleq \{s \in [t_1, T] \,|\, \boldsymbol{z}(s) \notin D\}$ be the set of "violation times" after (and possibly including) t_1. Note that $\tau_{t_1} \geq t_2$ is equivalent to the statement $t_1 \leq t_2 \leq \tau_{t_1} \leq S_1$ (where the last inequality refers to a set lower bound), and the first claim is immediate. The contrapositive is then also established, namely

$$\begin{aligned} \tau_{t_1} < t_2 &\iff \exists s \in [t_1, t_2) \text{ s.t. } \boldsymbol{z}(s) \notin D && (34)\\ &\iff S_{t_1} \cap [t_1, t_2) \neq \emptyset. && (35)\end{aligned}$$

Moving on to the second claim, note that $S_{t_1} = S_0 \cap [t_1, T]$, where S_0 is defined analogously to S_{t_1} above. Therefore,

$$S_0 \cap [t_1, t_2) = S_0 \cap [t_1, T] \cap [t_1, t_2) = S_{t_1} \cap [t_1, t_2). \quad (36)$$

Thus,

$$\begin{aligned} \tau_0 \geq t_1, \tau_{t_1} < t_2 &\iff t_1 \leq S_0, S_{t_1} \cap [t_1, t_2) \neq \emptyset && (37)\\ &\iff t_1 \leq S_0, S_0 \cap [t_1, t_2) \neq \emptyset && (38)\\ &\iff \tau_0 \in [t_1, t_2) && (39)\end{aligned}$$

and we are done.

The final set of claims follow directly from $z(t)$ càdlàgand D closed. ■

The following auxiliary lemma does most of the heavy lifting.

Lemma 3. *Consider process $\boldsymbol{x}(t)$ under dynamics (1) and C^2 function $g : X \mapsto \mathbb{R}$. Assume there exists a finite $\bar{c}$ such that*

1) *$\boldsymbol{f}_t$ is pathwise-bounded a.s. and $\mathrm{E} \int_0^T \|\boldsymbol{f}_t\|_2^2 \,\mathrm{d}t \leq \bar{c}^2$.*
2) *$\mathrm{E}\,\|G_t\|_2^2 \leq \bar{c}^2$ for all t and $\mathrm{E} \int_0^T \mathrm{tr}(G_t G_t^{\mathrm{T}}) \,\mathrm{d}t < \infty$.*
3) *Assumptions 1 and 2 hold with respect to $\boldsymbol{f}, G$ and g.*

For any t let $\boldsymbol{a}_t$ and H_t represent the gradient and Hessian of g at $\boldsymbol{x}(t)$, and

$$\begin{aligned} {}^t\hat{z}(s) &\triangleq g\big(\boldsymbol{x}(t)\big) + \int_t^s h_t \,\mathrm{d}s' + \int_t^s \boldsymbol{\sigma}_t \,\mathrm{d}\boldsymbol{w}(s')\\ h_s &\triangleq \boldsymbol{a}_s^{\mathrm{T}} \boldsymbol{f}_s + \frac{1}{2}\mathrm{tr}\left(G_s^{\mathrm{T}} H_s G_s\right)\\ \boldsymbol{\sigma}_s &\triangleq \boldsymbol{a}_s^{\mathrm{T}} G_s \end{aligned}$$

be a constant-coefficient approximation to $z(s) \triangleq g\big(\boldsymbol{x}(s)\big)$ for $s \geq t$. Then there exists a random $M_\omega < \infty$ a.s. such that

$$P\Big(\sup_{s' \in [t,s]} |{}^t\hat{z}(s') - z(s')| > (s-t)^p M_\omega\Big) \leq (s-t)^{2-2p} \quad (40)$$

for any $p < 1$ and $s \geq t$.

Proof: In the following, we will at several points make use of the **sum-of-squares (SOS) inequality**: For any $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^m$

$$\|\boldsymbol{a} + \boldsymbol{b}\|_2^2 \leq 2\,\|\boldsymbol{a}\|_2^2 + \|\boldsymbol{b}\|_2^2 \,. \quad (41)$$

Additionally we rely on the **Itô isometry** for Brownian motion $\boldsymbol{w}(t)$, which follows directly from Yong and Zhou [25, Prop. 5.2] (also Karatzsas and Shreve [10, Prop. 2.10]) and the independent increments property.

$$\mathrm{E}\left\|\int_{t_1}^{t_2} A_t \,\mathrm{d}\boldsymbol{w}(t)\right\|_2^2 = \mathrm{E}\int_{t_1}^{t_2} \mathrm{tr}(A_t A_t)^{\mathrm{T}} \,\mathrm{d}t \quad (42)$$

for any progressively-measurable A_t.

As a first step, we will show

$$\mathrm{E}\,\|\boldsymbol{x}(s) - \boldsymbol{x}(t)\|_2^2 \leq (s-t)\bar{c}^2 \quad \forall s \leq t \in [0, T]. \quad (43)$$

Starting from the left-hand-side,

$$\begin{aligned} \mathrm{E}\,\|\boldsymbol{x}(s) - \boldsymbol{x}(t)\|_2^2 &= \mathrm{E}\left\|\int_t^s \boldsymbol{f}_{s'} \,\mathrm{d}s' + \int_t^s G_{s'} \,\mathrm{d}\boldsymbol{w}(s')\right\|_2^2 && (44)\\ &\leq 2\,\mathrm{E}\left\|\int_t^s \boldsymbol{f}_{s'} \,\mathrm{d}s'\right\|_2^2 + 2\,\mathrm{E}\left\|\int_t^s G_{s'} \,\mathrm{d}\boldsymbol{w}(s')\right\|_2^2 && (45)\\ &= 2\,\mathrm{E}\int_t^s \int_t^s \boldsymbol{f}_{s_1}^{\mathrm{T}} \boldsymbol{f}_{s_2} \,\mathrm{d}s_1 \,\mathrm{d}s_2 + 2\,\mathrm{E}\int_t^s \mathrm{tr}(G_{s'} G_{s'}^{\mathrm{T}}) \,\mathrm{d}s' && (46)\end{aligned}$$

where in (45) we use the SOS inequality, and in (46) we appeal to the Itô isometry (42). Evaluating the first term, application of Cauchy-Schwarz to the integrand produces

$$\begin{aligned} &2\,\mathrm{E}\int_t^s \int_t^s \boldsymbol{f}_{s_1}^{\mathrm{T}} \boldsymbol{f}_{s_2} \,\mathrm{d}s_1 \,\mathrm{d}s_2\\ &\quad\leq 2\,\mathrm{E}\int_t^s \int_t^s \max\left(\|\boldsymbol{f}_{s_1}\|_2^2, \|\boldsymbol{f}_{s_2}\|_2^2\right) \mathrm{d}s_1 \,\mathrm{d}s_2 && (47)\\ &\quad\leq 2\,\mathrm{E}\int_t^s \int_t^s \left(\|\boldsymbol{f}_{s_1}\|_2^2 + \|\boldsymbol{f}_{s_2}\|_2^2\right) \mathrm{d}s_1 \,\mathrm{d}s_2 && (48)\\ &\quad\leq 4(s-t)\bar{c}^2 && (49)\end{aligned}$$

by assumption of square-integrability. After leveraging an assumption to bound the integrand in its second term, (46) can now be bounded

$$\mathrm{E}\,\|\boldsymbol{x}(s) - \boldsymbol{x}(t)\|_2^2 \leq 4(s-t)\bar{c}^2 + 2(s-t)\bar{c}^2 \quad (50)$$

and after absorbing constants into $\bar{c}$ we are done. ✓

Next we show that the drift term h_t is pathwise-bounded. Recall that g being C^2 ensures that $\boldsymbol{a}_t$ and H_t are continuous and therefore pathwise-bounded over $[0, T]$ a.s.. Furthermore, note that Assumption 2 implies that either G_t is bounded or $H_t = 0$, so in either case $\mathrm{tr}(G_t^{\mathrm{T}} H_t G_t)$ must be pathwise-bounded. From our assumption that $\boldsymbol{f}_t$ is pathwise-bounded, it clearly follows that h_t is also pathwise-bounded, say by $M_\omega < \infty$ almost surely.

Now we proceed to show the main claim (40). Itô's rule [25, Thm. 5.5] justifies the given definitions of h_s and $\boldsymbol{\sigma}_s$, in the sense that

$$z(s) = z(t) + \int_t^s h_{s'} \,\mathrm{d}s' + \int_t^s \boldsymbol{\sigma}_{s'} \,\mathrm{d}\boldsymbol{w}(s'). \quad (51)$$

The approximation gap $|z(s) - {}^t\hat{z}(s)|$

$$= \left| \int_t^s (h_{s'} - h_t)\,\mathrm{d}s' + \int_t^s (\boldsymbol{\sigma}_{s'} - \boldsymbol{\sigma}_t)\,\mathrm{d}\boldsymbol{w}(s') \right| \tag{52}$$

$$\le \int_t^s \underbrace{|h_{s'} - h_t|}_{\le 2M_\omega}\,\mathrm{d}s' + \left| \underbrace{\int_t^s (\boldsymbol{\sigma}_{s'} - \boldsymbol{\sigma}_t)\,\mathrm{d}\boldsymbol{w}(s')}_{\triangleq \xi_{t,s}} \right| \tag{53}$$

$$\le 2(s-t)M_\omega + |\xi_{t,s}| \tag{54}$$

where in (53) we've applied our pathwise-bound on h_s. We've also introduced the shortcut $\xi_{t,s}$ to represent the Itô integral.

Note that under Assumptions 1 and 2,

$$\|\boldsymbol{\sigma}_s - \boldsymbol{\sigma}_t\|_2 = \left\| G_s^{\mathrm{T}} \boldsymbol{a}_s - G_t^{\mathrm{T}} \boldsymbol{a}_t \right\|_2 \tag{55}$$

$$= \left\| G_s^{\mathrm{T}} (\boldsymbol{a}_s - \boldsymbol{a}_t) + (G_s - G_t)^{\mathrm{T}} \boldsymbol{a}_t \right\|_2 \tag{56}$$

$$\le 2L \, \|x(s) - x(t)\|_2^2 . \tag{57}$$

It follows that the second moment of $\xi_{t,s}$ can be bounded via the Itô isometry (42) as

$$\mathrm{E}\,|\xi_{t,s}|^2 = \mathrm{E} \int_t^s \|\boldsymbol{\sigma}_s - \boldsymbol{\sigma}_t\|_2^2 \,\mathrm{d}s' \tag{58}$$

$$\le \mathrm{E} \int_t^s 4L^2 \, \|x(s') - x(t)\|_2^2 \,\mathrm{d}s' \tag{59}$$

$$\le 4L^2 \int_t^s (s'-t)\bar{c}^2 \,\mathrm{d}s' \tag{60}$$

$$\le 2(s-t)^2 \bar{c}^2 L^2 \tag{61}$$

where in (60) we've appealed to the recently-proven (43).

We then appeal to Doob's maximal inequality [25, Thm. 4.5] for the martingale $\xi_{t,s}$, which gives for any p

$$P\Big(\sup_{s' \in [t,s]} |\xi_{t,s}| > (s-t)^p \bar{c} L \Big) \le \frac{\mathrm{E}\,|\xi_{t,s}|^2}{\big((s-t)^p \bar{c} L\big)^2} \tag{62}$$

$$\le 2(s-t)^{2-2p}. \tag{63}$$

Let $E \subset \Omega$ refer to the event that the condition in the left-hand-side of (63) fails. Returning to (54), it is clear that for any $\omega \in E$ and $p < 1$,

$$\sup_{s' \in [t,s]} |z(s') - {}^t\hat{z}(s')| \le 2(s-t)M_\omega + (s-t)^p \bar{c} L \tag{64}$$

$$\le (s-t)^p M_\omega \tag{65}$$

where we've assumed WLOG that $M_\omega \ge \bar{c}L$. Recalling from (63) that $P(E^c) \le 2(s-t)^{2-2p}$, we are done. ■

Theorem 1

Proof: Define the approximating and target events, respectively, as

$$A_n \triangleq \big\{ \omega \in \Omega \mid \max_j \sup_s z_j^{(n)}(s) \le 0 \big\} \text{ and}$$

$$E \triangleq \big\{ \omega \in \Omega \mid \max_j \sup_s z_j(s) \le 0 \big\}.$$

Then ε_n-PUC of $\boldsymbol{z}^{(n)}(s)$ and $\boldsymbol{z}(s)$ implies that there exist subsets $S_n \subseteq \Omega$ such that for any $\omega \in S_n$

$$\left\| \boldsymbol{z}^{(n)}(s) - \boldsymbol{z}(s) \right\|_2 \le \varepsilon_n M_\omega \tag{66}$$

and that $P(S_n) \to 1$. Define the joint events

$$B_n \triangleq A_n \cap S_n \text{ and } E_n \triangleq E \cap S_n.$$

By the additivity of measure over disjoint sets, it is easy to verify that

$$P(A_n) = P(B_n) + P(A_n \cap S_n^c)$$

and because $P(A_n \cap S_n^c) \le P(S_n^c) \to 0$, it must follow that $|P(A_n) - P(B_n)| \to 0$. An analogous argument establishes that $P(E_n) \to P(E)$. Thus, if we can simply show that $|P(B_n) - P(E_n)| \to 0$, we will be done.

Again, using the additivity of measure, we have

$$P(B_n) = P(B_n \cap E_n) + P(\underbrace{B_n \cap E_n^c}_{\triangleq C_n}) \text{ and}$$

$$P(E_n) = P(E_n \cap B_n) + P(\underbrace{E_n \cap B_n^c}_{\triangleq D_n})$$

and it will be sufficient to show that the probability of "disagreement" $P(C_n) + P(D_n) \to 0$.

From here, we can consider each of the m elements of the vector processes $\boldsymbol{z}(s)$ and $\boldsymbol{z}^{(n)}(s)$ independently. This is because $P(C_n)$ can be written

$$P\big(S_n \bigwedge \max_j \sup_s z_j^{(n)}(s) \le 0 \bigwedge \max_j \sup_s z_j(s) > 0\big) \tag{67}$$

$$\le \sum_{l=1}^m P\big(S_n \bigwedge \max_j \sup_s z_j^{(n)}(s) \le 0 \bigwedge \sup_s z_l(s) > 0\big) \tag{68}$$

$$\le \sum_{l=1}^m \underbrace{P\big(S_n \bigwedge \sup_s z_l^{(n)}(s) \le 0 \bigwedge \sup_s z_l(s) > 0\big)}_{P(C_{n,l})} \tag{69}$$

where in (68) we've used the union bound and in (69) we've relaxed the probabilistic statement. So if we can show that if each term $P(C_{n,j})$ decays to zero (which involves only the j-th channel) decays to 0, then $P(C_n)$ must also decay to 0. Furthermore, the PUC criterion for the vector process implies a similar criterion for each of the j elemental processes. An analogous decomposition can be performed for D_n, so for the remainder we consider each of the j channels independently.

Define the random variable $e_n \triangleq \sup_s \left\| \boldsymbol{z}^{(n)}(s) - \boldsymbol{z}(s) \right\|_2$, allowing $e_n = \infty$ if the supremum does not exist. Then $z_j(s) \in [z_j^{(n)}(s) - e_n, z_j^{(n)}(s) + e_n]$ for all j, s.

First, consider $C_{n,j}$, which by construction is a subset of S_n, implying (66) and therefore $e_n(\omega) \le \varepsilon_n M_\omega$ holds in $C_{n,j}$.

$$P(C_{n,j}) = P\big(S_n \bigwedge \sup_s z_j^{(n)}(s) \le 0 \bigwedge \sup_s z_j(s) > 0\big)$$

$$\le P\big(S_n \bigwedge \sup_s z_j(s) \in (0, e_n]\big)$$

$$\le P\big(\sup_s z_j(s) \in (0, \varepsilon_n M_\omega]\big)$$

Because the interval approaches the empty set monotonically as $n \to \infty$, it is clear that $P(C_{n,j}) \to 0$ for each j.

Similarly for $D_{n,j}$, we have

$$\begin{aligned} P(D_{n,j}) &= P\big(S_n \bigwedge \sup_s z_j(s) \leq 0 \bigwedge \sup z_j^{(n)}(s) > 0\big) \\ &\leq P\big(S_n \bigwedge \sup_s z_j(s) \in (-e_n, 0]\big) \\ &\leq P\big(\sup_s z_j(s) \in (-\varepsilon_n M_\omega, 0]\big) \end{aligned}$$

In this case, the latter probability converges monotonically to $P\big(\sup z_j(s) = 0\big)$, which by assumption equals 0. Therefore, $P(D_n)$ also converges to 0. Altogether, we have that

$$\begin{aligned} |P(A_n) - P(E)| \leq{}& |P(A_n) - P(B_n)| \\ &+ |P(B_n) - P(E_n)| \\ &+ |P(E_n) - P(E)| \to 0 \end{aligned}$$

completing the proof. ■

Proposition 1

Proof: From Lemma 3 we already have a similar statement for each element $\hat{y}_j^{(n)}(s)$ and $y_j(s) = g_j\big(\boldsymbol{x}(s)\big)$. A fundamental relation between the l_1 and l_2 norms in $\mathbb{R}^m$ gives

$$|\hat{y}_j^{(n)}(s) - y_j(s)| \leq \alpha \ \forall j \implies \left\|\hat{\boldsymbol{y}}^{(n)}(s) - \boldsymbol{y}(s)\right\|_2 \leq m\alpha$$

for any $\alpha > 0$. For any timestep $t_i \in \mathcal{T}$, Lemma 3 states that for any j

$$\underbrace{P\Big(\sup_{s \in [t_i, t_{i+1})} |\hat{y}_j^{(n)}(s) - y_j(s)| > \delta_n^p M_\omega\Big)}_{\triangleq S^c_{n,i,j}} \leq \delta_n^{2-2p}. \tag{70}$$

Letting $S_{n,i,j}$ be the event that error is "small" for the j-th channel at the i-th timestep, define S_n as the event that all such errors are small

$$S_n \triangleq \bigcap_{i=0}^{k_n - 1} \bigcap_{j=1}^{m} S_{n,i,j}.$$

Then by the union bound the probability of S_n failing is upper-bounded

$$P(S_n^c) \leq \sum_{i=0}^{k_n-1} \sum_{j=1}^{m} P(S^c_{n,i,j}) \leq m k_n \delta_n^{2-2p} \leq mcT\delta_n^{1-2p}. \tag{71}$$

Taking $p = \frac{1}{4}$, $P(S_n^c)$ clearly goes to 0 as $\delta_n \to 0$. Furthermore, by construction $\omega \in S_n$ implies that

$$\left\|\hat{\boldsymbol{y}}^{(n)}(s) - \boldsymbol{y}(s)\right\|_2 \leq m\delta_n^{\frac{1}{4}} M_\omega \quad \forall s \in [0, T]. \tag{72}$$

and defining $\varepsilon_n \triangleq m\delta_n^{\frac{1}{4}}$ the proof is complete. ■

B. Reduced Quadratures: Second-Order Gaussian Systems

We would like to evaluate the following n_x-dimensioned integral for each constraint j

$$\begin{aligned} &\Phi_{\hat{y}_j}(t_i, t_{i+1}; \mu_i) = \\ &\quad \int_X \mathbb{1}(\boldsymbol{x} \in X_{\text{safe}}) \psi\big(g_j(\boldsymbol{x}), h_j(\boldsymbol{x}), \|\boldsymbol{\sigma}_j(\boldsymbol{x})\|_2, \Delta t_i\big) \, \mathrm{d}\mu_i(\boldsymbol{x}) \end{aligned} \tag{73}$$

which requires some form of numeric quadrature evaluation.

Note that discrete-time direct methods based on (6) also appeal to evaluation of a similar integral

$$P\big(\boldsymbol{x}(t_i) \in X^c_{\text{safe}}\big) = \int_X \mathbb{1}(\boldsymbol{x} \notin X_{\text{safe}}) \, \mathrm{d}\mu_i(\boldsymbol{x}). \tag{74}$$

Upon application, the dimensionality of both (73) and (74) can often be significantly reduced, particularly when μ_i refers to a multivariate Gaussian density.

Many physical systems evolve as nonlinear "integrators", that is, the state space can be partitioned as $\boldsymbol{x} = (\boldsymbol{p}, \boldsymbol{p}, \star)$ where $\star$ represents "other" state, such that

$$\mathrm{d}\boldsymbol{p}(t) = \boldsymbol{v}(t)\,\mathrm{d}t + G_p\big(\boldsymbol{p}(t)\big)\,\mathrm{d}\boldsymbol{w}(t), \tag{75}$$

where $\boldsymbol{p}$ can be interpreted as a "position" vector in a workspace $\mathbb{R}^{n_p}$, and G_p refers to the corresponding rows of G. It is also often the case that safety constraints depend exclusively on this position state; that is $\boldsymbol{g}(\boldsymbol{x}) = \boldsymbol{g}(\boldsymbol{p})$. Note that (75) is furthermore independent of control.

In light of (75) and the position-only dependence of g_j, we can write (74) and (73) as

$$P\big(\boldsymbol{x}(t_i) \in X^c_{\text{safe}}\big) = \int_{\mathbb{R}^{n_p}} \mathbb{1}\big(\boldsymbol{g}(\boldsymbol{p}) \notin \mathcal{O}^-\big) \, \mathrm{d}\mu_i(\boldsymbol{p}) \tag{76}$$

and

$$\begin{aligned} &\Phi_{\hat{y}_j}(t_i, t_{i+1}; \mu_i) = \\ &\int_{\mathbb{R}^{n_p}} \mathbb{1}\big(\boldsymbol{g}(\boldsymbol{p}) \in \mathcal{O}^-\big) \int_{\mathbb{R}^{n_p}} \psi\big(\boldsymbol{p}, h_j(\boldsymbol{p}, \boldsymbol{v})\big) \, \mathrm{d}\mu_i(\boldsymbol{v} \,|\, \boldsymbol{p}) \, \mathrm{d}\mu_i(\boldsymbol{p}) \end{aligned} \tag{77}$$

where with a slight abuse of notation $\mu_i\big(\dot{\boldsymbol{p}} \,|\, \boldsymbol{p}\big)$ and $\mu_i(\boldsymbol{p})$ represent the corresponding conditioned or marginal distributions. Recalling from (24), $h_j(\boldsymbol{p}, \boldsymbol{v})$ is affine in $\boldsymbol{v}$

$$h_j(\boldsymbol{p}, \boldsymbol{v}) = \frac{1}{2}\mathrm{tr}\left(G_p(\boldsymbol{p})^{\mathrm{T}} H(\boldsymbol{p})_{j,p} G_p(\boldsymbol{p})\right) + \boldsymbol{a}_j^{\mathrm{T}}(\boldsymbol{p})\boldsymbol{v}. \tag{78}$$

When μ_i represents a multivariate Gaussian, we can consider the scalar drift $v_{j,\boldsymbol{p}} \triangleq \boldsymbol{a}_j^{\mathrm{T}}(\boldsymbol{p})\boldsymbol{v} \in \mathbb{R}$ and then (77) can be written

$$\int_{\mathbb{R}^{n_p}} \mathbb{1}\big(\boldsymbol{g}(\boldsymbol{p}) \in \mathcal{O}^-\big) \int_{\mathbb{R}} \psi(\boldsymbol{p}, v_{j,\boldsymbol{p}}) \, \mathrm{d}\mu_i(v_{j,\boldsymbol{p}} \,|\, \boldsymbol{p}) \, \mathrm{d}\mu_i(\boldsymbol{p}) \tag{79}$$

which can now be evaluated in dimension $n_p + 1$.

1) The Locally-Deterministic Case: Consider the case $G_p = 0$; this corresponds to the case that no noise is "injected" directly into the $\boldsymbol{p}$ channel of the continuous dynamics. This is in fact commonly the case for physical systems, as it is often assumed that disturbances act in the space of forces or torques (i.e., the $\boldsymbol{v}$ dynamics). In this case, $\boldsymbol{\sigma_j} = \boldsymbol{a}_j^{\mathrm{T}} G_p = 0$ uniformly, and it is straightforward to verify $h_j(\boldsymbol{p}, \boldsymbol{v}) = v_{j,\boldsymbol{p}}$ and that

$$\psi(z, v, 0, \Delta t) = \mathbb{1}\big(z + v\Delta t > 0\big). \tag{80}$$

In this case (79) simplifies to

$$\int_{\mathbb{R}^{n_p}} \mathbb{1}\big(\boldsymbol{g}(\boldsymbol{p}) \in \mathcal{O}^-\big) \phi\Big(\frac{\boldsymbol{g}(\boldsymbol{p})}{\Delta t}; -\bar{v}_j(\boldsymbol{p}), \sigma_j(\boldsymbol{p})\Big) \, \mathrm{d}\mu_i(\boldsymbol{p}) \tag{81}$$

where $\bar{v}_j(\boldsymbol{p})$, $\sigma_j(\boldsymbol{p})$, and ϕ refer to the mean, standard deviation, and CDF of the normal distribution $\mu_i(v_{j,\boldsymbol{p}} \,|\, \boldsymbol{p})$. This implies that $\Phi_{\hat{y}_j}(t_i, t_{i+1}; \mu_i)$ can be evaluated over only n_p dimensions.

C. Simulated Dubin's System

Our experimental validation relies on a simulated second-order Dubin's car with state $\boldsymbol{x} = (\boldsymbol{p}, \boldsymbol{v}, \theta, \omega) \in \mathbb{R}^6$, and control $\boldsymbol{u} = (c, \alpha)$. θ and ω capture the heading angle and angular rate, respectively, while c refers to forward-pointing thrust and α the angular acceleration. The time-invariant, nonlinear dynamics are given by

$$\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{u}) = \begin{bmatrix} \dot{\boldsymbol{p}} \\ \dot{\boldsymbol{v}} \\ \dot{\theta} \\ \dot{\omega} \end{bmatrix} = \begin{bmatrix} \boldsymbol{v} \\ cR(\theta)\boldsymbol{e}_1 \\ \omega \\ \alpha \end{bmatrix} \tag{82}$$

with constant noise matrix

$$G = 0.05 \begin{bmatrix} 0 & 0 & 0 \\ I_2 & 0 & 0 \\ 0 & 0.1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{83}$$

Note that, for this system, we can compute $P(\boldsymbol{x}(t_i) \notin X_{\text{safe}})$ (required for discrete-time methods) with a quadrature of dimension $n_p - 1 = 1$. Fortunately, because this system satisfies the "locally-deterministic" criteria described in Appendix B1 evaluating $\Phi_{\hat{\boldsymbol{y}}}$ requires $n_p = 2$ dimensions, an increase of only one.

To simulate output-feedback control, we introduce a simple observation process at each timestep k

$$\boldsymbol{y}_k = \boldsymbol{x}(t_k) + \boldsymbol{\nu} \tag{84}$$

where $\boldsymbol{\nu} \sim \mathcal{N}(0, 0.0001 I_6)$. Then a corresponding LQG-style controller is constructed to track a nominal trajectory that also defines the linearization point.