J Autom Reasoning (2018) 60:43–62
https://doi.org/10.1007/s10817-017-9413-9

Safe Autonomy Under Perception Uncertainty Using Chance-Constrained Temporal Logic

Susmit Jha[1] · **Vasumathi Raman**[2] · **Dorsa Sadigh**[3] · **Sanjit A. Seshia**[3]

Received: 6 December 2016 / Accepted: 4 May 2017 / Published online: 26 May 2017
© Springer Science+Business Media Dordrecht 2017

Abstract Autonomous vehicles have found wide-ranging adoption in aerospace, terrestrial as well as marine use. These systems often operate in uncertain environments and in the presence of noisy sensors, and use machine learning and statistical sensor fusion algorithms to form an internal model of the world that is inherently probabilistic. Autonomous vehicles need to operate using this uncertain world-model, and hence, their correctness cannot be deterministically specified. Even once probabilistic correctness is specified, proving that an autonomous vehicle will operate correctly is a challenging problem. In this paper, we address these challenges by proposing a *correct-by-synthesis* approach to autonomous vehicle control. We propose a probabilistic extension of temporal logic, named Chance Constrained Temporal Logic (C2TL), that can be used to specify correctness requirements in presence of uncertainty. C2TL extends temporal logic by including chance constraints as predicates in the formula which allows modeling of perception uncertainty while retaining its ease of reasoning. We present a novel automated synthesis technique that compiles C2TL specification into mixed integer constraints, and uses second-order (quadratic) cone programming to synthesize optimal control of autonomous vehicles subject to the C2TL specification. We also present a risk distribution approach that enables synthesis of plans with lower cost without increasing the overall risk. We demonstrate the effectiveness of the proposed approach on a diverse set of illustrative examples.

✉ Susmit Jha
jha@csl.sri.com

Vasumathi Raman
vasumathi.raman@gmail.com

Dorsa Sadigh
dsadigh@eecs.berkeley.edu

Sanjit A. Seshia
sseshia@eecs.berkeley.edu

1 SRI International, Menlo Park, CA, USA

2 Zoox, Inc., Menlo Park, CA, USA

3 UC Berkeley, Berkeley, CA, USA

Keywords Autonomy · Temporal logic · Safe Control

1 Introduction

The rapid increase in computation power [24] and improved scalability of AI techniques [14] have resulted in a wide-scale adoption of autonomous systems. Their adoption into safety-critical applications such as autonomous driving, make it imperative that these systems operate correctly. Currently, these systems are often designed manually, and their certification relies on tests and extensive requirements on the design process. These are complex systems with tightly-coupled components that implement control, perception and logical decision-making, and proving the correctness of manual design of these systems is challenging [31,40]. The difficulty of this task is further amplified by the uncertain environment in which these systems operate, and the inherent probabilistic nature of the statistical techniques used to observe the environment. Further, the notion of correctness applied for electronic and software systems are no longer sufficient due to the presence of inherent uncertainty in environment and statistical machine learning algorithms used in perception. Ignoring such uncertainty is unrealistic and abstracting it as non-determinism leads to impractically conservative design. We require a new approach to specify correctness requirements in presence of uncertainty, along with techniques to ensure the satisfaction of these requirements by the autonomous systems. In this paper, we address this challenge by defining a new specification language, Chance Constrained Temporal Logic (C2TL), that extends signal temporal logic to capture perception uncertainty. We present a novel approach to designing autonomous control algorithms that are guaranteed to satisfy C2TL properties.

An autonomous control system can be conceptually divided into two key subsystems: a perception pipeline to observe the world, and a control pipeline comprising high-level reasoning and low-level motion planning. Both these subsystems are well-studied in the control and robotics literatures, and there has been a lot of interest recently in quantifying uncertainty in perception [13] as well as control under uncertainty [4]. The traditional approach to the design of autonomous systems decouples perception uncertainty and control by using probabilistic thresholds in perception to ignore low probability events and model higher probability events using non-determinism. The control is designed with respect to this conservative model. This decoupling leads to overly conservative control in practice, and also makes it difficult to establish formal guarantees and prove safety of the overall composed system with perception and control components. For example, given a safety property that requires a vehicle to avoid obstacles and a probabilistic obstacle perception system, it is impossible to satisfy the safety property deterministically. Chance constraints [35] provide a natural way to specify probabilistic correctness properties, but so far, their application has been limited to specifying invariant-like properties. On the other hand, temporal logics such as computational temporal logic (CTL) [19] and linear temporal logic (LTL) [32] have emerged as effective specification languages for specifying and verifying dynamic behaviour of hardware-software systems. Extensions of temporal logic for cyberphysical systems include signal temporal logic (STL) [15], which allows expressing real-valued dense-time temporal properties. STL has been used for verifying and synthesizing automated control subject to complex specifications, including history-dependent and timing requirements. STL does not model stochastic nature of the environment and perception subsystems used to observe the environment. The use of noise variables to model uncertainty in dynamics has been deployed for stochastic control [16,17,44] but they rely on uniform modelling of different sources of uncertainty.

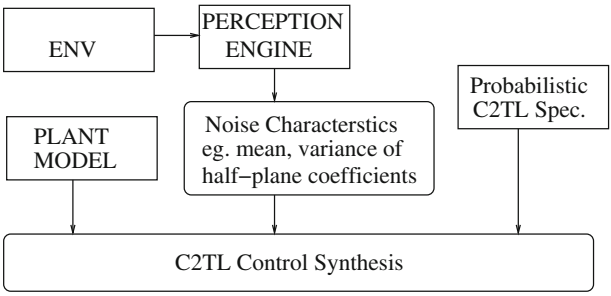

Fig. 1 Safe control synthesis under perception uncertainty

Perception uncertainty affects only the estimate of current state and does not contribute to uncertainty in temporal evolution. Perception uncertainty is not a design artefact but instead, it arises out of physics constraints or quality of available sensors and perception algorithms, and hence, they must be included in specifying the correctness requirement of the overall system. There are also other sources of uncertainty such as those arising from noisy prediction models which affect not just the perception of current state but the predicted temporal evolution of the environment.

Our goal is to devise a specification and synthesis framework for constructing safe controllers that are aware of the probabilistic correctness guarantees of perception subsystem, and enable guarantees on the overall autonomous system and not just on the decoupled subsystems. Figure 1 illustrates the overall architecture of the C2TL-constrained autonomous system that integrates noisy characteristics of the perception system into control synthesis.

We propose chance-constrained temporal logic (C2TL) as an extension of temporal logic, where the leaf predicates in the logic can be chance constraints. C2TL is an effective specification language for the autonomous control of systems operating under perception uncertainty. We show that C2TL formulae can be compiled into mixed integer constraints; thus, C2TL strikes the right balance between expressiveness and ease of reasoning. Second order cone programming can be used to automatically synthesize optimal control satisfying the C2TL specifications. We make the following contributions in this paper:

1. We define *Chance Constrained Temporal Logic* (C2TL) and demonstrate its use to specify the correctness of autonomous vehicle system control.
2. We formulate the problem of synthesizing autonomous vehicle control subject to C2TL specifications while optimizing a quadratic cost function; we reduce this problem to a second order cone program that can be solved using scalable tools such as CVXOPT [3].
3. We present a novel risk distribution approach that alleviates the conservativeness of the synthesized control for C2TL specifications and enables discovering more optimal solutions without sacrificing correctness.

This paper is a significantly extended and revised version of a conference paper [20]. In particular, it includes a novel risk distribution approach that allows synthesis of control with lower cost while still satisfying the C2TL specifications.

2 Background and Related Work

Projects such as the DARPA Urban Challenge [39] and the VisLab Intercontinental Autonomous Challenge [9] have been instrumental in spurring the development and mat-

uration of autonomous vehicle technology. In addition to ground vehicles, autopilots have also found applications in manned and unmanned aircrafts [18] as well as under-water vehicles [36]. One key area where autonomous systems still struggle is in dealing with unexpected situations and planning under uncertainty, arising from stochastic environments or noisy perception. We briefly review the relevant literature in perception, safe and stochastic control, and specification of probabilistic properties to summarize the current state of the art.

Most autonomous systems learn about their environment using sensors such as cameras and LIDAR units to infer the environment state, which is maintained in the form of probabilistic beliefs [12,25,26]. Uncertainty in these probabilistic beliefs arise from two sources. First, the environment states are often dynamic and change over time. Second, the information gathered from sensors is often not sufficient to exactly infer the environment state. As an example, consider a popular perception technique like *simultaneous localization and mapping* [5] (SLAM), which is used for determining the current position of an autonomous vehicle. The estimated position of the vehicle and the coordinates of other entities in the map are often assumed to have Gaussian noise. Aside from localization and mapping, another critical perception challenge for autonomous vehicles is obstacle detection and tracking [8,27]. Camera and laser range finders are used to locally detect and avoid obstacles during navigation for a previously constructed map. This is particularly useful in the presence of dynamic objects whose locations are not fixed in the environment map. The uncertainty in the parametric models representing the obstacles is usually also modelled using Gaussian random variables. The proposed C2TL specifications incorporate these Gaussian models of uncertainty in perception by allowing the predicates in the formulae to be chance constraints [35] over Gaussian random variables.

Safe control of autonomous systems using reachability analysis has been well-studied in literature where the specification is restricted to reach-avoid properties requiring that a particular target state be reached while avoiding unsafe states [29,30,42]. More recently, safe control optimization techniques have been developed which allow exploration of control parameter space and online learning of optimal controller while remaining safe [2,7]. These techniques rely on learning probabilistic model of uncertainty either offline or online at runtime and computation of reachable sets. Our approach is orthogonal to techniques for estimating uncertainty and we focus on safe autonomous control given probabilistic guarantees on the accuracy of the perception subsystem. Further, we consider more expressive properties of the system and environment than reach-avoid properties. Controller synthesis from temporal properties expressed in linear temporal logic (LTL) and signal temporal logic (STL) have also been proposed for robotic applications. In particular, automated synthesis of receding horizon control from STL properties using mixed integer linear programming has proved to be an efficient and scalable approach for controller synthesis with deterministic constraints [37,38]. We adopt a similar constraint-solving based approach to controller synthesis from C2TL that extends STL with probabilistic chance-constraints.

The control of stochastic systems has also been extensively investigated [10,21,33,34]. The goal of these techniques is to determine a control policy that maximizes the probability of remaining within a safe set during a finite time horizon [1]. This safe control problem is usually reformulated as a stochastic optimal control problem with multiplicative costs over a controlled Markov chain. Linear-Quadratic-Gaussian method and its extensions for nonlinear stochastic systems subject to control constraints have also been proposed [43,45]. In contrast, our goal is to satisfy a probabilistic temporal logic specification while optimizing over a given cost metric. This can be naturally modelled using chance constrained programs [11,28]. Chance constrained programming was originally introduced for solving probabilistic constraints which guarantees constraint satisfaction up to a specified proba-

bilistic limit while optimizing a cost function. It is used for uncertainty modeling in various engineering fields [23,47]. For a detailed recent survey of the literature on chance constrained programming approaches, the interested reader is directed to [35]. Here, we extend chance constraints to temporal logic specifications. Another dimension along which we extend existing stochastic control techniques [46] is in our consideration of non-convex feasible spaces, which is critical for autonomous vehicles operating in environments with obstacles. Recently, there has been interest in modelling perception noise for stochastic control particularly in context of autonomous vehicle control [46,47]. However, extension of these techniques to non-convex feasible spaces is critical to model realistic environments of autonomous vehicles which could have multiple obstacles. Our constraint-solving based formulation of synthesizing optimal control accomplishes this without any explicit convex hull approximation.

Chance constraints [23] can be used to specify probabilistic invariants of the system. Probabilistic computation tree logic and probabilistic linear temporal logic [22] extend temporal logic and allow the quantification of uncertainty in the satisfaction of temporal properties. Our work combines chance-constraint based uncertainty specification with recent progress in specifying requirements for cyber-physical systems. Signal temporal logic (STL) [15] has been proposed for specifying behaviour of continuous and hybrid systems, because it combines dense time modalities with numerical predicates over continuous state variables. C2TL extends STL to specify probabilistic temporal properties, by allowing predicates to be *chance constraints* over continuous state variables rather than just real-valued functions. The uncertainty is restricted to probabilistic predicates, and temporal operators are not probabilistic; this is in contrast to other probabilistic extensions of temporal logics [22]. We show that C2TL can be used to specify correctness requirements for an autonomous vehicle under perception uncertainty. We also present a reduction from C2TL constraints to mixed integer constraints. Thus, C2TL provides a balance between expressiveness of the specification language and efficiency of automated synthesis.

3 Chance Constraint Temporal Logic

In this section, we first define *Chance Constrained Temporal Logic* (C2TL), and then illustrate how the correctness of autonomous vehicle control can be specified using C2TL. We then describe how C2TL specifications can be compiled into overapproximate but deterministic constraints. We then formulate the problem of synthesizing the correct control of autonomous systems as a second order cone programming problem. The cost being optimized is quadratic and optimization is done with respect to conic constraints over the state variables and perception coefficients.

Notation: The correctness property is specified over the system state variables $X = \{x_1, x_2, \ldots, x_n\}$, which represent the position of the vehicle, its velocity, acceleration, orientation, angular velocities and other relevant parameters. The state of the system at time t is denoted by $\mathbf{x}_t$.

In this work, half-planes form the basic unit of representation of knowledge acquired through perception. This assumption is key to the reduction of the problem to a mixed integer conic program, and is motivated by the observation that perception algorithms often employ half-plane learning techniques such as Bayesian linear regression and classifiers. For example, an obstacle can be perceived as an intersection of half-planes which represent the

convex hull of the obstacle. Half-planes are represented as:

$$\phi_{lin} : \mathbf{a}_i \mathbf{x}_t + b_i \leq 0 \text{ or } \mathbf{a}_i \mathbf{x}_t + b_i < 0$$

where the coefficients $\mathbf{a}_i, b_i$ are inferred by perception algorithms. Due to uncertainty in perception, the coefficients are not deterministically known: rather, we only know the probability distribution over the coefficients. Let $Dom(\mathbf{a}_i)$, $Dom(b_i)$ denote the domain of the coefficients, and $p(\mathbf{a}_i)$, $p(b_i)$ denote the respective probability density functions. So, the constraints from perception are not deterministic, but instead hold with an associated probability, that is,

$$Pr(\mathbf{a}_i \mathbf{x}_t + b_i \leq 0) \geq 1 - \delta \; or \; Pr(\mathbf{a}_i \mathbf{x}_t + b_i < 0) \geq 1 - \delta$$

We denote the control inputs of the autonomous system, which are the values to be synthesized, by U; the value at each time instant t is $\mathbf{u}_t$. A trace of system states and control values is denoted by $\tau : \mathbb{R}_{\geq 0} \rightarrow X \times U$ where $\tau(t) = (\mathbf{x}_t, \mathbf{u}_t)$.

Our definition of chance constrained temporal logic as a probabilistic extension of signal temporal logic is motivated by two key observations:

- For specifications applied to autonomous systems, temporal aspects of correctness arise from mission requirements such as reaching specific positions in sequence while staying away from particular regions. These temporal aspects of mission requirements do not usually have any associated uncertainty.
- Perception gathers information about a particular instant of time, and uncertainty in perception is hence reflected only in the predicates computed on the system states at a given time, and not on the temporal operators.

We therefore introduce chance constraints at the atomic predicate level of our logic. The syntax definition of C2TL is as follows:

$$\begin{array}{lcl} \phi_{det} & := & \phi_{lin} \mid \phi_{lin} \wedge \phi_{lin} \mid \neg \phi_{lin} \\ \phi_{cc} & := & [Pr(\phi_{det}) \geq 1 - \delta] \mid \neg \phi_{cc} \mid \sim \phi_{cc} \mid \phi_{cc} \wedge \phi_{cc} \mid \phi_{cc} \vee \phi_{cc} \mid \phi_{cc} U_{[a,b]} \phi_{cc}, \end{array}$$

where:

- *linear predicate* ϕ_{lin} over the variables $v \subseteq X \cup U$ is of the form: $\phi_{lin}(v) : \mathbf{a}_i v + b_i \leq 0$ or $\mathbf{a}_i v + b_i < 0$. We can represent constraint $\mathbf{a}_i v + b_i > 0$ as $-\mathbf{a}_i v - b_i \leq 0$, and $\mathbf{a}_i v + b_i \geq 0$ as $-\mathbf{a}_i v - b_i < 0$.
- *deterministic predicate* ϕ_{det} is a Boolean combination of linear predicates if $\mathbf{a}_i, b_i$ are fixed constants.
- *chance-constraint* [11] is a probabilistic extension of deterministic predicates and is of the form $Pr(\phi_{det}) \geq 1 - \delta$. where $0 \leq \delta \leq 1$ represents uncertainty about whether the inequality holds, and the coefficients are random variables with Gaussian probability distribution associated to them.

The coefficients $c = (\mathbf{a}, b)$ in chance-constraints ϕ_{cc} are random variables. We denote their probability distribution by $p(c)$. If ϕ_{cc} is a chance-constraint of the form $Pr(\phi_{det}) \geq 1 - \delta$, we can compute $Pr(\phi_{det}) = \int_{c \in R(\phi_{det}, v)} p(c) dc$ where $R(\phi_{det}, v)$ denotes the set of coefficients that satisfy the corresponding deterministic predicate ϕ_{det} with variables v. Directly computing this integral is difficult and we provide an efficient approximation method for *likely* chance-constraints.

C2TL admits the standard *globally* (G), *eventually* (F) and *until* (U) operators of temporal logic; here we restrict discussion to the *until* (U) operator, which can be used to represent all of the others. The subscripts of the operators denote the time interval associated with the

property, as in STL. The satisfaction of a C2TL formula over a trace τ at time t is defined recursively as follows:

$$
\begin{aligned}
\tau(t) &\models \phi_{lin} && \Leftrightarrow && \phi_{lin}(\tau(t)) \\
\tau(t) &\models \phi^1_{lin} \wedge \phi^2_{lin} && \Leftrightarrow && \phi^1_{lin}(\tau(t)) \wedge \phi^2_{lin}(\tau(t)) \\
\tau(t) &\models \neg\phi_{lin} && \Leftrightarrow && \neg\phi_{lin}(\tau(t)) \\
\tau(t) &\models [Pr(\phi_{det}) \geq 1-\delta] && \Leftrightarrow && p_c(\phi_{det}, \tau(t)) \geq 1-\delta \\
\tau(t) &\models \neg[Pr(\phi_{det}) \geq 1-\delta] && \Leftrightarrow && p_c(\phi_{det}, \tau(t)) < 1-\delta \\
\tau(t) &\models \sim[Pr(\phi_{det}) \geq 1-\delta] && \Leftrightarrow && \tau(t) \models [Pr(\neg\phi_{det}) \geq 1-\delta] \\
\tau(t) &\models \phi^1_{cc} \wedge \phi^2_{cc} && \Leftrightarrow && \tau(t) \models \phi^1_{cc} \wedge \tau(t) \models \phi^2_{cc} \\
\tau(t) &\models \phi^1_{cc} \vee \phi^2_{cc} && \Leftrightarrow && \tau(t) \models \phi^1_{cc} \vee \tau(t) \models \phi^2_{cc} \\
\tau(t) &\models \phi^1_{cc} U_{[a,b]} \phi^2_{cc} && \Leftrightarrow && \exists t_1\ t+a \leq t_1 \leq t+b \wedge \tau(t_1) \models \phi^2_{cc} \\
& && && \wedge (\forall t_2\ t \leq t_2 \leq t_1 \Rightarrow \tau(t_2) \models \phi^1_{cc})
\end{aligned}
$$

As a special case, when $\delta = 0$, chance constraints become deterministic. Chance constraints have two kinds of negations:

- *logical* negation denoted by $\neg$, and
- *probabilistic* negation denoted by $\sim$

For example, consider a deterministic formula $[-x < 0]$ and its logical negation $[x \leq 0]$, and corresponding chance constraints $\phi_{cc} \equiv Pr([-x < 0]) \geq 1-\delta$ and the probabilistic negation $\sim\phi_{cc} \equiv Pr([x \leq 0]) \geq 1-\delta$. If $\delta = 0.8$, then $\phi_{cc} \equiv Pr([-x < 0]) \geq 0.2$, that is, $Pr([x \leq 0]) < 0.8$. This is consistent with $\sim\phi_{cc} \equiv Pr([x \leq 0]) \geq 0.2$. Thus, it is possible for both ϕ_{cc} and its probabilistic negation $\sim\phi_{cc}$ to be simultaneously true.

The following theorem relates probabilistic negation and logical negation when $\delta < 0.5$. This case is relevant because it corresponds to "likely" chance constraints, where the probability of violation is less than 0.5. In practice, most useful constraints obtained from perception have significantly high confidence and δ is very small.

Theorem 1 *If $\delta < 0.5$, probabilistic negation implies logical negation, that is, $\sim\phi_{cc} \Rightarrow \neg\phi_{cc}$. If $\delta > 0.5$, logical negation implies probabilistic negation.*

Proof From the definition of C2TL formula, $\neg\phi_{cc} \equiv \neg[Pr(\phi_{det}) \geq 1-\delta]$ and $\sim\phi_{cc} \equiv Pr(\neg\phi_{det}) \geq 1-\delta$.

Now, $\delta < 0.5 \equiv \delta < 1-\delta$. So, $Pr(\neg\phi_{det}) < \delta \Rightarrow Pr(\neg\phi_{det}) < 1-\delta$, that is,
$\neg[Pr(\neg\phi_{det}) < \delta] \Leftarrow \neg[Pr(\neg\phi_{det}) < 1-\delta]$ by contrapositivity.
$\neg[Pr(\neg\phi_{det}) < 1-\delta] \equiv Pr(\neg\phi_{det}) \geq 1-\delta$ and so,
$\neg[Pr(\neg\phi_{det}) < \delta] \Leftarrow Pr(\neg\phi_{det}) \geq 1-\delta$.
Further, $Pr(\neg\phi_{det}) < \delta \equiv Pr(\phi_{det}) \geq 1-\delta$ and so,
$\neg[Pr(\phi_{det}) \geq 1-\delta] \Leftarrow Pr(\neg\phi_{det}) \geq 1-\delta$, that is, $\neg\phi_{cc} \Leftarrow \sim\phi_{cc}$.
Hence, $\sim\phi_{cc} \Rightarrow \neg\phi_{cc}$ when $\delta < 0.5$.
The proof for the other case proceeds similarly with the direction of implication reversed. □

4 Automated Synthesis of Autonomous Vehicle Control

We now describe how the correctness properties of an autonomous system can be specified using Chance Constrained Temporal Logic (C2TL). Any set of obstacles can be approximated by an union of a finite number of convex polytopes. The planes forming the convex polytopes are only probabilistically known, due to perception uncertainty. A convex polytope is a conjunction of half-planes (linear constraints), and can be represented as

$$\bigwedge_i (\mathbf{a}_i \mathbf{x}_t + b_i > 0)$$

where the coefficients $\mathbf{a}_i \sim \mathcal{N}(\mathbf{a}_i^{\mu}, \mathbf{a}_i^{\Sigma})$ are assumed to be Gaussian variables whose mean $\mathbf{a}_i^{\mu}$ and variance $\mathbf{a}_i^{\Sigma}$ are estimated by the perception pipeline. $\mathcal{N}$ denotes the Gaussian distribution. Since the coefficients are Gaussian, collision with obstacles cannot be ruled out deterministically. Let δ_{obs} be the user-specified threshold for the maximum allowable probability of collision with obstacles. This collision avoidance property is specified in C2TL as:

$$Pr\left(\bigvee_i \mathbf{a}_i \mathbf{x}_t + b_i \leq 0\right) \geq 1 - \delta_{obs}$$

The property of avoiding multiple obstacles j is specified as:

$$Pr\left(\bigwedge_j \bigvee_i \mathbf{a}_{ij} \mathbf{x}_t + b_{ij} \leq 0\right) \geq 1 - \delta_{obs}$$

We assume that the map consists of static and dynamic obstacles as well as real or virtual walls that restrict the vehicle to be within a bounded region, but outside of obstacle areas. Let $\mathbf{a}_{ij}$ be the coefficients of the obstacles and $\mathbf{w}_{ij}$ be the coefficients of the perceived walls. The unobstructed map with uncertainty can thus be represented using the formula:

$$\begin{aligned}\phi_{map} := &\left[Pr\left(\bigwedge_j \bigvee_i \mathbf{a}_{ij} \mathbf{x}_t + b_{ij} \leq 0\right) \geq 1 - \delta_{obs}\right] \\ &\wedge \left[Pr\left(\bigwedge_j \bigvee_i \mathbf{w}_{ij} \mathbf{x}_t + b_{ij} \leq 0\right) \geq 1 - \delta_{wall}\right]\end{aligned}$$

where $\mathbf{a}_{ij} \sim \mathcal{N}(\mathbf{a}_{ij}^{\mu}, \mathbf{a}_{ij}^{\Sigma})$ represents the uncertain perception of obstacles, and $\mathbf{w}_{ij} \sim \mathcal{N}(\mathbf{w}_{ij}^{\mu}, \mathbf{w}_{ij}^{\Sigma})$ represents the uncertain perception of walls (which in practice includes uncertainty in self-localization). Similar constraints can be added for other parameters of an autonomous system such as constraints on speed or acceleration based on the system's current location in the map.

Apart from the safe navigation requirement represented by the global property $G(\phi_{map})$, a second set of useful specifications on autonomous vehicles corresponds to the mission requirements. For example, the vehicle must reach its final destination within some time-bound t_{max}. Because of uncertainty in perception, we can not guarantee this property deterministically. Given a user-specified probability threshold $\delta_{mission}$ of failing to achieve the mission goals, the goal of reaching the destination is specified as $F_{[0,t_{max}]}(Pr(\mathbf{x} = \mathbf{x}_{dest}) \geq 1 - \delta_{mission})$. Other examples include the requirement that an autonomous car wait at a stop

sign until all cross-traffic arriving at the intersection before it passes, and that an aircraft flies straight without turning until it reaches the safe velocity range for turning. These properties can be specified using *until* properties, $\phi_1 U_{[0,t]} \phi_2$. We denote the set of mission constraints by $\phi_{mission}$.

The overall specification for the safe control of the autonomous system is thus $\phi_{map} \wedge \phi_{mission}$: that is, the system achieves the temporal specification of mission goals while remaining safe with respect to the map. We note that the focus of this paper is on autonomous vehicles, but C2TL can also be used to specify behavior of other autonomous systems such as robotic manipulators, and the techniques presented in this paper extend beyond this application domain.

Next, we present a translation of C2TL constraints over Gaussian random variables to deterministic constraints. The constraints are linear with respect to system (state) variables and conic overall due to uncertain coefficients. Note that without half-planes as our basic unit, these constraints may well be non-linear, but the rest of our results would still hold, and the problem could be solved using a solver capable of handling such non-linear constraints. The first part of the translation deals with temporal logic formulae and Boolean combinations of atomic constraints. The second part of translation focuses on elementary chance constraints, and reduces those to deterministic constraints.

We focus on chance constraints with violation probability threshold less than 0.5. As discussed in Sect. 3, probabilistic negation is not the same as logical negation when violation probability (δ) can be 0.5 or more, and hence, we will need two $\{0, 1\}$ integer variables to represent the truth value of each chance constraint, to account for the four cases depending on the truth value of the chance constraint and its probabilistic negation. In [41], such an approach is taken and two $\{0, 1\}$ integer variables p^ϕ and q^ϕ are introduced for each formula ϕ. For likely (violation probability $\delta < 0.5$) chance constraints, one $\{0, 1\}$ integer variable can be used for over-approximation by Theorem 1. Similar to the STL encoding provided in [37,38], we introduce Boolean, that is, $\{0, 1\}$ integer variables m_t^ϕ for each constraint ϕ and time t. These Boolean variables are related in the same way as for the STL encoding.

- Negation: $m_t^{\neg\phi} = 1 - m_t^\phi$
- Conjunction: $m_t^{\phi^1 \wedge \phi^2} = \min(m_t^{\phi^1}, m_t^{\phi^2})$
- Disjunction: $m_t^{\phi^1 \vee \phi^2} = \max(m_t^{\phi^1}, m_t^{\phi^2})$
- Until: $m_t^{\phi^1 U_{[a,b]} \phi^2} = \max_{t' \in [t+a, t+b]}(\min(m_{t'}^{\phi^2}, \min_{t'' \in [t,t']}(m_{t''}^{\phi^1})))$

The next challenge is in translating the probabilistic chance constraints over Gaussian variables to deterministic mixed integer constraints. We need to consider chance constraints only of the form:

$$\phi_{cc}^{elem} \equiv Pr\left(\bigwedge_j \bigvee_i^{N_j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} \leq 0\right) \geq 1 - \delta_{tm}$$

We need to conservatively over-approximate ϕ_{cc}^{elem} using mixed integer constraints which are satisfiable only if ϕ_{cc}^{elem} is satisfiable. ϕ_{cc}^{elem} can be rewritten as

$$Pr\left(\bigwedge_{i,j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - M z_{ij} \leq 0\right) \geq 1 - \delta_{tm} \wedge \bigwedge_j \left(\sum_i z_{ij} < N_j \wedge z_{ij} \in \{0, 1\}\right),$$

where N_j is the number of constraints in the j-th disjunction, $z_{i,j}$ are $\{0, 1\}$ variables and M is a sufficiently large positive number. This transformation uses the big-M reduction common

in non-convex optimization [6] [1]. The above equivalence holds because at least one z_{ij} is 0 for each j since $\sum_i z_{ij} < N_j$ and $z_{ij} \in \{0, 1\}$, and thus, at least one of the constraints in $\bigvee_i^{N_j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} \leq 0$ must be true for each j.

Next, we use Boole's inequality to decompose the conjunction in the probabilistic chance constraint as follows.

$$Pr\left(\bigwedge_{i,j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_{ij} \leq 0\right) \geq 1 - \delta_{tm} \Leftrightarrow \; Pr\left(\bigvee_{i,j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_{ij} > 0\right) < \delta_{tm}.$$

$$\text{Further, } Pr\left(\bigvee_{i,j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_{ij} > 0\right) < \sum_{i,j} Pr(\mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_{ij} > 0)$$

since the probability of union of events is less than the sum of the individual probabilities of the occurrence of each event.

Next, we introduce new variables $0 \leq \epsilon_{ij} \leq 1$ with $\sum_{i,j} \epsilon_{ij} < \delta_{tm}$, and conservatively approximate the chance constraint as:

$$Pr\left(\bigwedge_j \bigvee_i^{N_j} \mathbf{a}_{ij}\mathbf{x}_t + b_{ij} \leq 0\right) \geq 1 - \delta_{tm} \;\Leftarrow\; \bigwedge_{i,j} Pr(\mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_{ij} \leq 0) \geq 1 - \epsilon_{ij}$$

$$\wedge \bigwedge_{ij} 0 \leq \epsilon_{ij} \leq 1 \wedge \sum_{ij} \epsilon_{ij} < \delta_{tm} \wedge \bigwedge_j \left(\sum_i z_{ij} < N_j\right) \wedge \bigwedge_{i,j} z_{ij} \in \{0, 1\}$$

With $N = \sum_j N_j$, we choose $\epsilon_{ij} = \delta_{tm}/N$, which corresponds to uniform risk allocation among the probabilistic constraints above. Since $\mathbf{a}_{ij}$ is a Gaussian random variable, the linear combination of Gaussian variables $\mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_j$ is also Gaussian. Further, the uniform risk allocation ensures that the violation probability bounds are constant.

So, $Pr(\mathbf{a}_{ij}\mathbf{x}_t + b_{ij} - Mz_j \leq 0) \geq 1 - \epsilon_{ij}$ can be translated to a deterministic constraint

$$z_j = 0 \Rightarrow \mu_{ij}\mathbf{x}_t + b_{ij} - \texttt{ErfInv}(\epsilon_{ij})||\Sigma_{ij}^{1/2}\mathbf{x}_t||_2 \leq 0$$

where μ_{ij} and Σ_{ij} are mean and variances of the coefficients $\mathbf{a}_{ij}$. `ErfInv` is the Gaussian inverse error function. Since ϵ_{ij} is constant, we can directly obtain $\texttt{ErfInv}(\epsilon_{ij})$ by looking up the table for the Gaussian inverse error function. A similar approach is used in [46] for the synthesis of control inputs with respect to chance constraints. Consequently, the probabilistic chance constraints are reduced to a set of deterministic constraints. This completes the translation of C2TL constraints to a set of deterministic constraints over the system variables.

The following theorem summarizes the conservative nature of the above translation. Given the control specification for an autonomous vehicle ψ^{C2TL}, the above translation generates ψ^{MI} which conservatively approximates ψ^{C2TL}.

Theorem 2 *Given C2TL constraints ψ^{C2TL}, the translation presented above will generate a set of mixed integer constraints ψ^{MI} such that $\psi^{MI} \Rightarrow \psi^{C2TL}$.*

[1] Given a disjunctive constraint of the form $\mathbf{a}_1 x + b_1 \leq 0 \vee \mathbf{a}_2 x + b_2 \leq 0$, the big-M reduction translates it to $\mathbf{a}_1 x + b_1 - Mz_1 \leq 0 \wedge \mathbf{a}_2 x + b_2 - Mz_2 \leq 0 \wedge z_1 + z_2 < 2$ where $z_1, z_2 \in \{0, 1\}$ and M is chosen to be larger than any possible value of $\mathbf{a}_1 x + b_1$ and $\mathbf{a}_2 x + b_2$.

The conservativeness of ψ^{MI} arises from the following approximations:

- We use the sum of the probabilities of chance constraints to upper-bound the probability of their disjunction. If the constraints are completely independent of each other, the sum of their individual probabilities is exactly the probability of their disjunction. The approximation is small if the constraints are mostly independent, which is often the case for specifying autonomous vehicle systems, since obstacles usually do not overlap.
- We use a uniform risk allocation of the violation probability bounds for each individual constraint. In Sect. 5, we present a risk distribution technique to alleviate the conservativeness introduced by uniform risk allocation.

Thus, the translation of C2TL constraints to mixed integer constraints is conservative, but the approximation introduced is expected to be reasonably tight.

The goal of synthesizing optimal control for autonomous vehicles is to automatically generate the control inputs $\mathbf{u}$. The control inputs applied at time k are denoted by $\mathbf{u}_k$. Often, the dynamical system can be approximated by *linearizing the system* around the current point of operation and using *model predictive* or *receding horizon control*. A detailed discussion on model predictive control for signal temporal logic can be found in [37]. We employ a similar approach here.

A finite parametrization of a linear system assuming piecewise constant control inputs yields the following difference equation:

$$\mathbf{x}_{k+1} = A_k \mathbf{x}_k + B_k \mathbf{u}_k,$$

where $\mathbf{x}_k \in \mathcal{R}^{n_x}$ is the system state in n_x dimensions, $\mathbf{u}_k \in \mathcal{R}^{n_u}$ denotes the n_u control inputs, and A_k, B_k are coefficients representing linear system dynamics around the state $\mathbf{x}_k$. We consider the control problem over a bounded time horizon T, that is, $0 \leq k \leq T$.

Further, the control inputs $\mathbf{u}_k$ at all time steps k are required to be in a convex feasible region $\mathcal{F}_u$, that is,

$$\mathcal{F}_u \equiv \bigwedge_{i=1}^{N_g} \left(g_i^T \mathbf{u} \leq c_i \right); \quad \bigwedge_k \mathbf{u}_k \in \mathcal{F}_u$$

where the convex region $\mathcal{F}_u$ is represented as intersection of N_g half-planes.

The state variables are required to satisfy the autonomous vehicle correctness specification ψ_{ap}^{C2TL}, that is, $\mathbf{x}_k \models \psi_{ap}^{C2TL}$ for all k. We can conservatively approximate the autonomous vehicle correctness specification by ψ_{ap}^{MI} as discussed earlier, that is, $\mathbf{x}_k \models \psi_{ap}^{MI} \Rightarrow \mathbf{x}_k \models \psi_{ap}^{C2TL}$

In addition to correctness specification, the synthesized vehicle control is also expected to minimize a user-specified cost function $J(\mathbf{x}, \mathbf{u})$. We restrict the cost function J to be quadratic in order to ensure that solving the control synthesis problem is computationally efficient. Quadratic functions can capture cost metrics of the form $\sum_i \mathbf{u}_k^\dagger U^\dagger U \mathbf{u}_k + \mathbf{x}_k^\dagger S^\dagger S \mathbf{x}_k$ with appropriate scaling vectors U and S, where $\dagger$ denotes the transpose of a matrix. These can represent metrics such as fuel consumption as well as metrics on the vehicle path.

Problem 1 *(Autonomous Vehicle Control)*

$$\begin{aligned} &\arg\min_{\mathbf{u}} \; J(\mathbf{x}, \mathbf{u}) \\ &\text{s.t.} \quad \mathbf{x}_{k+1} = \mathbb{A}_k \mathbf{x}_k + \mathbb{B}_k \mathbf{u}_k, k = 1 \ldots T, \mathbf{u}_k \in \mathcal{F}_u, \mathbf{x}_k \models \psi_{ap}^{C2TL} \end{aligned}$$

Problem 2 *(Conservative Autonomous Control)*

$$\begin{aligned} &\arg\min_{\mathbf{u}} \; J(\mathbf{x}, \mathbf{u}) \\ &\text{s.t.} \quad \mathbf{x}_{k+1} = \mathbb{A}_k \mathbf{x}_k + \mathbb{B}_k \mathbf{u}_k, k = 1 \ldots T, \mathbf{u}_k \in \mathcal{F}_u, \mathbf{x}_k \models \psi_{ap}^{MI} \end{aligned}$$

Recall that every solution to Problem 2 also solves Problem 1. Moreover, for a bounded time horizon T and a quadratic cost function, since all the constraints are linear in system variables and conic due to the presence of uncertain coefficients, the conservative autonomous control problem can be solved using scalable second order (quadratic) cone programming tools such as CVXOPT [3]. The following theorem summarizes the correctness guarantee:

Theorem 3 *The solution to Problem 2 is sound with respect to Problem 1: if control inputs are synthesized for the conservative problem, they are guaranteed to satisfy the specified correctness property* ψ_{ap}^{C2TL}.

This theorem follows from Theorem 2 because $\mathbf{x}_k \models \psi_{ap}^{C2TL} \Leftarrow \mathbf{x}_k \models \psi_{ap}^{MI}$. Note, however, that the proposed synthesis method (i.e. solving the more efficiently solvable conservative problem using second order cone programming) is incomplete for the autonomous control problem due to the conservative approximation of C2TL constraints ($\psi_{ap}^{C2TL} \Leftarrow \psi_{ap}^{MI}$). The incompleteness relates to degree of conservative approximation introduced in the translation of C2TL constraints to mixed integer constraints.

5 Risk Distribution for Optimal Control

In Sect. 4, we presented our approach to derive autonomous control from high-level chance-constraint temporal logic (C2TL) specifications using a conservative deterministic approximation. One of the sources of approximation is a uniform risk allocation. We show how optimization based risk distribution can be used to make the synthesis approach less conservative for convex C2TL properties. In case of non-convex properties, we fix the value of the z variables used in the convex encoding to their assignment in the computation of optimal solution assuming a fixed allocation presented in Sect. 4. The risk distribution approach presented here allocates risk non-uniformly by adjusting the solution for uniform risk. The key intuition is that autonomous control has naturally different levels of risks along a trajectory; a vehicle has higher risk when it is close to an obstacle. Thus, a synthesis approach which uses non-uniform risk distribution would discover more optimal control compared to uniform risk allocation. Recall the definition of problem 1 where the chance-constraint temporal logic has been compiled into conjunction of individual chance-constraints using the algorithm presented in Sect. 4. We modify the definition by including the risks $\overline{\epsilon} = (\epsilon_{11}, \epsilon_{12}, \ldots, \epsilon_{21}, \epsilon_{22}, \ldots)$ allocated to each constraint as a parameter of the cost.

$$\begin{aligned} &\arg\min_{\mathbf{u}} \quad J(\mathbf{x}, \mathbf{u}, \overline{\epsilon}) \text{ s.t. } \mathbf{x}_{k+1} = \mathbb{A}_k \mathbf{x}_k + \mathbb{B}_k \mathbf{u}_k, k = 1 \ldots T, \mathbf{u}_k \in \mathcal{F}_u, \\ &\bigwedge_i \mu_{ik} \mathbf{x}_k + b_{ik} - \texttt{ErfInv}(\epsilon_{ik}) ||\Sigma_{ik}^{1/2} \mathbf{x}_k||_2 \leq 0 \, \textit{for each } k \end{aligned}$$

The uniform risk allocation corresponds to setting $\epsilon_{ik} = \delta_{tm}/N$ for all i, k. We show that the cost function J is monotonous in the ϵ_{ik} parameters.

Theorem 4 $\frac{\partial J^*}{\partial \epsilon_{ik}} \leq 0$ *for all* i, k. *The optimal cost* J^*, *computed by solving the above optimization function, monotonically decreases with increase in* ϵ_{ik}.

Proof Let $\overline{\epsilon}^1$ and $\overline{\epsilon}^2$ be two risk assignments. We say that $\overline{\epsilon}^1 \leq \overline{\epsilon}^2$ if and only if $\epsilon_{ik}^1 \leq \epsilon_{ik}^2$ for all i, k. We denote the feasible region for $(\mathbf{x}, \mathbf{u})$ corresponding to $\overline{\epsilon}^1$ and $\overline{\epsilon}^2$ as $R(\overline{\epsilon}^1)$ and $R(\overline{\epsilon}^2)$. Now, the derivative of the inverse error function for Gaussian distribution is given by $d(\texttt{ErfInv})/d(\epsilon) = 1/2\sqrt{\pi}\exp[\texttt{ErfInv}(x)^2] > 0$. Clearly, ErfInv monotonically increases with ϵ. Thus,

$$\epsilon_{ik}^1 \leq \epsilon_{ik}^2 \Rightarrow \Big(\mu_{ik}\mathbf{x}_k + b_{ik} - \texttt{ErfInv}(\epsilon_{ik}^1)||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2 \leq 0 \Rightarrow \mu_{ik}\mathbf{x}_k + b_{ik} - \texttt{ErfInv}(\epsilon_{ik}^2)||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2 \leq 0\Big)$$

So, $\overline{\epsilon}^1 \leq \overline{\epsilon}^2 \Rightarrow R(\overline{\epsilon}^1) \subseteq R(\overline{\epsilon}^2)$. The optimal cost $J^*(\mathbf{x}, \mathbf{u}, \overline{\epsilon}^2)$ is found by searching over $R(\overline{\epsilon}^2)$ while the optimal cost $J^*(\mathbf{x}, \mathbf{u}, \overline{\epsilon}^1)$ is found by searching over a superset $R(\overline{\epsilon}^1)$ and so, $J^*(\mathbf{x}, \mathbf{u}, \overline{\epsilon}^2) \leq J^*(\mathbf{x}, \mathbf{u}, \overline{\epsilon}^1)$ if $\overline{\epsilon}^1 \leq \overline{\epsilon}^2$. Thus, $J^*(\mathbf{x}, \mathbf{u}, \overline{\epsilon})$ is a decreasing function in ϵ. □

Our approach for risk distribution relies on incremental revision of risk allocation using the monotonicity result in Theorem 4. Let $\overline{\epsilon}^1$ be the uniform initial risk assignment, that is, $\epsilon_{ik}^1 = \delta_{tm}/N$ for all i, k, with the corresponding optimal cost $J(\overline{\epsilon}^1)$. We need to find a revision sequence of risk assignments $\overline{\epsilon}^1, \overline{\epsilon}^2, \overline{\epsilon}^3, \ldots$ with corresponding optimal costs $J(\overline{\epsilon}^1) \leq J(\overline{\epsilon}^2) \leq J(\overline{\epsilon}^3) \ldots \leq J(\overline{\epsilon}^n)$. We can terminate this sequence after a fixed number of iterations or when a numerical convergence criteria is met, that is, $J(\overline{\epsilon}^n) - J(\overline{\epsilon}^{n-1}) \leq \Delta$ for some fixed threshold Δ.

We show how $\overline{\epsilon}^{p+1}$ can be constructed from $\overline{\epsilon}^p$ to generate the above sequence. For all the i, k constraints that are not active with $\overline{\epsilon}^p$, that is,

$$\mu_{ik}\mathbf{x}_k + b_{ik} < \texttt{ErfInv}(\epsilon_{ik}^p)||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2$$

we find $\epsilon_{ik}^{p'} < \epsilon_{ik}^p$ such that the following is satisfied:

$$\mu_{ik}\mathbf{x}_k + b_{ik} \leq \texttt{ErfInv}(\epsilon_{ik}^{p'})||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2 \leq \texttt{ErfInv}(\epsilon_{ik}^p)||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2$$

The inactive constraints are still inactive but they have become tighter. For the active constraints, the risk associated to them are kept the same, that is, $\epsilon_{ik}^{p'} = \epsilon_{ik}^p$. So, the feasibility region has become strictly smaller for risk distribution $\overline{\epsilon}^{p'}$ and the same set of constraints are active as those for $\overline{\epsilon}^p$. So, the optimum cost will remain the same, that is, $J(\overline{\epsilon}^p) = J(\overline{\epsilon}^{p'})$.

After the risks have been tightened, the total cumulative risk remaining to relax the active constraints is given by $\rho = \sum_{ik}\epsilon_{ik}^p - \sum_{ik}\epsilon_{ik}^{p'}$. If the number of active constraints is M, then we can relax the risk in each of the active constraints by ρ/M to obtain $\overline{\epsilon}^{p+1} = \overline{\epsilon}^{p'} + \rho/M$. For all the inactive constraints, $\overline{\epsilon}^{p+1} = \overline{\epsilon}^{p'}$. So, $\overline{\epsilon}^{p+1} < \overline{\epsilon}^{p'}$. Due to the monotonicity theorem, $J(\overline{\epsilon}^{p+1}) \leq J(\overline{\epsilon}^{p'})$. Thus, $J(\overline{\epsilon}^{p+1}) \leq J(\overline{\epsilon}^p)$.

The formal algorithm for risk distribution is presented below. We initialize with uniform risk. The numerical convergence criteria is used to terminate the risk distribution algorithm. The algorithm terminates if the improvement in the computed cost is less than 1% of the current cost. The algorithm also terminates if all the constraints are tight which implies that a locally optimal risk assignment has been found. It is possible that none of the constraints associated with probabilistic risk is tight because the solution is constrained by other deterministic constraints. The algorithm terminates in this case because risk redistribution would not improve the cost.

Algorithm: Non-uniform Risk Distribution: algorithm starts with an initialization to uniform risk assignment, total number of constraints is N

$\epsilon_{ik}^1 \leftarrow \delta_{tm}/N$ for all i, k, $p \leftarrow 1$, `NotConverged` $\leftarrow$ `true`
Solve the optimization problem with $\overline{\epsilon}^p$ to obtain the cost $J(\overline{\epsilon}^p)$
while `NotConverged` **do**
  $N_{active} \leftarrow$ number of active constraints in the optimization problem, $\rho \leftarrow 0$
  for each inactive constraint (i, k) **do**
    $\epsilon_{i,k}^{p+1} \leftarrow 0.5\, \epsilon_{i,k}^p + 0.5\, \texttt{Erf}((\mu_{ik}\mathbf{x}_k + b_{ik})/||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2)$
    // Satisfies $\mu_{ik}\mathbf{x}_k + b_{ik} \leq \texttt{ErfInv}(\epsilon_{ik}^{p+1})||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2 \leq \texttt{ErfInv}(\epsilon_{ik}^{p})||\Sigma_{ik}^{1/2}\mathbf{x}_k||_2$
    $\rho \leftarrow \rho + \epsilon^{p+1} - \epsilon^p$
  $\delta \leftarrow \rho/N_{active}$
  for each active constraint (i, k) **do**
    $\epsilon_{i,k}^{p+1} \leftarrow \epsilon_{i,k}^p + \delta$
  Solve the optimization problem with $\overline{\epsilon}^{p+1}$ to obtain the cost $J(\overline{\epsilon}^{p+1})$
  `NotConverged` $\leftarrow J^*(\overline{\epsilon}^{p+1}) \leq 1.01 \times J^*(\overline{\epsilon}^p)$ and $N_{active} \neq 0$ and $N_{active} \neq N$
  $p \leftarrow p + 1$
return $\overline{\epsilon}^p$

6 Case Studies

We now experimentally demonstrate the effectiveness of our approach. All experiments were done on a Intel Core-i7 2.9 GHz x 8 machine with 16 GB memory.

Navigation in an uncertain map:

The first case-study considers the problem of navigation in an uncertain map from [48]. A point mass with two modes – moving forward and turning – is expected to navigate safely in the map shown in Fig. 2. The walls in the map and the obstacle in the center are modelled using probabilistic constraints that incorporate the uncertainty in perception. The uncertain walls are illustrated in the map by sampling values of the coefficients and drawing the corresponding walls. The probabilistic safety requirement in this case is a global property requiring that the vehicle avoid the walls and obstacles with a very high probability. The objective function being optimized is quadratic in the final state as well as the control inputs: $f(\mathbf{x}, \mathbf{u}) = 50(\mathbf{x}_N - \mathbf{x}_{dest})^T(\mathbf{x}_N - \mathbf{x}_{dest}) + 0.001 \sum_i \mathbf{u}_i^T \mathbf{u}_i$, where $\mathbf{x}_{dest}$ is the destination state $(2, 1)$. The C2TL safety constraint is $Pr[G(\mathbf{x}(1) \leq 0.8 \rightarrow \mathbf{x}(0) \leq 1.7 \wedge \mathbf{x}(0) \geq 1.7 \rightarrow \mathbf{x}(1) \geq 0.8 \wedge ((\mathbf{x}(1) \leq a \wedge \mathbf{x}(1) \geq b) \vee (\mathbf{x}(1) \leq c \wedge \mathbf{x}(1) \geq d)) \wedge ((\mathbf{x}(0) \leq e \wedge \mathbf{x}(0) \geq f) \vee (\mathbf{x}(0) \leq g \wedge \mathbf{x}(0) \geq h))] \geq 1 - \delta$. The coefficients a, b, c, d, e, f, g, h are Gaussian random variables with mean: 2.6, 2, 0.1, −0.1, 0.1, −0.3, 2.2, 1.4 respectively, and they have the same variance of 0.06. The violation probability δ is chosen to be 0.01 and 0.001.

Monte Carlo simulation was used to estimate the probability of constraint violation. For each simulation, the location of the walls and the obstacles was determinized by sampling from the corresponding Gaussian distribution. We then checked whether the automatically generated path intersected with the walls or obstacles, violating the safety requirement. When the violation probability in the C2TL specification was set to 0.001, Monte Carlo trials did not find a single instance out of 10000 simulations in which the property was violated. We increased the violation probability to 0.01, and found 8 out of 10000 simulations that violated the probability; i.e., the estimated violation probability was 0.0008. When compared to the approach in [48] and approximating chance-constraints by sampling, the method proposed in this paper takes 4.1 s instead of 25.2 s to compute a sequence of control inputs.

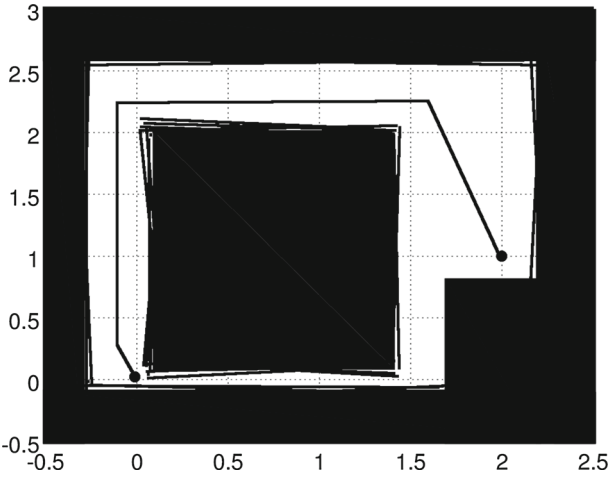

Fig. 2 Uncertain map navigation: $\mathbf{x}(0)$, $\mathbf{x}(1)$ are x and y-axis

This demonstrates how the proposed approach conservatively approximates the specified probabilistic constraint, generating a motion plan that satisfies the probabilistic safety property. Observe that although the cost minimizes the path length, the generated path goes around the obstacle, taking the longer path. The shorter path would violate the C2TL safety constraints due to the uncertainty in the location of the obstacles and walls. This is shown in Fig. 2. We illustrate the uncertain walls with multiple lines.

Lane Change:

The second case-study is on the synthesis of control for an autonomous vehicle such as a car, trying to pass a tractor-trailer in an adjacent lane, as described in [49]. The trailer can probabilistically switch into the passing car's lane. If the car is ahead of the trailer when the trailer initiates a lane change, then the car should accelerate, and if the car is behind the trailer when the trailer initiates the lane change, the car should decelerate. If the trailer switches lanes when it is just adjacent to the car, the car has no action to prevent an accident. Thus, a completely safe course of action is not possible for the autonomous car and it can only try to keep the risk below a user-specified threshold by passing the trailer quickly and not staying in the unsafe region for long. The uncertainty arises due to a probabilistic model of when the trailer will switch lanes, based on the car's observations of its behaviour. The states of the car $\mathbf{x}_k$ is a vector comprising of its relative longitudinal position and velocity, that is, $\mathbf{x}_k = \begin{bmatrix} p_k \\ v_k \end{bmatrix}$. The system dynamics is given by $\mathbf{x}_{k+1} = A\mathbf{x}_k + Bu_k$ where $A = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 0.5\Delta t^2 \\ \Delta t \end{bmatrix}$. The car does not move laterally but the trailer moves laterally and its perceived lateral position at time t is given the Gaussian random variable y_t. $y_t = 0$ is the trailer's original lane and $y_t = 1$ denotes the lane of the car. The system starts with $p = -5$, that is, the car is behind the trailer. But due to the probabilistic perception of the trailer's lateral movement, the requirements are given by following C2TL constraints that ensure safety along with $Pr[G_{[0,1045]}((-2 \leq p \leq 2) \Rightarrow y \geq 1) \wedge F_{[0,1045]}(p > 2)] \geq 1 - \delta$. We consider a time horizon of length 1045 and the cost function is the quadratic sum of control inputs. We require the separation between the car and trailer to be above a safe limit with a high probability. The

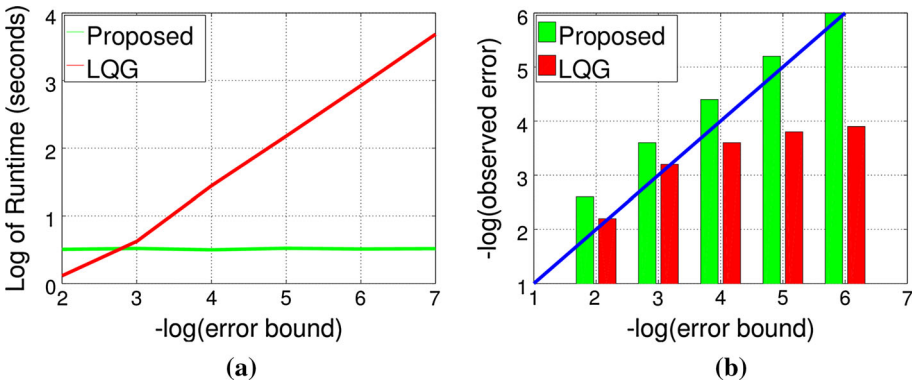

Fig. 3 **a** Runtime comparison, **b** accuracy comparison

threshold of violating the specification was set to $\delta = 0.015$. The cost function was the time spent behind the trailer but not in the same lane. Monte Carlo simulations of the generated controller showed that the actual threshold of violation is 0.0004.

In order to compare with LQG-based sampling techniques, we change the cost function to incorporate temporal logic requirements by penalizing the car for coming close to trailer. Further, we replace the noisy observation y_t by the corresponding linear Gaussian dynamics. In Fig. 3a, we compare runtime of the synthesis technique for each specified violation probability. While our proposed technique's runtime is not very sensitive to the violation probability, the runtime of the sampling-based approach increases sharply due to the increase in the number of required simulation runs. In Fig. 3b, we present the violation probability observed in Monte Carlo simulations when both approaches are given the same runtime, by restricting the number of simulation runs. All bars above the diagonal line satisfy the probabilistic constraint, while bars below it do not (note the negative log scale on y-axis as well as x-axis). No violations were found for our proposed technique for error bounds 10^{-6} and lower. Thus, the proposed method always satisfies the specification, whereas sampling fails to do so for smaller error bounds.

Passing a Vehicle Using Oncoming Traffic Lane:

The third case-study is from recent work by Xu et al. [50]. In this case-study, a vehicle's lane is blocked and it needs to move into the lane of oncoming traffic to go around the obstacle. The perception pipeline on the vehicle estimates the position and the speed of oncoming traffic before deciding to get into the oncoming traffic lane.

The state of the vehicle $\mathbf{x} = [x\ y\ \theta]$, and the control input $u = [v\kappa]$ where x and y are the position, θ is the angle, κ is curvature v is the speed. The dynamics of the vehicle is given by time-varying linear model: $\mathbf{x}_t = A_t\mathbf{x}_{t-1} + B_t u_{t-1}$ where $A_t = \begin{bmatrix} 1 & 0 & -v_{t-1}\sin\theta_{t-1}\Delta t \\ 0 & 1 & v_{t-1}\cos\theta_{t-1}\Delta t \\ 0 & 0 & 1 \end{bmatrix}$ and $B_t = \begin{bmatrix} \cos\theta_{t-1}\Delta t & 0 \\ \sin\theta_{t-1}\Delta t & 0 \\ 0 & v_{t-1}\Delta t \end{bmatrix}$. The static obstacle is fixed in first lane ($y = 0$) between $x = 5$ and $x = 6$, and the noisy perceived position and speed of oncoming traffic at time t is given by the x_t^m, y_t^m, v_t^m. Due to uncertainty in perception, we can not deterministically guarantee safe maneuvering of the vehicle, but we require that the probability of collision

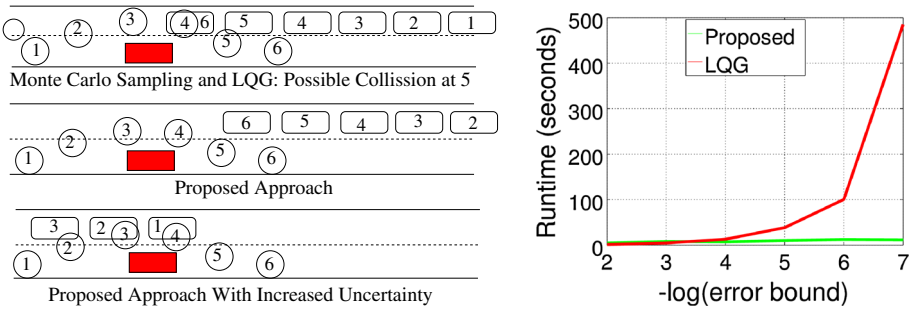

Fig. 4 **a** Illustration of synthesized control. **b** Runtime versus $-\log(\epsilon)$. *Left* Positions of the autonomous vehicle (*circle*) and oncoming traffic (*rectangle*) at different (1–6) time steps are shown. The *red rectangle* is the obstacle. *Right* Runtime comparison for different violation probability bounds

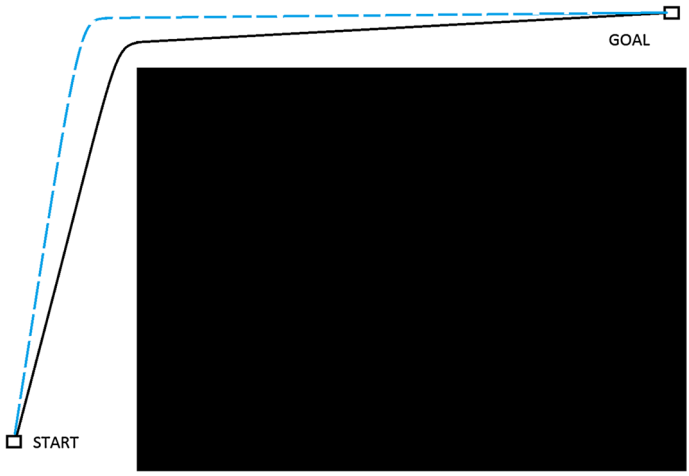

Fig. 5 Impact of risk distribution on trajectory

with oncoming traffic or with the obstacle in the vehicle's lane is below a threshold of ϵ. The C2TL constraint is $Pr[G_{[0,1000]}(y_t^m - y < 0.8 \Rightarrow (x - x^m > 1 \vee x - x^m < -1) \wedge (5 \leq x \leq 6 \Rightarrow y \geq 1)) \wedge F_{[0,1000]}(x \geq 8)] \geq 1 - \epsilon$. The cost function measures the time taken to re-enter the lane after crossing the obstacle.

We illustrate the qualitative nature of the synthesized control in Fig. 4a. For violation probability $\epsilon = 0.0001$, the control synthesized by the sampling-based technique in time comparable to our approach (4 s) is not probabilistically safe. The control synthesized using the proposed technique relies on speeding up and getting around the obstacle before the oncoming traffic. When we increase the standard deviation in the perception of the speed of the oncoming traffic by 10X, the control synthesized by our approach picks a less optimum, higher-cost solution in order to meet the safety violation probability requirement, which slows the vehicle and waits for the oncoming traffic to pass before going around the obstacle. Figure 4b shows that the runtime of the sampling-based approach increases rapidly with a decrease in ϵ, while it does not change significantly for our technique.

Risk Distribution:

In the last case study, we demonstrate how risk distribution allows synthesis of more optimal control than uniform risk allocation in the navigation map shown in Fig. 5. The cost metric is the length of the path and non-uniform risk allocation improves the cost by 6%. The total risk $\epsilon = 0.01$. The total number of iterations of the risk distribution algorithm was 4 and the total runtime was 119 s. The dotted blue line is trajectory with uniform risk and solid black line is trajectory with non-uniform risk allowing it to come closer to obstacle.

7 Conclusion

In this paper, chance constrained temporal logic (C2TL) is proposed to capture correctness specifications in the presence of uncertainty. Our technique relies on approximating the probabilistic C2TL specification constraints with conservative deterministic constraints, and then, solving the control problem using second order cone programming. The autonomous vehicle control synthesized by our technique is guaranteed to satisfy the probabilistic specifications. Our approach does not address noisy dynamics and assumes that the dynamical system is deterministic. Further, it is restricted to linear dynamics. It also requires pre-characterization of noise in perception and assumes that the noise characteristics at runtime remain within these bounds. In practice, uncertainty in perception changes with environment and a more effective approach would adapt to the changes in uncertainty. The proposed approach is a first-step towards design of autonomous systems with assurance in presence of perception uncertainty.

References

1. Abate, A., Prandini, M., Lygeros, J., Sastry, S.: Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems. Automatica **44**(11), 2724–2734 (2008)
2. Akametalu, A.K., Fisac, J.F., Gillula, J.H., Kaynama, S., Zeilinger, M.N., Tomlin, C.J.: Reachability-based safe learning with gaussian processes. In: 53rd IEEE Conference on Decision and Control, pp. 1424–1431. IEEE (2014)
3. Andersen, M.S., Dahl, J., Vandenberghe, L.: Cvxopt: A python package for convex optimization, version 1.1. 6. Available at cvxopt. org, (2013)
4. Åström, K.J.: Introduction to Stochastic Control Theory. Courier Corporation, North Chelmsford (2012)
5. Bailey, T., Durrant-Whyte, Hugh: Simultaneous localization and mapping (slam): Part ii. IEEE Robot. Autom. Mag. **13**(3), 108–117 (2006)
6. Belotti, P., Lee, J., Liberti, L., Margot, F., Wachter, A.: Branching and bounds tightening techniques for non-convex MINLP. Optim. Methods Softw. **24**, 597–634 (2009)
7. Berkenkamp, F., Schoellig, A.P.: Safe and robust learning control with gaussian processes. In: Control Conference (ECC), 2015 European, pp. 2496–2501. IEEE, (2015)
8. Bernini, N., Bertozzi, M., Castangia, L., Patander, M., Sabbatelli, M.: Real-time obstacle detection using stereo vision for autonomous ground vehicles: A survey. In: ITSC, pp. 873–878. IEEE, (2014)
9. Broggi, A., et al.: Autonomous vehicles control in the VisLab intercontinental autonomous challenge. Ann. Rev. Control **36**(1), 161–171 (2012)
10. Cassandras, Christos G., Lygeros, John: Stochastic Hybrid Systems, vol. 24. CRC Press, Boca Raton (2006)
11. Charnes, A., Cooper, W.W., Symonds, G.H.: Cost horizons and certainty equivalents: an approach to stochastic programming of heating oil. Manag. Sci. **4**(3), 235–263 (1958)
12. De Nijs, R., Ramos, S., Roig, G., Boix, X., Gool, L.V., Kuhnlenz, K: On-line semantic perception using uncertainty. In: IROS, pp. 4185–4191. IEEE, (2012)
13. Devroye, Luc, Györfi, László, Lugosi, Gábor: A Probabilistic Theory of Pattern Recognition, vol. 31. Springer, Berlin (2013)

14. Dietterich, T.G., Horvitz, Eric J.: Rise of concerns about AI: reflections and directions. Commun. ACM **58**(10), 38–40 (2015)
15. Donzé, A., Maler, O.: Robust satisfaction of temporal logic over real-valued signals. In: FORMATS, pp. 92–106, (2010)
16. Fu, J., Topcu, U.: Computational methods for stochastic control with metric interval temporal logic specifications. In: CDC, pp. 7440–7447, (2015)
17. Fu, J., Topcu, U.: Synthesis of joint control and active sensing strategies under temporal logic constraints. IEEE Trans. Autom. Control **61**(11), 3464–3476 (2016)
18. Goerzen, C., Kong, Zhaodan, Mettler, Bernard: A survey of motion planning algorithms from the perspective of autonomous uav guidance. J. Intell. Robot. Syst. **57**(1–4), 65–100 (2010)
19. Huth, Michael, Ryan, Mark: Logic in Computer Science: Modelling and Reasoning about Systems. Cambridge University Press, Cambridge (2004)
20. Jha, S., Raman, V.: Automated synthesis of safe autonomous vehicle control under perception uncertainty. In: NASA Formal Methods, pp. 117–132 (2016)
21. Koutsoukos, X., Riley, D.: Computational methods for reachability analysis of stochastic hybrid systems. In: HSCC, pp. 377–391. Springer, Berlin (2006)
22. Kwiatkowska, M., Norman, G., Parker, D.: Prism: Probabilistic symbolic model checker. In: Computer Performance Evaluation: Modelling Techniques and Tools, pp. 200–204. Springer, Berlin (2002)
23. Li, P., Arellano-Garcia, H., Wozny, Gnter: Chance constrained programming approach to process optimization under uncertainty. Comput. Chem. Eng. **32**(1–2), 25–45 (2008)
24. Mack, Chris, et al.: Fifty years of moore's law. IEEE Trans. Semicond. Manuf. **24**(2), 202–207 (2011)
25. Martinet, P., Laugier, C., Nunes, U.: Special issue on perception and navigation for autonomous vehicles. IEEE Robot. Autom. Mag. **21**(1), 26–27 (2014)
26. Mathys, D.C., et al.: Uncertainty in perception and the hierarchical Gaussian filter. Front. Hum. Neurosci. **8**, 825 (2014)
27. McGee, T.G., Sengupta, R., Hedrick, K.: Obstacle detection for small autonomous aircraft using sky segmentation. In: ICRA 2005, pp. 4679–4684. IEEE (2005)
28. Miller, Bruce L., Wagner, Harvey M.: Chance constrained programming with joint constraints. Oper. Res. **13**(6), 930–945 (1965)
29. Mitchell, I., Tomlin, C.J.: Level set methods for computation in hybrid systems. In: International Workshop on Hybrid Systems: Computation and Control, pp. 310–323. Springer, Berlin (2000)
30. Mitchell, Ian M., Bayen, Alexandre M., Tomlin, Claire J.: A time-dependent Hamilton–Jacobi formulation of reachable sets for continuous dynamic games. IEEE Trans. Autom Control **50**(7), 947–957 (2005)
31. Patchett, C., Jump, M., Fisher, M.: Safety and certification of unmanned air systems. Eng. Technol. Ref. **1**, 1 (2015)
32. Pnueli, A.: The temporal logic of programs. In: Providence, pp. 46–57 (1977)
33. Prajna, Stephen, Jadbabaie, Ali, Pappas, George J: A framework for worst-case and stochastic safety verification using barrier certificates. IEEE Trans. Autom. Control **52**(8), 1415–1428 (2007)
34. Prandini, Maria, Jianghai, Hu: Stochastic reachability: theory and numerical approximation. Stoch. Hybrid Syst. Autom. Control Eng. Ser. **24**, 107–138 (2006)
35. Prékopa, András: Stochastic Programming, vol. 324. Springer, Berlin (2013)
36. Pshikhopov, V.K., Medvedev, M.Y., Gaiduk, A.R., Gurenko, B.V.: Control system design for autonomous underwater vehicle. In: 2013 Latin American Robotics Symposium and Competition (2013)
37. Raman, V., Donzé, A., Maasoumy, M., Murray, R.M., Sangiovanni-Vincentelli, A.L., Seshia, S.A.: Model predictive control with signal temporal logic specifications. In CDC, pp. 81–87 (2014)
38. Raman, V., Donzé, A., Sadigh, D., Murray, R.M., Seshia, S.A.: Reactive synthesis from signal temporal logic specifications. In: HSCC, pp. 239–248 (2015)
39. Rouff, Christopher, Hinchey, Mike: Experience from the DARPA Urban Challenge. Springer, Berlin (2011)
40. Rushby, J.: New challenges in certification for aircraft software. In: EMSOFT, pp. 211–218. ACM (2011)
41. Sadigh, D., Kapoor, A.: Safe control under uncertainty with probabilistic signal temporal logic. In: Robotics: Science and Systems XII, (2016)
42. Summers, S., Kamgarpour, M., Lygeros, J., Tomlin, C.: A stochastic reach-avoid problem with random obstacles. In: Proceedings of the 14th International Conference on Hybrid Systems: Computation and Control, pp. 251–260. ACM (2011)
43. Sun, W., van den Berg, J., Alterovitz, R.: Stochastic Extended LQR: Optimization-Based Motion Planning Under Uncertainty, pp. 609–626. Springer, Cham (2015)
44. Svorenova, M., Kretínský, J., Chmelik, M., Chatterjee, K., Cerná, I., Belta, C.: Temporal Logic Control for Stochastic Linear Systems Using Abstraction Refinement of Probabilistic Games. In: HSCC, pp. 259–268 (2015)

45. Todorov, E., Li, W.: A generalized iterative LQG method for locally-optimal feedback control of constrained nonlinear stochastic systems. In: American Control Conference, 2005. Proceedings of the 2005, vol. 1, pp. 300–306. IEEE (2005)
46. Vitus, M.: Stochastic Control Via Chance Constrained Optimization and its Application to Unmanned Aerial Vehicles. PhD thesis, Stanford University, (2012)
47. Vitus, M.P., Tomlin, C.J.: Closed-loop belief space planning for linear, Gaussian systems. In: ICRA, pp. 2152–2159. IEEE (2011)
48. Vitus, M.P., Tomlin, C.J.: A hybrid method for chance constrained control in uncertain environments. In: CDC, pp. 2177–2182 (2012)
49. Vitus, M.P., Tomlin, C.J.: A probabilistic approach to planning and control in autonomous urban driving. In: CDC, pp. 2459–2464 (2013)
50. Xu, W., Pan, J., Wei, J., Dolan, J.M.: Motion planning under uncertainty for on-road autonomous driving. In: ICRA, pp. 2507–2512. IEEE (2014)