Safety Assessment for Stochastic Linear Systems using Enclosing Hulls of Probability Density Functions

Matthias Althoff, Olaf Stursberg, and Martin Buss

***Abstract*— This contribution addresses the problem of computing the probability that a linear system with uncertain inputs reaches an unsafe region in the state space. The probability of reaching unsafe states is bounded by an upper limit, by intersecting enclosing hulls of the probability density function for time intervals with the specified unsafe regions. Disturbances are modeled as white Gaussian noise, whose mean is modeled as uncertain within specified sets. This allows to consider white non-Gaussian noise in an over-approximative manner. The presented approach is efficient in the sense that high-dimensional systems can be handled.**

I. Introduction

In recent years, the growing complexity of technical systems together with an increasing demand for the compliance with system requirements has driven the development of algorithmic verification methods. A focus was to investigate techniques for verifying safety properties of systems with deterministic dynamics. In many applications, however, a pure yes/no-decision about safety is unsatisfactory, because a strict safety requirement for a system with partly uncertain dynamics may severely limit the system's operability or availability; examples are scenarios in air traffic [1] or road traffic [2]. This paper hence investigates stochastic verification techniques that lead to a probability for the safe execution of linear systems. The verification is performed algorithmically by computing enclosing hulls of probability density functions, and determining the probability of intersecting with unsafe sets.

An obvious approach for exploring stochastic systems is Monte-Carlo simulation [3] – but, a large number of simulations are necessary to obtain a result that has *sufficiently* converged to the exact probability of hitting an unsafe state set. In addition, this approach is a non-conservative approximative technique and thus does not qualify for verification. Especially in the hybrid system community, various approaches towards reachability analysis of stochastic systems have been developed in recent years. Barrier certificates can be applied to compute upper bounds for the probability of entering unsafe sets of hybrid systems without explicitly computing reachable sets [4]. Algorithmic or numerical techniques for stochastic verification of hybrid systems have been developed in [5], [6], [7], [8]. These approaches compute probabilistic reachable sets by performing a discretization of the continuous state space, what allows to approximately compute probabilistic reachable sets using Markov chains. The advantage of this technique is that a large class of stochastic hybrid systems can be handled. The main drawback is the limitation to relatively low dimension of the continuous state space (in the range of 4-6 continuous states). This is due to the exponential growth of the number of discrete states introduced for partitioning the continuous state space.

In this paper, the special case of linear continuous dynamics is addressed in order to circumvent the discretization of the state space which allows to consider systems of relatively large scale. The disturbance of the linear system is modeled as white Gaussian noise whose mean value is uncertain within a specified set U. As briefly recapitulated in this work, the probability distribution of linear systems subject to white Gaussian noise is well-known. Furthermore, the computation of reachable sets subject to unknown, but bounded disturbances U has been computed e.g. in [9], [10], [11], [12], [13]. However, the combination of both, white Gaussian noise with uncertain inputs of unknown probability distribution is novel to the authors' knowledge. Due to the uncertain mean of the white Gaussian noise within U, there exist infinitely many probability density functions for this problem. For this reason, the solution is represented by enclosing hulls which include all possible probability density functions of the system. This is also done for the solution of time intervals (not only time points), such that the probability of reaching unsafe states can be computed as an over-approximation.

II. System Model

The system under consideration is defined by the following linear stochastic differential equation (SDE) which is also known as the multivariate Ornstein-Uhlenbeck process [14]:

$$\begin{aligned} \dot{x} &= Ax(t) + u(t) + C\xi(t), \\ x(0) &\in \mathbb{R}^n,\ u(t) \in U \subset \mathbb{R}^n,\ \xi \in \mathbb{R}^m \end{aligned} \tag{1}$$

where A and C are matrices of proper dimension and A has full rank. There are two kinds of inputs: the first input u is Lipschitz continuous and can take any value in $U \subset \mathbb{R}^n$ for which no probability distribution is known. The second input $\xi \in \mathbb{R}^m$ is white Gaussian noise. The combination of both inputs can be seen as a white Gaussian noise input, where the mean value is unknown within the set U.

Next, the solution of the multivariate Ornstein-Uhlenbeck process in (1) for a single input trajectory $u(t)$ is recalled,

Matthias Althoff and Martin Buss are with the Institute of Automatic Control Engineering (LSR), Technische Universität München, 80290 München, Germany. Email: {althoff,mb}@tum.de

Olaf Stursberg is with the Institute of Control and System Theory, Dept. of Electrical Eng., University of Kassel, Germany. Email: stursberg@uni-kassel.de

which is well-known as:

$$\mathcal{X}(t) = e^{At}\mathcal{X}(0) + \int_0^t e^{A(t-\tau)}u(\tau)d\tau + \int_0^t e^{A(t-\tau)}CdW, \tag{2}$$

where $\frac{dW}{dt} = \xi$ and $W(t)$ is the Wiener process which is also called Brownian motion. Due to the superposition principle of linear systems, the above solution is computed separately for $\mathcal{X}_d = e^{At}\mathcal{X}(0) + \int_0^t e^{A(t-\tau)}u(\tau)d\tau$ and $\mathcal{X}_s(t) = \int_0^t e^{A(t-\tau)}CdW$. Assuming that the initial state has a Gaussian distribution, $\mathcal{X}_d(t) = \mathcal{N}(\mu(t), \Sigma(t))$, where $\mathcal{N}(\mu, \Sigma)$ is a random variable of Gaussian distribution with expected value μ and covariance matrix Σ: $\mu_d(t) = e^{At}\mu(0) + \int_0^t e^{A(t-\tau)}u(\tau)d\tau$ and $\Sigma_d(t) = e^{At}\Sigma(0)e^{At^T}$. The random variable $\mathcal{X}_s(t) = \mathcal{N}(0, \Sigma_s(t))$ has also a Gaussian distribution as shown in [14, p. 109]:

$$\Sigma_s(t) = \int_0^t e^{A(t-\tau)}CC^T e^{A^T(t-\tau)}d\tau.$$

The integral of $\Sigma_s(t)$ can be explicitly evaluated if $AA^T = A^TA$. On that account, the system equation (1) is diagonalized by defining $x^* = Q^{-1}x$ where Q is the matrix of eigenvectors of A, such that $A^* = Q^{-1}AQ = \mathrm{diag}(\lambda)$, $C^* = Q^{-1}C$ and λ is the vector of eigenvalues. Hence, $\Sigma_s(t) = Q\Sigma_s^*(t)Q^T$ and the solution of $\Sigma_s^*(t)$ [14, p.109] is: $[\Sigma_s^*(t)]_{ij} = \frac{(C^*C^{*T})_{ij}}{\lambda_i+\lambda_j}(1 - e^{(-\lambda_i-\lambda_j)t})$.

III. Definition of Reachable Sets and Enclosing Probabilistic Hulls

For the case $C = 0$ in (1), the stochastic differential equation becomes an ordinary differential equation (ODE).

Definition 1: The exact reachable set $R^e(r)$ of (1) is defined as $R^e(r) = \{x(r)|x(t)$ is a solution of (1) $\forall t \in [0, r]$, $C = 0$, $x(0) \in X_0 \subset \mathbb{R}^n\}$. □

An over-approximated reachable set $R(r)$ is defined as $R(r) \supseteq R^e(r)$ and the over-approximated reachable set for the time interval $t \in [0, r]$ is the union of all sets $R(t)$ within $t \in [0, r]$: $R([0, r]) := \bigcup_{t\in[0,r]} R(t)$.
In the probabilistic setting ($C \neq 0$), the probability density function (PDF) at time $t = r$ of the random process $\mathcal{X}(t)$ defined by (1) for a specific trajectory $u(t) \in U$ is denoted by $f_{\mathcal{X}}(x, r)$.

Definition 2: The *enclosing probabilistic hull* (EPH) of all possible probability density functions $f_{\mathcal{X}}(x, r)$ is denoted by $\bar{f}_{\mathcal{X}}(x, r)$ and defined as: $\bar{f}_{\mathcal{X}}(x, r) = \sup\{f_{\mathcal{X}}(x, r)|\mathcal{X}(t)$ is a solution of (1) $\forall t \in [0, r]$, $u(t) \in U$, $f_{\mathcal{X}}(x, 0) = f_0\}$. □

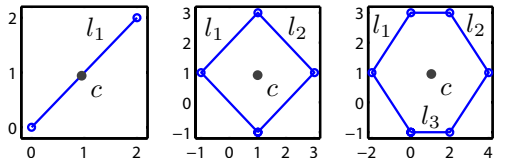
The enclosing probabilistic hull for a time interval is defined as $\bar{f}_{\mathcal{X}}(x, [0, r]) = \sup\{\bar{f}_{\mathcal{X}}(x, t)|t \in [0, r]\}$.

IV. Representation of Enclosing Probabilistic Hulls

The representation of enclosing probabilistic hulls is introduced step-by-step: First, the representation of sets with zonotopes is introduced. Next, it is shown that random variables with Gaussian distribution can be represented by probabilistic zonotopes. Finally, probabilistic zonotopes with uncertain mean are defined which are used as the representation for enclosing probabilistic hulls.
Zonotopes Z (see e.g. [13]) are sets that are defined as:

$$Z = \left\{x \in \mathbb{R}^n \middle| x = c + \sum_{i=1}^{p} \beta^{(i)}g^{(i)}, \quad -1 \leq \beta^{(i)} \leq 1\right\}$$

where $c, g^{(1)}, \ldots, g^{(p)}$ are vectors of $\mathbb{R}^n$, c is referred to as the *center* and $g^{(i)}$ are referred to as the *generators* of Z. Zonotopes are denoted by $Z = (c, g^{(1\ldots p)})$, and the order of a zonotope is $\frac{p}{n}$. A zonotope can also be seen as the Minkowski sum[1] of the finite set of line segments $l_i = [-1, 1]g^{(i)}$. This alternative definition gives a good impression of how a zonotope is built by adding the line segments, see Fig. 1.



(a) $c + l_1$ (b) $c + l_1 + l_2$ (c) $c + l_1 + l_2 + l_3$

Fig. 1. Construction of a zonotope: generators are added from left to right.

By replacing the intervals $\beta^{(i)} \in [-1, 1]$ with pairwise independent Gaussian distributed random variables $\mathcal{N}^{(i)}(0, 1)$, one can define a Gaussian zonotope with certain mean:

Definition 3 (G-Zonotope with Certain Mean): A Gaussian zonotope (G-zonotope) with certain mean is defined as a random variable $\mathcal{Z}$:

$$\mathcal{Z} = c + \sum_{i=1}^{q} \mathcal{N}^{(i)}(0, 1) \cdot \underline{g}^{(i)},$$

where $\underline{g}^{(1)}, \ldots, \underline{g}^{(q)}$ are the generators, which are underlined in order to distinguish them from generators of regular zonotopes. G-zonotopes are denoted by calligraphic letters $\mathcal{Z} = (c, \underline{g}^{(1\ldots q)})$. □

For further derivations, it is advantageous to show that G-zonotopes with certain mean have a multivariate Gaussian probability density function.

Proposition 1 (Gaussian Distribution of G-Zonotopes): The probability density function of a G-zonotope with certain mean and of order greater than one ($q > n$) can be formulated as a multivariate Gaussian distribution with

$$f_{\mathcal{Z}} = (2\pi)^{-\frac{q}{2}} \det(\Sigma)^{-\frac{1}{2}} \exp(-0.5(x - c)^T\Sigma^{-1}(x - c)),$$
$$\Sigma = \underline{G}\underline{G}^T$$

where Σ is the covariance matrix, c is the mean value and $\underline{G} = \begin{bmatrix}\underline{g}^{(1)} & \ldots & \underline{g}^{(q)}\end{bmatrix}$ is the matrix of probabilistic generators.

[1]Minkowski sum of two sets A, B: $A + B = \{a + b|a \in A, b \in B\}$; Minkowski sum is always assumed if two sets are added

Proof: Due to the independence of the random variables $\mathcal{N}^{(i)}$ of the generators, the joint distribution is computed as the product of the PDFs of each random variable:

$$f_{\mathcal{N}}^{(1\dots q)}(y) := \prod_{l=1}^{q} f_{\mathcal{N}}^{(l)} = \prod_{l=1}^{q} (\sqrt{2\pi})^{-1} \exp(-0.5{y^{(l)}}^2) \\ \stackrel{!}{=} (2\pi)^{-\frac{q}{2}} \det(\Sigma)^{-\frac{1}{2}} \exp(-0.5 y^T \Sigma^{-1} y), \tag{3}$$

from which follows that $\Sigma = I$ and I is the identity matrix. Next, the random variables $\mathcal{N}^{(i)}$ of the generators are mapped to the random vector $\mathcal{Z}$ of the zonotope: $\mathcal{Z} = c + \underline{G}\mathcal{N}$ and $\mathcal{N} = \begin{bmatrix}\mathcal{N}^{(1)} & \dots & \mathcal{N}^{(q)}\end{bmatrix}^T$, such that $\mu^* = c$ and $\Sigma^* = \underline{G}\underline{G}^T$ which follows from the addition and multiplication rule of random variables with Gaussian distribution. ■

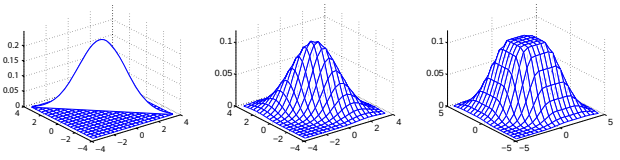
In order to represent enclosing probabilistic hulls $\bar{f}_{\mathcal{X}}$, the multivariate Gaussian distribution is extended by an uncertain mean as mentioned before:

Definition 4 (G-Zonotope with Uncertain Mean): A G-zonotope with uncertain mean, denoted by $\mathscr{Z}$, is defined as a G-zonotope $\mathcal{Z}$, where the center is uncertain and can have any value within a zonotope Z, which is denoted by:

$$\mathscr{Z} := Z \boxplus \mathcal{Z}, \quad Z = (c, g^{(1\dots p)}),\ \mathcal{Z} = (0, \underline{g}^{(1\dots q)}).$$

G-zonotopes with uncertain mean are also denoted by $\mathscr{Z} = (c, g^{(1\dots p)}, \underline{g}^{(1\dots q)})$. If the probabilistic generators can be represented by the covariance matrix Σ ($q > n$), one can also write $\mathscr{Z} = (c, g^{(1\dots p)}, \Sigma)$. □

As $\mathscr{Z}$ is neither a set nor a random vector, there does not exist a probability density function describing $\mathscr{Z}$. However, one can obtain an enclosing probabilistic hull which is similarly defined as in Def. 2: $\bar{f}_{\mathscr{Z}} = \sup\left\{f_{\mathcal{Z}} \middle| E[\mathcal{Z}] \in Z\right\}$, where $E[\,]$ returns the expectation and Z, $\mathcal{Z}$, $\mathscr{Z}$ are defined as in Def. 4. Combinations of sets with random vectors have also been investigated, e.g. in [15], [16]. Analogously to a zonotope, it is shown in Fig. 2 how the enclosing probabilistic hull (EPH) of a G-zonotope with two non-probabilistic and two probabilistic generators is built step-by-step from left to right.



(a) PDF of $(0, \underline{g}^{(1)})$. (b) PDF of $(0, \underline{g}^{(1,2)})$. (c) EPH of $(0, g^{(1\dots 2)}, \underline{g}^{(1\dots 2)})$.

Fig. 2. Construction of a G-zonotope.

V. Operations on Stochastic Sets

The use of zonotopes is motivated by the fact that they are closed under Minkowski addition and linear transformation [13]. Given are two zonotopes $Z_1 = (c_1, g^{(1\dots p)})$, $Z_2 = (c_2, h^{(1\dots q)})$ and a matrix $L \in \mathbb{R}^{n\times n}$. It follows that $Z_1 + Z_2 = (c_1 + c_2, g^{(1\dots p)}, h^{(1\dots q)})$ and $LZ_1 = (Lc_1, Lg^{(1\dots p)})$. The multiplication rule is trivial and the addition rule follows from the fact that a zonotope is defined as the Minkowski addition of generators. The addition of a G-zonotope $\mathscr{Z}_1 = (c_1, g^{(1\dots p)}, \Sigma_1)$ with another G-zonotope $\mathscr{Z}_2 = (c_2, h^{(1\dots q)}, \Sigma_2)$ and the linear map is:

$$\mathscr{Z}_1 + \mathscr{Z}_2 = (c_1 + c_2, g^{(1\dots p)}, h^{(1\dots q)}, \Sigma_1 + \Sigma_2) \\ L\mathscr{Z}_1 = (Lc, Lg^{(1\dots p)}, L\Sigma_1 L^T), \tag{4}$$

where the addition and the multiplication rule of zonotopes and random variables with Gaussian distribution have been applied. An operator that needs to be defined for further computations, is the confidence set operator:

Proposition 2 (Confidence set operator): The confidence set operator $\eta(\mathcal{Z}, m)$ transforms a zero-mean G-zonotope $\mathcal{Z}$ with n ($\hat{=}$ system dimension) probabilistic generators to a zonotope Z whose generators are a multiple of the probabilistic generators:

$$\eta(\mathcal{Z}, m) = (0, g^{(1\dots n)}), \quad g^{(i)} = m \cdot \underline{g}^{(i)},\ m \in \mathbb{R}^+. \tag{5}$$

The choice of n generators is no loss of generality as they can represent arbitrary multivariate Gaussian distributions, see Prop. 1. The obtained set encloses realizations of $\mathcal{Z}$ by a probability of $\mathrm{erf}(\frac{m}{\sqrt{2}})^n$ where $\mathrm{erf}()$ is the error function.

Proof: The probability $P[-m < \mathcal{N}(0,1) < m] = \mathrm{erf}(\frac{m}{\sqrt{2}})$ is well known. Choosing n generators, the event that a value lies in the set spanned by them is $\mathrm{erf}(\frac{m}{\sqrt{2}})^n$. ■

The confidence set operator of a stochastic zonotope with uncertain mean is defined as $\eta(\mathscr{Z}, m) := Z + \eta(\mathcal{Z}, m)$. A special confidence set is the γ-confidence set ($m = \gamma$). Computations for states outside the γ-confidence set in $\Psi = \mathbb{R}^n \backslash \eta(\mathscr{Z}, \gamma)$ are not regarded for enclosing probabilistic hull computations. Instead of computing with probability distributions within Ψ, only the probability that a state is in Ψ is preserved, as shown later ($\int_\Psi f_{\mathscr{Z}} dx = 1 - \mathrm{erf}(\frac{\gamma}{\sqrt{2}})^n$).

VI. Computation of Enclosing Probabilistic Hulls

First, a procedure for computing reachable sets is recalled, which is then adopted for the computation of enclosing probabilistic hulls. The presented basic steps are applied in many algorithms (e.g. [12], [11], [13], [17]) in order to compute the reachable set for a time interval $t \in [0, r]$:

1) Computation of the reachable set $\hat{R}(r)$ at time $t = r$ without input.
2) Generation of an enclosing hull $\mathcal{EH}(R(0), \hat{R}(r))$, where $\mathcal{EH}()$ is the enclosing hull operator.
3) Enlargement of the enclosing hull to enclose all trajectories under the specified disturbances for the time interval $t \in [0, r]$.

These basic steps are illustrated in Fig. 3. In the following, the steps (1) to (3) are discussed for the probabilistic setting.

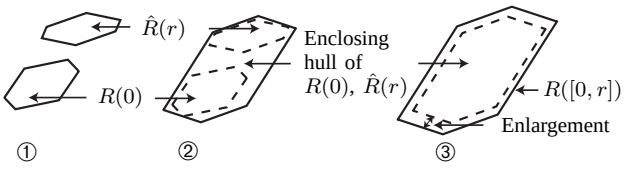


Fig. 3. Computation of reachable sets - overview.

A. Time Interval Solution without Input

For a linear system (1), the reachable set without input is computed for the time $t = r$ by:

$$\mathscr{R}(r) = e^{Ar}\mathscr{R}(0).$$

The time interval solution for the enclosing probabilistic hull is a more complicated issue. The problem is approached by separating computations for sets and probability density functions, which is realized by splitting up the G-zonotopes with uncertain mean $\mathscr{R}$ into zonotopes R and G-zonotopes with zero mean $\mathcal{R}$.
In a first step, the evolution of the PDF value of a point after a linear mapping is investigated:

Proposition 3 (PDF-value evolution of a point): The change of a PDF value for a point by a factor $e^{-\mathrm{tr}(A)t}$ due to a mapping e^{At} is given by :

$$f_{\mathcal{R}}(x',t) = e^{-\mathrm{tr}(A)t} f_{\mathcal{R}}(x,0), \quad x' = e^{At}x,$$

where $\mathrm{tr}()$ is the trace of a matrix.

Proof: Given is an infinitesimal parallelotope (zonotope of order one) which is spanned by generators of the generator matrix $\underline{G}$. The volume of a parallelotope can be computed by the determinant of the generators: $V = 2^n \det(\underline{G})$. After the mapping by e^{At}, the volume is obtained as $V' = 2^n \det(e^{At}\underline{G}) = 2^n \det(e^{At}) \det(\underline{G})$. The ratio of the value of the probability density function before and after the mapping is determined by the ratio of the volumes of the infinitesimal parallelotopes, see e.g. [18, p. 145]: $\frac{f_{\mathcal{R}}(x',t)}{f_{\mathcal{R}}(x,0)} = \frac{V}{V'} = \frac{1}{\det(e^{At})}$. Furthermore, it is well known that $\det(e^{At}) = e^{\mathrm{tr}(At)}$ such that $\det(e^{At})^{-1} = e^{-\mathrm{tr}(A)t}$. ■

From the monotonicity of $e^{-\mathrm{tr}(A)t}$ it follows that the PDF values have a maximum for $t = 0$ or $t = r$ if $t \in [0, r]$. The idea for the computation of an enclosing probabilistic hull is the following: Pick the probability distribution for the time point where the PDF-values have a maximum, and assume this PDF for the whole time interval $t \in [0, r]$. Additionally, compute a set ΔR in which each point is uncertain within $t \in [0, r]$. By taking the maximum PDF-values within the considered time interval and by adding the uncertainty ΔR, an enclosing probabilistic hull is generated. In order to obtain a bounded set ΔR, the computation is restricted to the states originating from the γ-confidence set.
In [17], where the reachability of non-stochastic linear systems with uncertain parameters has been investigated, the following over-approximation has been introduced:

$$\Delta x(t) = x(t) - x(0) \subseteq \frac{t}{r}(e^{Ar} - I + F)x(0),\ \forall t \in [0, r].$$

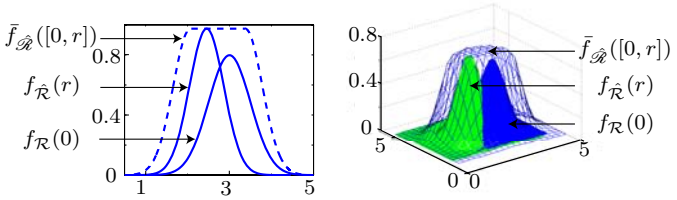
By substituting $x(0)$ with $\eta(\mathcal{R}(0), \gamma)$, one obtains

$$\Delta R = (e^{Ar} - I + F)\eta(\mathcal{R}(0), \gamma), \tag{6}$$

which contains all variations $\Delta x(t) = x(t) - x(0)\ \forall t \in [0, r]$, such that $\eta(\mathcal{R}([0, r]), \gamma) \subseteq \eta(\mathcal{R}(0), \gamma) + \Delta R$. For details on the computation of F, the interested reader is referred to [17]. Equation (6) and Prop. 3 allow to formalize the aforementioned idea for an enclosing probabilistic hull $\hat{\mathscr{R}}^*([0, r])$ starting in $\mathcal{R}(0)$ without input ($u = 0$):

$$\hat{\mathscr{R}}^*([0,r]) = \Delta R \boxplus \mathcal{R}^* \text{ for } x(0) \in \eta(\mathcal{R}(0), \gamma),$$
$$\Delta R = (e^{Ar} - I + F)\eta(\mathcal{R}(0), \gamma),$$
$$\mathcal{R}^* = \begin{cases} \mathcal{R}(0), & \text{if } \mathrm{tr}(A) > 0 \\ \mathcal{R}(r), & \text{otherwise.} \end{cases}$$

The reachable set $R([0, r])$ for the non-probabilistic case is computed from $R(0)$ as shown in [17]. Due to the superposition principle, the overall G-zonotope without input is $\hat{\mathscr{R}}([0, r]) = R([0, r]) \boxplus \hat{\mathscr{R}}^*([0, r])$.
Numerical examples for the computation of $\bar{f}_{\hat{\mathscr{R}}}([0, r])$ can be found in Fig. 4 for a one- and two dimensional-case. For time intervals $[kr, (k + 1)r]$, $k \in \mathbb{N}^+$, the G-zonotope is computed as $\hat{\mathscr{R}}([kr, (k + 1)r]) = e^{Akr}\hat{\mathscr{R}}([0, r])$.



(a) One dimensional example. (b) Two dimensional example.

Fig. 4. Enclosure of two Gaussian distributions.

B. Time Interval Solution with Input

Due to the superposition principle of linear systems, the G-zonotope $\bar{\mathscr{R}}([kr, (k+1)r])$ due to the input can be computed separately. It is first shown that the input solution $\bar{\mathscr{R}}([kr, (k+1)r]$ for general time intervals $t \in [kr, (k + 1)r]$ can be computed based on a single time interval solution for $t \in [0, r]$ combined with the solution for $t = kr$.

Proposition 4 (Input solution): The enclosing probabilistic hull $\bar{\mathscr{R}}([kr, (k + 1)r]$ due to input $v = u + C\xi$ can be computed as $\bar{\mathscr{R}}([kr, (k + 1)r]) = e^{A\cdot kr}\bar{\mathscr{R}}([0, r]) + \bar{\mathscr{R}}(kr)$

Proof: The input solution in (2) due to the input $v = u + C\xi$, can be reformulated as $x_s((k + 1)r) = e^{A\cdot kr}\int_0^r e^{A(r-\tau)}v(\tau)d\tau + \int_r^{(k+1)r} e^{A((k+1)r-\tau)}v(\tau)d\tau = e^{A\cdot kr}x_s(r) + x_s(kr)$. ■

The G-zonotope $\bar{\mathscr{R}}([0, r])$ is over-approximated using the γ-confidence set $\eta(\bar{\mathscr{R}}([0, r]), \gamma)$. Without loss of generality, one can assume that the set of possible inputs $u \in U$ contains the origin, such that the origin is element of $\eta(\bar{\mathscr{R}}(t), \gamma)$, $\forall t$. In case, that U does not contain the origin, one can add an artificial input $\tilde{u}$, such that $v = u + \tilde{u} + C\xi$ and $0 \in U$. The solution of the constant input $\tilde{u}$ can be separately obtained

and added to the reachable set. As the origin is element of $\eta(\bar{\mathscr{R}}(t),\gamma)$, $\forall t$, the reachable set $\eta(\bar{\mathscr{R}}([0,r]),\gamma)$ is growing from the origin, such that the reachable set for $t \in [0,r]$ equals the reachable set at $t = r$, and the input solution can be over-approximated by:

$$\eta(\bar{\mathscr{R}}([0,r]),\gamma) = \eta(\bar{\mathscr{R}}(r),\gamma) = \bar{R}(r) + \eta(\bar{\mathcal{R}}(r),\gamma).$$

The reachable set $\bar{R}(r)$ for $u \in U$ is obtained as presented in [17] and the covariance matrix $\Sigma_s(r)$ of the G-zonotope $\bar{\mathcal{R}}(r) = (0, \Sigma_s(r))$ is computed as shown in Sec. II. Using the obtained results, Alg. 1 for the computation of enclosing probabilistic hulls of h time intervals, can be formulated:

Algorithm 1 Compute $\mathscr{R}$.

Input: $\hat{\mathscr{R}}([0,r])$, $\bar{R}(r)$, $\bar{\mathcal{R}}(r)$ and γ
Output: $\mathscr{R}([kr,(k+1)r])$
  $\bar{\mathscr{R}}(r) = \bar{R}(r) \boxplus \bar{\mathcal{R}}(r)$
  $\mathscr{R}([0,r]) = \hat{\mathscr{R}}([0,r]) + \eta(\bar{\mathscr{R}}(r),\gamma)$
  for $k = 1 \ldots \zeta$ **do**
    $\mathscr{R}([kr,(k+1)r]) = e^{Ar}\mathscr{R}([(k-1)r,kr]) + \bar{\mathscr{R}}(r)$
  end for

C. Probability of Entering an Unsafe Set

The enclosing probabilistic hulls allow to compute the probability that the system state is in an unsafe set within a certain time interval. The over-approximated probability $\bar{p}([kr,(k+1)r])$ of hitting an unsafe set B, which is over-approximated by a polytope B, is computed in general as:

$$\bar{p}([kr,(k+1)r]) = \int_B \bar{f}_{\mathscr{R}}([kr,(k+1)r])dx.$$

In order to be able to efficiently over-approximate the above integral, the enclosing probabilistic hulls are over-approximated by polytopes, see Fig. 5. This is done by computing the maximum values $h_1^{max}, h_2^{max}, \ldots$ of the enclosing probabilistic hulls for corresponding confidence regions $Q_1 = \eta(\mathscr{R},\gamma)\backslash\eta(\mathscr{R},m_1)$, $Q_2 = \eta(\mathscr{R},m_1)\backslash\eta(\mathscr{R},m_2), \ldots$ and $\gamma > m_1 > m_2 > \ldots > 0$, see Fig. 5.

The enclosure by polytopes P_i allows to compute an over-approximated probability for entering the unsafe set B. The probabilities outside the γ-confidence set are considered with the probability $1 - \mathrm{erf}(\frac{\gamma}{\sqrt{2}})^{2n}$ which is squared in contrast to Prop. 2 in order to account for the homogeneous and the particulate solution:

$$\bar{p} = 1 - \mathrm{erf}(\frac{\gamma}{\sqrt{2}})^{2n} + \sum_i V(Q_i \cap B), \qquad (7)$$

where $V()$ is an operator that returns the volume of a geometric object.

D. Extension for non-Gaussian and (Un-)Bounded Probabilistic Initial Sets and Inputs

The presented approach can be extended to non-Gaussian initial sets and white non-Gaussian noise by enclosing them with enclosing probabilistic hulls $\bar{\mathscr{R}}(0)$ and $\bar{\mathscr{R}}(r)$, see Fig. 6. Additionally, if the sets N of non-zero PDF-values are bounded and lie within γ-confidence sets (see Fig. 6), it is possible to guarantee the safety of a system ($N \subseteq \gamma$-set for initial state and the disturbance). In this case, the exact PDF-values are only non-zero within the γ-confidence set of the reachable sets as these are invariant sets. From this follows that the probability of hitting an unsafe set according to (7) changes to $\bar{p} = \sum_i V(Q_i \cap B)$ which is possibly 0.

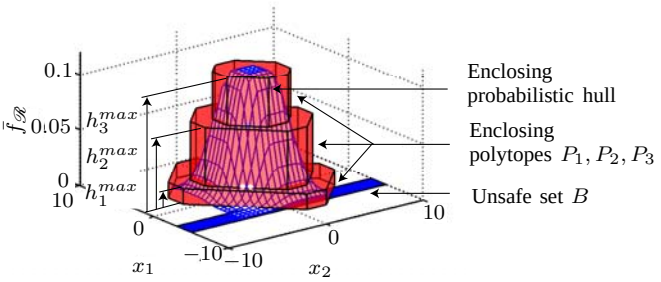


Fig. 5. Over-approximation of a prob. zonotopes by piecewise uniform distributions.

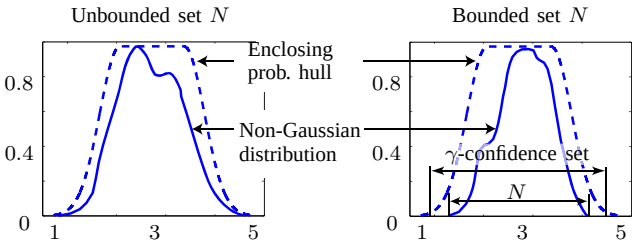


Fig. 6. Enclosure of non-Gaussian distributions.

VII. Numerical Examples

For the illustration of the presented techniques, the examples in [13] are enhanced with white noise. The first example is two dimensional:

$$\dot{x} = \begin{bmatrix} -1 & -4 \\ 4 & -1 \end{bmatrix} x + \begin{bmatrix} [-0.01, 0.01] \\ [-0.01, 0.01] \end{bmatrix} + \begin{bmatrix} 0.7 & 0 \\ 0 & 0.7 \end{bmatrix} \xi.$$

Several simulations with the specified distribution of initial values are illustrated in Fig. 7(a). The corresponding enclosing probabilistic hulls $\bar{f}_{\mathscr{R}}([kr,(k+1)r])$ are plotted in Fig. 7(b) for $k = 1 \ldots 250$, where the sampling time is chosen to $r = 0.01$. Note that the values of $\bar{f}_{\mathscr{R}}([kr,(k+1)r])$ are visualized by the colorbar on top of the plot.
The second example is of dimension 5, and with a system matrix as specified in [13]:

$$\dot{x} = Ax + u + 0.5 \cdot I \cdot \xi,$$

$$A = \begin{bmatrix} -1 & -4 & 0 & 0 & 0 \\ 4 & -1 & 0 & 0 & 0 \\ 0 & 0 & -3 & 1 & 0 \\ 0 & 0 & -1 & -3 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{bmatrix}, \quad u \in U = \begin{bmatrix} [-0.1, 0.1] \\ \vdots \\ [-0.1, 0.1] \end{bmatrix}^T.$$

The projections ($\mathscr{R}' = P\mathscr{R}$, $P \in \mathbb{R}^{2\times n}$) of the enclosing probabilistic hulls for a sampling time of $r = 0.04$ are presented in Fig. 8 together with the unsafe set $x_2 < -1.5$. The over-approximated probability that the state is in an

unsafe set, is shown in Fig. 9 for time points and time intervals and also for different time step sizes, such that the over-approximation due to the enclosure of probability distributions for time intervals can be seen.
Additionally, G-zonotopes $\mathscr{R}([kr,(k+1)r])$ for 500 time intervals for higher order systems with randomly generated matrices A and C have been computed (the order of zonotopes has been limited to 5). The computation times are presented in the table below and are obtained by a desktop computer (3.7 GHz) in Matlab.

Dimension n	5	10	20	50	100
CPU-time [sec]	0.72	1.29	2.61	8.97	29.1

VIII. Conclusion

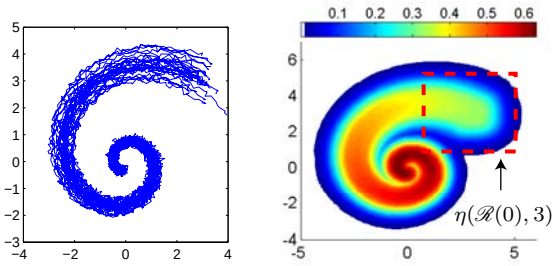
The computation of enclosing probabilistic hulls for linear stochastic differential equations with white noise and uncertain inputs has been presented for high dimensional systems. The combination of Gaussian noise with uncertainties specified by sets allows to over-approximate the probability of entering unsafe sets for non-Gaussian initial distributions and non-Gaussian white noise. For the extension to nonlinear or hybrid systems, one would have to apply a Gaussian-mixture approach for which the underlying algorithms could benefit from the results presented here.

Acknowledgements

The authors gratefully acknowledge partial financial support by the Deutsche Forschungsgemeinschaft (German Research Foundation) within the Transregional Collaborative Research Centre 28 *Cognitive Automobiles*.

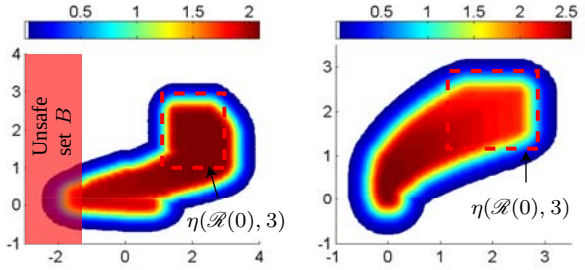
References

[1] J. Hu, M. Prandini, and S. Sastry, "Aircraft conflict detection in presence of a spatially correlated wind field," *IEEE Transactions on Intelligent Transportation Systems*, vol. 6, pp. 326–340, 2005.
[2] M. Althoff, O. Stursberg, and M. Buss, "Stochastic reachable sets of interacting traffic participants," in *Proc. of the IEEE Intelligent Vehicles Symposium*, 2008, pp. 1086–1092.
[3] R. Rubinstein, *Simulation and the Monte Carlo Method*. Wiley & Sons, 2007.
[4] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, vol. 52, pp. 1415–1428, 2007.
[5] M. Prandini and J. Hu, *Stochastic hybrid systems*. Taylor & Francis Group/CRC Press, 2006, ch. Stochastic reachability: Theoretical foundations and numerical approximation., pp. 107–138.



(a) Simulation examples. (b) Enclosing probabilistic hulls.

Fig. 7. Simulation and enclosing probabilistic hulls of the two-dim. system.



(a) Projection on x_2, x_3. (b) Projection on x_4, x_5.

Fig. 8. Enclosing probabilistic hulls of the five dimensional system.

[6] ——, *Stochastic hybrid systems: theory and safety critical applications*. Springer, 2006, ch. A stochastic approximation method for reachability computations, pp. 107–139.
[7] X. Koutsoukos and D. Riley, "Computational methods for reachability analysis of stochastic hybrid systems," in *Hybrid Systems: Computation and Control*, ser. LNCS 3927. Springer, 2006, pp. 377–391.
[8] A. Abate, S. Amin, M. Prandini, J. Lygeros, and S. Sastry, "Computational approaches to reachability analysis of stochastic hybrid systems," in *Hybrid Systems: Computation and Control*, ser. LNCS 4416. Springer, 2007, pp. 4–17.
[9] F. M. Schlaepfer and F. C. Schweppe, "Continuous-time state estimation under disturbances bounded by convex sets," *IEEE Transactions on Automatic Control*, vol. 17, pp. 197–205, 1972.
[10] A. B. Kurzhanski and P. Varaiya, "Ellipsoidal techniques for reachability analysis," in *Hybrid Systems: Computation and Control*, ser. LNCS 1790. Springer, 2000, pp. 202–214.
[11] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," in *IEEE Transactions on Automatic Control*, vol. 48, no. 1, 2003, pp. 64–75.
[12] O. Stursberg and B. H. Krogh, "Efficient representation and computation of reachable sets for hybrid systems," in *Hybrid Systems: Computation and Control*, ser. LNCS 2623. Springer, 2003, pp. 482–497.
[13] A. Girard, "Reachability of uncertain linear systems using zonotopes," in *Hybrid Systems: Computation and Control*, ser. LNCS 3414. Springer, 2005, pp. 291–305.
[14] C. W. Gardiner, *Handbook of Stochastic Methods*, H. Haken, Ed. Springer, 1983.
[15] D. Berleant, "Automatically verified reasoning with both intervals and probability density functions," *Interval Computations*, vol. 2, pp. 48–70, 1993.
[16] D. Berleant and C. Goodman-Strauss, "Bounding the results of arithmetic operations on random variables of unknown dependency using intervals," *Reliable Computing*, vol. 4, pp. 147–165, 1998.
[17] M. Althoff, O. Stursberg, and M. Buss, "Reachability analysis of linear systems with uncertain parameters and inputs," in *Proc. of the 46th IEEE Conference on Decision and Control*, 2007, pp. 726–732.
[18] H. Stark and J. Woods, *Probability, Random Processes, and Estimation Theory for Engineers*. Prentice Hall, 1994.

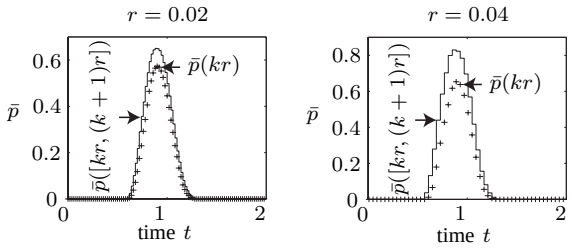


Fig. 9. Over-approximated probability that the state enters the unsafe set: time interval and time point solution.