Verification of Gaussian Processes

Andrea Patane

Motivation:

- Widely used in safety critical applications
- Need to incorperate the uncertainty of probabalistic models into safety analysis

⊛ No method exists for this yet (contribution)

Background:

Prior Distribution

$f \sim GP$

{distribution over function space}

Conditioned model

$f \sim GP | x$

[We keep only the functions from the prior that justify the data.]

Important Note, the posterior can be done analytically, not the case in Bayesian Deep learning.

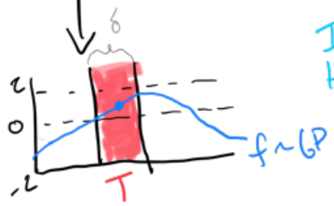
Problem Formulation:

Probabalistic Invariance
(local robustness)

$$\phi(x^*, T, \delta) :=$$

$$P(\exists x' \in T \text{ s.t. } \|z(x') - z(x^*)\| > \delta)$$

Does the change for x^* to x' induce a large change in the output of the GP?



Intuition for ϕ:
How many 'f' are safe according to the defined bounds

Methods:

- Computing via sampling is not tractable so we want a formal way to get values for ϕ

  [Note: you can do kind of formal things for intractable case.]

I have left the proof sketch for the slides

Experiments:

Because Neural Nets with single layer and infinite width gives a GP, we can use this method to gain some insights about how neural nets may behave with respect to ϕ

Main insight for Neural nets is that variance changes very slowly as the "depth" of the neural network grows.

[see last slide].