Pulina团队的文章概述

2010 【An abstraction-refinement approach to verification of artificial neural networks】

2012 【Challenging SMT solvers to verify neural networks】被Reluplex多次引用[30]

2018 【Automated verification of neural networks: Advances, challenges and perspectives】

2019 【Verification and repair of neural networks: a progress report on convolutional models】

2020 【Verification of Neural Networks: Enhancing Scalability through Pruning】

1. Challenging SMT solvers to verify neural networks

摘要：本文评估了当前先进的SMT求解器在应对MLP验证的问题。验证技术的成熟与否是MLP是否能被应用在安全相关应用的关键，在先前的贡献中，我们已经证明了MLP的安全问题可以使用求解线性算术约束来解决（文中没有提到是哪篇文章证明的，我对这个还比较感兴趣）。然而MLP生成的encoding对于目前最先进的SMTsolver来说依然是复杂的。因此，在此提出的试验结果是为了向社区提出一个开放挑战和愿景。（所以这里只是做了一下试验，证明目前的solver性能不够，从而希望有人一起搞这件事？）

上面提到他们证明了神经网络的验证，至少是MLP，是可以用SMT解决的。可能涉及这个的文章有：第五篇文献Neural networks and their applications，第20、21篇文献。第20篇文献介绍了证明全局安全，第21篇文章证明局部安全。