Sujet de stage au laboratoire Heudiasyc UMR 7253 :

Titre/Title	NN verification through constrained programing
Encadrant(s) / Supervisor(s)	A. Jouglet,
Descriptif du sujet/ Project description	Altough neural networks (NNs) are more and more widespread and fashionable, they present several issues in safety- and security-critical scenarios. Verification of NNs is the effort to prove algorithmically the correctness of some of their behaviours. The main weakness NNs are subject to are called "adversiarial examples": slightly modified versions of inputs that produce correct results, which result in erroneous ones. The most common property that NNs are required to comply to is therefore robustness, i.e., the capability of maintaining their correct behaviour when the input is subject to some noise. Abstraction-based verification techniques aim to model the network behavior on a generalised set of inputs, such that it is possible to study the transformations occurring in the network layers. Exact and approximate models have been proposed and evaluated in the literature, but the main drawback they are subject to is the curse of dimensionality: the large number of parameters that define a NN often leads to intractability. Constraint-based techniques appear to be the most suitable to treat this problem, as the structure of the problem is incremental. The goal of this internship is to develop an exact model for NN verfication. In other words, we need to check that for some input, the NN transformation leads to a valid result. A first exact model is formulated as an Integer linear programming and a second one is based on constrained programming. The work to be done consists in writting these models and test them for realistics instances. A special focus will be put on the constrained programming method.
Pré-requis	Knowledge on IA and Optimisation.
Possibilité de poursuite en thèse/ Possibility of continuing in PhD	Possibly

Cette fiche doit être renvoyée à Séverine Paprzycki