Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Topological analysis of decision boundaries

Practical work

Maxim Mikhaylov

January 30, 2025

Supervisors: Prof. Dr. B. Gärtner, Dr. P. Schnider
Department of Computer Science, ETH Zürich

Abstract

This project investigates the application of topological data analysis (TDA) to the study of decision boundaries in machine learning classifiers. Decision boundaries partition the input space into regions corresponding to different class labels, and understanding their topology can provide deep insights into model behavior, particularly regarding overfitting and underfitting. Building upon the Labeled Vietoris-Rips complex framework, which was previously limited to binary classification, we extend it to handle multiclass classification problems.

Contents

Chapter 1

Introduction

1.1 Background

- ML is cool
- TDA is cool
- Decision boundaries are cool
- Why the intersection of these three may be cool

1.2 Objectives

Yoink from the proposal.

- Explore homological changes in decision boundaries during model training.
- Investigate connections between topological features and overfitting/underfitting.
- Extend the Labeled Vietoris-Rips complex to multiclass classification.

Chapter 2

Related work and theoretical background

2.1 Related work

Look at the review paper for this.

Do we need the theoretical background?

2.2 Theoretical background

2.2.1 Decision boundaries in machine learning

2.2.2 Topological data analysis

2.2.3 Persistent homology

2.2.4 Labeled Vietoris-Rips complex

2.2.5 Dowker complex

Chapter 3

Methodology

3.1 Datasets and models

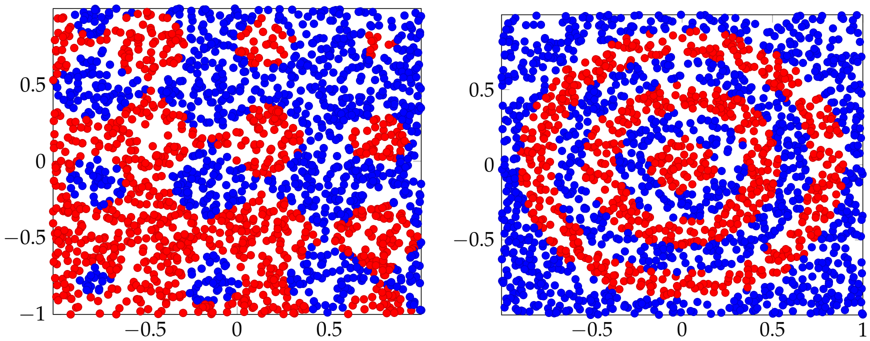
For evaulation we have used the MNIST [1] and FashionMNIST [2] datasets with the predefined training and testing splits. We have also used synthetic 2D and 3D binary classification datasets for more easily interpretable experiments. They are shown in Figures 3.1 and **??**. with each dataset consisting of 10000 points, uniformly sampled from $[-1, 1]^2$ and split into training and testing sets with a ratio of 0.8 : 0.2.

TODO: Maybe drop 3D

TODO: Describe model for 2D/3D if we need that

For MNIST and FashionMNIST, we have used:

1. A simple feed-forward neural network with layer sizes $784, 512, 128, 16, 10$, ReLU activations and a softmax output layer.
2. A convolutional neural network with a modification of the architecture given in https://github.com/pytorch/examples/tree/main/mnist. The modifications are:
   a) Addition of the `scale` parameter, which allows us to change the neural network width. It is a multiplicative factor for the number of channels in the convolutional layers and number of neurons in the fully connected layers.
   b) Addition of the `extra_cnn` parameter, which adds convolutional layers with $64 \cdot$ `scale` channels, 3×3 kernel size, 1 pixel padding and stride, as well as a ReLU activation.
   c) Additon of the `extra_linear` parameter, which similarly adds a fully connected layer with $128 \cdot$ `scale` neurons, as well as a ReLU activation.



(a) Many holes dataset **(b)** Nested annuli dataset

Figure 3.1: Synthetic 2D datasets

3.2 Metrics and evaluation

- Persistence diagrams
- Wasserstein distance
- Total bar length

Definition 3.1 *A* persistence diagram *is a multiset of points in* $\mathbb{R}^2$. *TODO: finish*

Definition 3.2 *The* Wasserstein distance *between two persistence diagrams* D_1 *and* D_2 *is defined as TODO: finish*

Definition 3.3 *The* total bar length *of a persistence diagram* D *is defined as*

$$\sum_{(b,d)\in D} d - b$$

3.3 Simplicial complex

- Labeled Vietoris-Rips complex
- Usage of `ripser++` and `giotto-ph`
- Generalization to multiclass classification
- Circumcircle filtering (show why it's needed in 2D, but not in high-dim)
- Dowker complex

Chapter 4

Results and discussion

4.1 Sampling stability on MNIST

Show that with the default parameters, the persistence diagrams change too much under sampling. Show it's stable under N=10.

4.2 Synthetic 2D and 3D data experiments

- Describe the data (or do it in the methodology?)
- Show what isn't captured correctly
- Show that CC filtering or the Dowker complex can help

4.3 Results on MNIST

- Accuracy of the model correlates with the Wasserstein distance and the total bar length
- "Elbow" behavior — first epochs have high changes in topological metrics, then it's flatter. Probably easier to show for Wasserstein distance, as the total bar length may be both high and low. Alternatively, show the difference between total bar length and GT total bar length.
- Underfitting and overfitting leads to worse topological metrics
- More accurate models have better topological metrics
- Size of the model doesn't impact the topological metrics (as long as the accuracy is the same for them)

4.4 Results on FashionMNIST

Hopefully, just show it's the same.

4.5 Results on multiclass classification

Show it's the same (?)

4.6 Comparison of CNN and MLP

If there's anything interesting

Appendix A

Dummy Appendix

You can defer lengthy calculations that would otherwise only interrupt the flow of your thesis to an appendix.

Bibliography

[1] Li Deng. The mnist database of handwritten digit images for machine learning research. *IEEE Signal Processing Magazine*, 29(6):141–142, 2012.

[2] Han Xiao, Kashif Rasul, and Roland Vollgraf. Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms, 2017.

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every semester paper, Bachelor's thesis, Master's thesis and any other degree paper undertaken during the course of studies, including the respective electronic versions.

Lecturers may also require a declaration of originality for other written papers compiled for their courses.

I hereby confirm that I am the sole author of the written work here enclosed and that I have compiled it in my own words. Parts excepted are corrections of form and content by the supervisor.

Title of work (in block letters):

Authored by (in block letters):
For papers written by groups the names of all authors are required.

Name(s): **First name(s):**

With my signature I confirm that
- I have committed none of the forms of plagiarism described in the 'Citation etiquette' information sheet.
- I have documented all methods, data and processes truthfully.
- I have not manipulated any data.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for plagiarism.

Place, date **Signature(s)**

For papers written by groups the names of all authors are required. Their signatures collectively guarantee the entire content of the written paper.