Machine Learning Techniques for Class Imbalances & Adversaries

Brendan Herger
Brendan.Herger@capitalone.com
Man, I suck at this game. Can you give me a few pointers?

I hate you.

0x3A28213A
0x6339392C,
0x7363682E.
Overview

Sampling
Feature Engineering
Modeling
Sampling
Observation Weighting

- Effect cost function by weighting every row at train time
- Some weights become features at predict time
- Weights include
  - Uniform weight
  - Observation age (staleness)
  - Random down-sampling
Observation Weighting

Weights

- Uniform Weight
- Decay Weight
SMOTE

• (Synthetic Minority Over-sampling Technique)

• Goal: Reduce effect of class imbalance

• Majority class: Down sample, with some probability

• Minority class: Create ‘synthetic’ observations

SMOTE

1. Select minority point
2. Select neighbor
3. Create new point

SMOTE

1. Select minority point
2. Select neighbor
3. Create new point

SMOTE

1. Select minority point
2. Select neighbor
3. Create new point

SMOTE

1. Select minority point
2. Select neighbor
3. Create new point

Observation Weighting
SMOTE Sampling
Features
Outlier Detection

- Goal: Create outlier score
- Train learner to re-create input vector
  - PCA: Reduce dimensionality, increase dimensionality
  - Neural Network: Train auto-encoder
- Measure distance from output vector to input vector

https://github.com/h2oai/h2o-training-book/blob/master/hands-on_training/anomaly_detection.md
Outlier Detection

Outlier score: $|X' - X|$
Label Propagation

• Goal: Identify networks of bad-actors

• Create graph (Nodes = actors, Edges = association strength)

• Label nodes (e.g. good actor or bad actor)

• ‘Relax’ labels through graph

Label Propagation

Low Rank Models

• Goal: Reduce dimensionality for dataset with many variables
• Reduce dimensionality with generalized PCA
• Model directly on components (latent factors)

https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md
Low Rank Models

https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md
LDA Topic modeling

• Goal: Reduce dimensionality for variable with many levels
• Method stolen from Natural Language Processing
• Create bags of words w/ maximum separation
• Identify new text by which bag of words was most likely to create it

LDA Topic modeling

Outlier Detection
Label Propagation
GLRM
LDA Topic Modeling
Modeling
Grid search

- Goal: Find optimal hyper-parameters for given class of models
- Create every possible permutation of hyper-parameters, and compute models until heat death of universe

https://github.com/h2oai/h2o-3/blob/master/h2o-docs/src/product/tutorials/GridSearch.md
Neural Networks

- See other talks
- Too complicated to cover here

https://github.com/h2oai/h2o-3/blob/master/h2o-docs/src/product/tutorials/GridSearch.md
Ensemble Modeling

- Goal: Leverage a diverse set of algorithms

- Train multiple classes of algorithms (tree based, linear, neural network), possibly with multiple hyper-parameters, combine scores with meta model

https://github.com/h2oai/h2o-3/blob/master/h2o-docs/src/product/tutorials/GridSearch.md
Ensemble Modeling

Data → Random Forest → Logistic Regression
Data → Neural Network → Logistic Regression
Data → Logistic Regression

Score

https://github.com/h2oai/h2o-3/blob/master/h2o-docs/src/product/tutorials/GridSearch.md
Genetic Algorithms & Artificial Immune Systems

• Goal: Score how similar a new authorization is to characteristic authorizations

• Train thresholds for likely / unlikely authorizations

• Compare incoming authorization to thresholds

Grid Search
Neural Networks
Ensemble models
Genetic Algorithms
Thanks!

Slides:

Brendan.Herger@capitalone.com