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?
0x3A28213A
0x6339392C,
0x7363682E.
I HATE YOU.

VAULT8

Overview

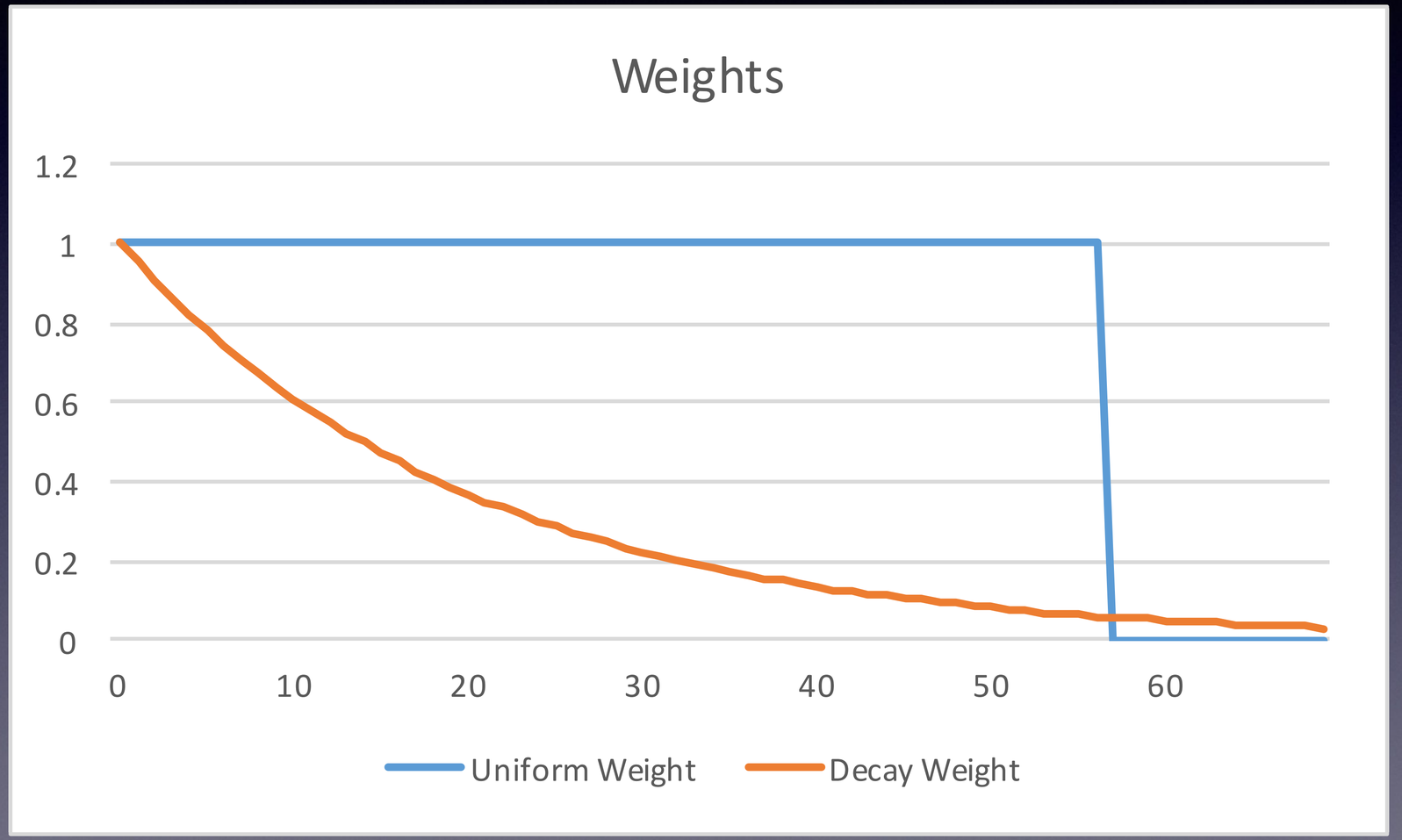
Sampling
Feature Engineering
Modeling

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



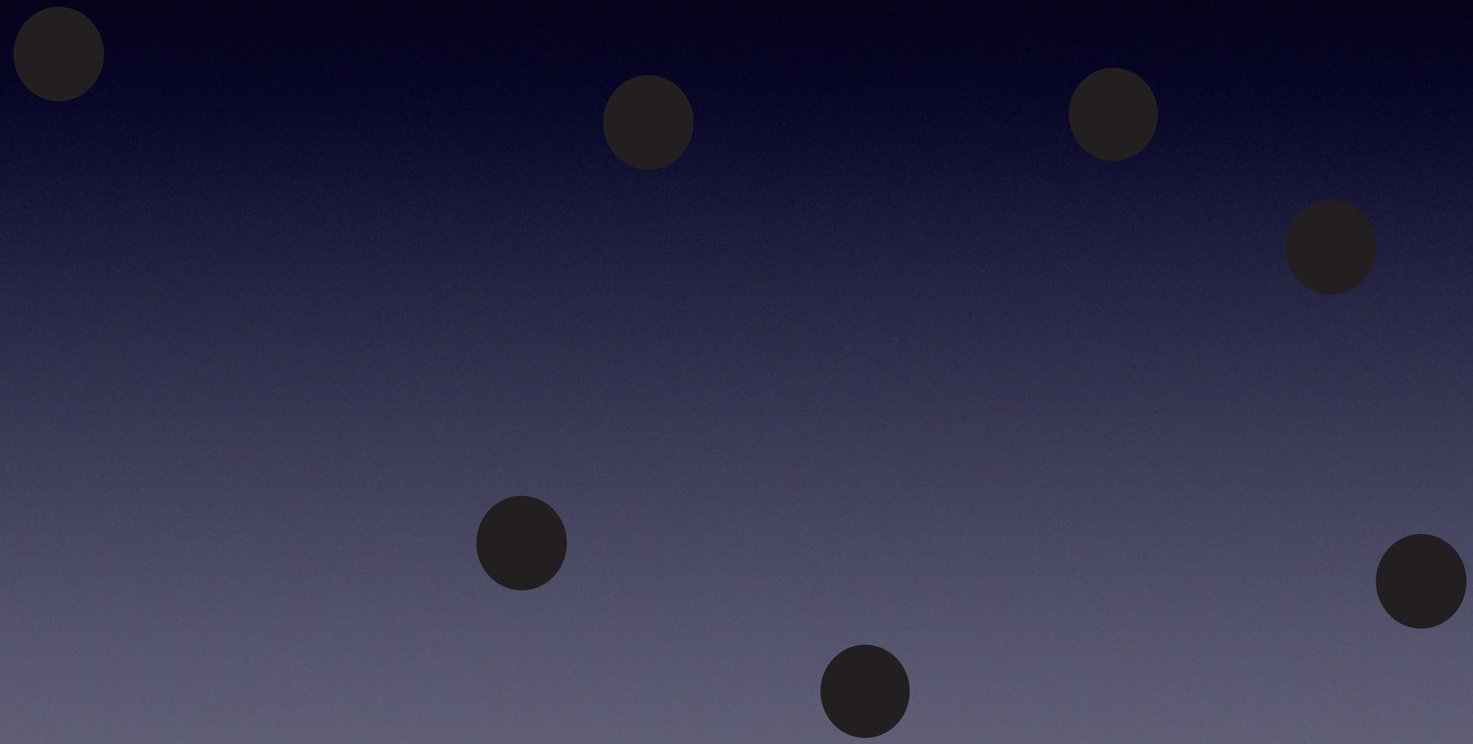
SMOTE

- (Synthetic Minority Over-sampling Technique)
- Goal: Reduce effect of class imbalance
- Majority class: Down sample, with some probability
- Minority class: Create ‘synthetic’ observations

https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

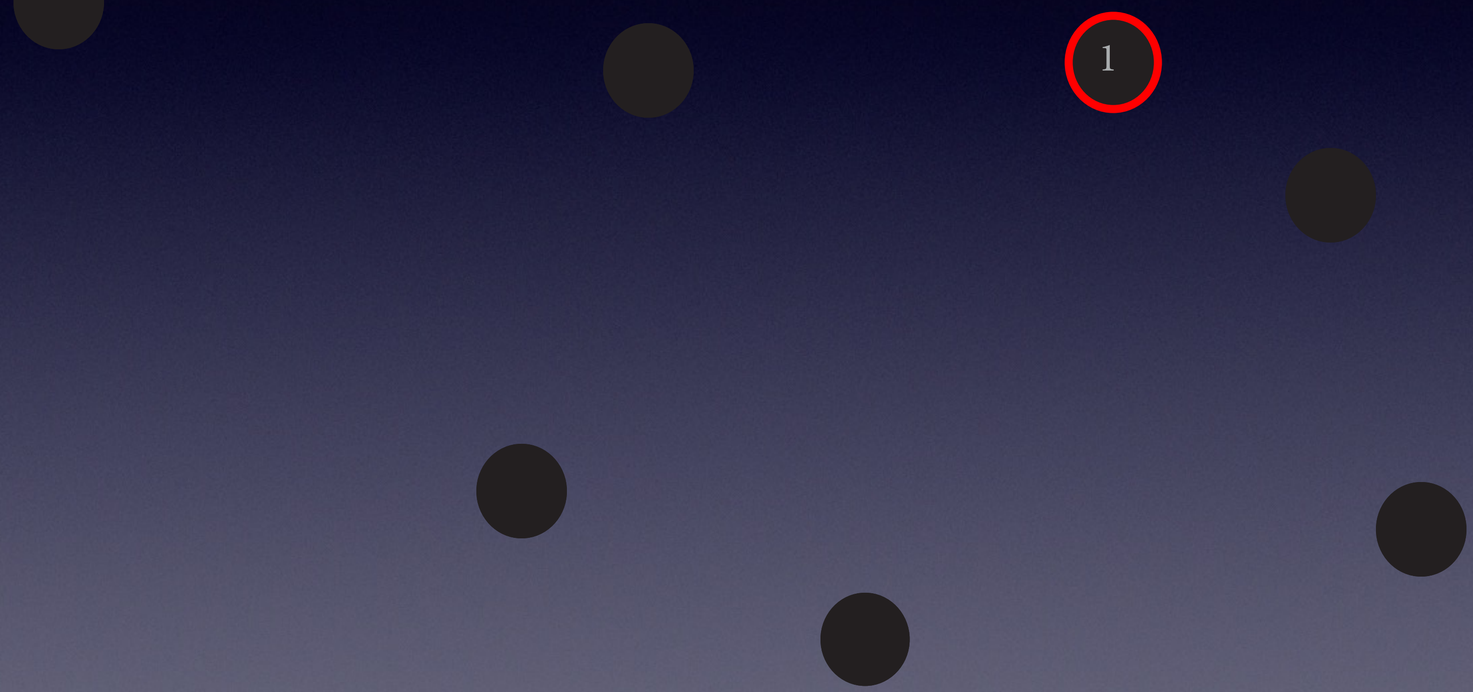
1. Select minority point
2. Select neighbor
3. Create new point



https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

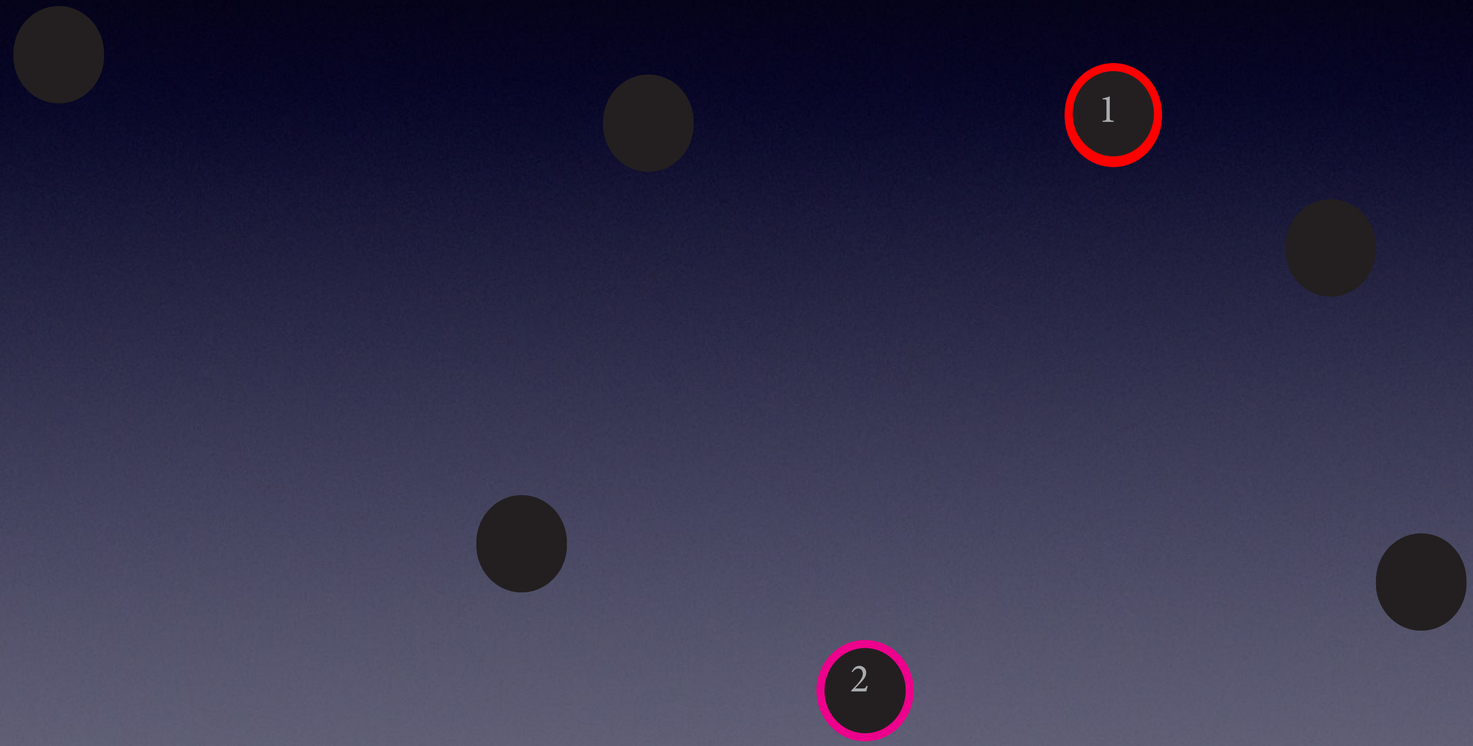
1. Select minority point
2. Select neighbor
3. Create new point



https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

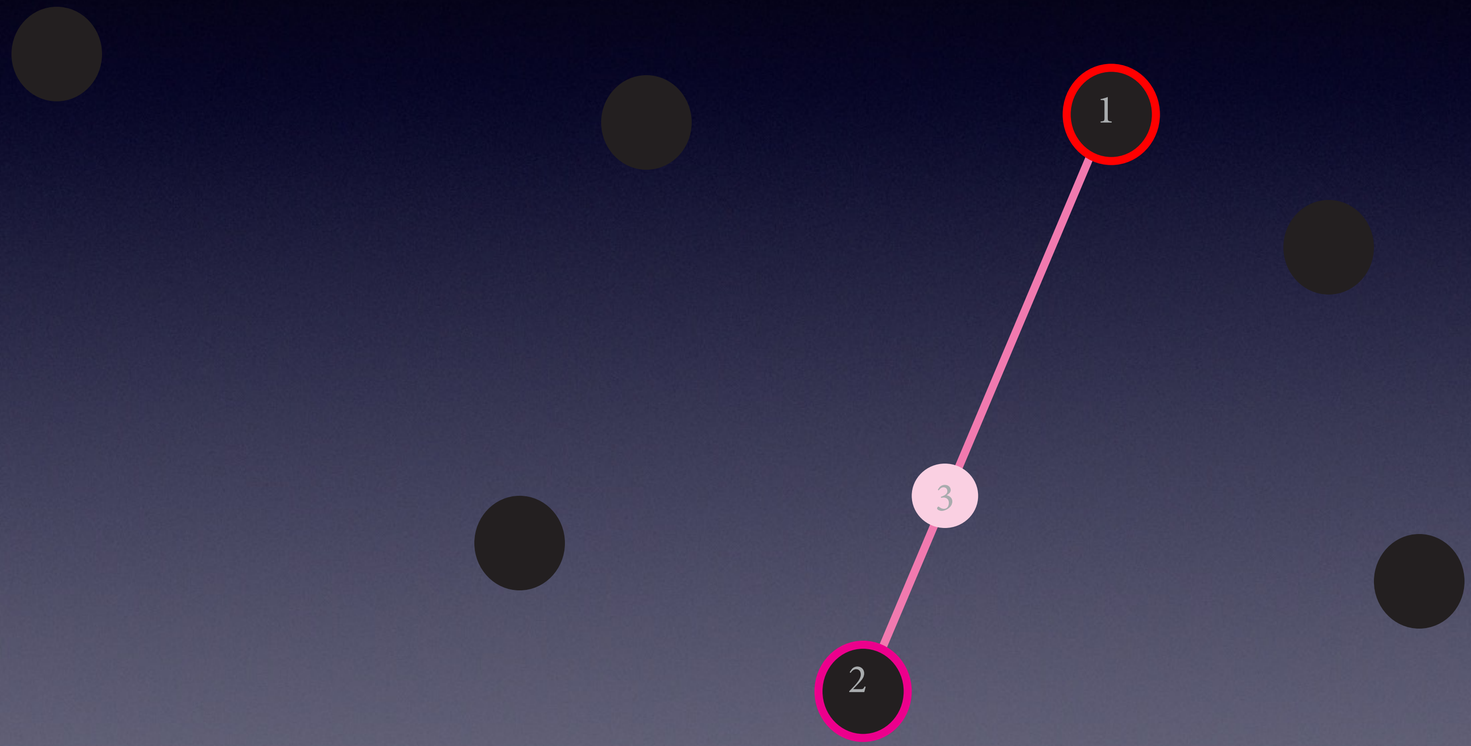
1. Select minority point
2. Select neighbor
3. Create new point



https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

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



https://www.jair.org/media/953/live-953-2037-jair.pdf

Observation Weighting
SMOTE Sampling

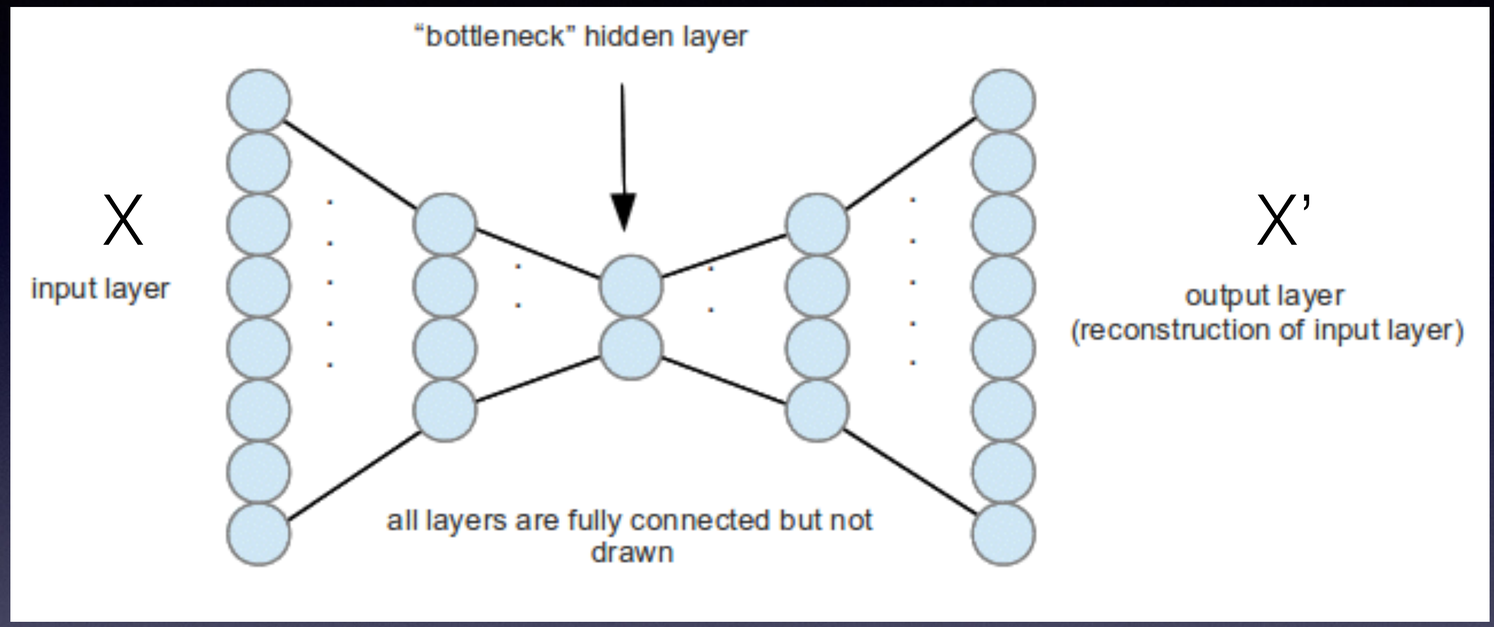
Features

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|

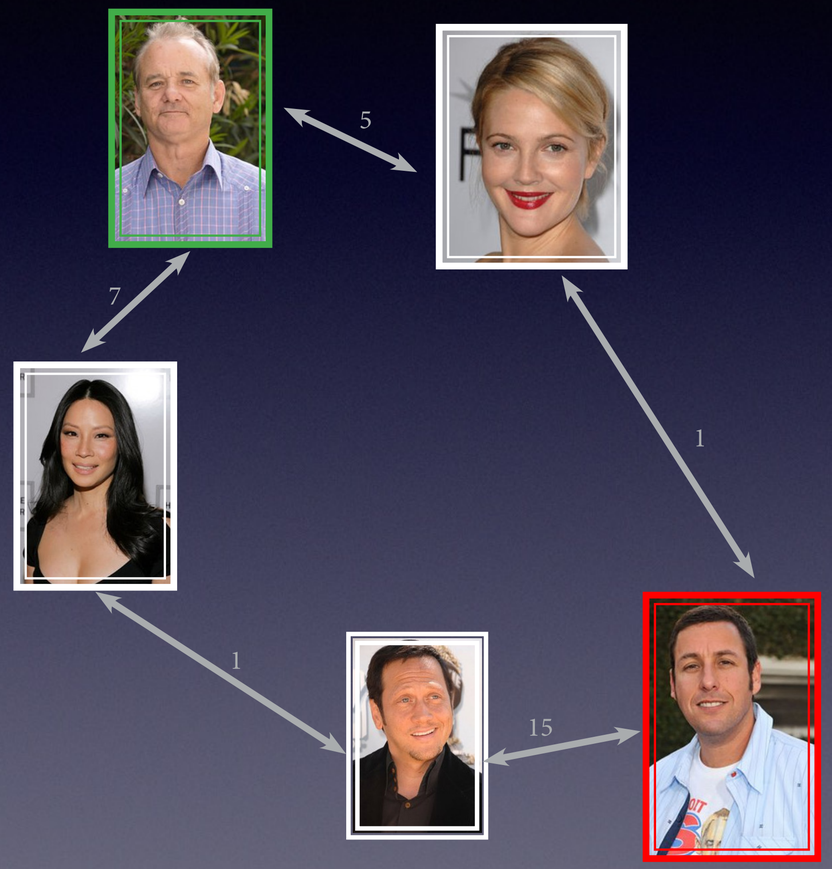
https://github.com/h2oai/h2o-training-book/blob/master/hands-on_training/anomaly_detection.md

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

http://research.microsoft.com/en-us/people/nicolasl/efficient_ssl.pdf
http://www.amstat.org/publications/jse/v23n2/hardin.pdf

Label Propagation



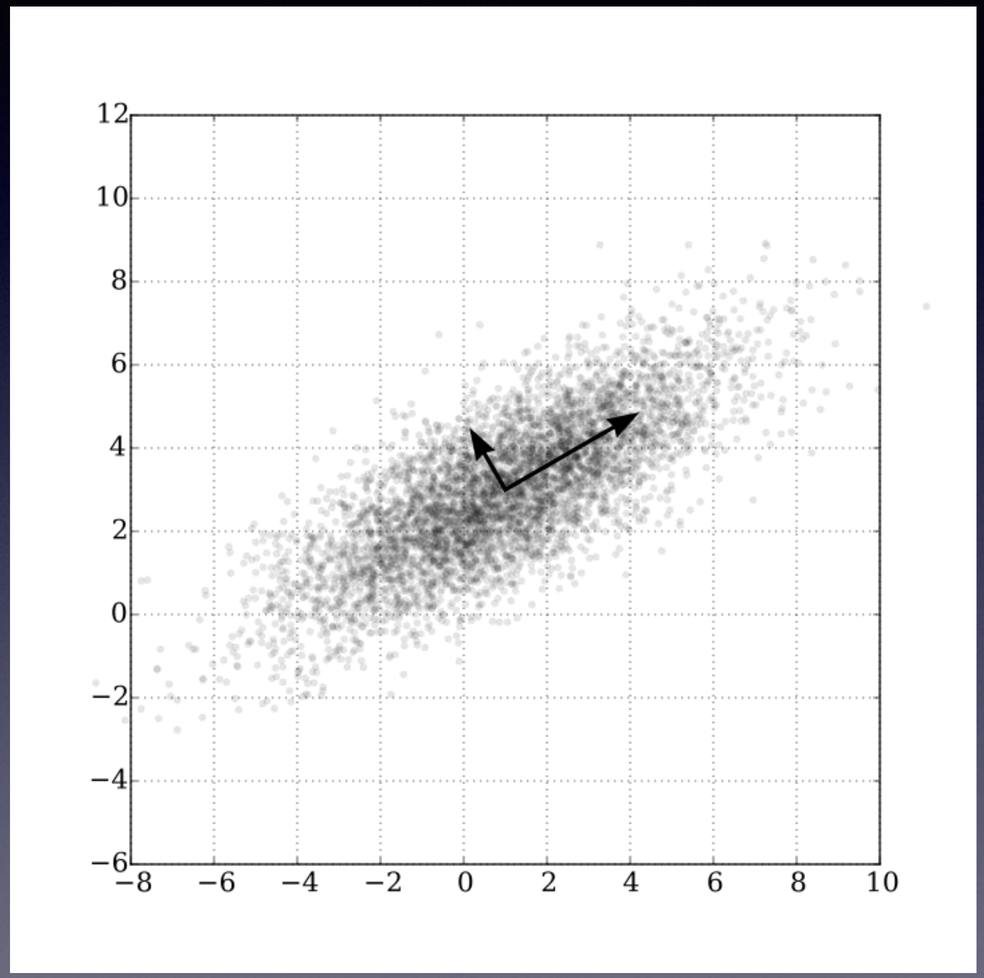
http://research.microsoft.com/en-us/people/nicolasl/efficient_ssl.pdf
http://www.amstat.org/publications/jse/v23n2/hardin.pdf

Low Rank Models

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

https://web.stanford.edu/~boyd/papers/pdf/glrm.pdf
https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md

Low Rank Models



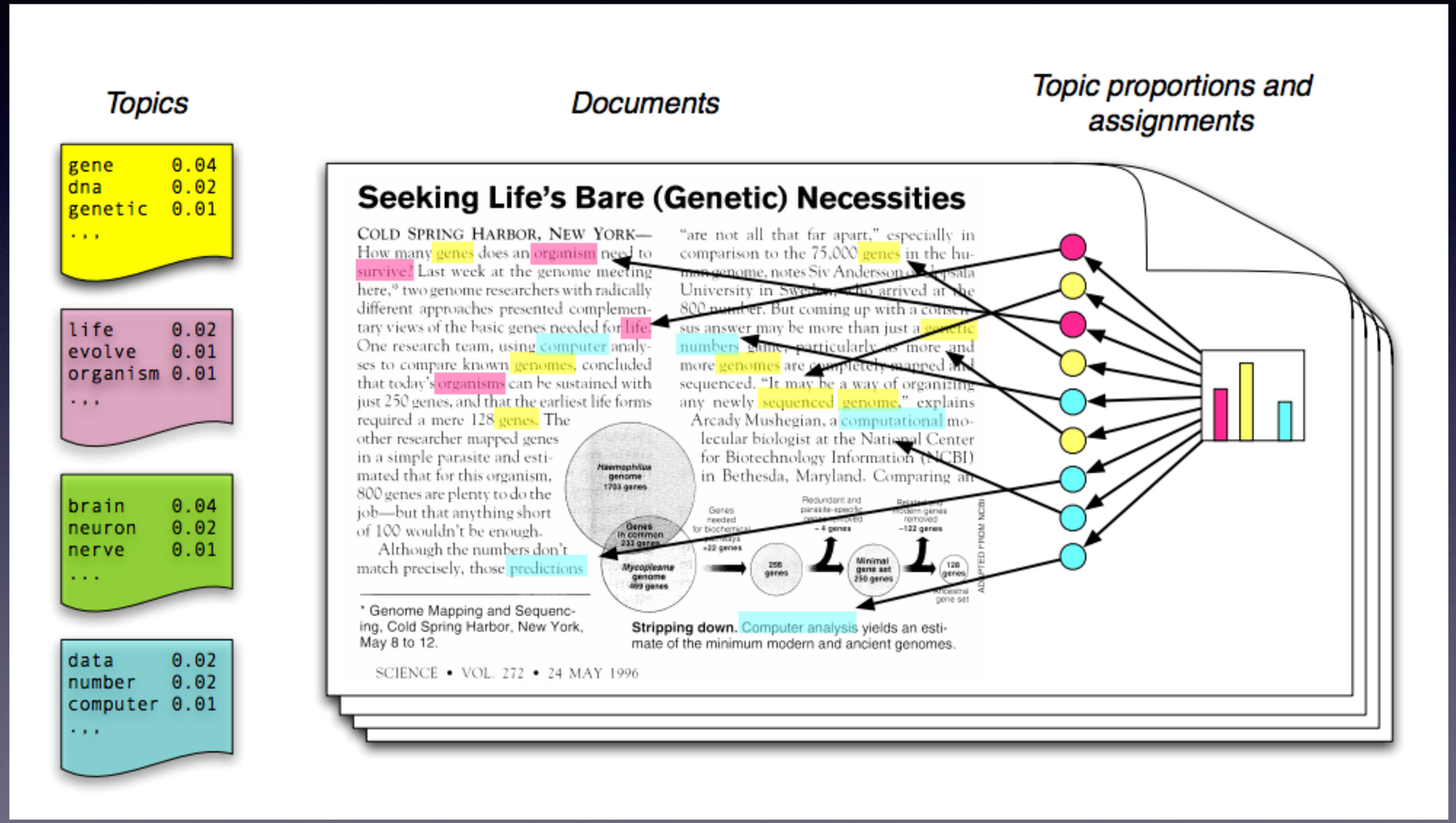
https://web.stanford.edu/~boyd/papers/pdf/glrm.pdf
https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md

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

https://www.cs.princeton.edu/~blei/papers/Blei2011.pdf
http://machinelearning.wustl.edu/mlpapers/paper_files/nips02-AA53.pdf

LDA Topic modeling



https://www.cs.princeton.edu/~blei/papers/Blei2011.pdf
http://machinelearning.wustl.edu/mlpapers/paper_files/nips02-AA53.pdf

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

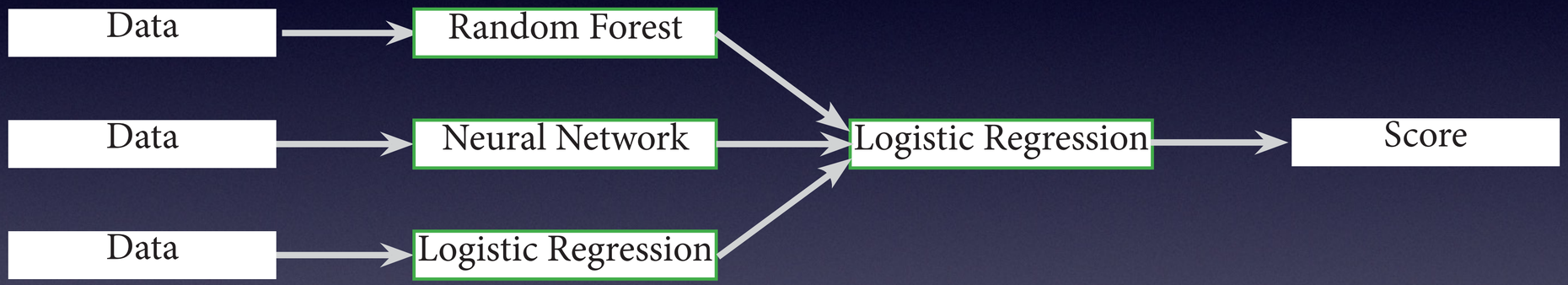
https://github.com/h2oai/h2o-3/blob/master/h2o-docs/src/product/tutorials/GridSearch.md

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



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

http://www.ijser.org/researchpaper%5CFraud-Detection-of-Credit-Card-Payment-System-by-Genetic-Algorithm.pdf

Grid Search
Neural Networks
Ensemble models
Genetic Algorithms

Thanks!

Slides:
https://github.com/bjherger/talks/blob/master/strata-ny-2016/Strata-2016-NY.pdf

Brendan.Herger@capitalone.com