Machine Learning with Opponents

Brendan Herger
Brendan.Herger@capitalone.com

Slides: https://goo.gl/D8Yxme

MAN, I SUCK AT THIS GAME. CAN YOU GIVE ME A FEW POINTERS?
0x3A28213A 0x6339392C, 0x7363682E.
I HATE YOU.

Overview

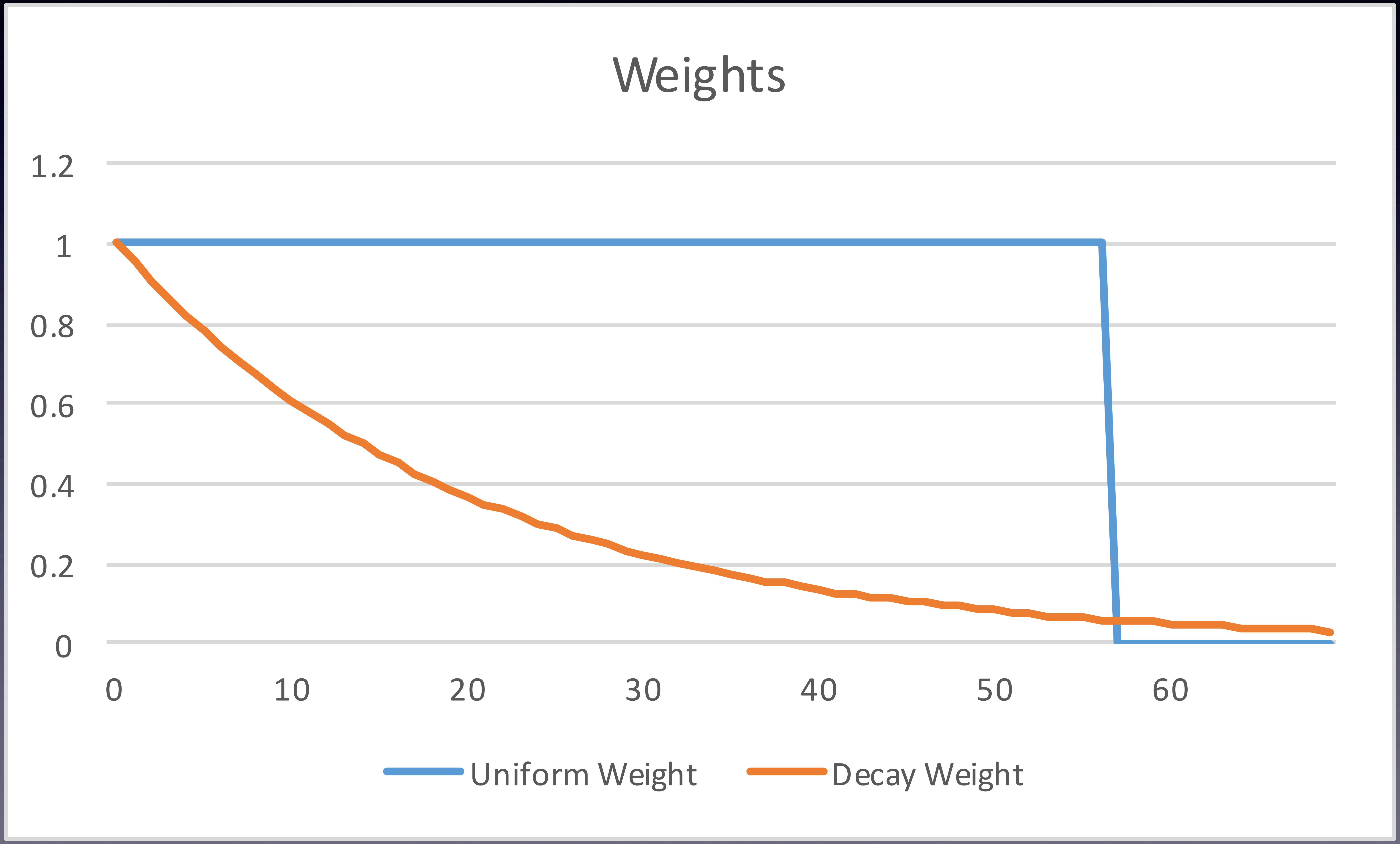
Sampling
Feature Engineering
Modeling

Sampling

Observation Weighting

- Effect cost function by weighting every row at train time
- Weights include
  - Uniform weight
  - Observation age (staleness)
  - Random down-sampling
  - Up-sampling known opponent attacks

Observation Weighting



SMOTE

(Synthetic Minority Over-sampling Technique)

- Goal: Better model rare events (opponent attacks)
- Majority class: Down sample, with some probability
- Minority class: Create ‘synthetic’ observations

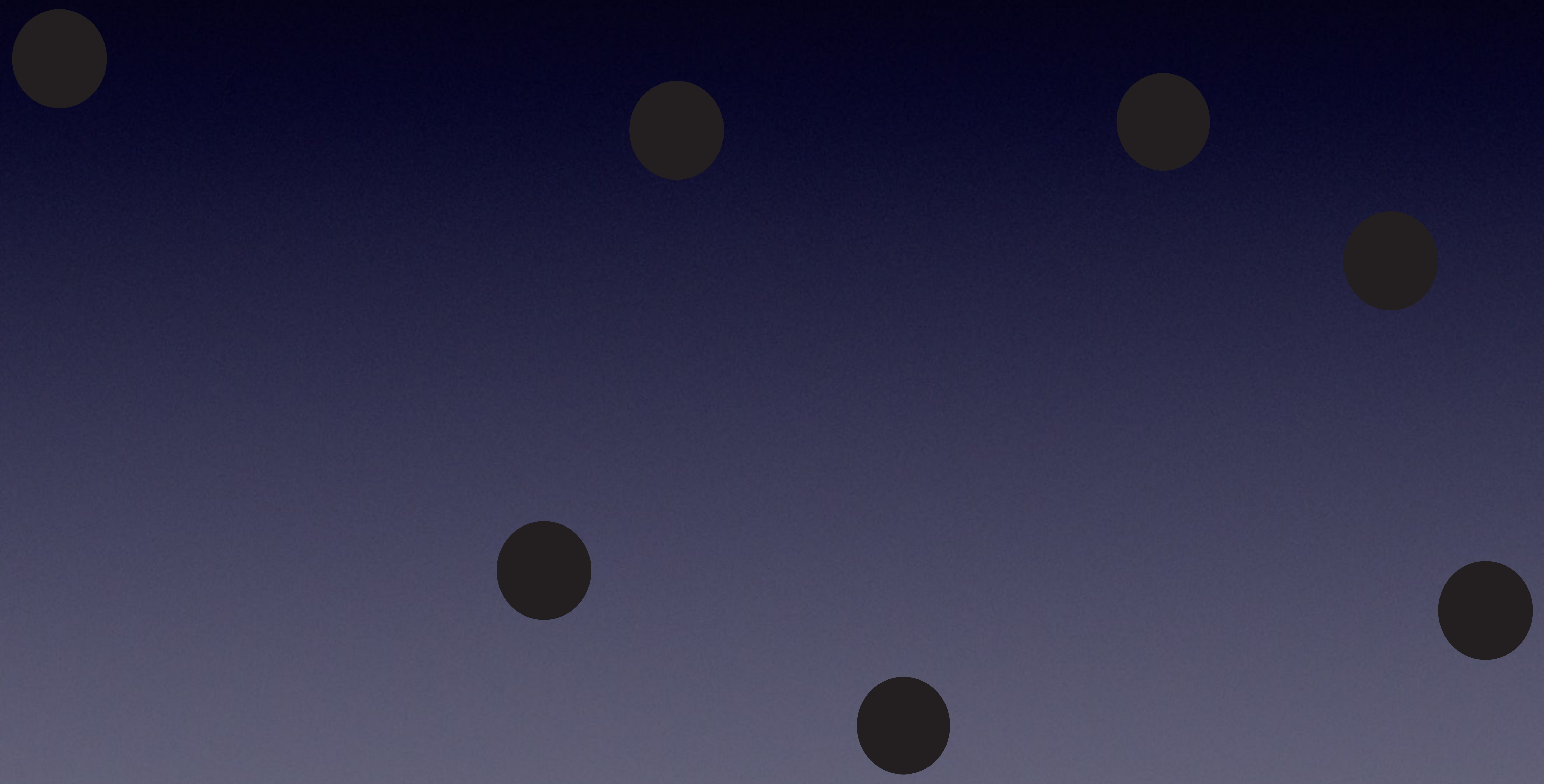
https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

1. Select minority point

2. Select neighbor

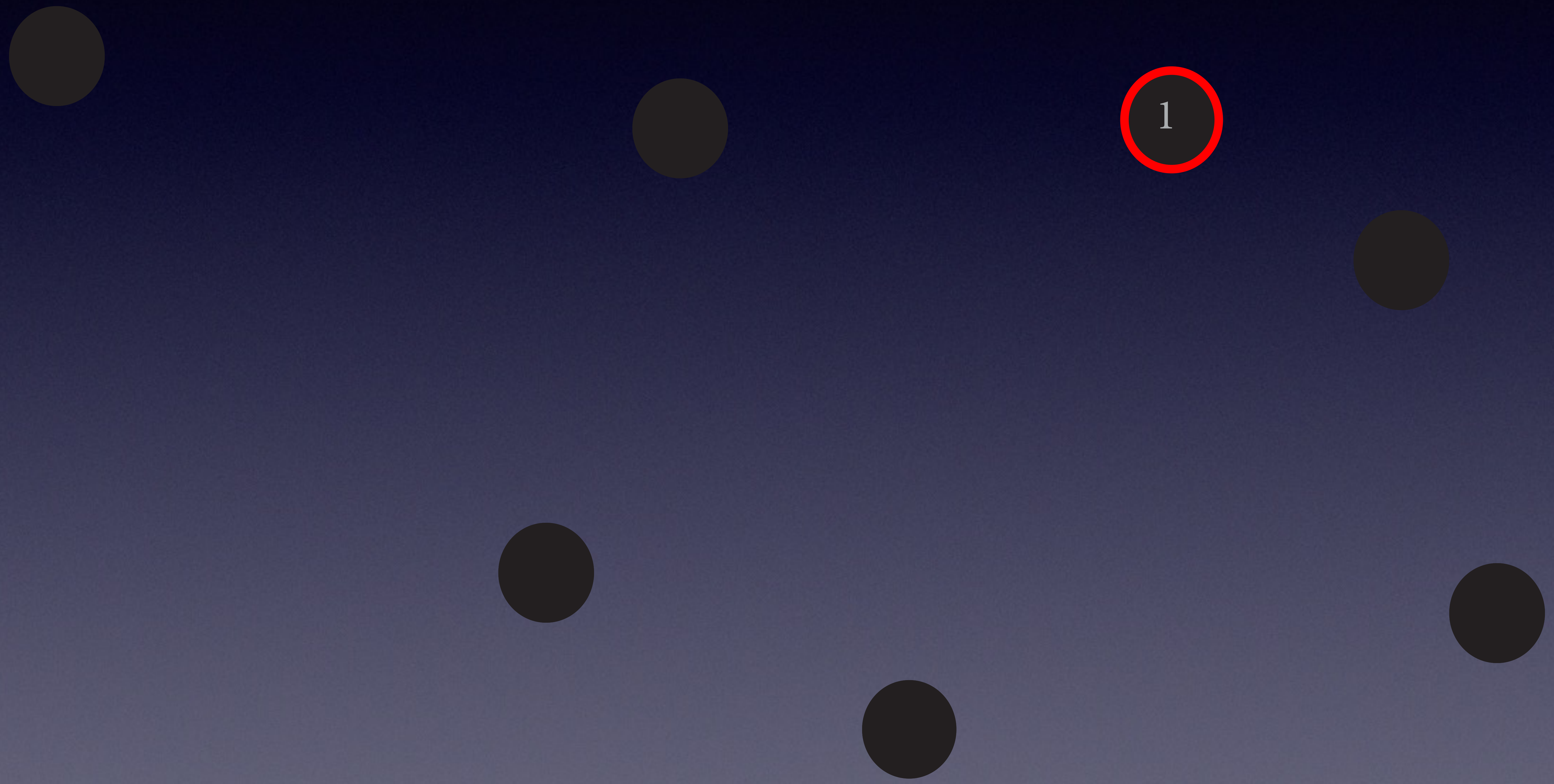
3. Create new point



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

SMOTE

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



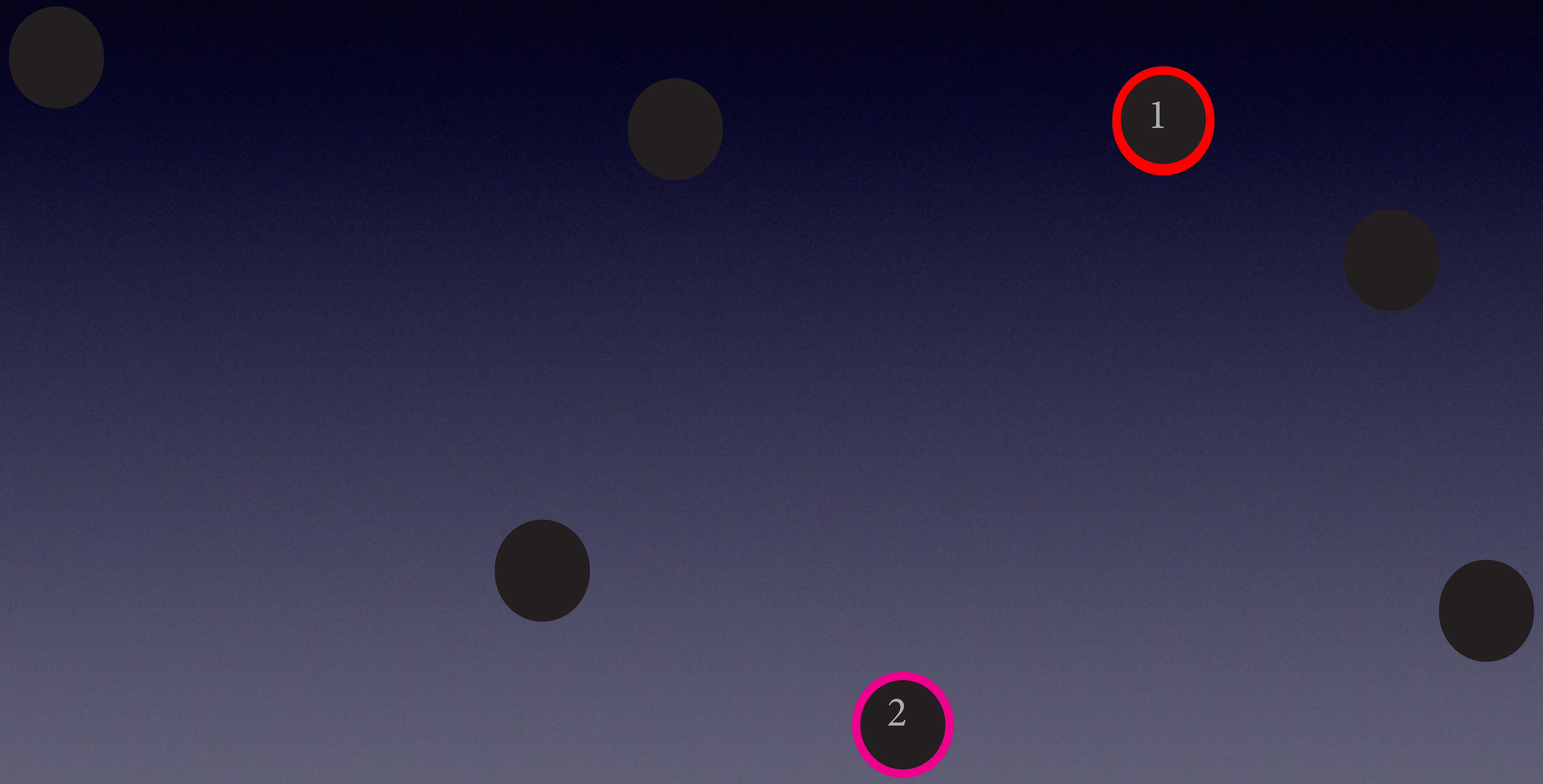
https://www.jair.org/media/953/live-953-2037-jair.pdf

SMOTE

1. Select minority point

2. Select neighbor

3. Create new point



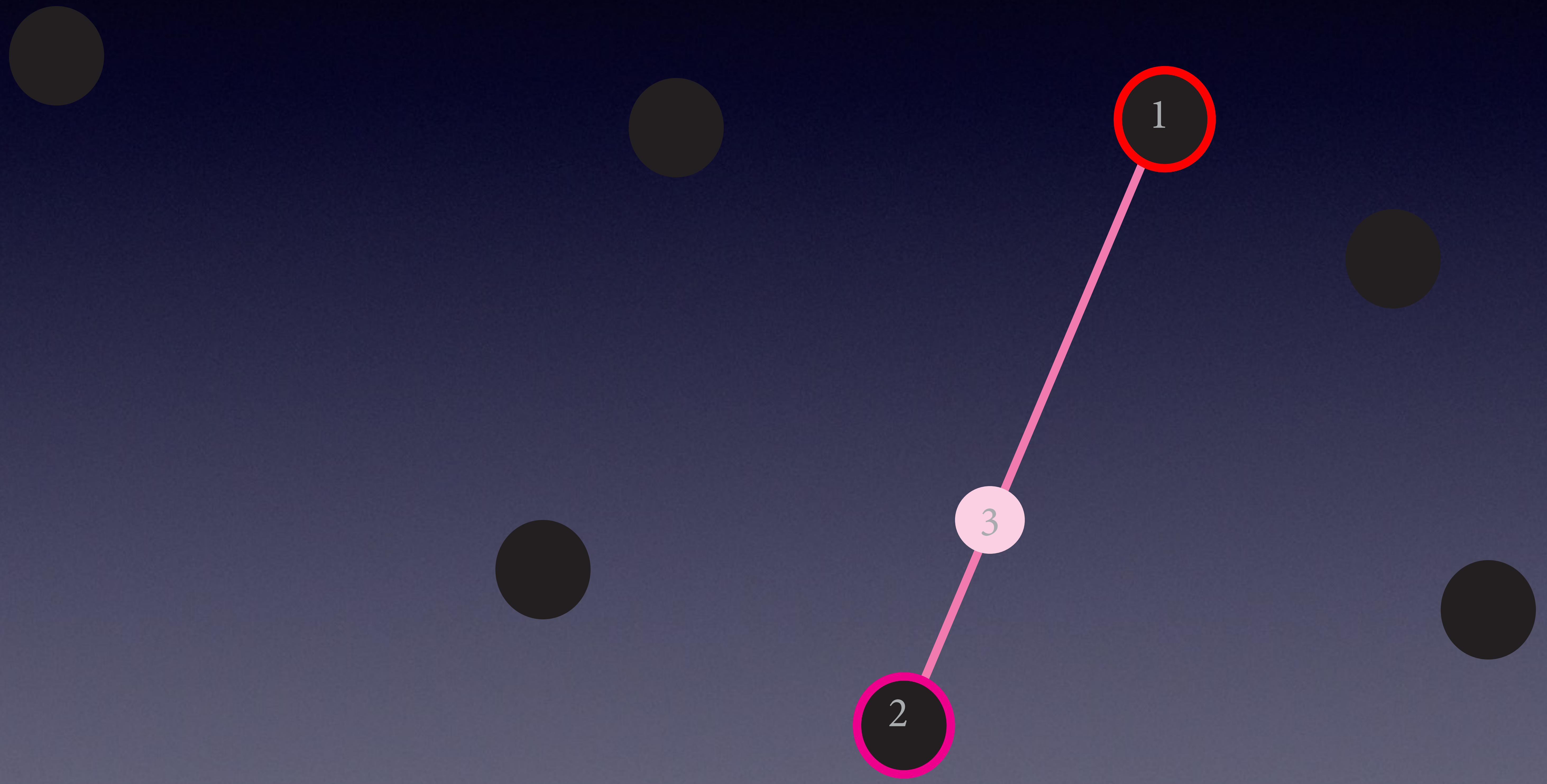
https://www.jair.org/media/953/live-953-2037-jair.pdf

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

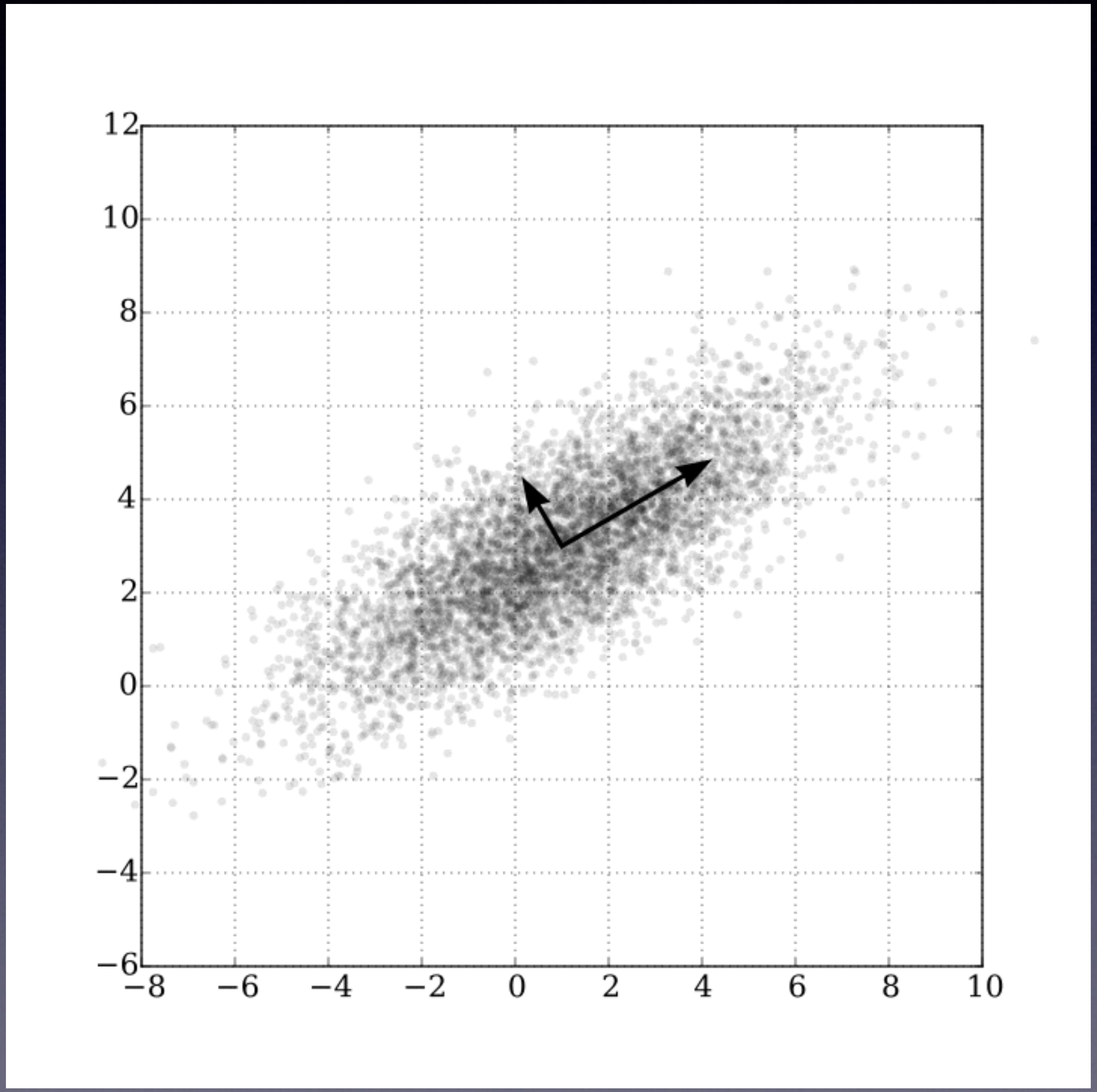
https://github.com/h2oai/h2o-training-book/blob/master/hands-on_training/anomaly_detection.md

Low Rank Models

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

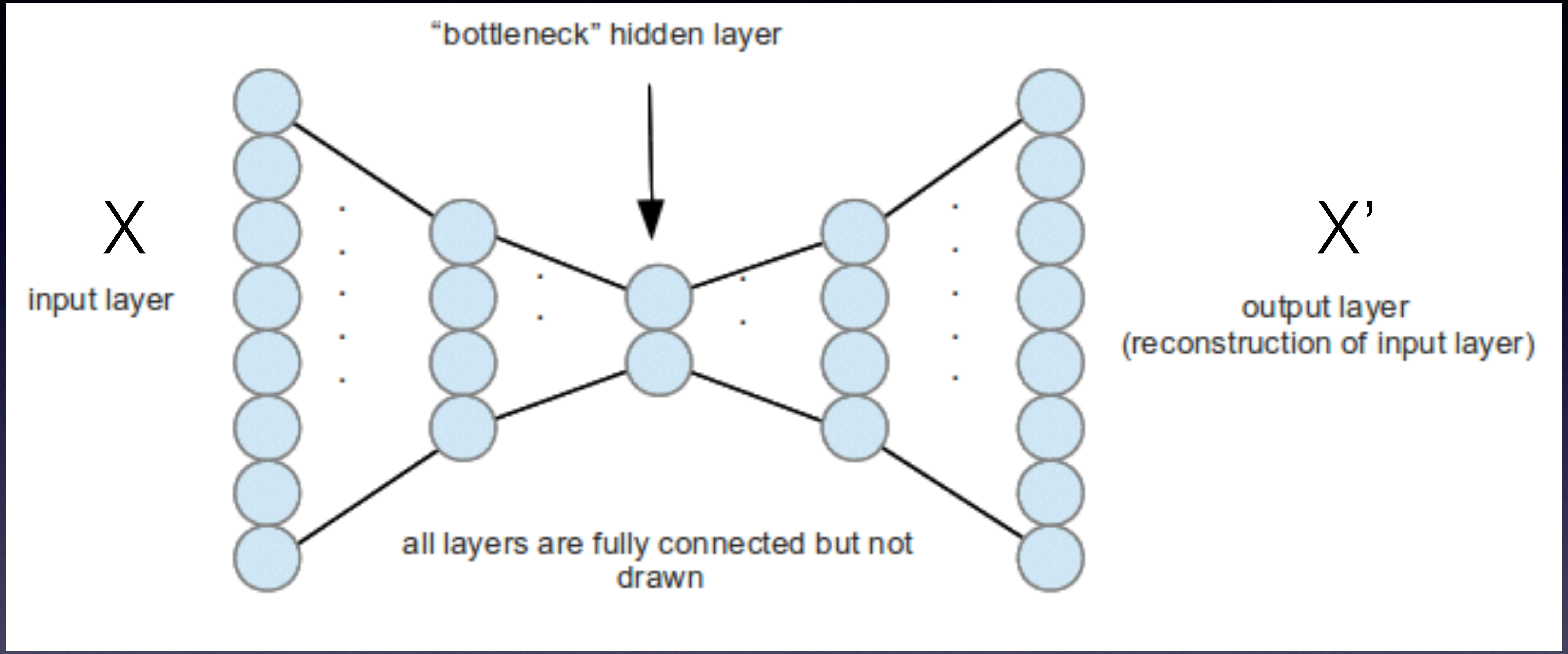
https://web.stanford.edu/~boyd/papers/pdf/glrm.pdf
https://github.com/h2oai/h2o-tutorials/blob/master/tutorials/glrm/glrm-tutorial.md

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

Outlier Detection


"bottleneck" hidden layer
X
input layer
X'
output layer
(reconstruction of input layer)
all layers are fully connected but not drawn

Outlier score: |X'-X|

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

Outlier Detection
GLRM

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

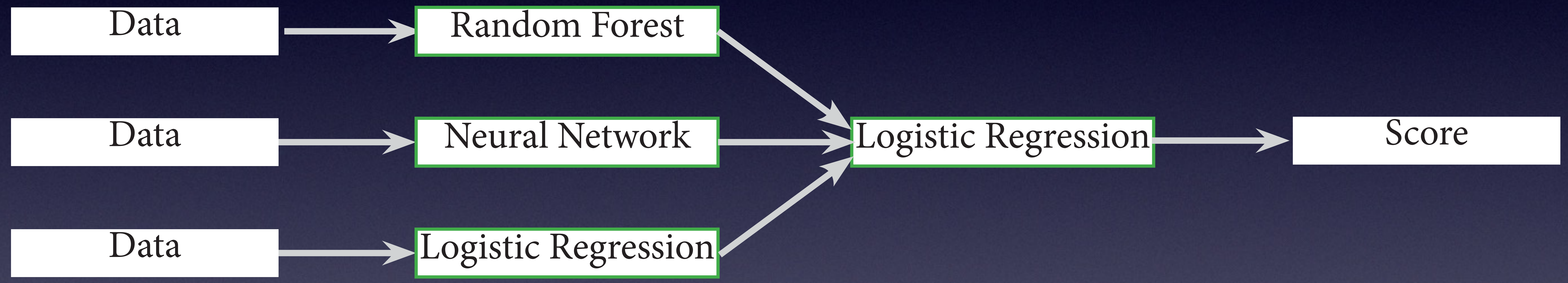
- Too complicated to cover here 😞
- Strengths: Able to capture complicated, non-linear relationships. Deals well with class imbalance
- Weaknesses: Difficult to train, many free parameters

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

We’re Hiring!

Thanks!

Slides: https://goo.gl/D8Yxme

Brendan.Herger@capitalone.com