

# Machine Learning Techniques for Class Imbalances & Adversaries

Brendan Herger  
[Brendan.Herger@capitalone.com](mailto: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

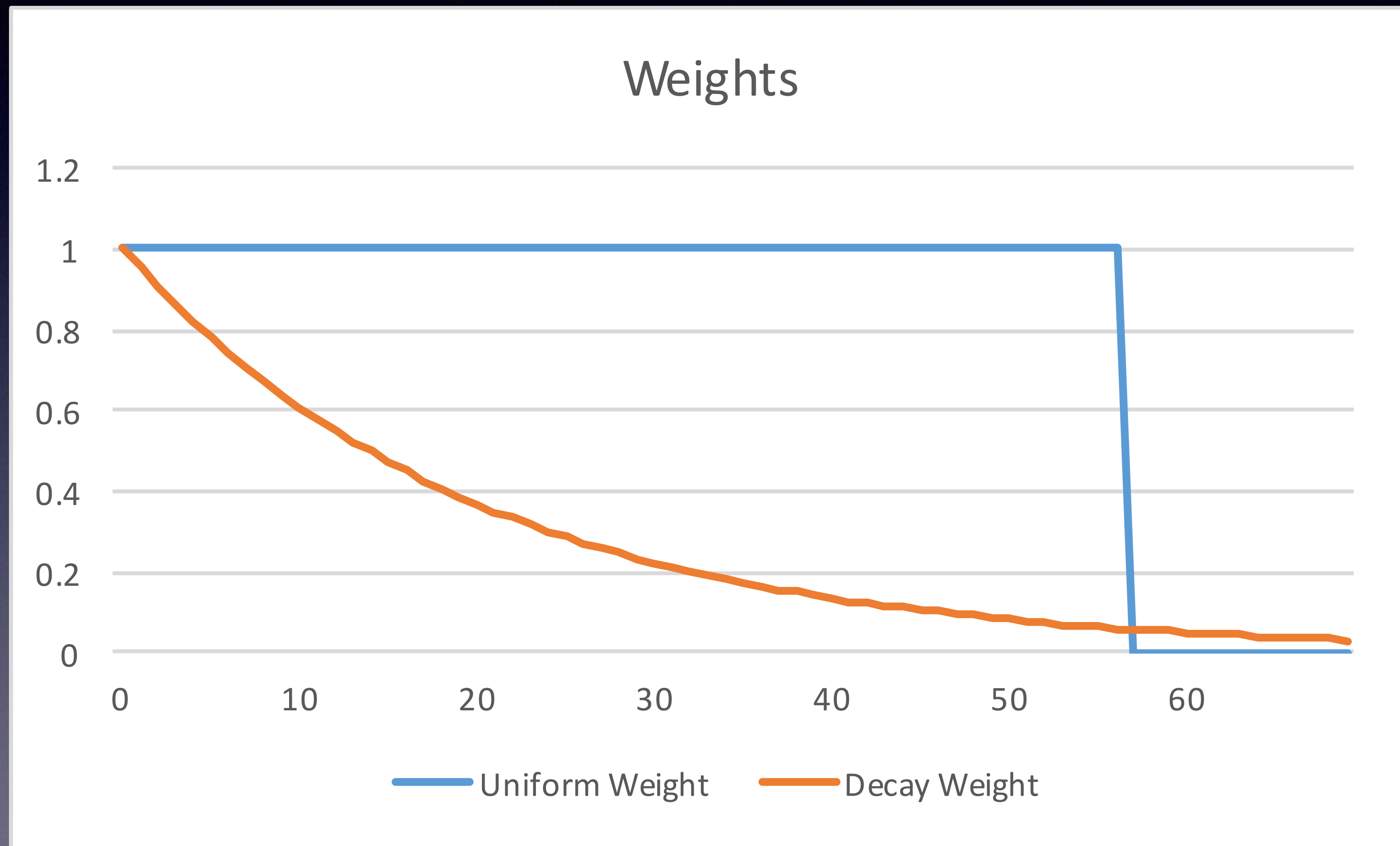


# Observation Weighting

- 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



# SMOTE

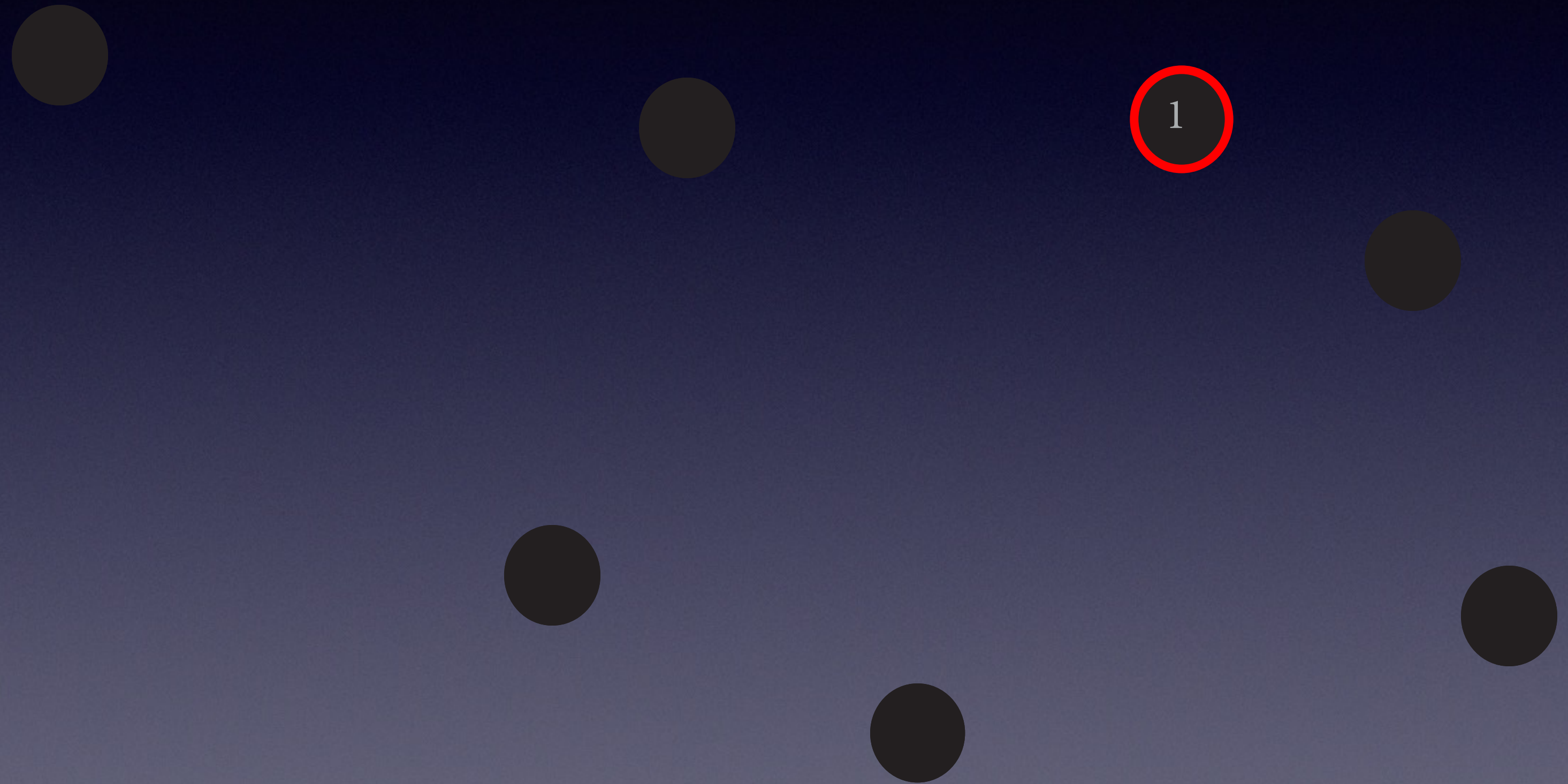
1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

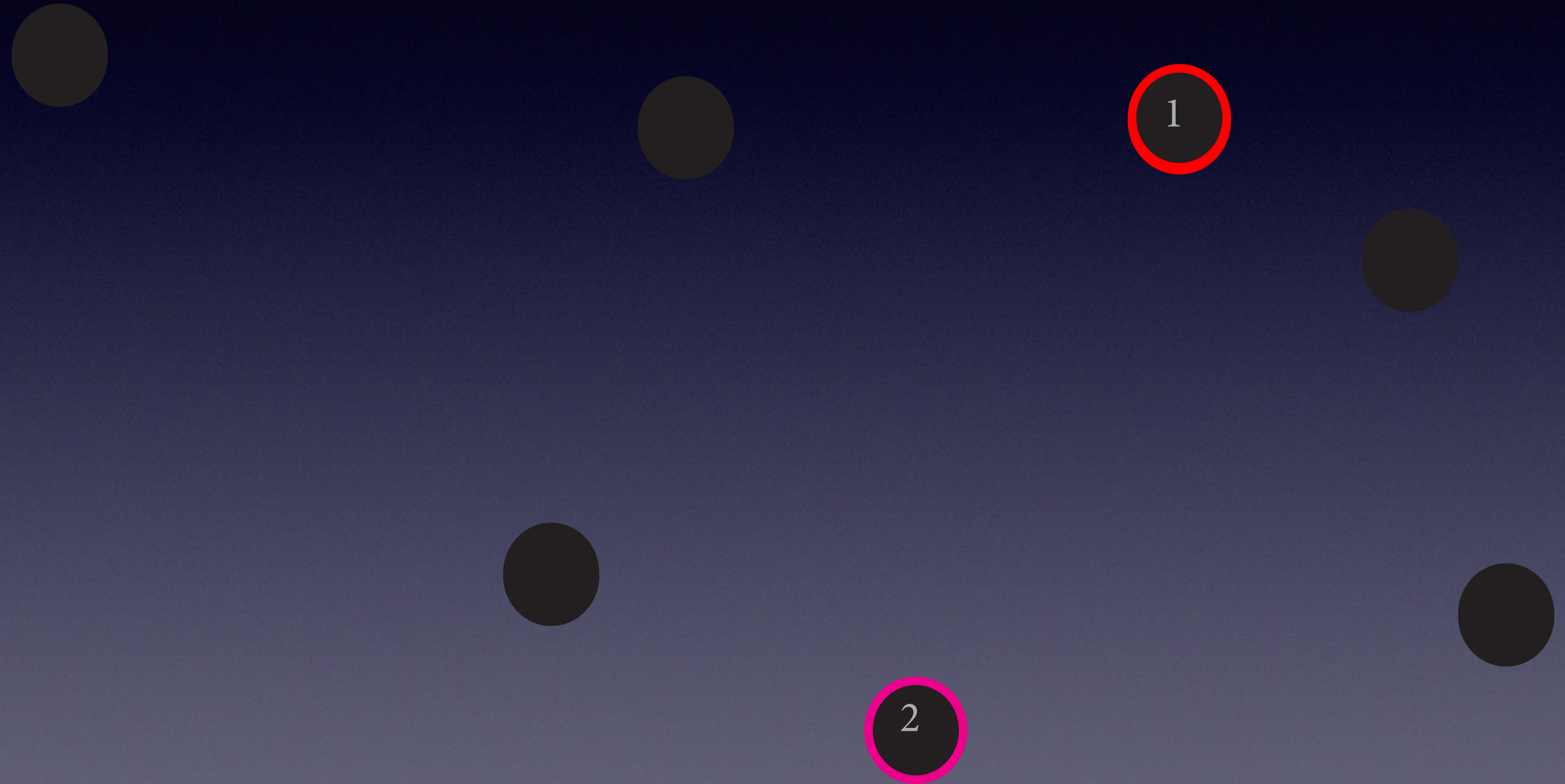
1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

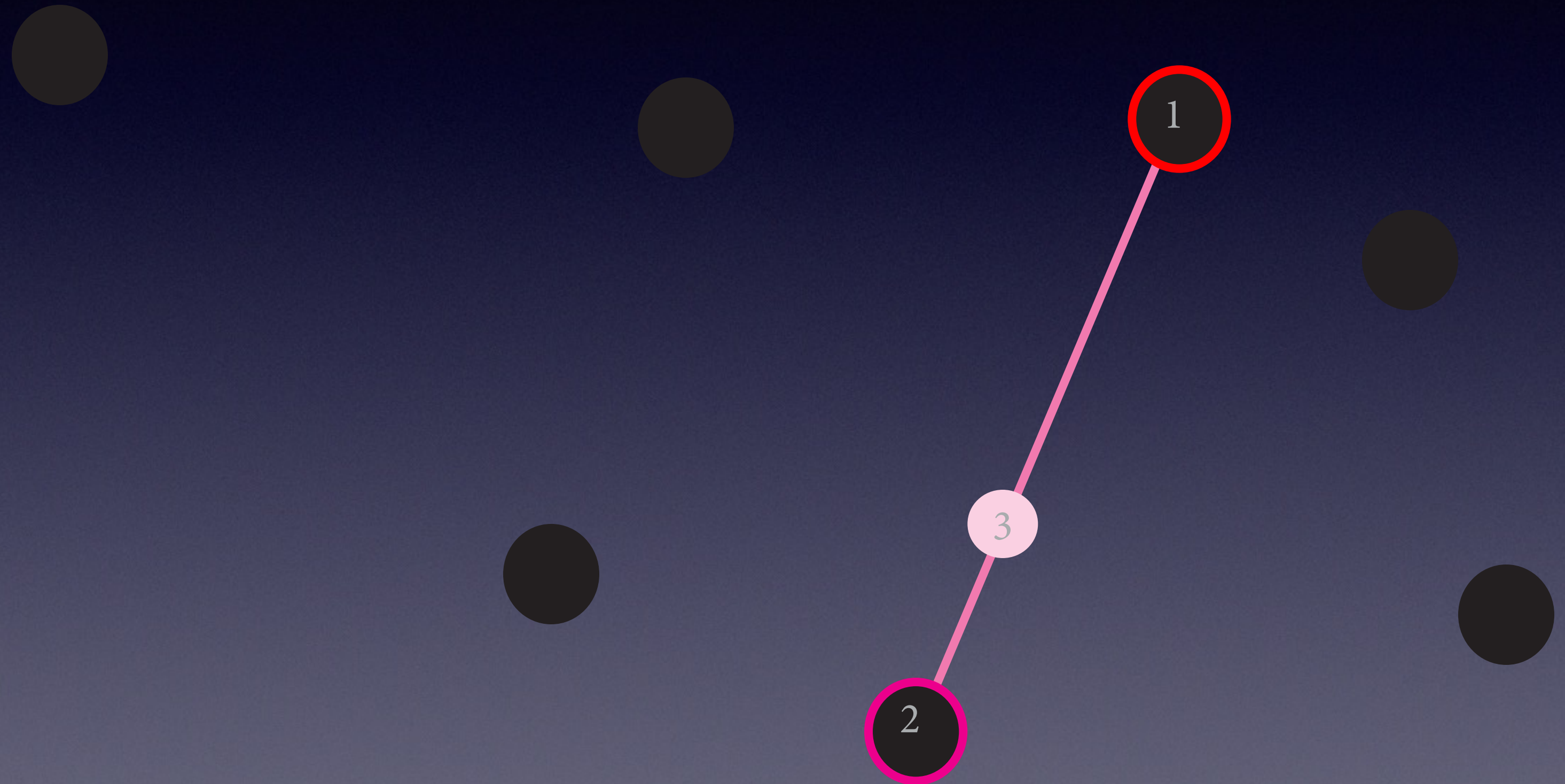
1. Select minority point
2. Select neighbor
3. Create new point





# SMOTE

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





# Observation Weighting SMOTE Sampling







# Features

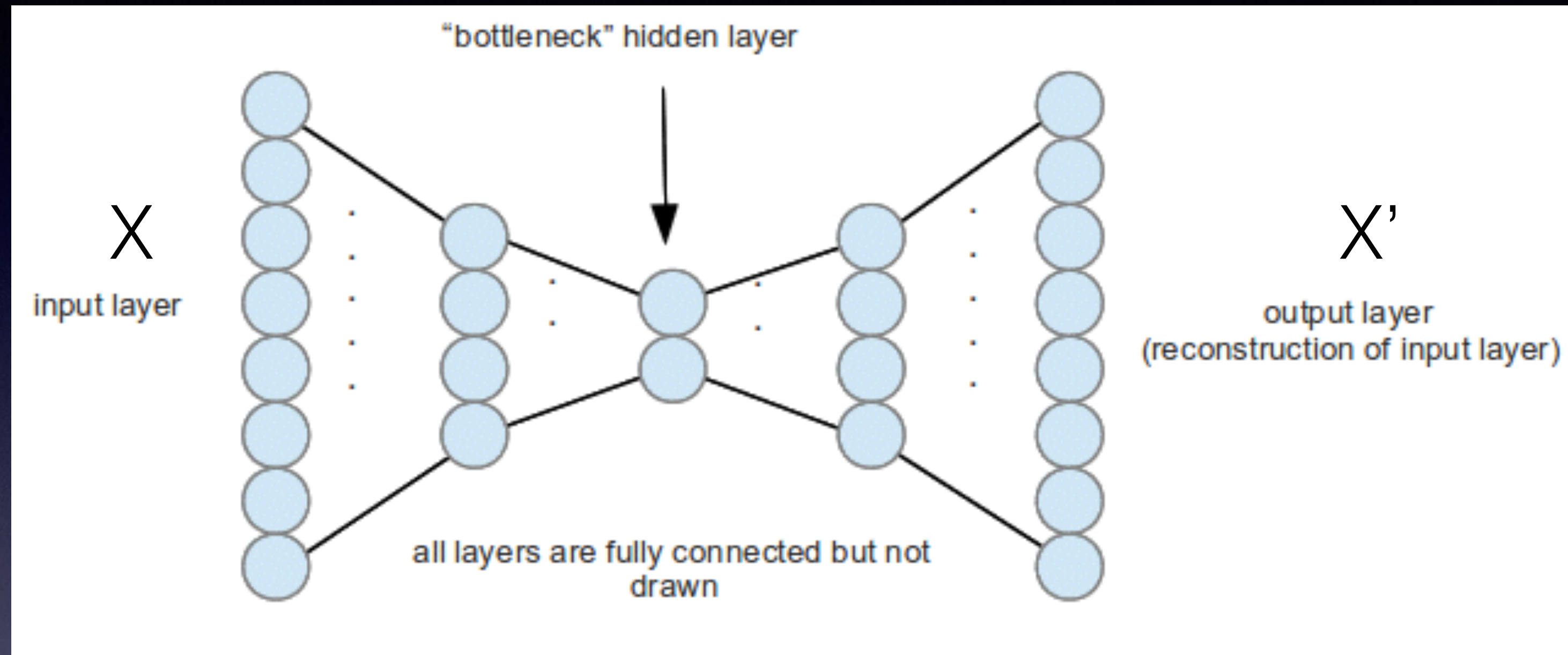


# Outlier Detection

- 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



# Outlier Detection



Outlier score:  $|X' - X|$

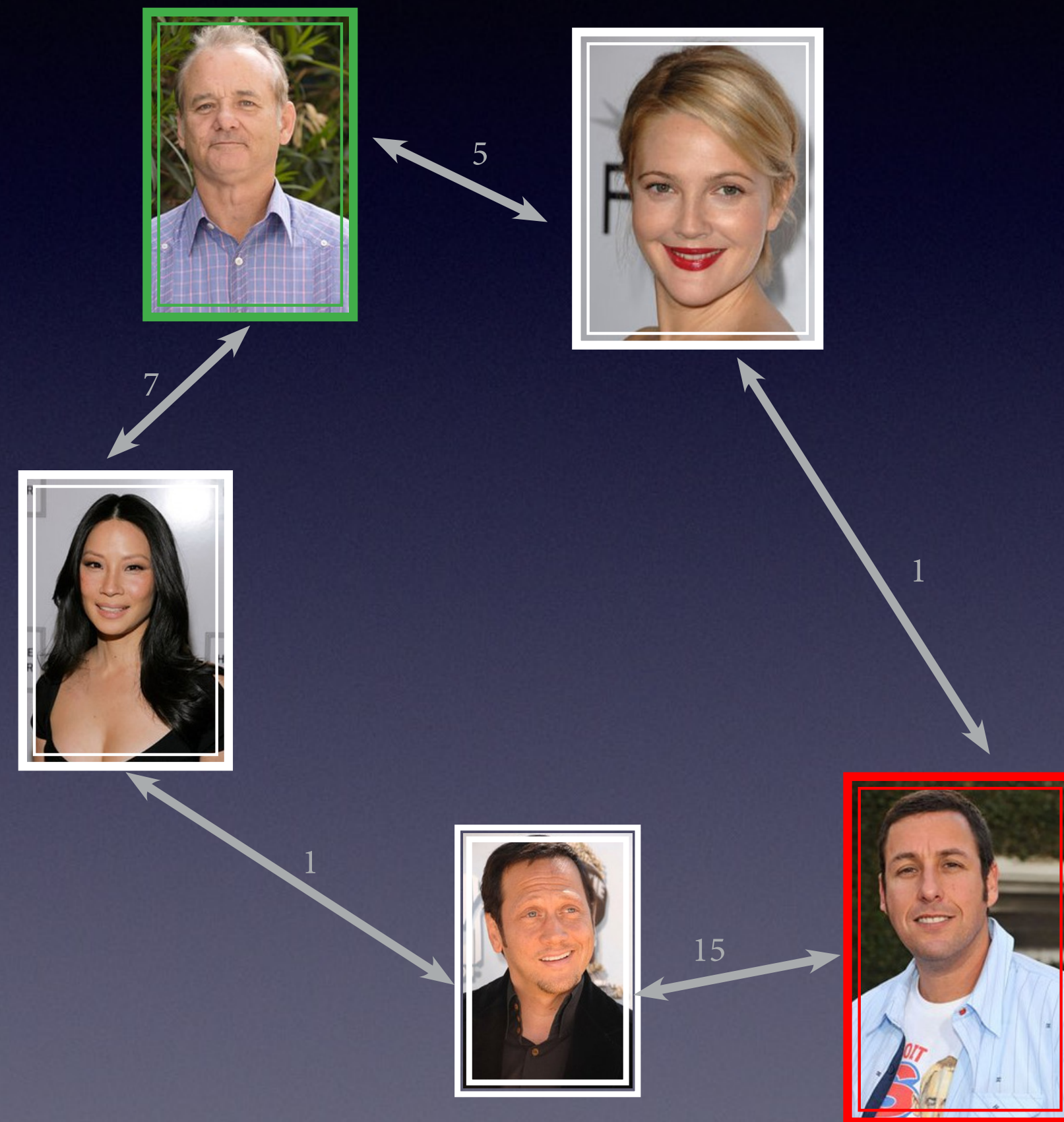


# Label Propagation

- 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



[http://research.microsoft.com/en-us/people/nicolasl/efficient\\_ssl.pdf](http://research.microsoft.com/en-us/people/nicolasl/efficient_ssl.pdf)  
<http://www.amstat.org/publications/jse/v23n2/hardin.pdf>

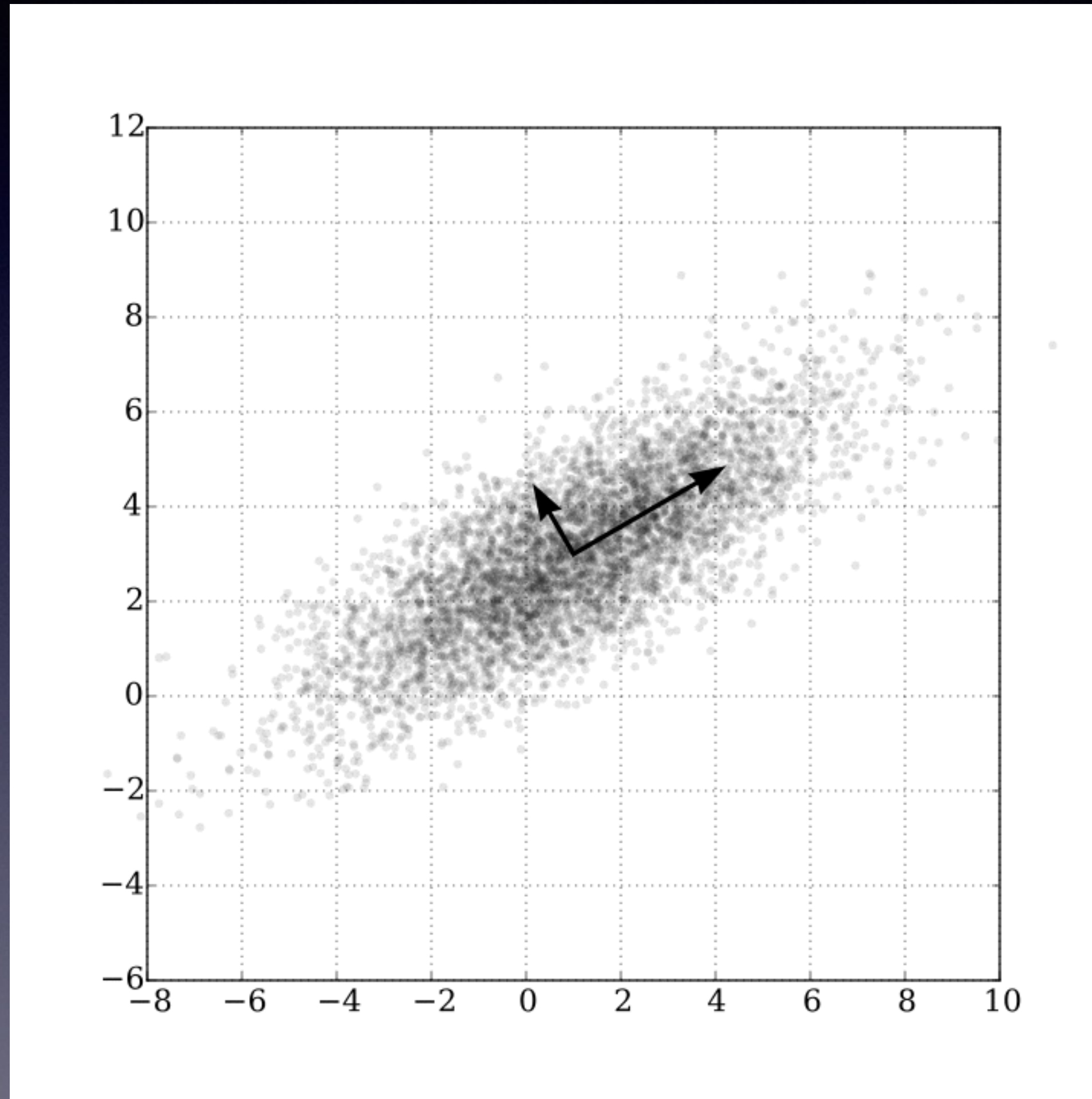


# Low Rank Models

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



# 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>

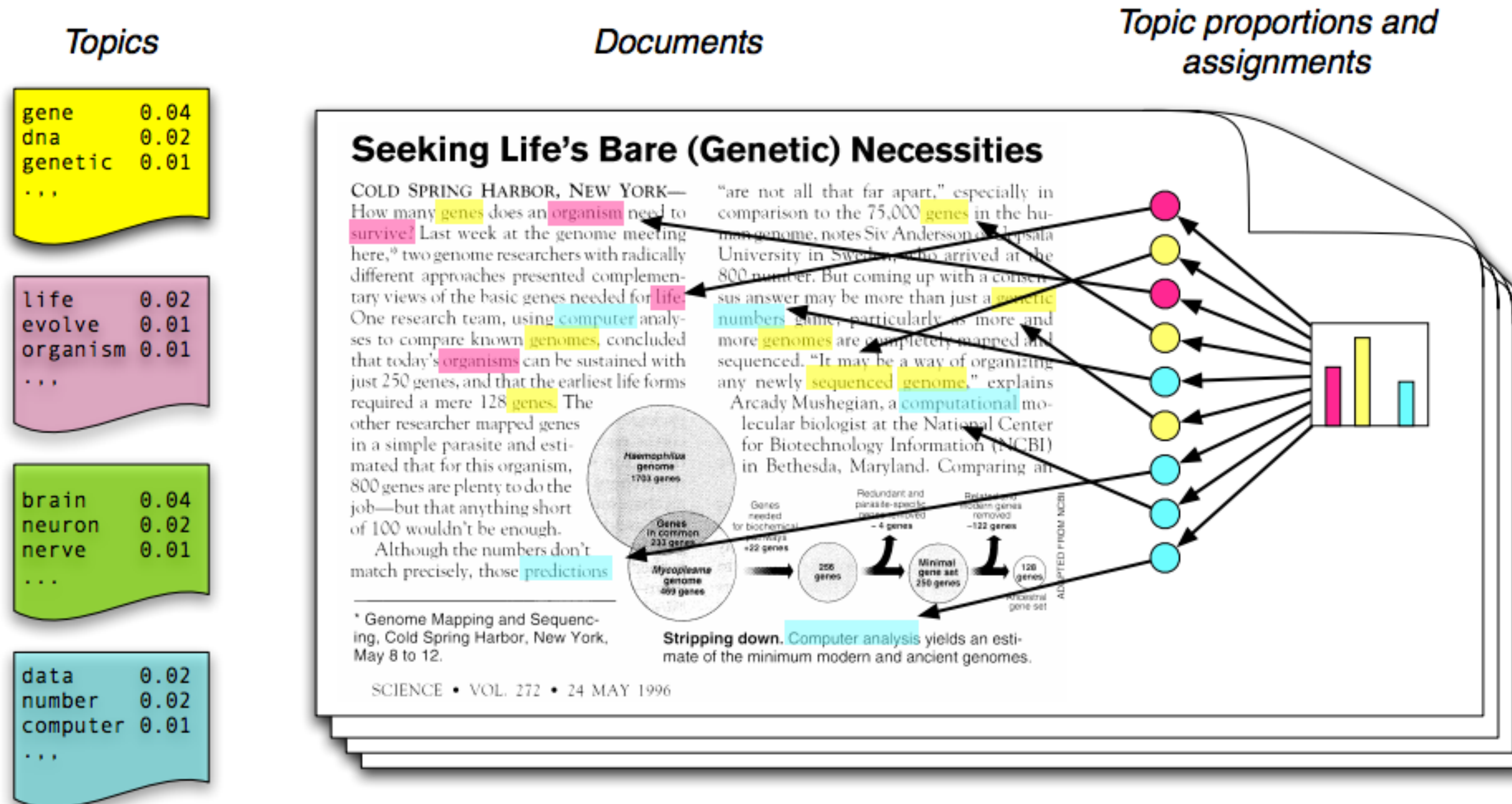


# LDA Topic modeling

- 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



# 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



# Neural Networks

- See other talks
- Too complicated to cover here

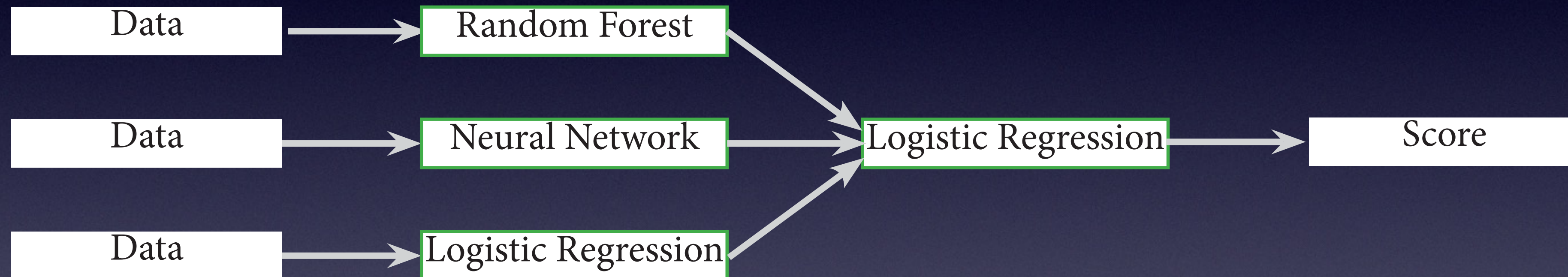


# Ensemble Modeling

- 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



# Ensemble Modeling





# 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:

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

[Brendan.Herger@capitalone.com](mailto:Brendan.Herger@capitalone.com)



