

DETECÇÃO DE ANOMALIAS

Luiz Celso Gomes-Jr/UTFPR

Apresentação

- Professor de Bancos de Dados, Ciência de Dados, Recuperação de Informação – UTFPR
- Interesses de Pesquisa: NLP, IR, Redes Complexas, ML, Big Data, privacidade
- “Virou” pesquisador em detecção de outliers recentemente

Agenda

- Definição
- Aplicações
- Tipos de anomalias
- Técnicas
 - Classificação
 - Vizinhos
 - Agrupamento
 - Espectrais
- ~~Grafos, Texto~~
- Perigos

Agenda

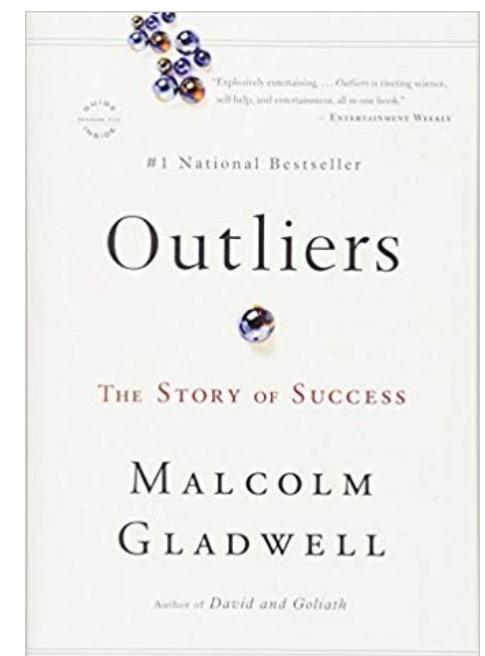
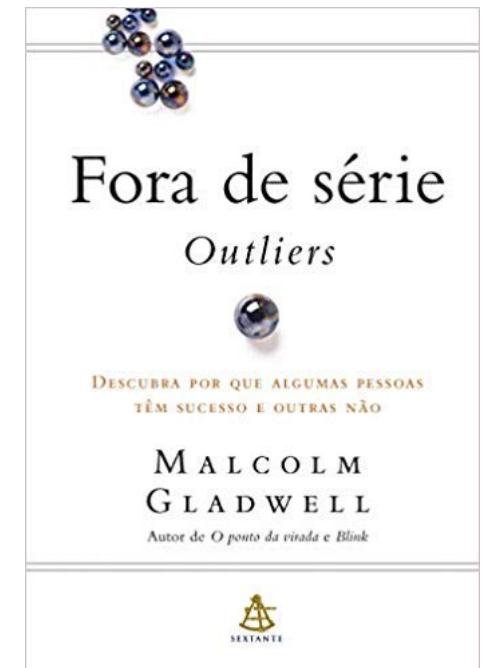
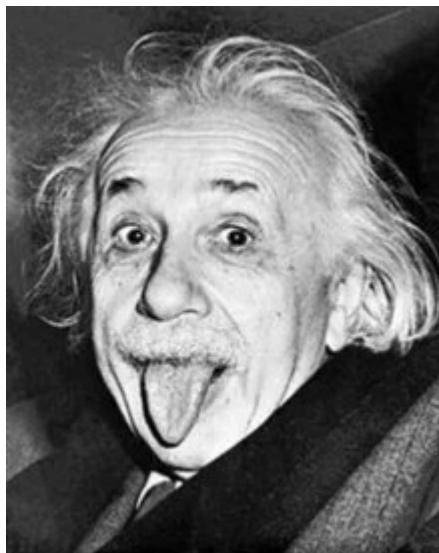
- Parte 1 – Teoria
- Parte 2 - Prática

Detecção de Anomalias



Detecção de anomalias se refere ao problema de encontrar padrões que desviam do comportamento esperado.

Anomalias



Outros nomes

- Outliers
- Observações discordantes
- Exceções
- Aberrações
- Surpresas
- Novidades
- Peculiaridades
- Contaminantes

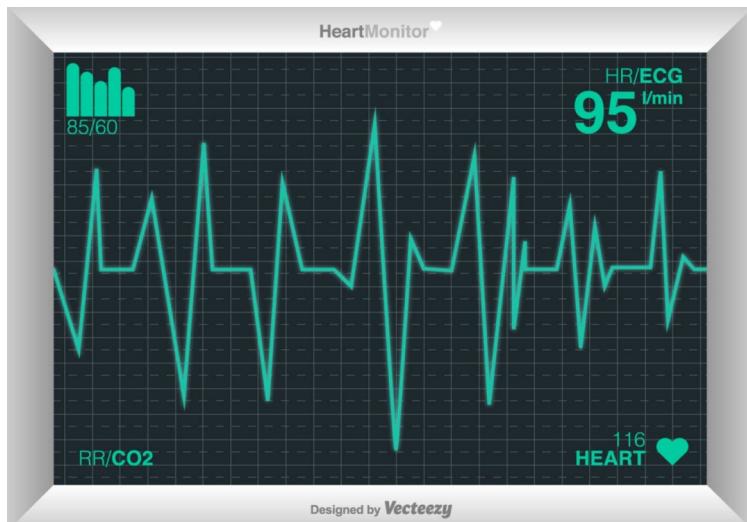
Aplicações

Aplicações

- Detecção de Fraude: cartões de crédito, seguros, manipulação do mercado financeiro, medidores de energia
- Segurança: detecção de intrusão (IDS), câmeras de vigilância, espionagem
- Detecção de Faltas: sistemas críticos industriais, transporte, abastecimento
- **Saúde: detecção de epidemias, monitores cardíacos, detecção de quedas, diagnóstico**

Saúde

Monitoramento Cardíaco



Detecção de quedas



Diagnóstico por Imagem

Saúde - COVID 19

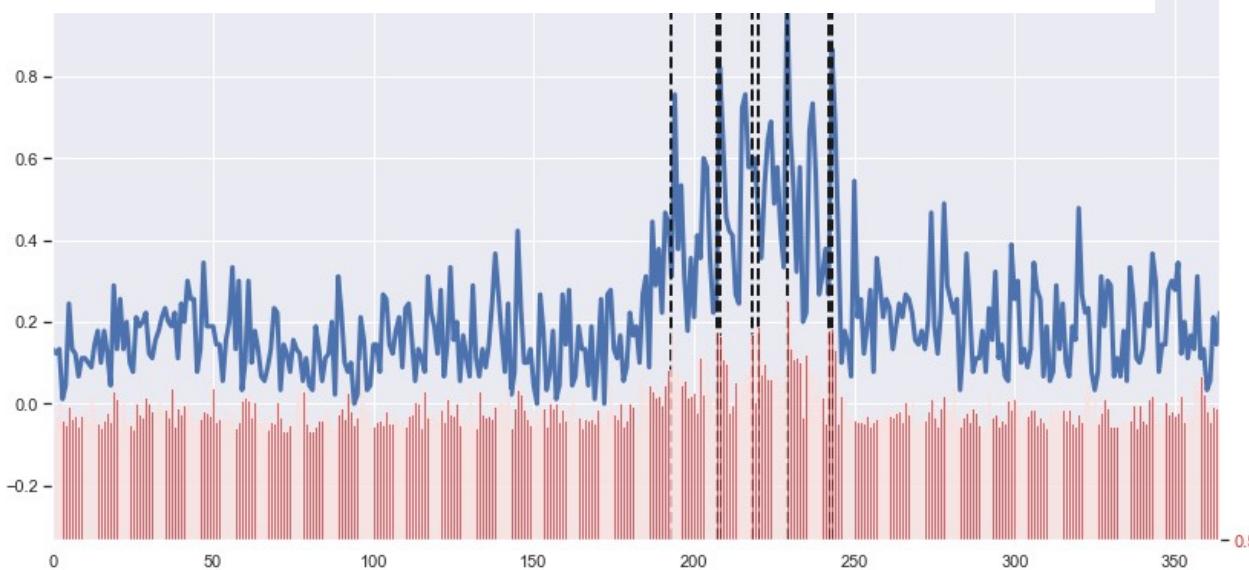
Monitoramento de quarentena

Assessing quarantine implementation - Spain



* Median of NO₂ measurements in the most affected city (Madrid), 5 days rolling average over time series

** Average daily NO₂ measurements from the begining of 2020 until the first day after 10 deaths



Detecção de Epidemias

Fraude

Clonagem de Cartão



Roubo de
Energia



Manipulação
de Mercado
Financeiro

Segurança

Câmeras de Vigilância



Detecção de Intrusão



Tesla: Modo
Sentinela

Militar



Vigilância/Espionagem

Detecção/destruição de mísseis

Texto

Correção de Texto



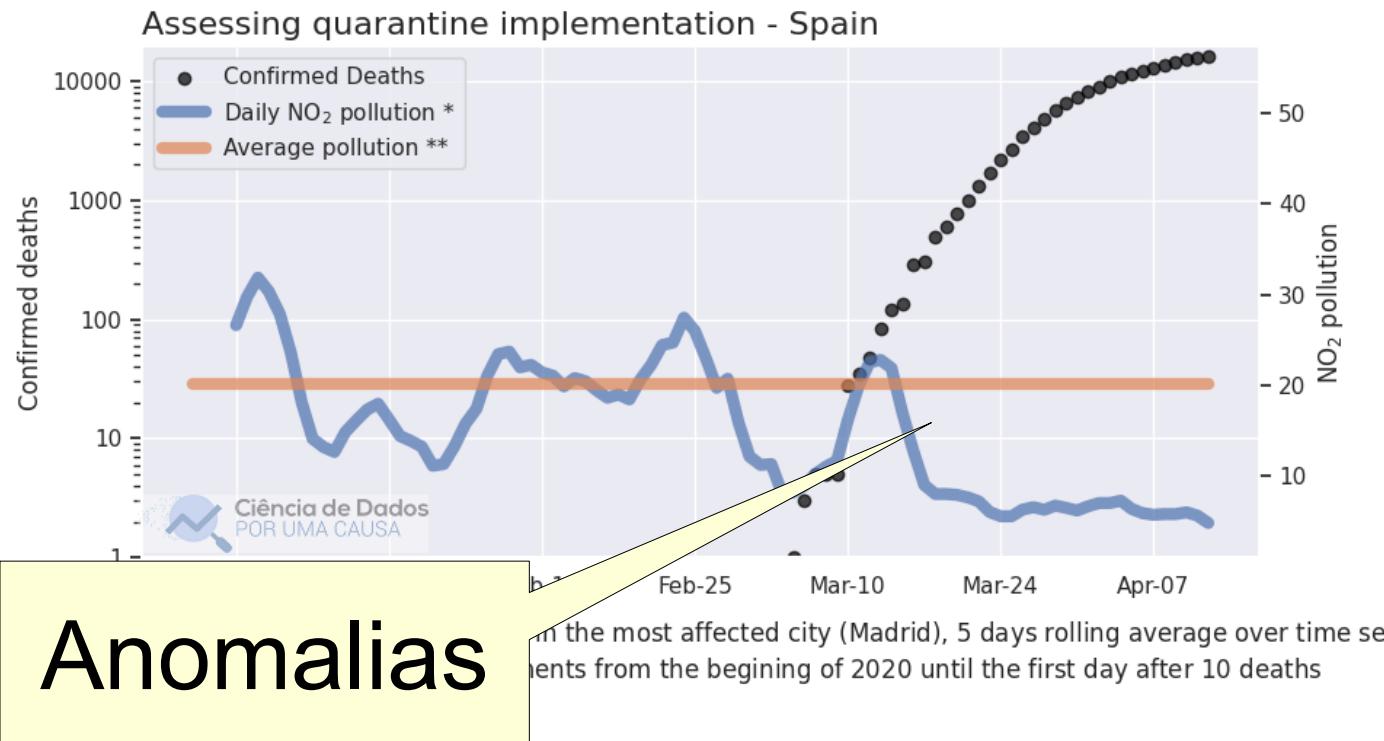
Diagnóstico de
Condições Psiquiátricas



Pesquisa@UTFPR

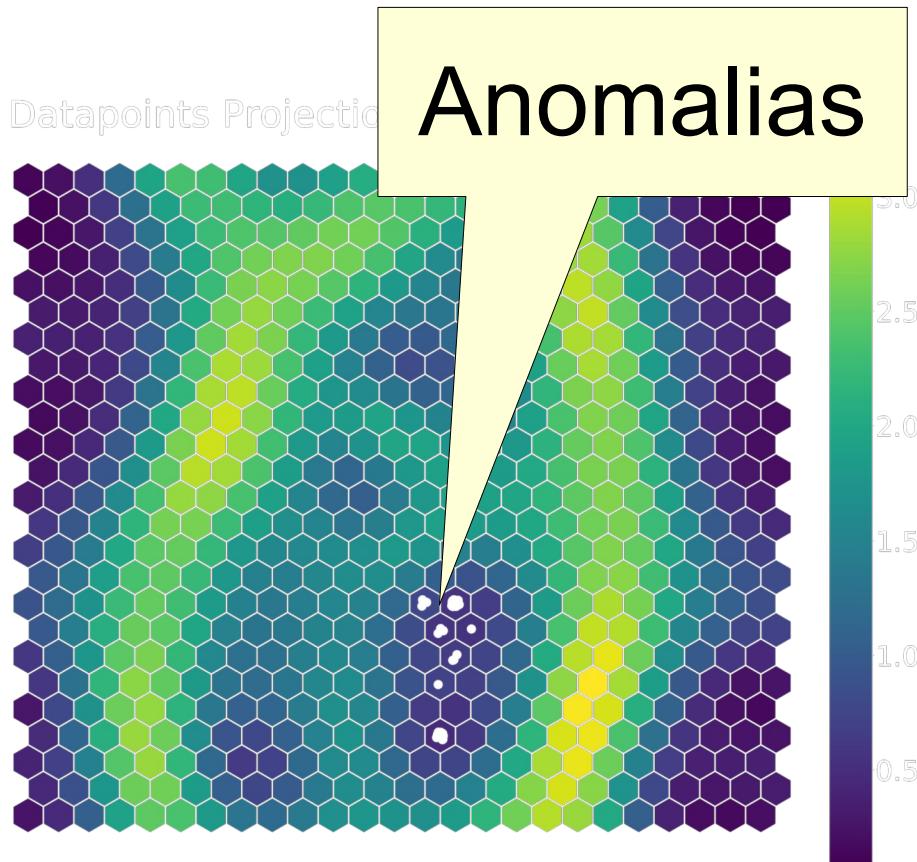
Detecção de Anomalias em Locomotivas

- Projeto: COVID-19 Como está meu país?
- Acompanhamento da intensidade da adesão à quarentena entre países.



Detecção de Anomalias em Locomotivas

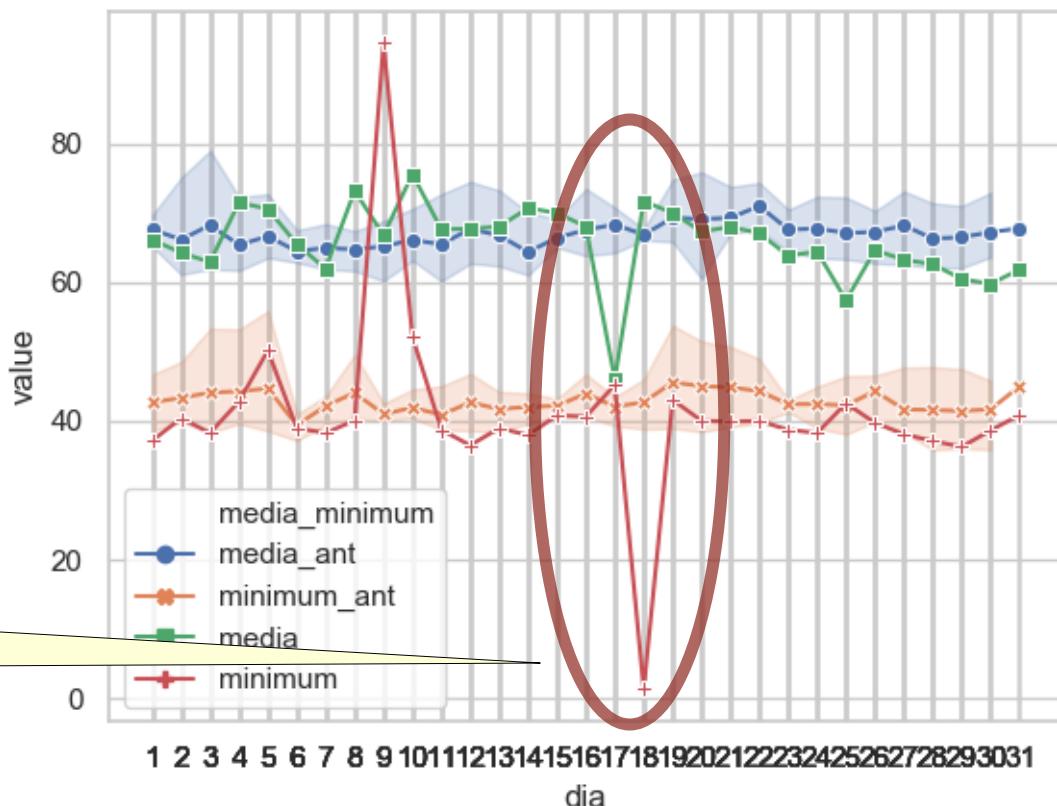
- Mestrando: Felipe Benghi
- Acompanhamento em tempo real do funcionamento de locomotivas ao redor do mundo.
- Determinação de parâmetros de controle
- Detecção e prevenção de falhas
- Auxílio aos técnicos em campo



Detecção de Anomalias em Distribuição de Água

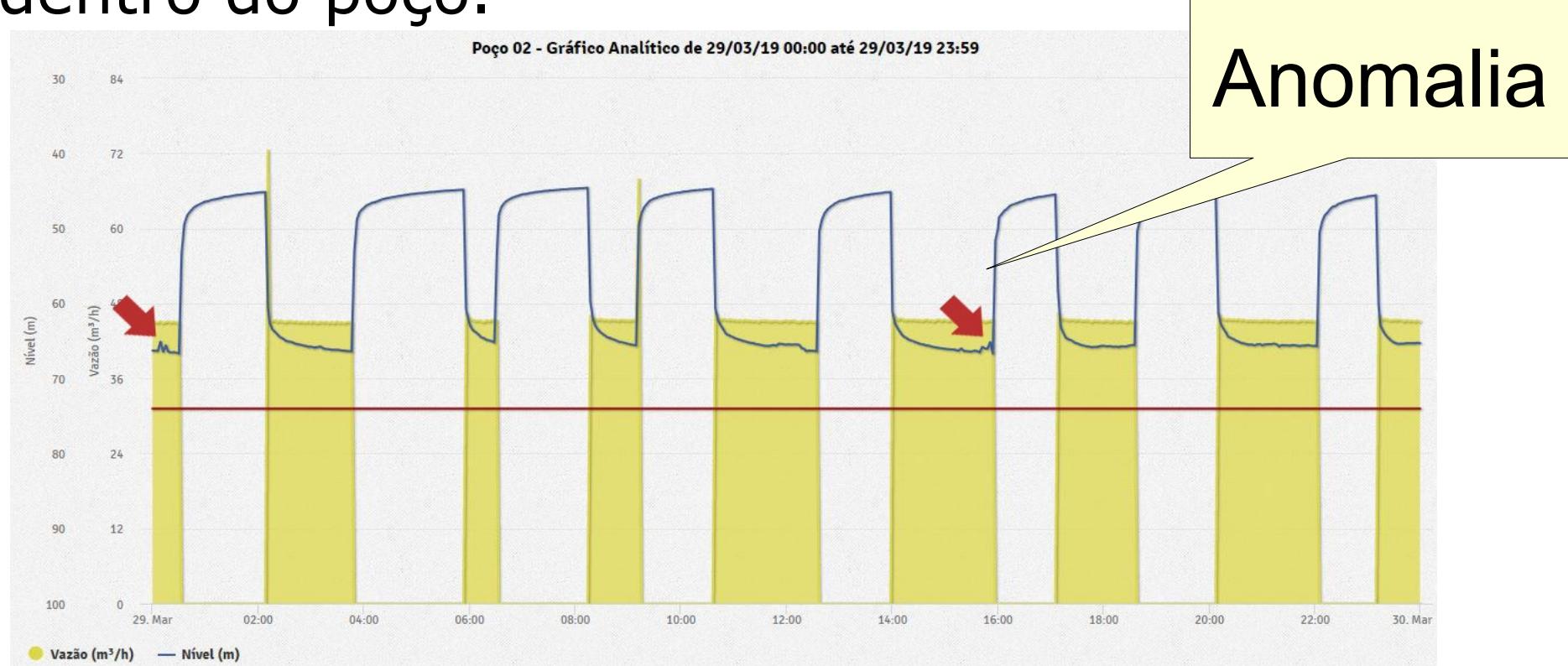
- Mestrando: Willian Muniz do Nascimento
- Análise de zonas de pressão de Curitiba
- Zona de pressão pode ser estação de tratamento, estação de distribuição, bairro, vila, etc.

Anomalia



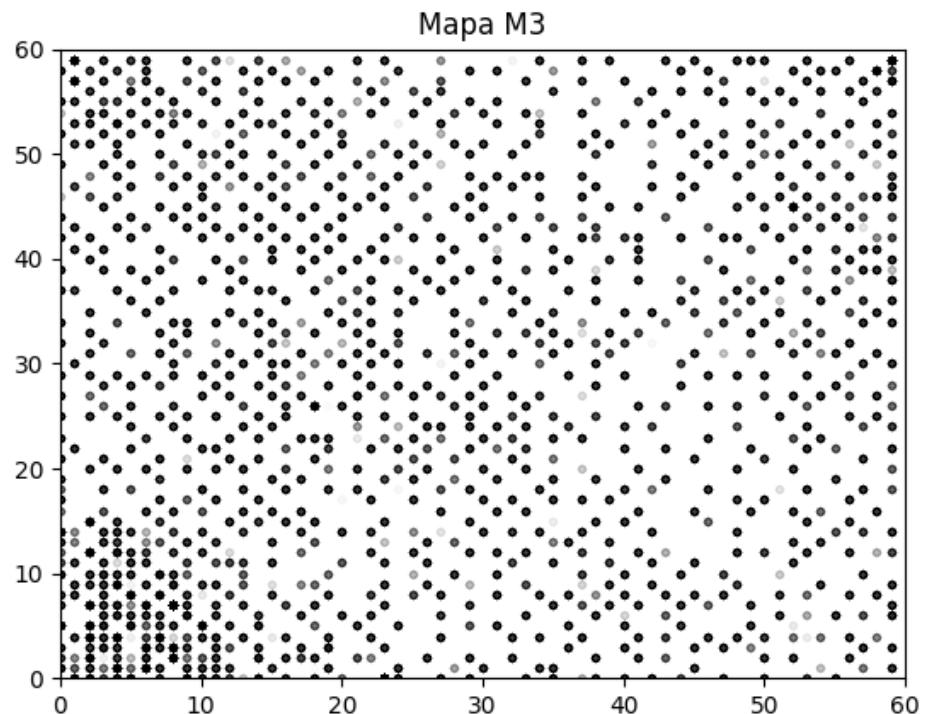
Detecção de Anomalias em Poços Profundos

- Mestrando: Dionei Miodutzki
- Variáveis mais importantes: volume de água retirado, vazão instantânea e nível da água dentro do poço.



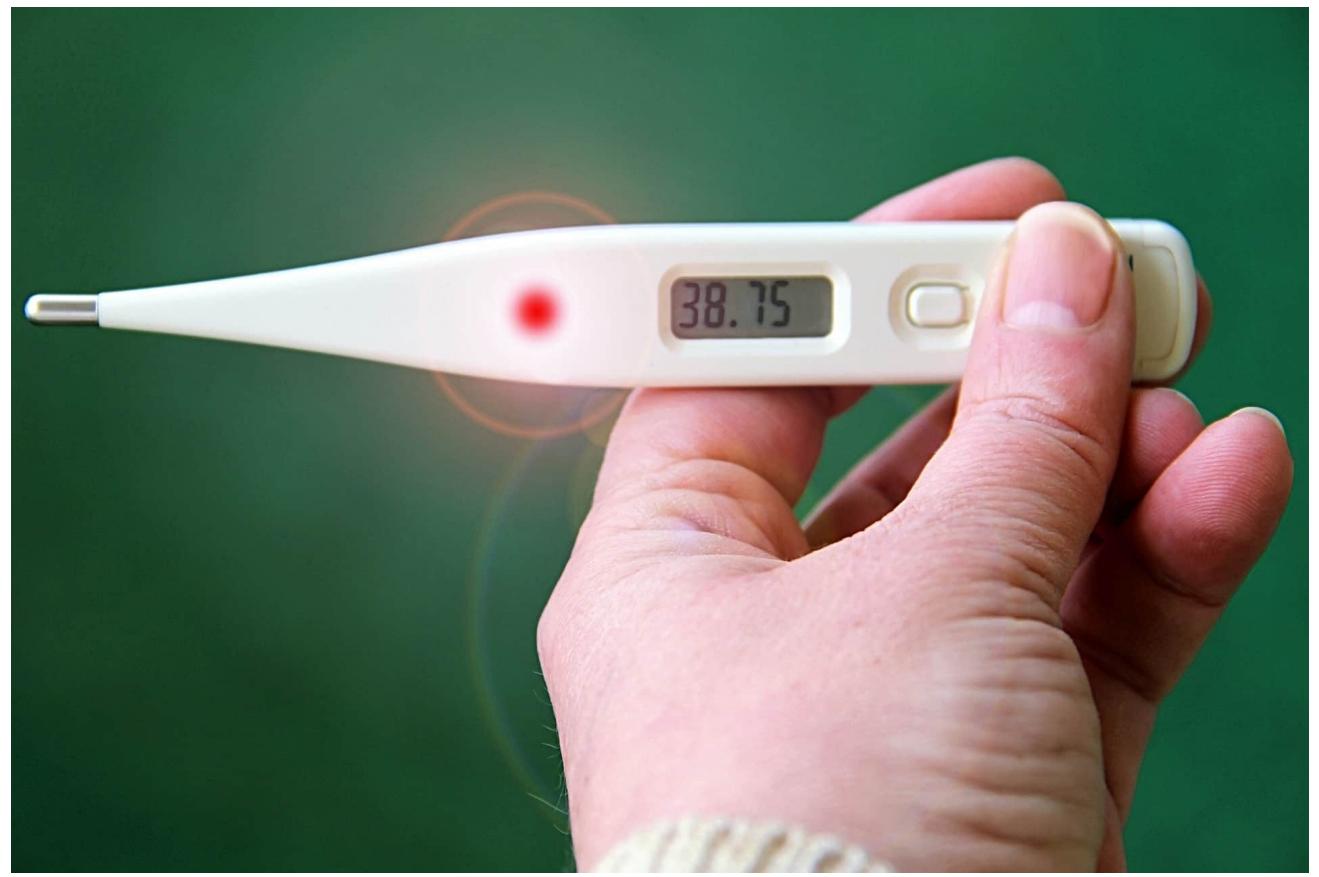
Detecção de Fraude em Energia Elétrica – Processamento Distribuído

- Análise de leituras de consumo de energia
- Muitas instâncias e alta dimensionalidade
- Construção de modelo SOM no Spark



Anomalias?

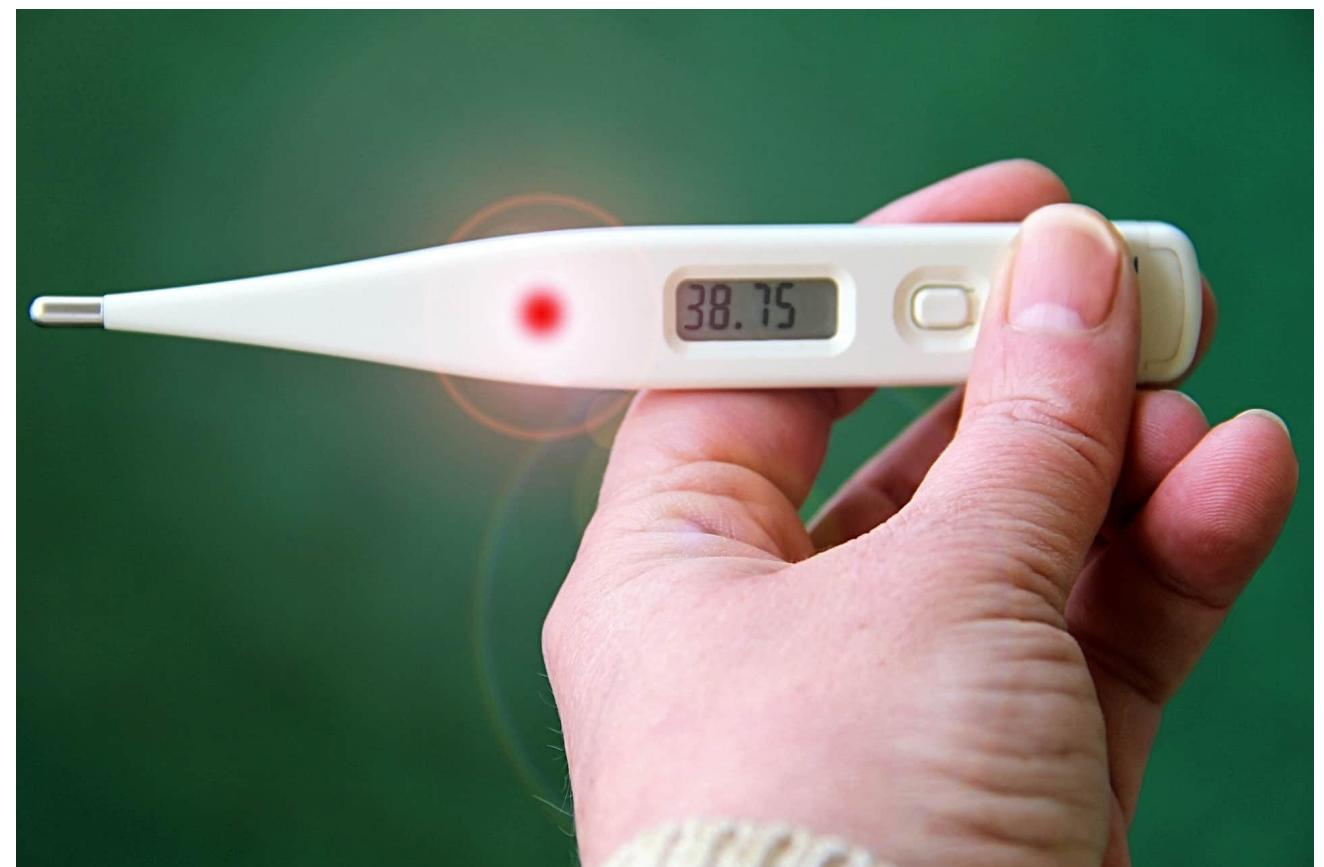
Temperatura: 36,4 – 36,3 – 36,7 – 36,6 – 36,6 – 40,4 – 36,3 – 36,5



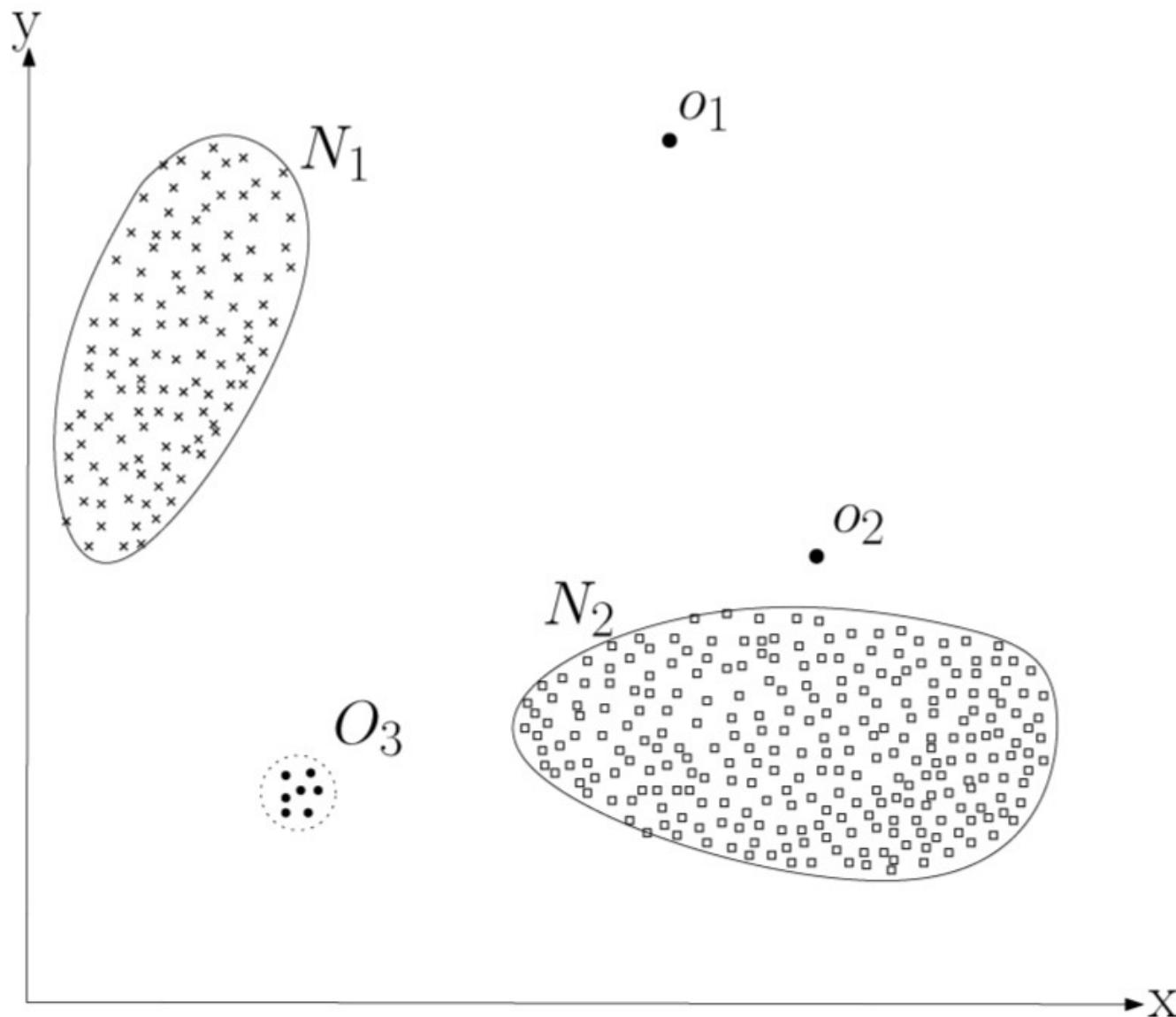
Anomalias?

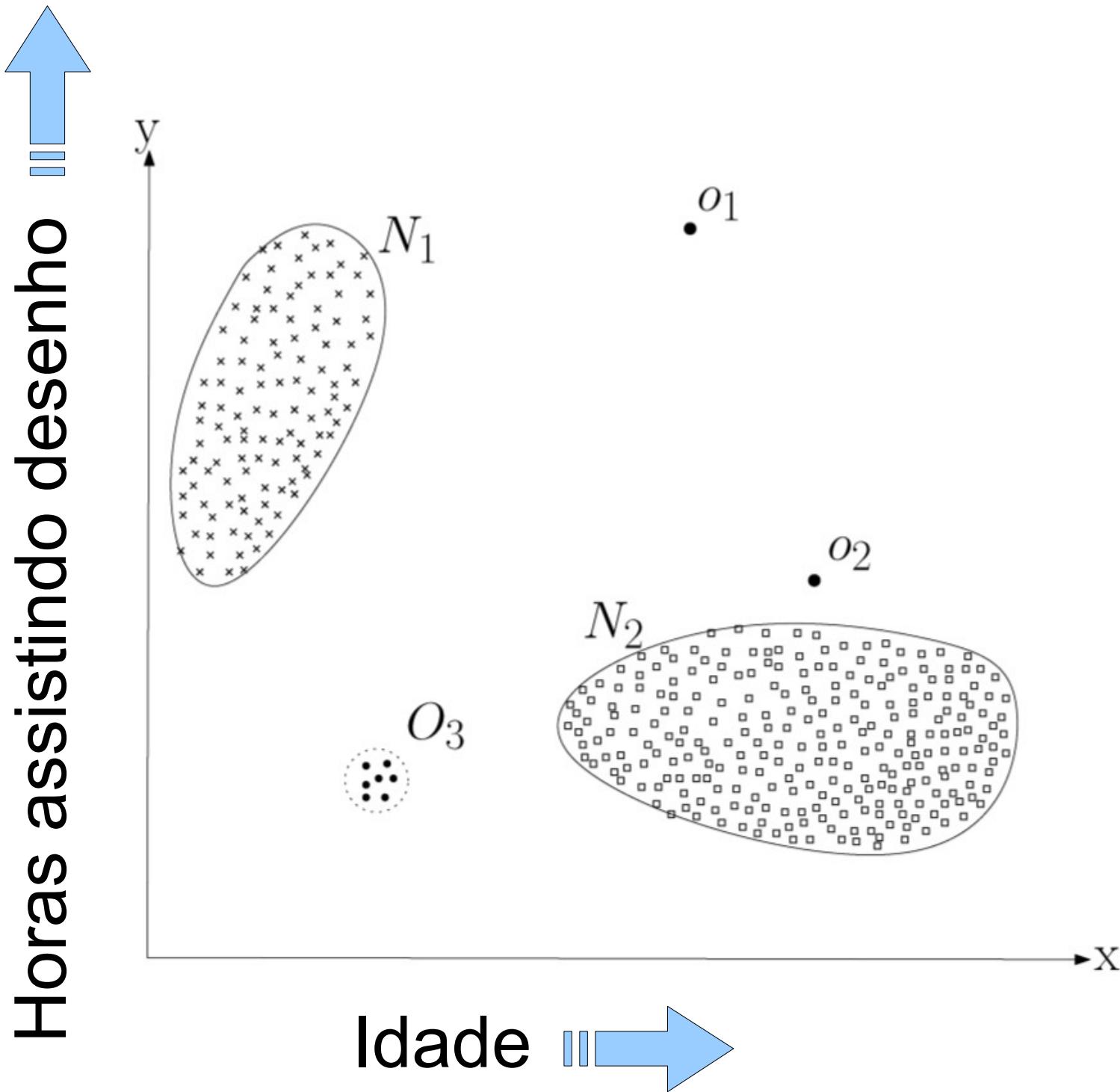
Temperatura: 36,4 – 36,3 – 36,7 – 36,6 – 36.6 – 40,4 – 36,3 – 36,5

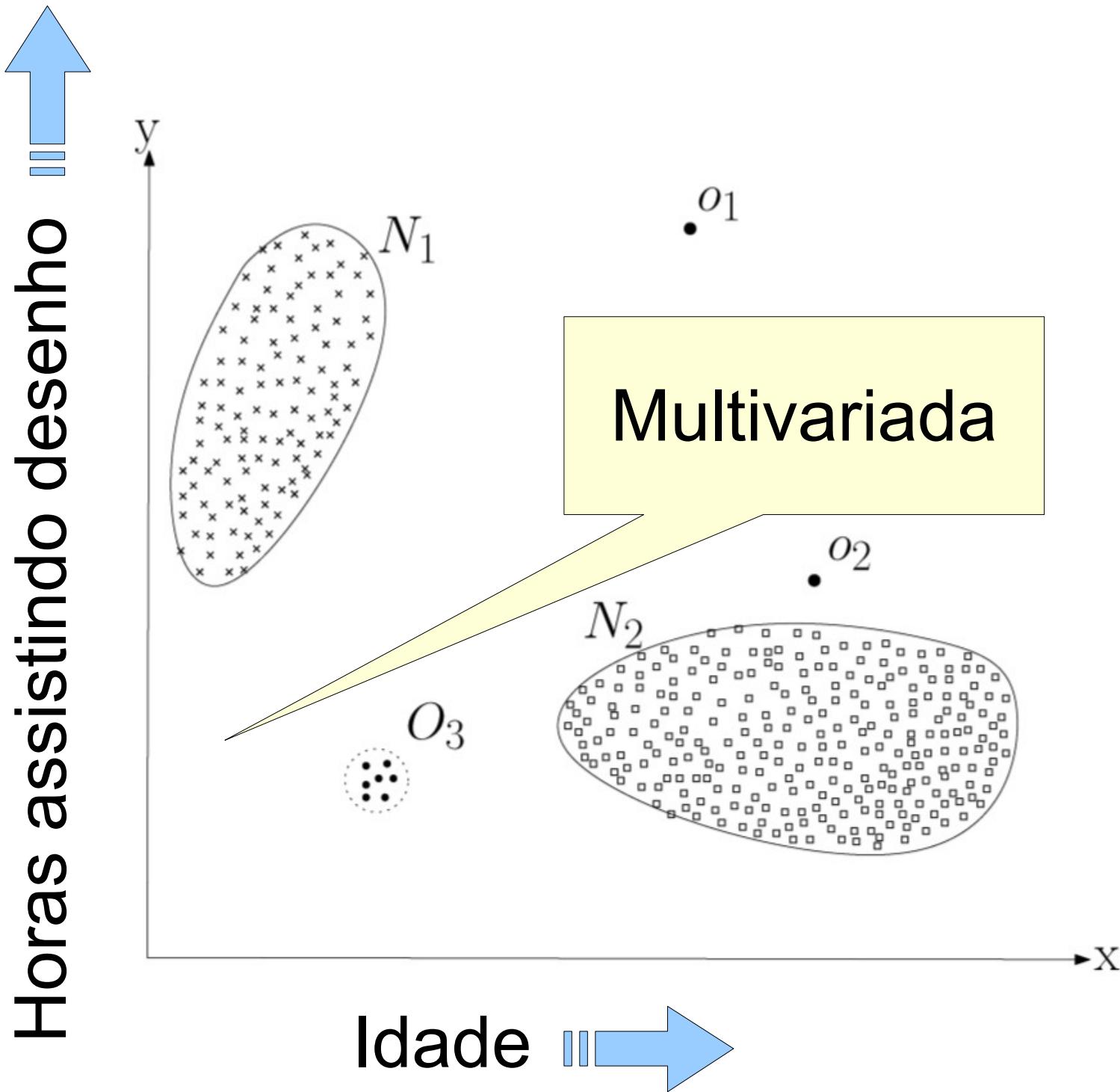
Monovariada

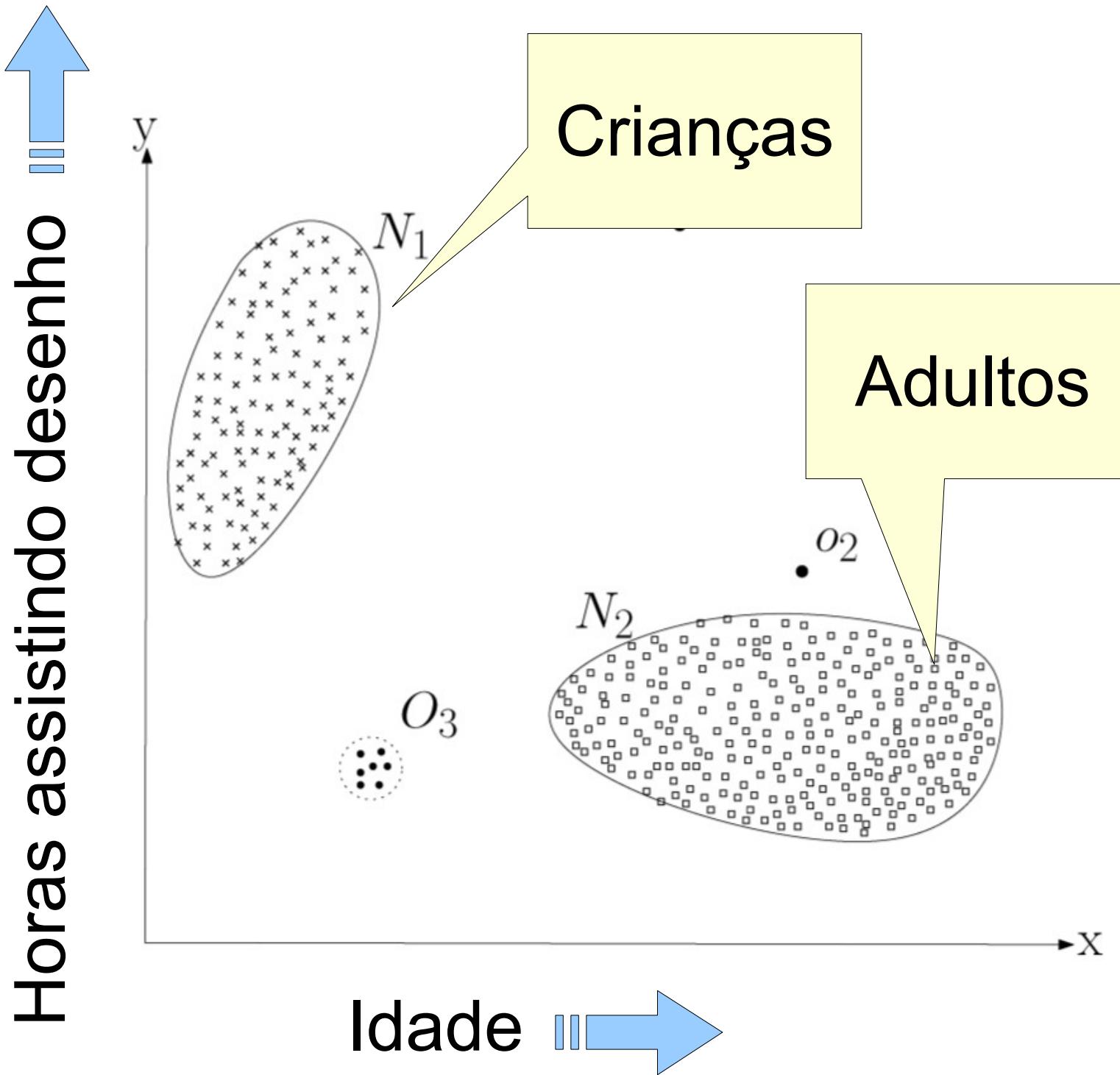


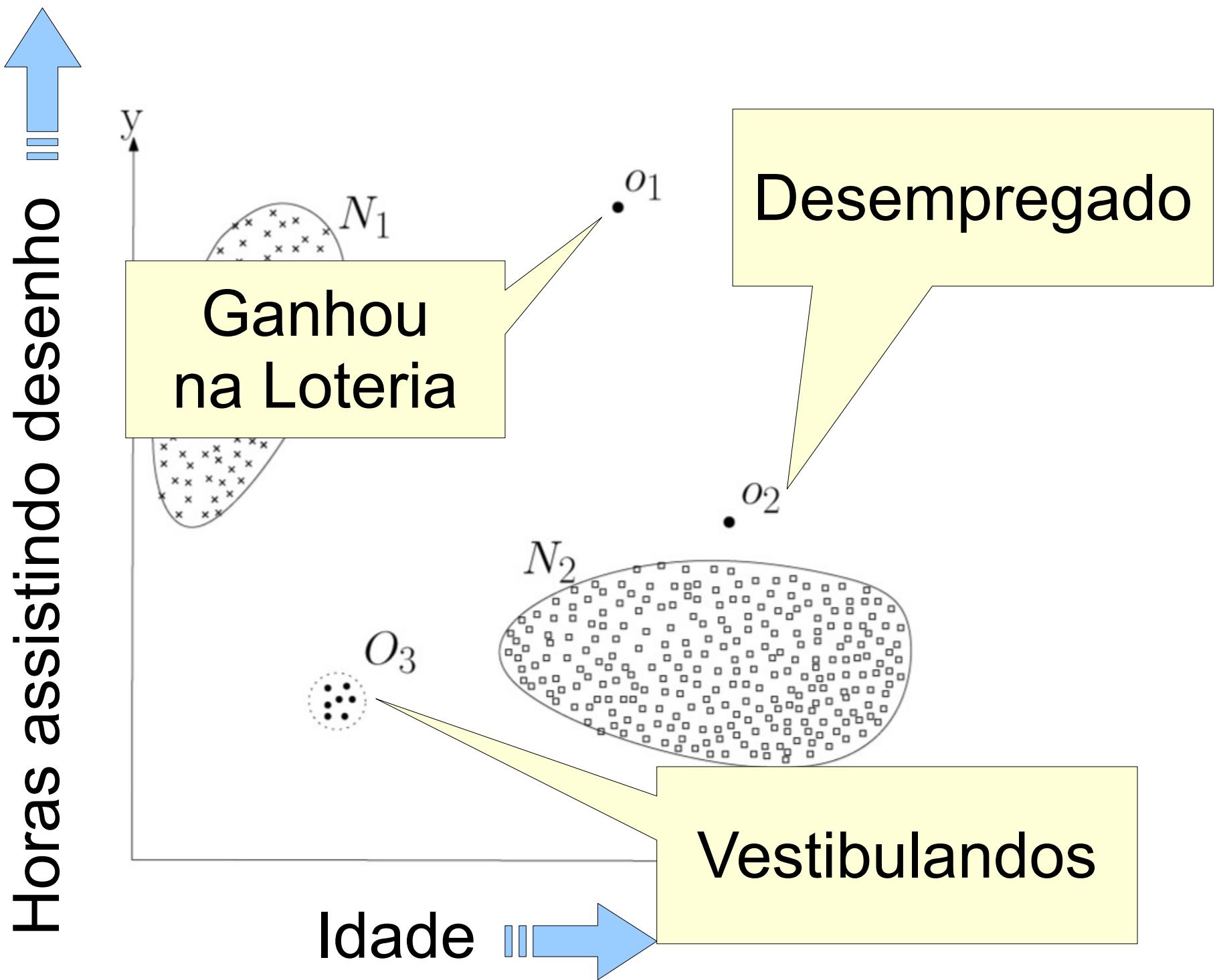
Anomalies?

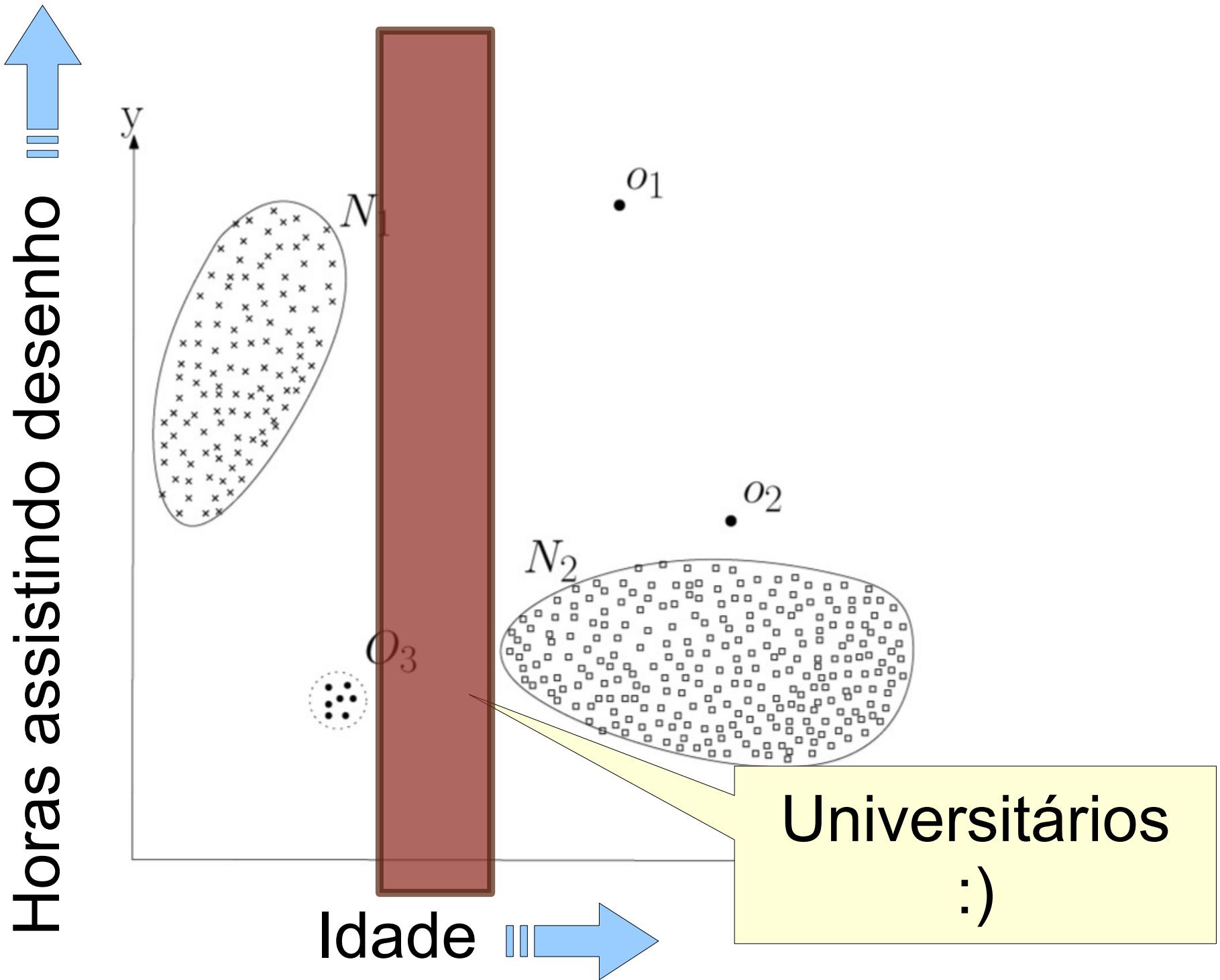












Desafios

- Definir a região de normalidade englobando todos os casos normais
- Divisão entre normal e anormal pode ser imprecisa
- Em casos de segurança e fraude, o agente se adapta para parecer normal
- Comportamento pode evoluir com o tempo

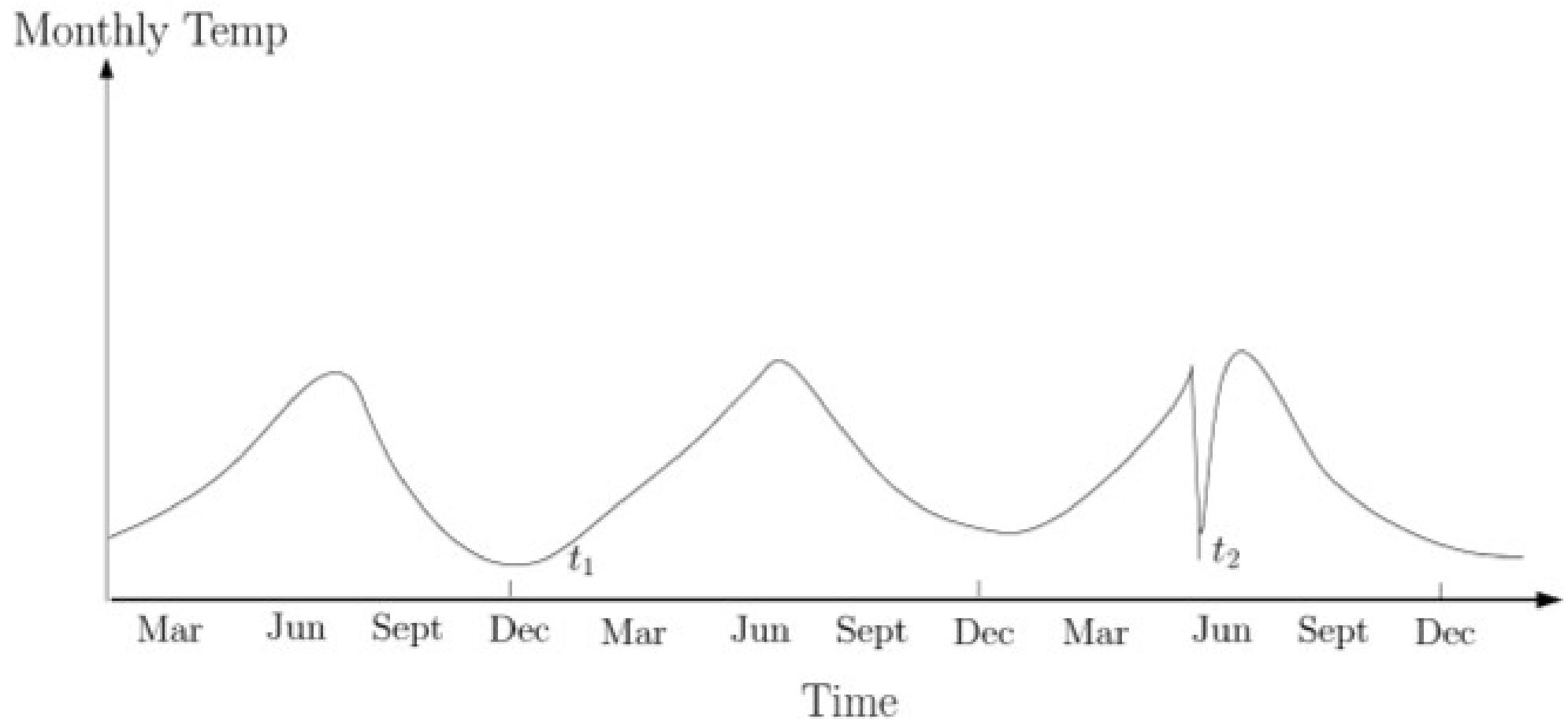
Desafios

- Domínios diferentes têm definições diferentes
- Pouca disponibilidade de dados classificados
- Distinção entre ruído e anomalias reais

Tipos de anomalias

- Anomalia pontual: uma instância dos dados está muito longe das outras. Exemplo: compra muito cara no cartão.
- Anomalia contextual: uma instância só é uma anomalia sob um determinado contexto. Exemplo: R\$200 em restaurante no período de férias pode ser normal.
- Anomalia coletiva: um conjunto de instâncias determina coletivamente um estado anômalo. Exemplo: Saque de dinheiro em locais distantes num período curto.

Anomalia de Contexto



Anomalia de Contexto

Boeing's stock is a drag on the Dow

The 2-day divergence between the performance of the S&P 500 and the Dow has been the greatest in years



Source: MarketWatch

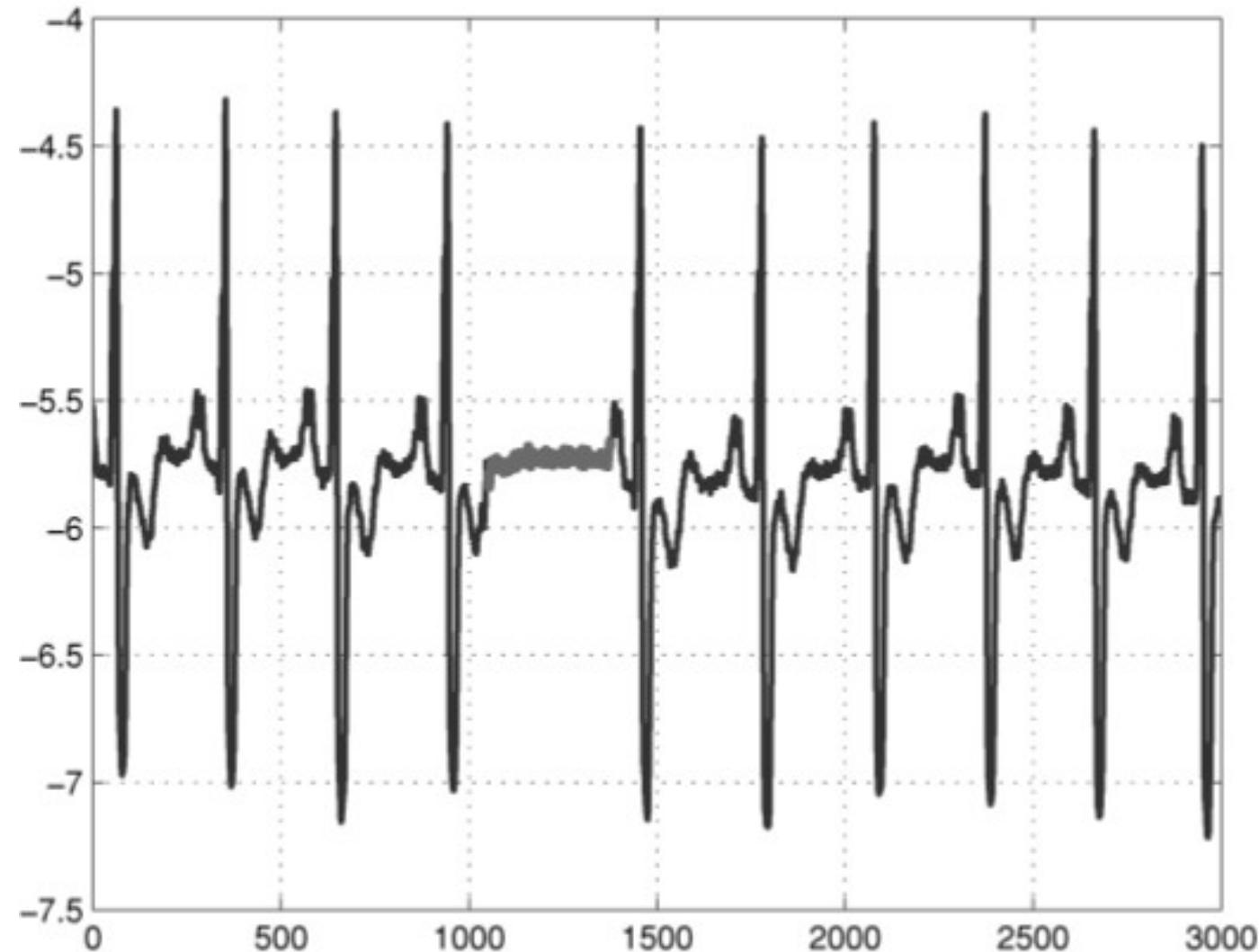
Anomalia de Contexto

- Atributos de contexto: determinam o contexto (vizinhança) da instância.
Exemplo: localização, timestamp
- Atributos de comportamento: medem características não-contextuais. Exemplo: valor da compra, temperatura do motor

Anomalias Coletivas

- Um conjunto de instâncias relacionadas caracteriza uma anomalia
- As instâncias em uma anomalia coletiva podem não ser anômalas isoladamente
- Exemplo: Log de eventos de segurança contendo (buffer-overflow, ssh, ftp) caracteriza um ataque com cópia de dados

Anomalias Coletivas



Arritmia Cardíaca

Dados de Entrada

- Coleção de instâncias (observação, registro, ponto, vetor, evento, amostra, entidade)
- Instâncias são descritas com um conjunto de atributos (variáveis, características, features, dimensões)
- Atributos possuem tipos: binário, categórico, contínuo
- Quantidade de atributos: univariado, bivariado, multivariado

Dados de Saída

- Classificação normal/anomalia
- Classificação + certeza
- Índice de anormalidade

Processo

Domínio da Aplicação

- Detecção de Intrusão
- Detecção de Fraude
- Diagnóstico
- Sistemas Críticos
- Militar...

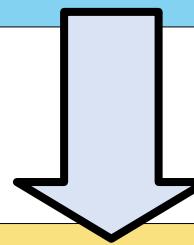
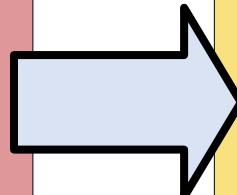
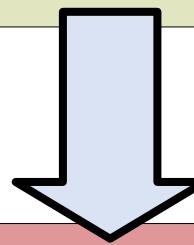
Área de Pesquisa

- Aprendizado de Máquina
- Mineração de Dados
- Estatística
- Teoria Espectral
- Teoria da Informação...

Características do Problema

- Natureza dos Dados
- Classificações
- Tipo de Anomalia
- Tipo de Saída...

Modelo de Detecção de Anomalia



Caso de estudo

Domínio da Aplicação

Detecção de epidemias

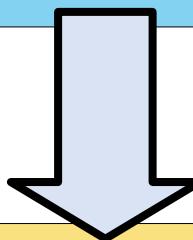
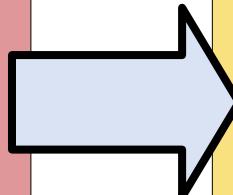
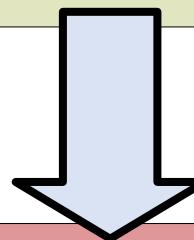
Área de Pesquisa

- Aprendizado de Máquina
- Não supervisionado

Características do Problema

- Registro de atendimento
- Sem info de normalidade
- Anomalia contextual
- Grau de anormalidade

Modelo de Detecção de Anomalia



Problemas Relacionados

- Classificação
- Detecção de novidade
- Remoção de ruído

Problemas Inversamente Relacionados

- Sistemas de Recomendação:
Recomendam algo dentro do “esperado”.
Modelo ajustado pode ser usado para
identificar o “inesperado” (anomalia)
- Clusterização: Identificam áreas de alta
densidade de observações. Podem ser
adaptados para identificar áreas de baixa
densidade (anomalias)

Abordagens

- Estatística
- Machine Learning
 - Classificação
 - Vizinho mais próximo
 - Clusterização
- Espectrais

Estatística

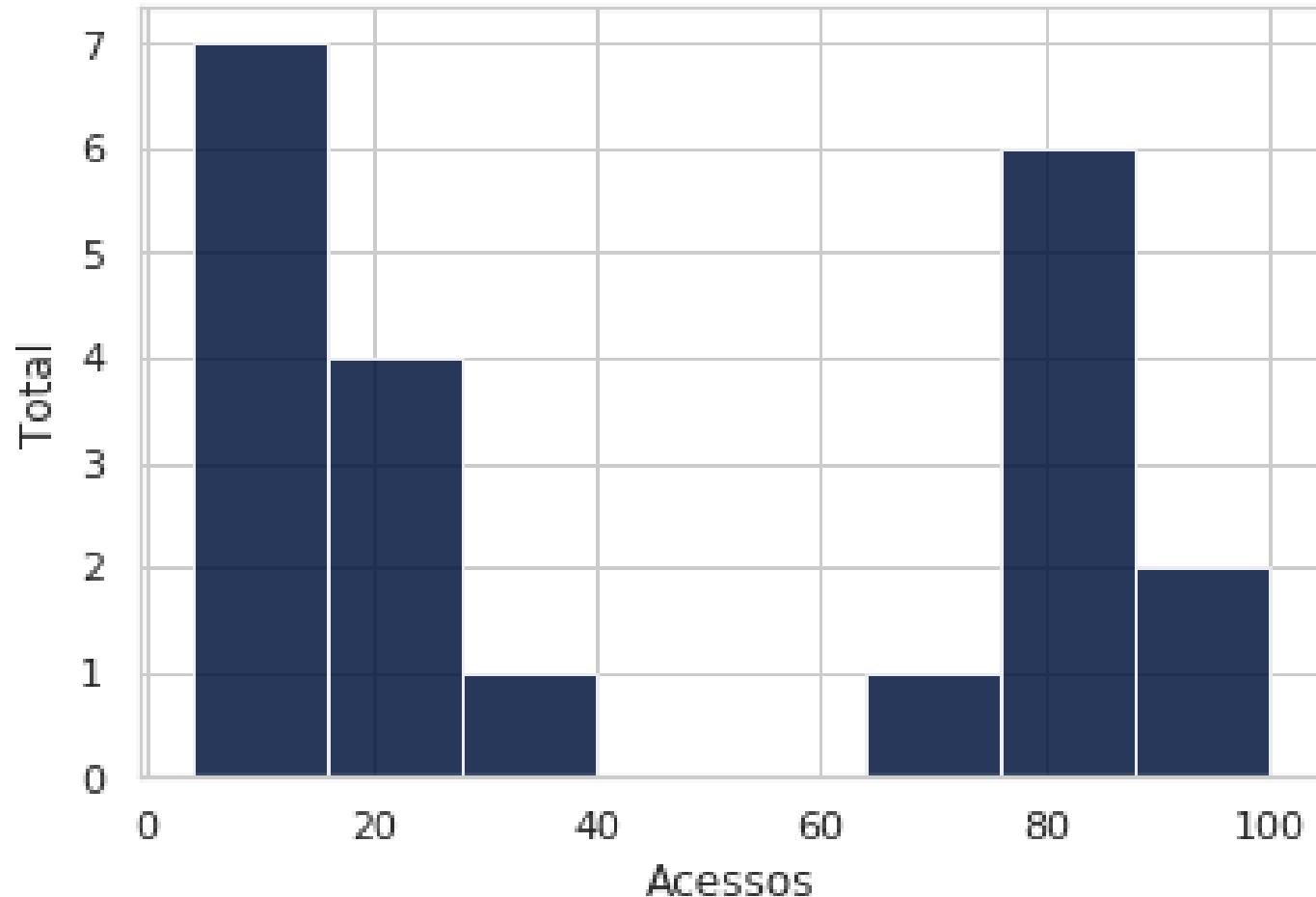
Ideia: Instâncias normais aparecem em regiões de alta probabilidade de um modelo estocástico. Anomalias aparecem em regiões de baixa probabilidade.

- Técnicas Não-Paramétricas
- Técnicas Paramétricas

Histograma

- Técnica não-paramétrica
- Anomalias são instâncias que pertenceriam a bins pequenas ou vazias
- Exemplo: número de acessos por hora em um servidor

Histograma

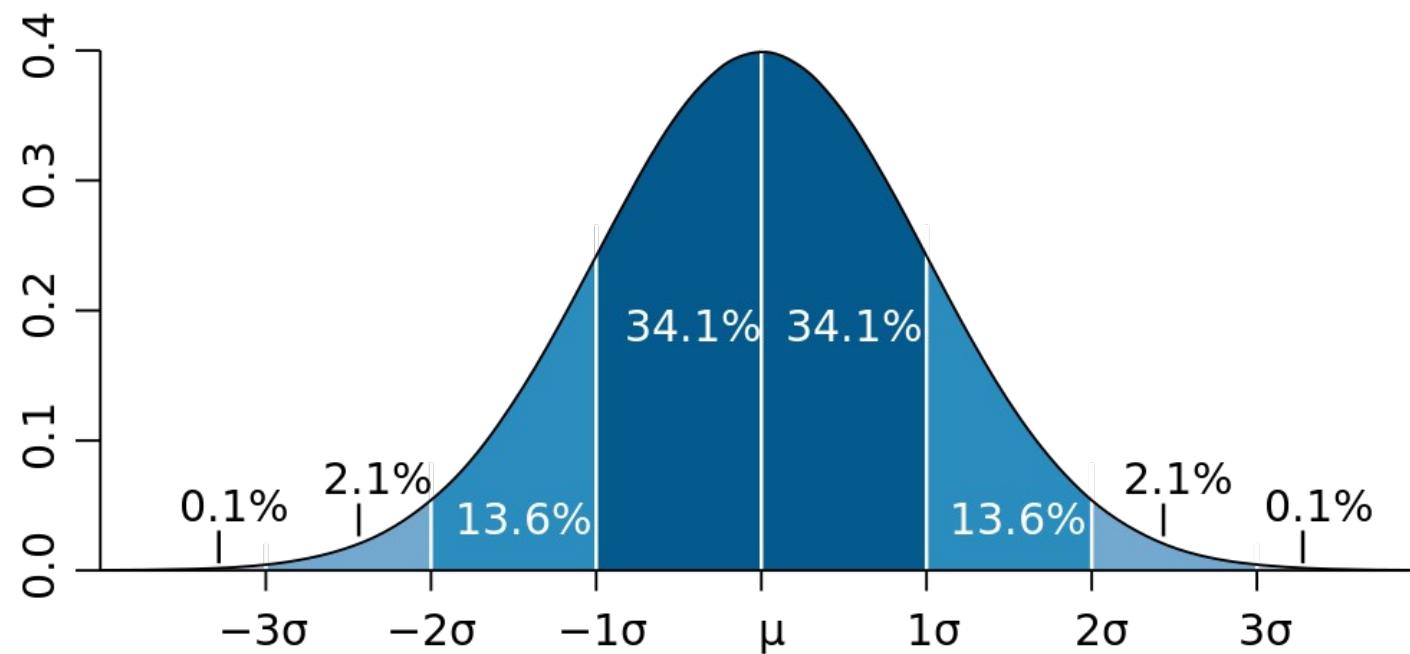


- 23 acessos/hora seria uma anomalia?
- e 56? e 200?

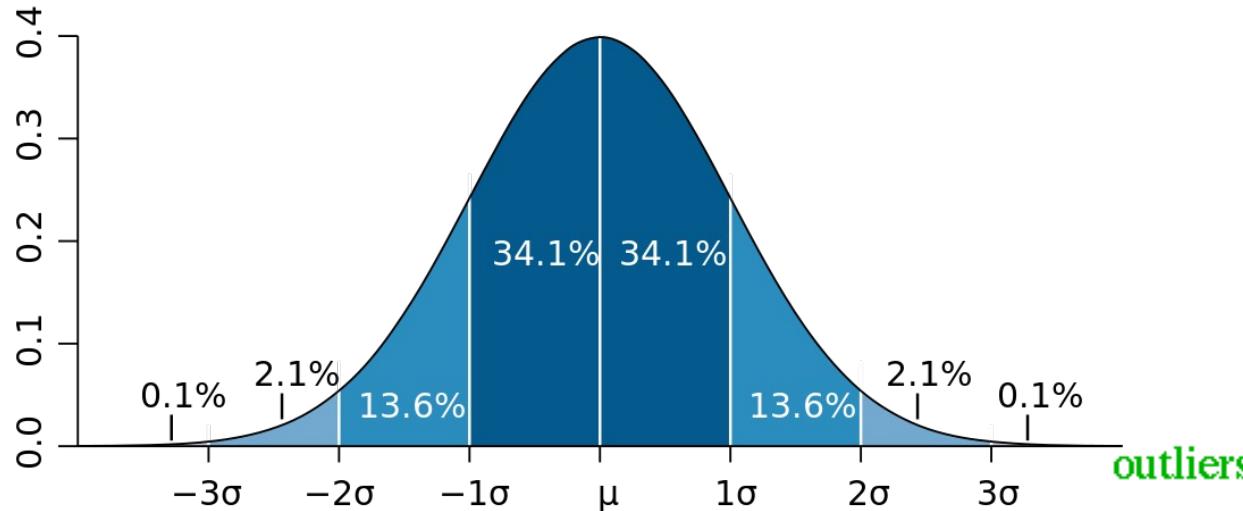
Modelo Gaussiano

- A distância do dado para a média é o índice de anomalia para instância
- Distância considerando a distribuição gaussiana (sigmas, z-scores)
- Um nível de corte determina o fronteira para classificação de anomalias

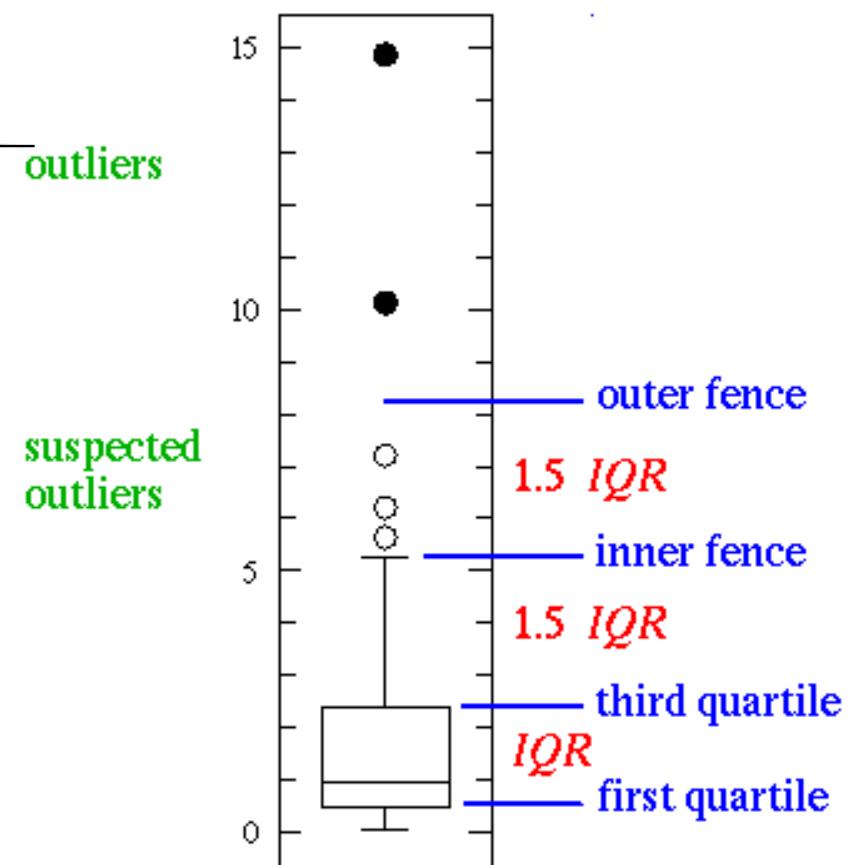
Modelo Gaussiano



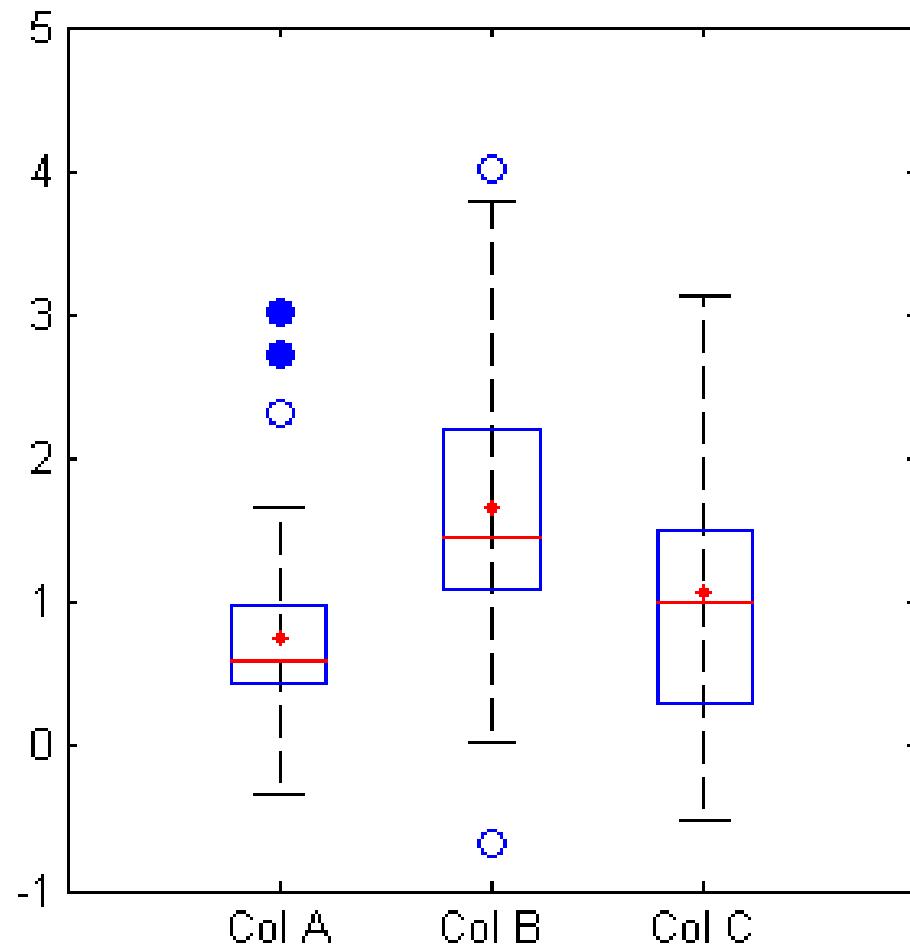
Box plot rule



média/desvio/paramétrico
→ mediana/quartis/não paramétrico



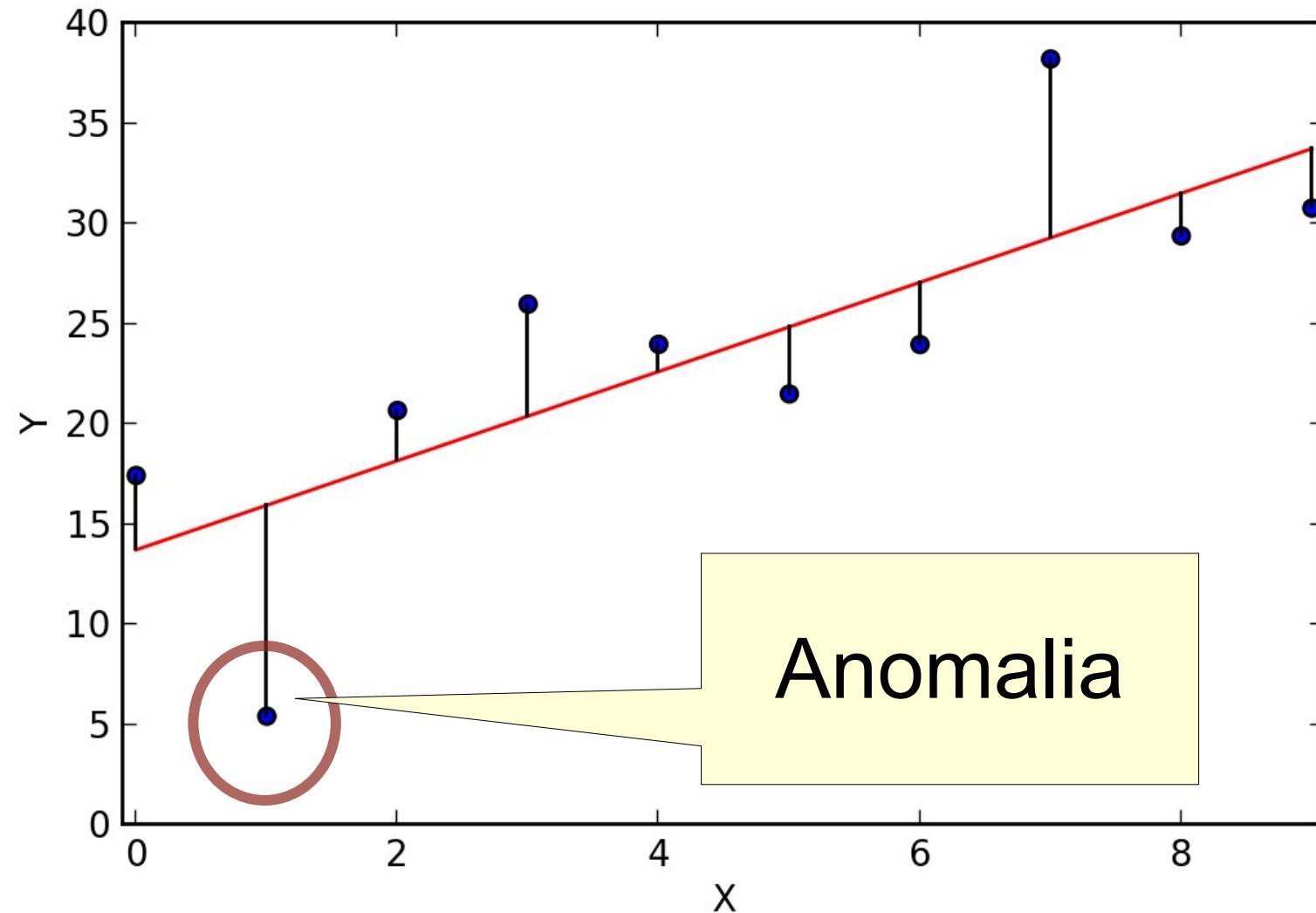
Box plot rule



Modelo de Regressão

- Ideia: Anomalias são observações com valores distantes do previsto pelo modelo de regressão
- Primeiro passo: Determinação dos parâmetros do modelo (fit)
- Segundo passo: Para cada instância de teste, usar o erro residual como representante do índice de anormalidade

Modelo de Regressão



Aprendizado de Máquina

- Supervisionado: Dados de classificação anômalo/normal disponíveis
- Semi-supervisionado: Apenas dados de instâncias normais
- Não supervisionado: Sem dados classificados para treinamento. Considera-se que instâncias normais são mais frequentes

Técnicas

- Baseadas em Classificação
- Vizinhos próximos
- Clusterização

Técnicas de Classificação

- Podem usar algoritmos bem estabelecidos e eficiente para gerar os modelos (SVM, Random Forests...)
- Fase de teste é eficiente (basta aplicar o modelo)
- Difícil obter bons dados de treinamento

Baseado em Vizinhos Próximos

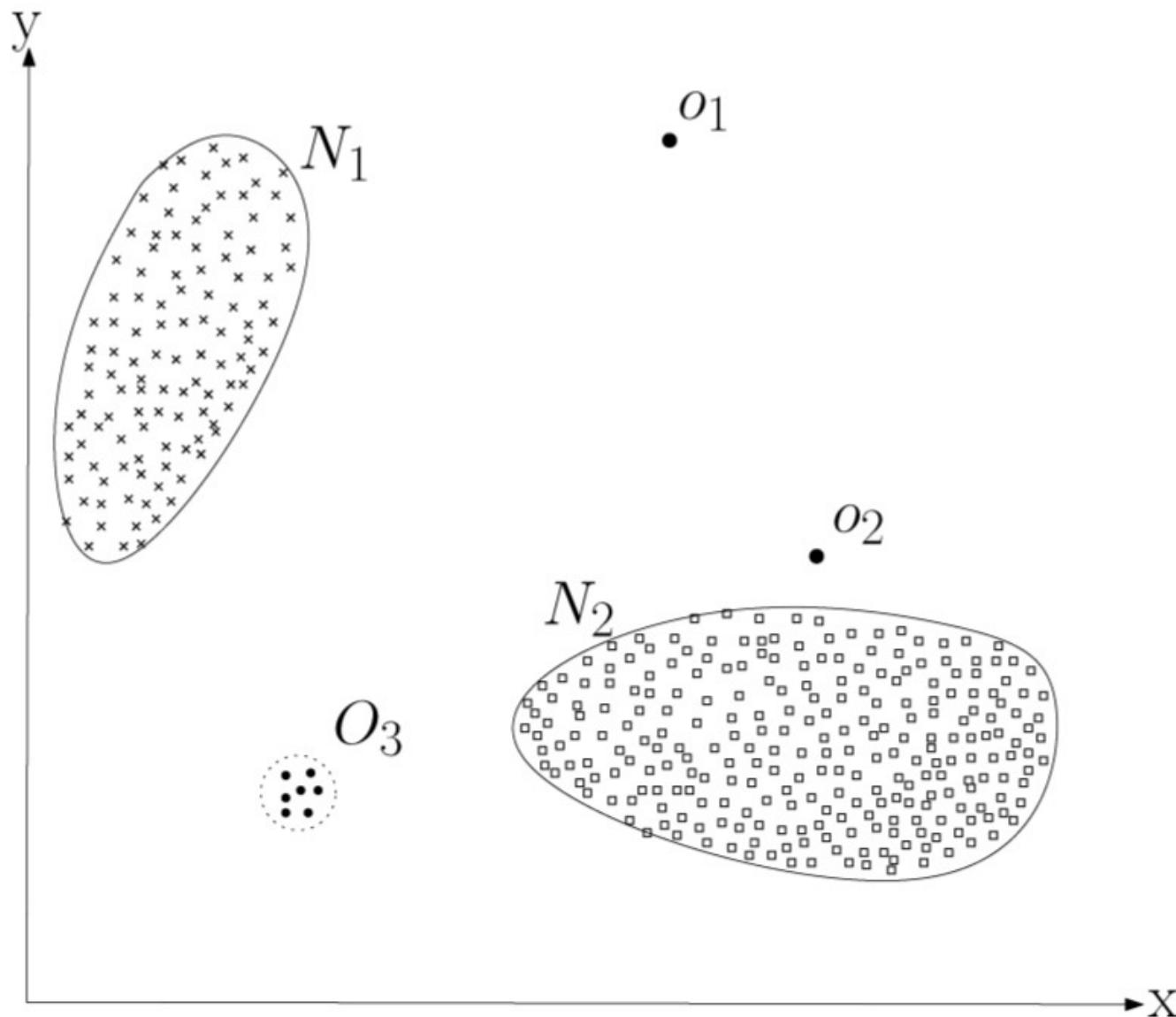
Intuição:

- Se meus vizinhos (observações) estão longe (no espaço das variáveis), provavelmente eu sou um outlier

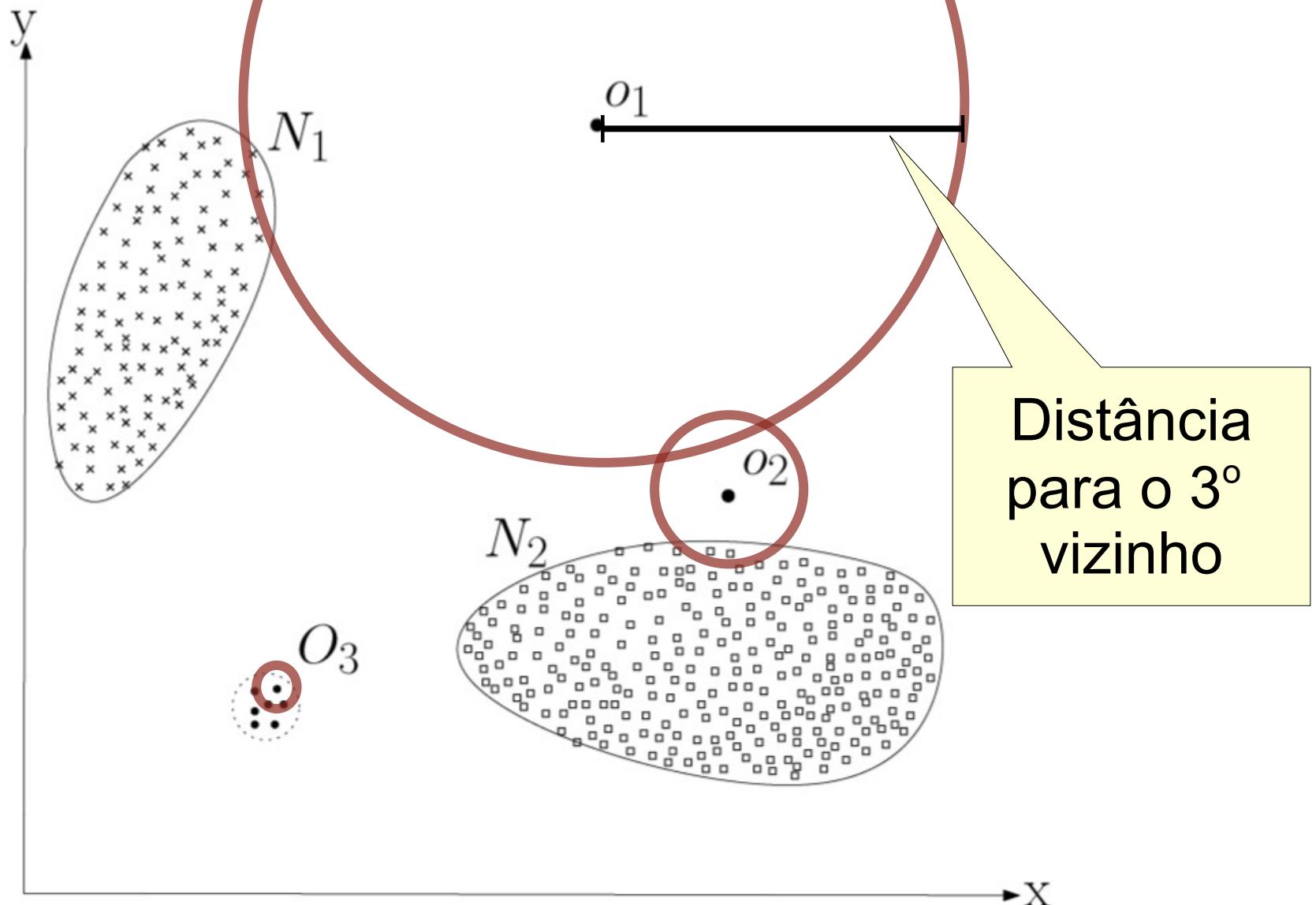
Baseado em Vizinhos Próximos

- Usar densidade da vizinhança para determinar normalidade
- Instâncias em vizinhanças de baixa densidade são consideradas anômalas
- Estimativa: para uma dada instância, a distância para seu k° vizinho mais próximo é equivalente ao raio de uma hiper-esfera centrada na instância contendo k outras instâncias
- Quanto maior este raio, maior a anormalidade

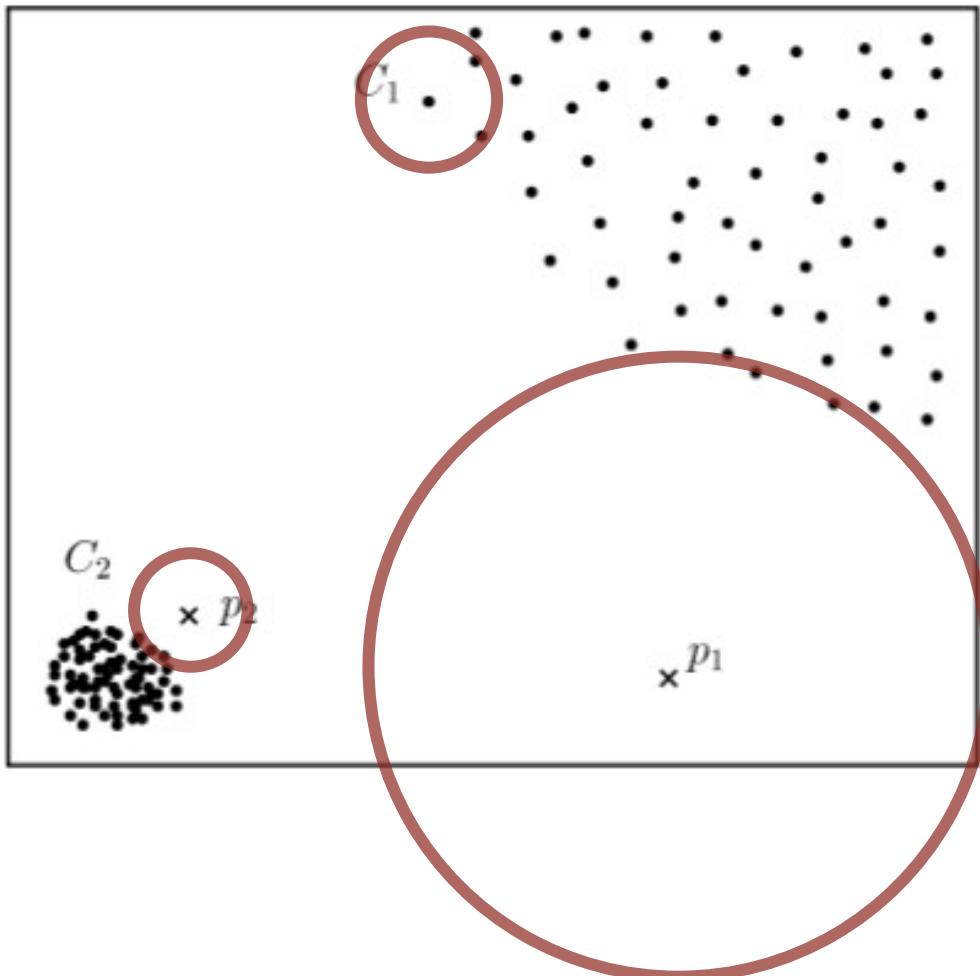
Anomalies?



Anomalias?



Densidade Relativa



Problemas com densidade variável:
P2 deveria ser anômalo, C1 não.

Baseado em Densidade Relativa

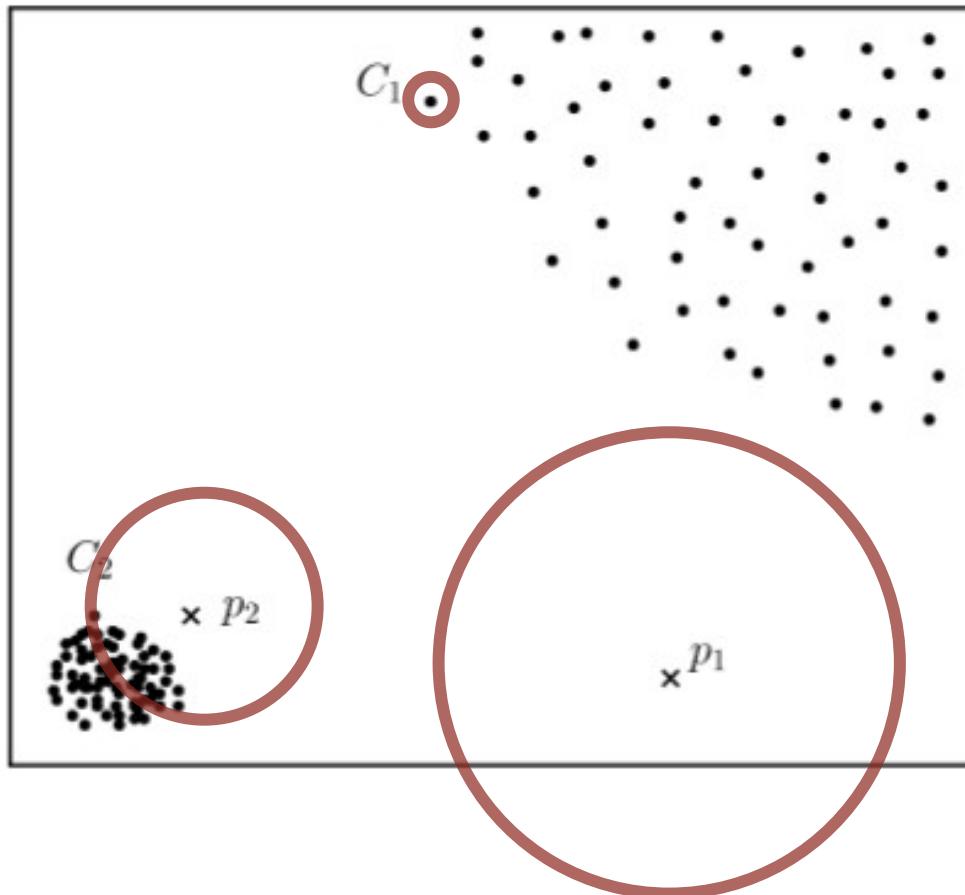
Intuição:

- Se meus vizinhos (observações) estão longe (no espaço das variáveis), provavelmente eu sou um outlier
- Mas se meus vizinhos também estão distantes dos vizinhos deles, então eu não sou tão outlier assim...

Local Outlier Factor (LOF)

- LOF score = razão da média da densidade local dos vizinhos pela densidade local da instância
- Ideia: se a densidade da instância é menor que a dos vizinhos, ela tende a ser uma anomalia
- É uma solução para o problema de densidade relativa

Densidade Relativa LOF



Usando LOF C_1 deixa de ser anômalo porque está em uma região tão densa quanto a dos vizinhos.

Baseadas em Agrupamento

- Ideia 1: Instâncias normais pertencem a um cluster
- Pode-se usar qualquer algoritmo que não force que todas as observações façam parte de um cluster. Ex: DBSCAN, ROCK, SNN
- Pode não ser o melhor modelo porque os algoritmos são otimizados para encontrar clusters, não anomalias

Baseadas em Agrupamento

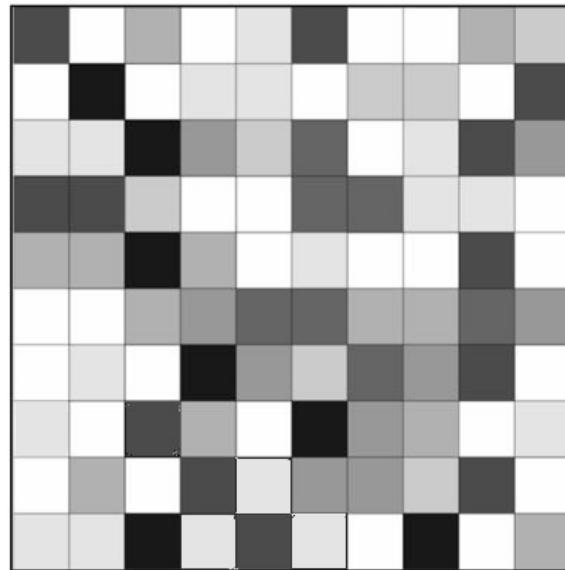
- Ideia 2. Instâncias normais estão próximas do centróide do cluster mais próximo
- Mais flexível que a abordagem anterior (score no lugar de decisão binária)
- Exemplos: Self Organizing Maps (SOM), K-means Clustering

Self Organizing Maps (SOM)

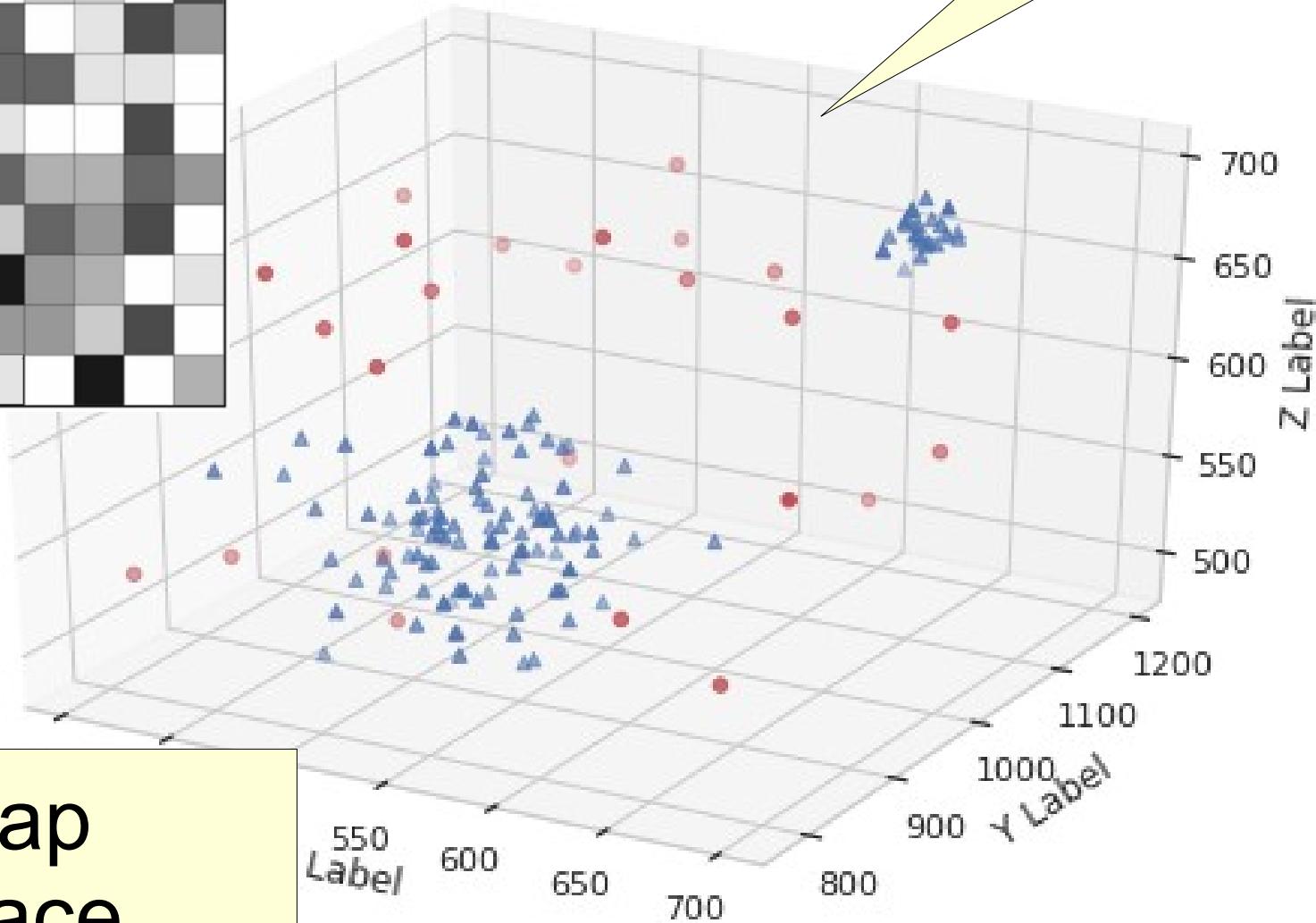
- Técnica de redução de dimensionalidade baseada em aprendizado competitivo
- Instâncias de teste “competem” por representatividade no mapa
- Também conhecidas como mapas de Kohonen.
- Amplamente usadas em detecção de anomalias semi-supervisionada (deteção de intrusão, falhas em aplicações industriais, fraude...)

SOM

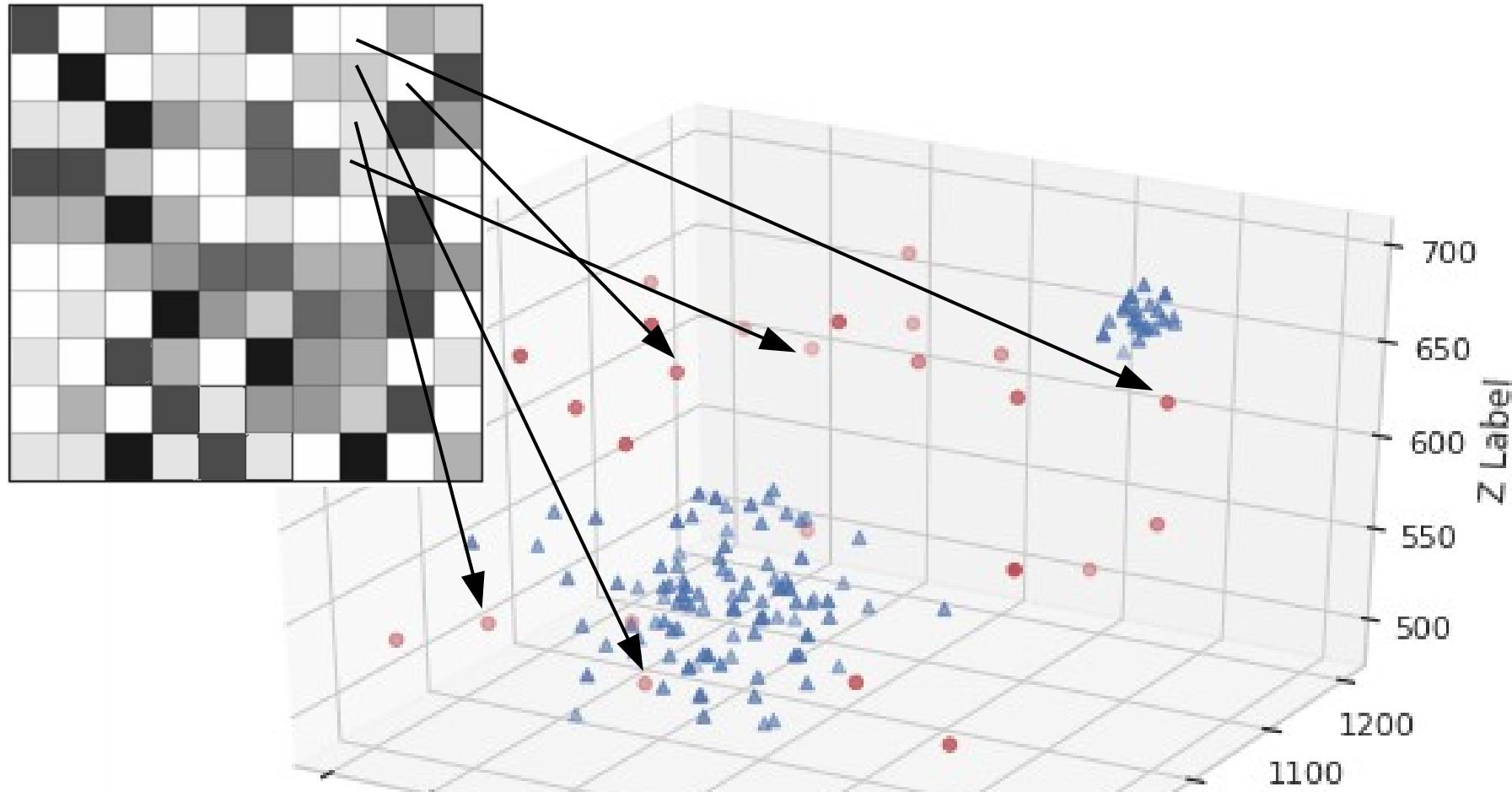
Input space



Map
space

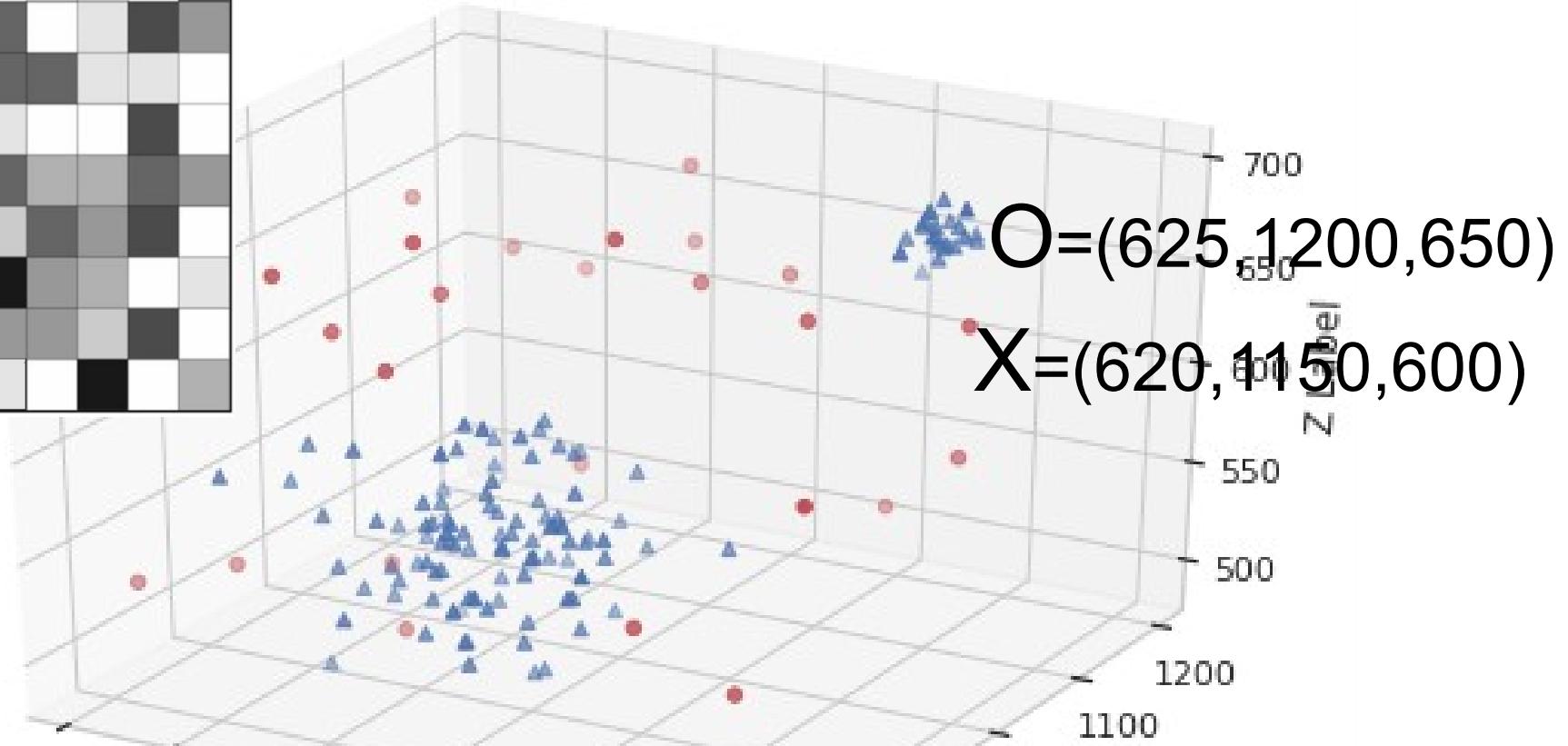
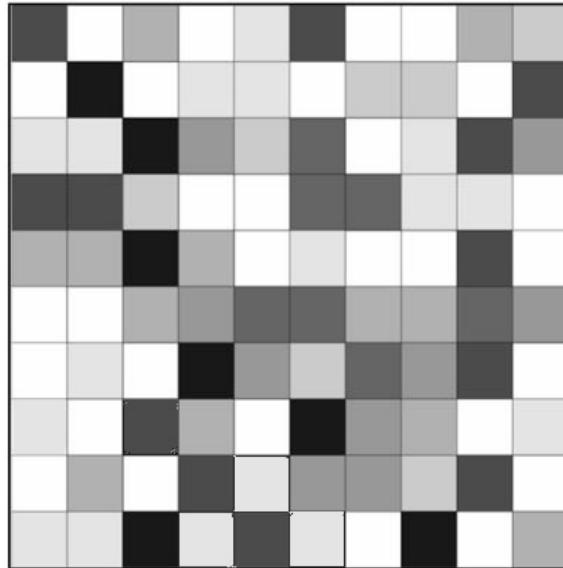


SOM - Inicialização



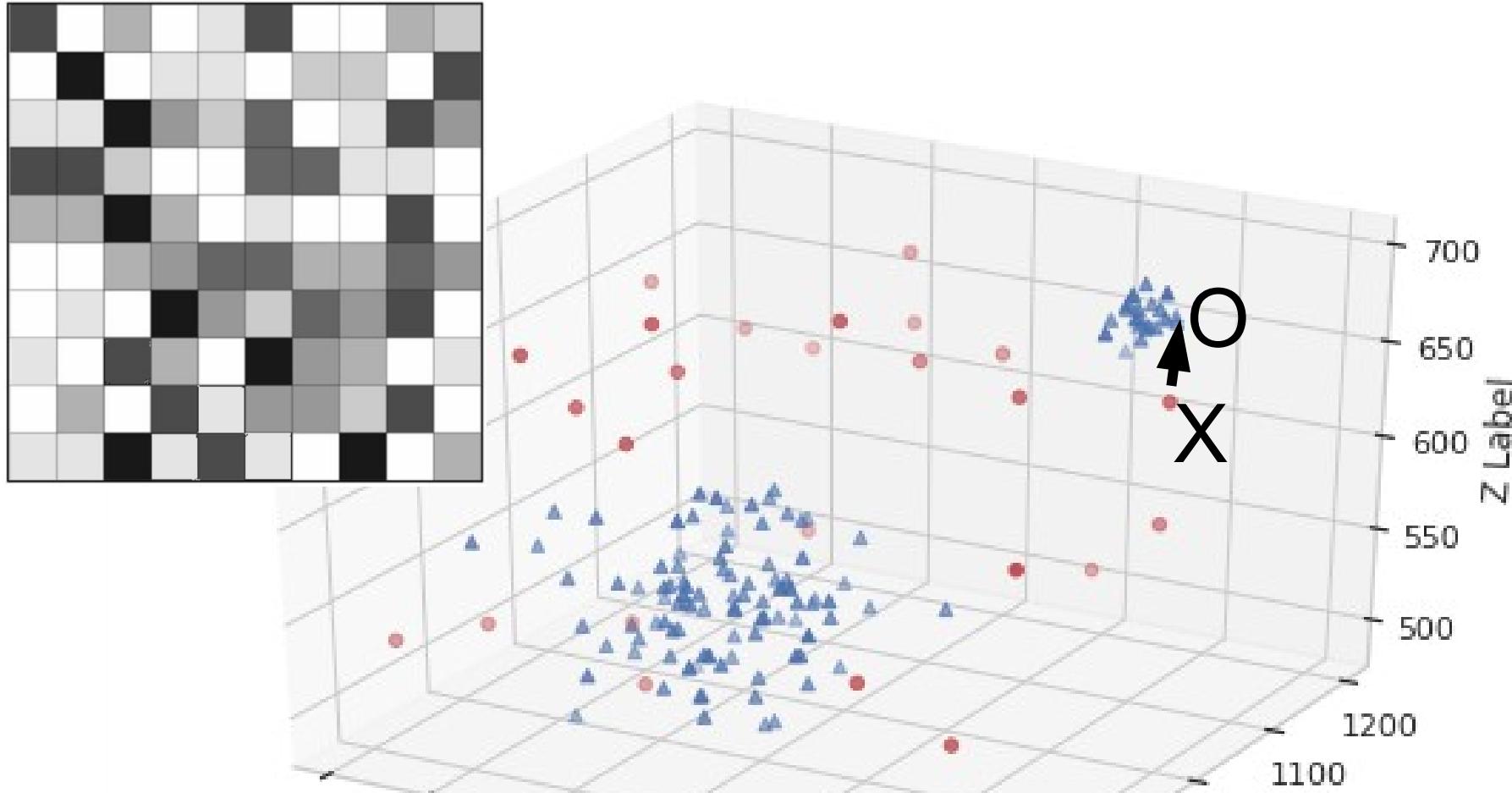
Cada célula do mapa recebe um endereço aleatório no Input Space

SOM - Treinamento



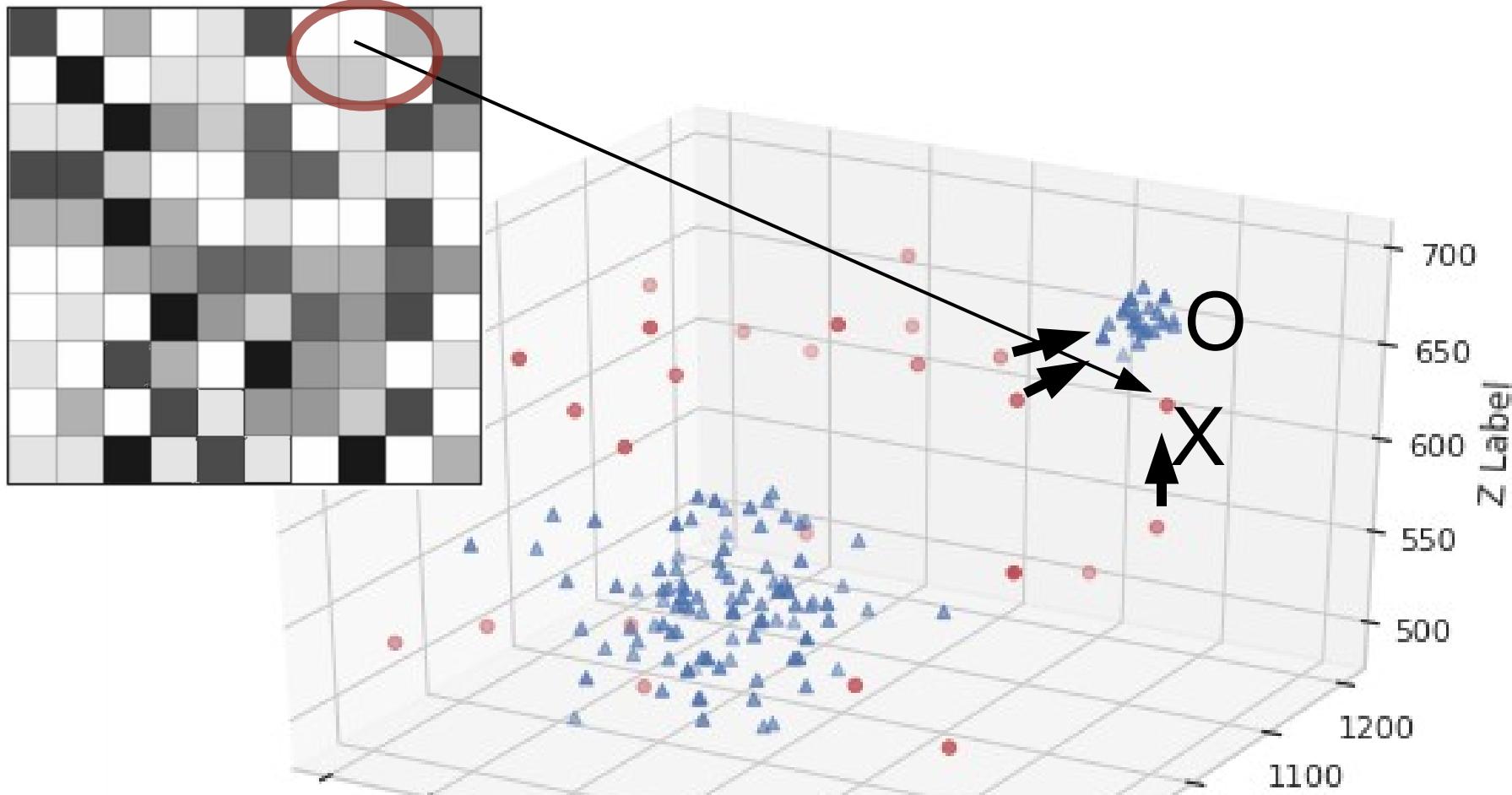
Uma observação (O) é escolhida. A célula mais próxima à observação no input space é encontrada (X).

SOM - Treinamento



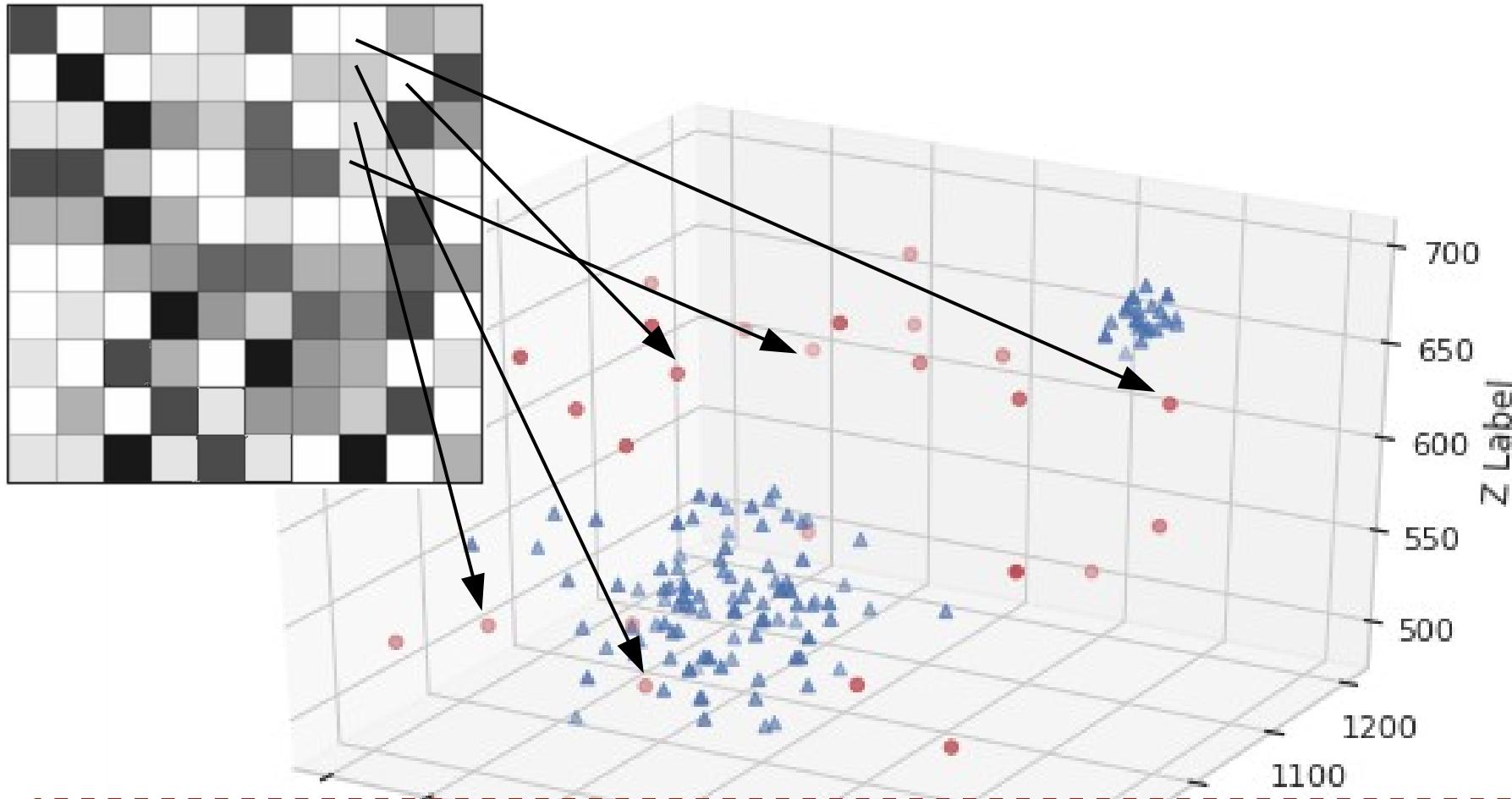
A célula (X) é aproximada da observação (O) no input space.

SOM - Treinamento



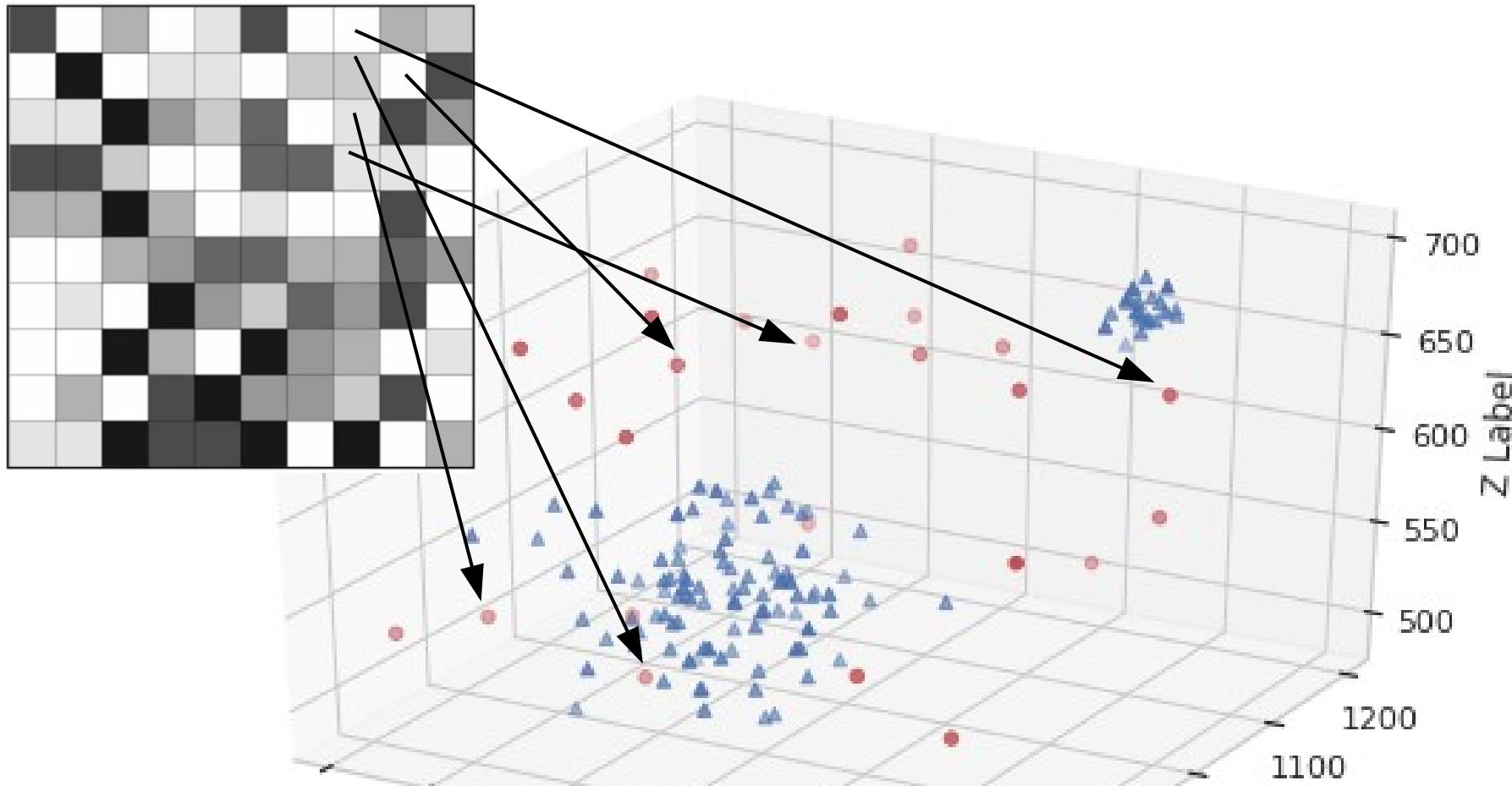
Os vizinhos da célula (no Map space) também são aproximados (no input space). Quanto mais distantes, menor é a força da aproximação.

SOM - Treinamento



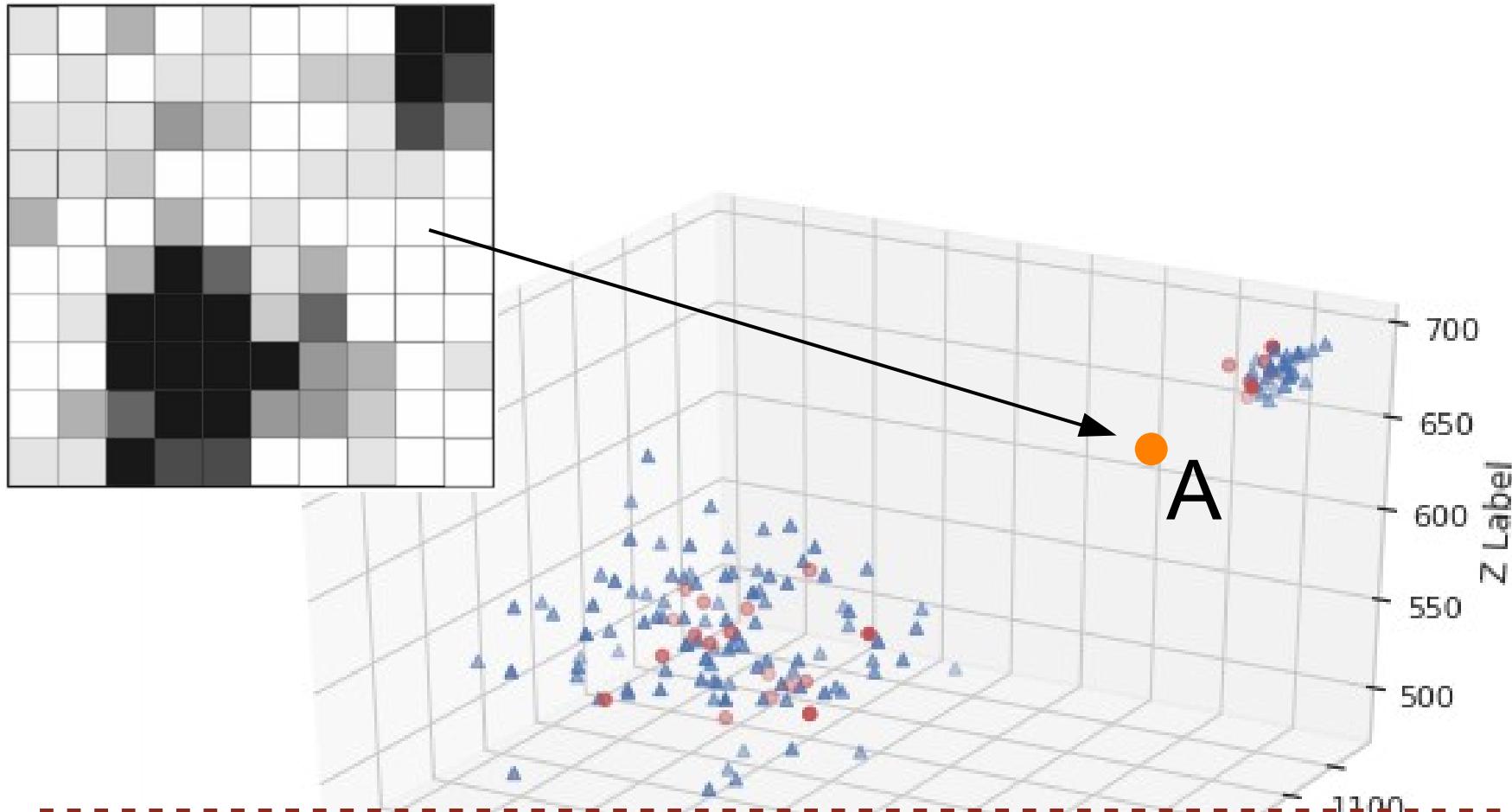
Repete para todos dados de entrada (possivelmente em múltiplas épocas).

SOM - Treinamento



Map space começa a formar padrões que refletem a distribuição do input space. Cada input (azul) é representado pela célula mais próxima (vermelho).

SOM - Mapa



No fim as densidades do mapa refletem as densidades de input space. Inputs anômalos (A) são os que são mapeados em regiões pouco densas do mapa.

Técnicas Espectrais

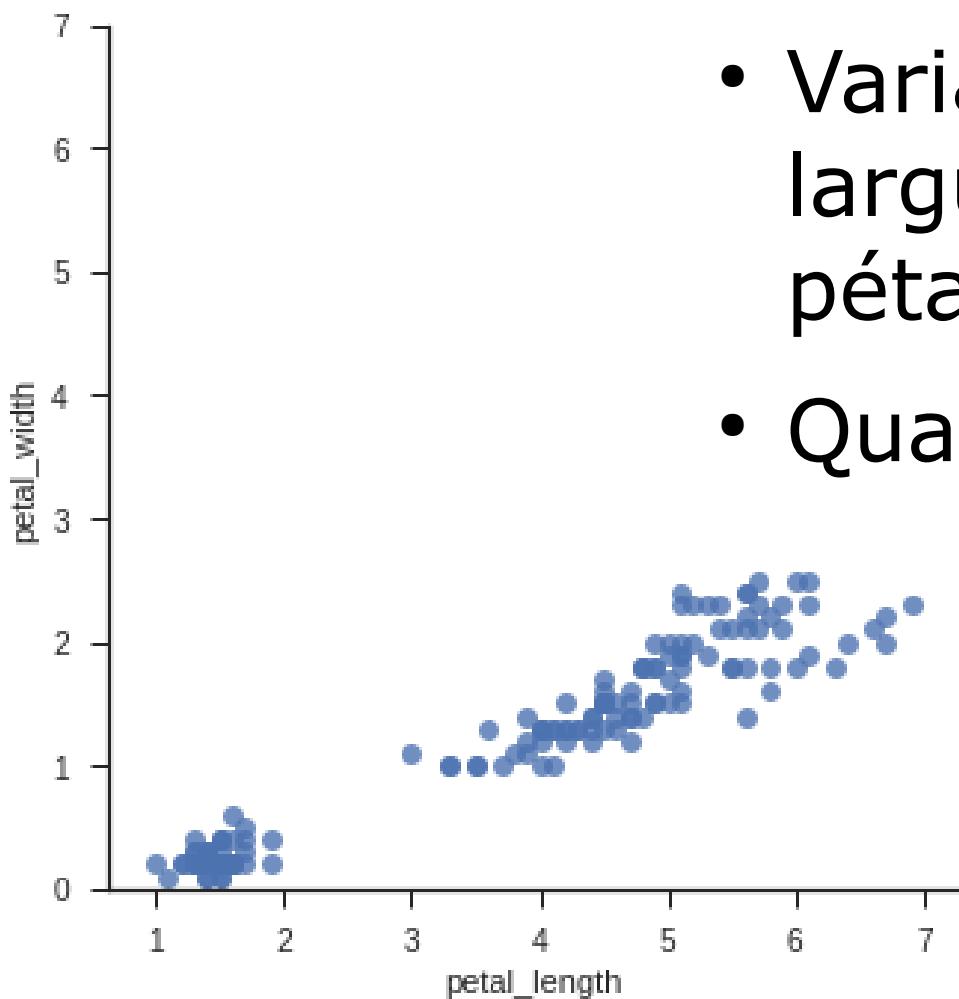
- Ideia: Os dados podem ser representados em um subespaço de menor dimensionalidade onde instâncias normais e anômalas aparecem separadas
- Requisito: Processo de redução de dimensionalidade deve preservar/maximizar variabilidade
- Técnica popular: PCA

Principal Component Analysis (PCA)

- Método de redução de dimensionalidade que combina dimensões altamente correlacionadas, maximizando variabilidade
- Exemplo: peso e altura são correlacionados, portanto há informação redundante

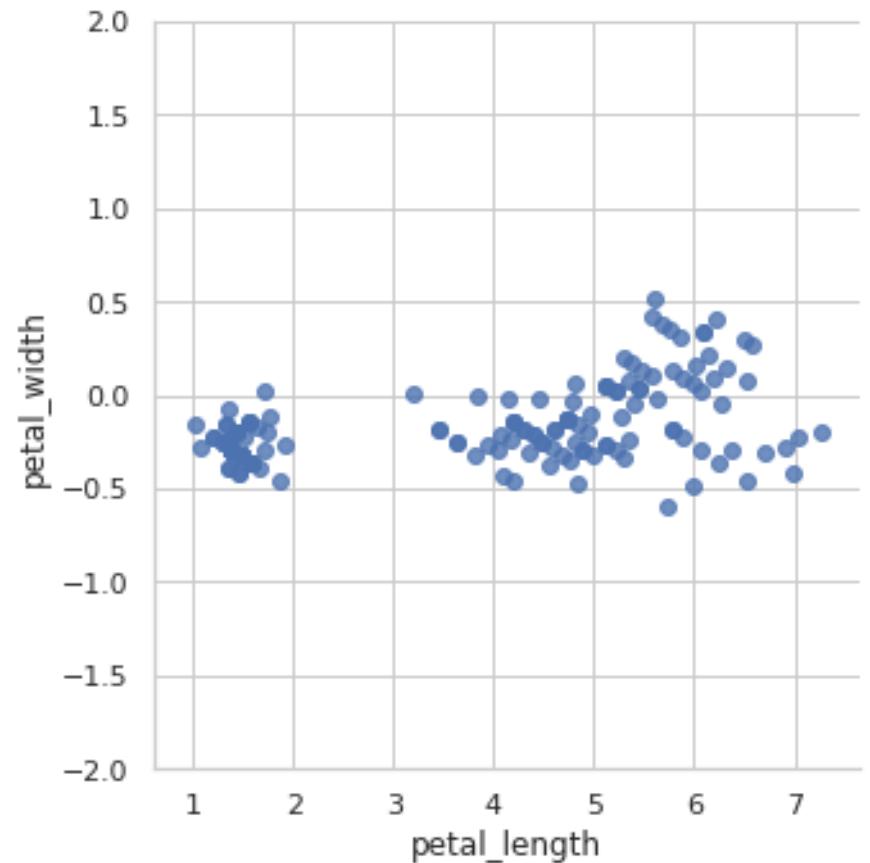
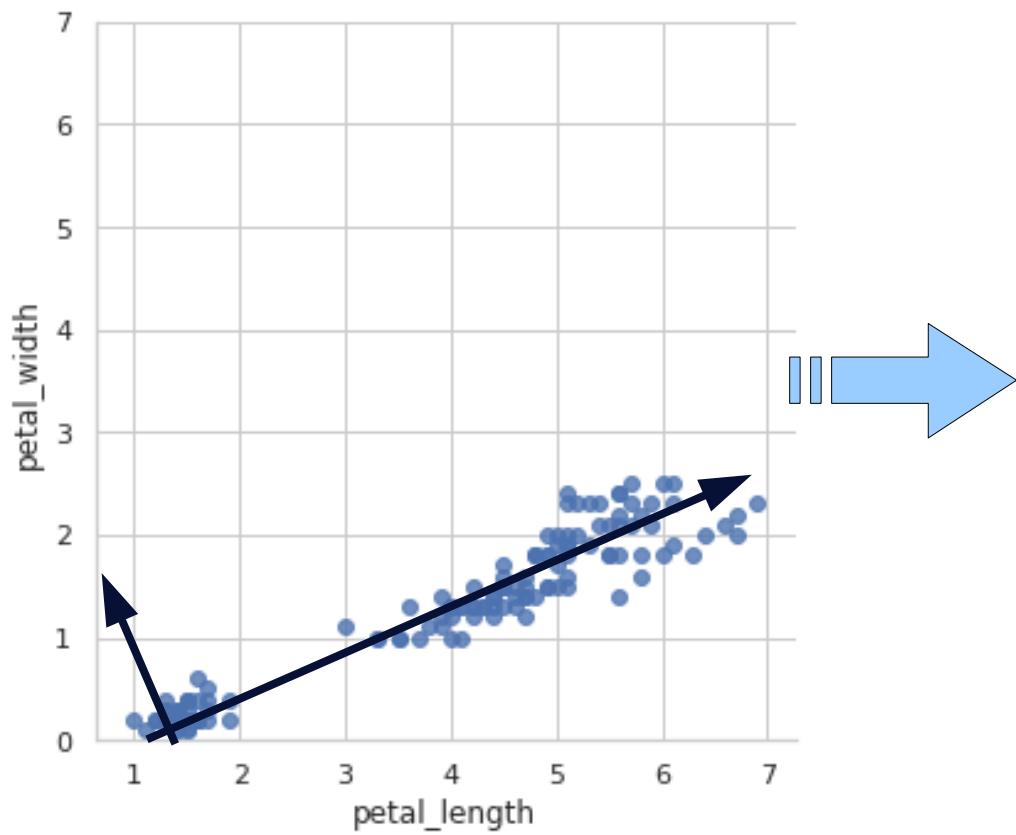
PCA - Intuição

- Dataset Iris (flores)
- Variáveis:
largura/cumprimento da
pétila
- Qual variável remover?



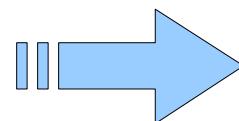
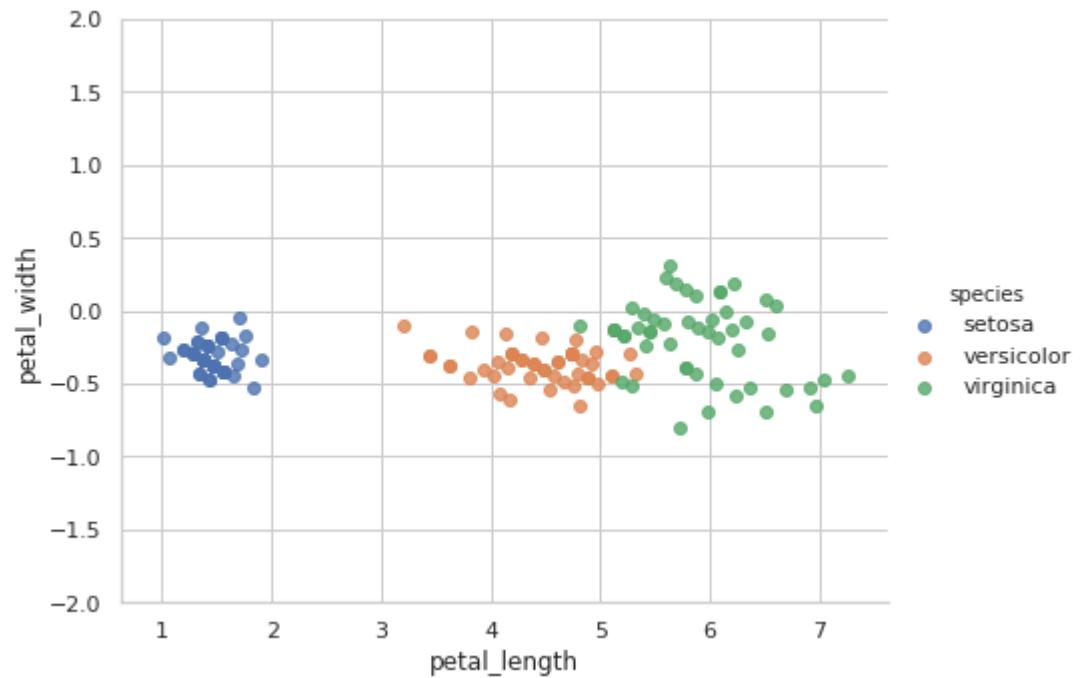
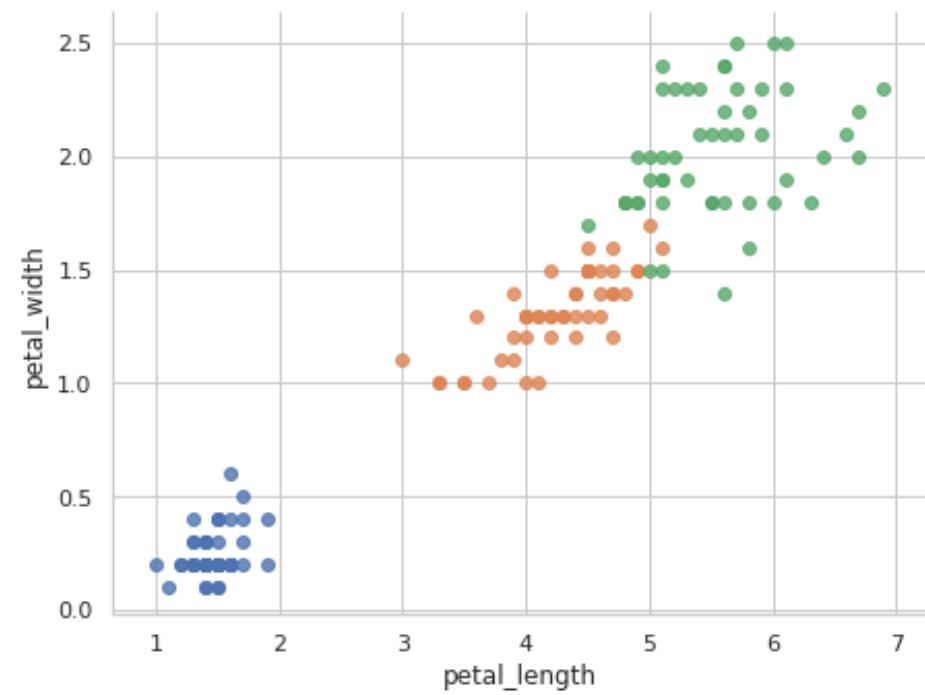
PCA - Intuição

- Que tal rotacionar os eixos para maximizar a variância?



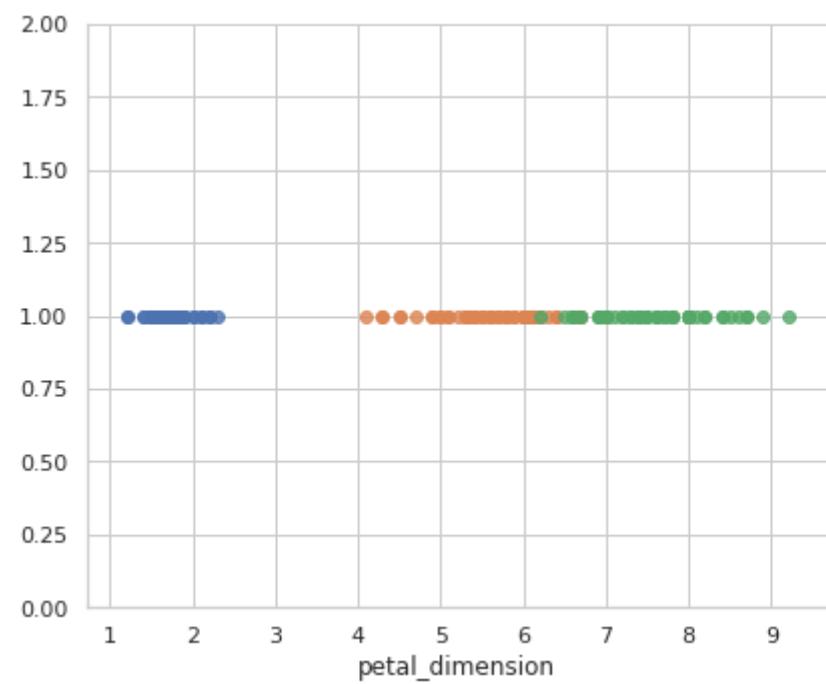
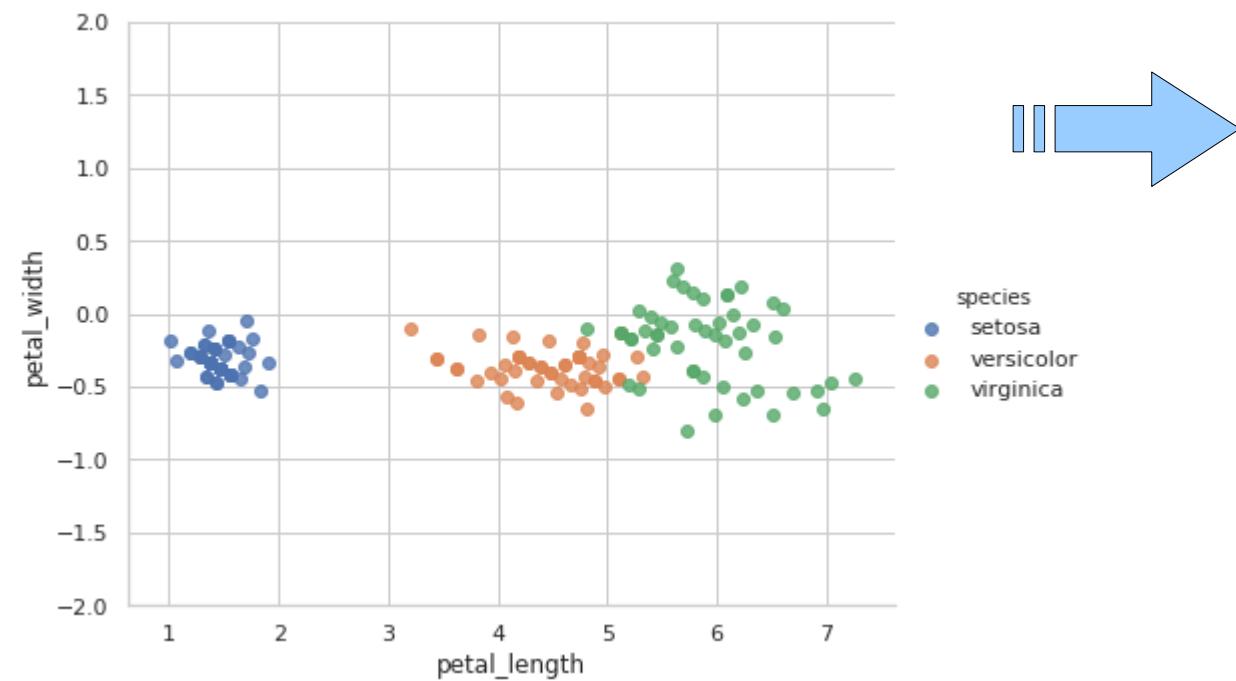
PCA - Intuição

- Que tal rotacionar os eixos para maximizar a variância?



PCA - Intuição

- E então manter apenas o eixo com maior variância



PCA - Intuição

- Que tal combinar variáveis correlacionadas?
- E.g. petal_width + petal_length = petal_dimension

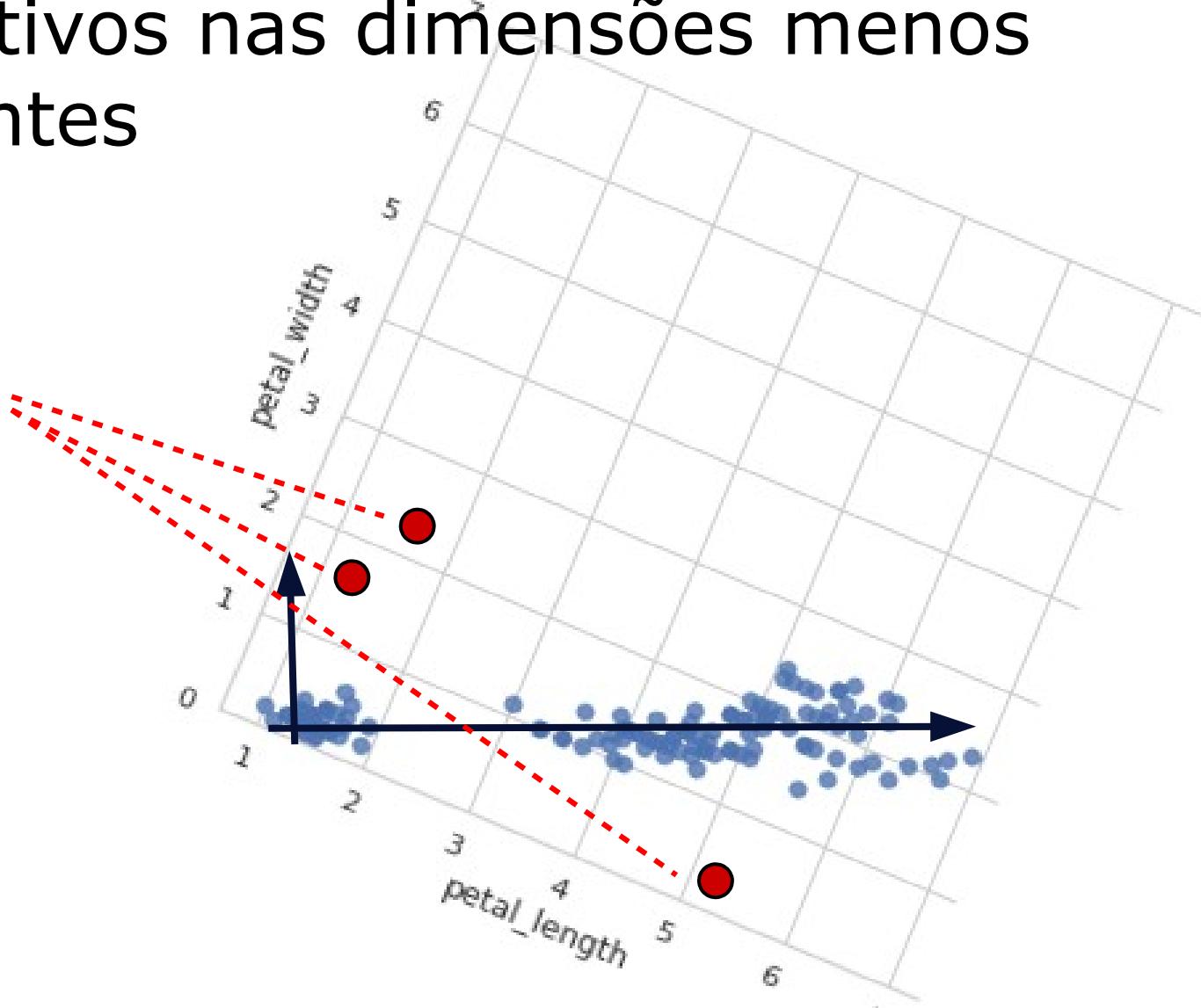
PCA - Processo

- Rotaciona eixos para maximizar a variância. Cada novo eixo é chamado de um componente principal
- A rotação mapeia as variáveis em novas variáveis não correlacionadas
- Cada componente principal representa uma combinação das variáveis originais
- Para reduzir a dimensionalidade, seleciona-se os componentes que mais preservam a variância

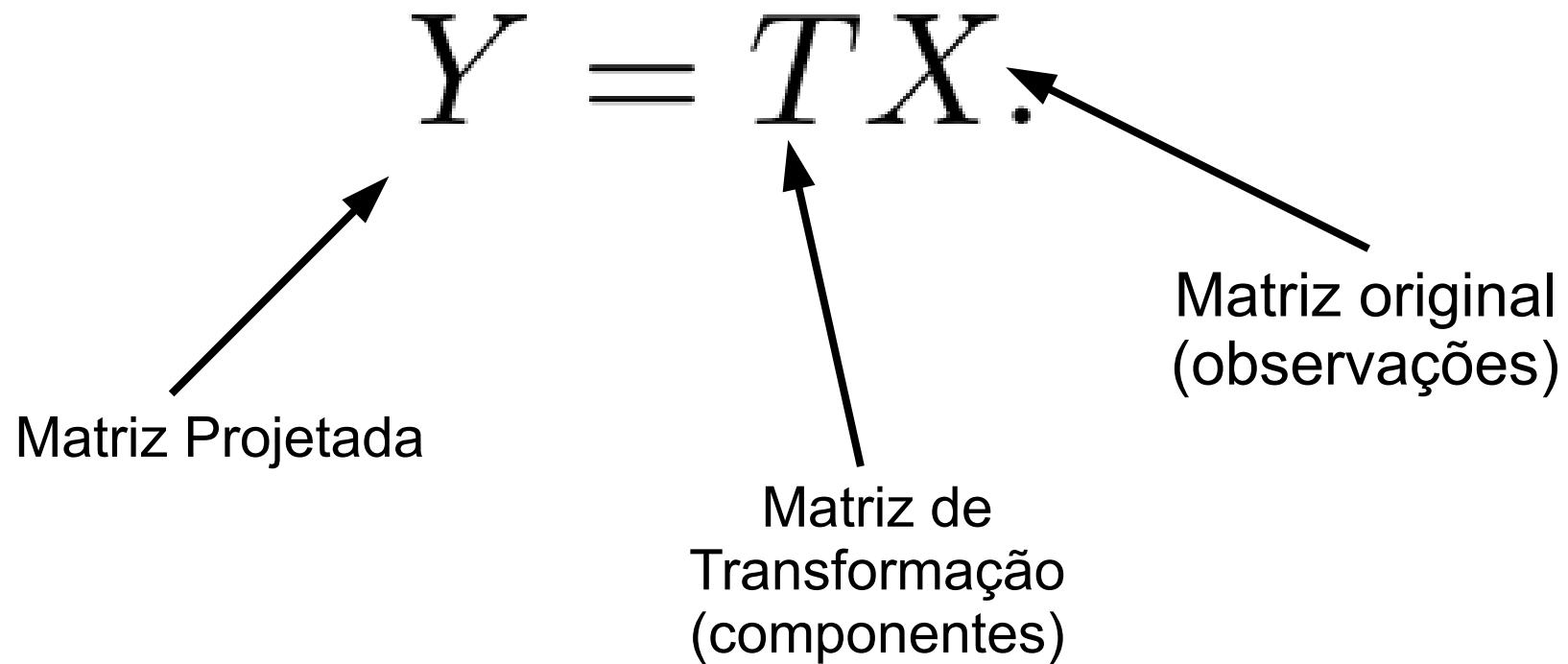
PCA - Anomalia

- Anomalias são observações com valores significativos nas dimensões menos importantes

Anomalias



Cálculo do PCA



Dimensões de X:

Q colunas representando objetos/indivíduos

N linhas representando valores das variáveis

Cálculo do PCA

- Normalize (center) measurements:

$$\hat{X}_i = X_i - \mu_{X_i}.$$

- Calculate covariance matrix:

$$K = Cov(\hat{X}) = \frac{1}{Q-1} \hat{X} \hat{X}^T.$$

Cálculo do PCA

- Calculate positive eigenvalues of K and respective eigenvectors. Order eigenvectors by eigenvalue to obtain T :
$$T = \begin{bmatrix} & \vec{v}_1 & \\ & \vdots & \\ & \vec{v}_N & \end{bmatrix}.$$
- Each line represents a principal component
- The proportion of the variance that each eigenvector represents can be calculated by dividing the eigenvalue corresponding to that eigenvector by the sum of all eigenvalues.

PCA – Iris Dataset

	sepal_length	sepal_width	petal_length	petal_width	species
0	5.1	3.5	1.4	0.2	setosa
1	4.9	3.0	1.4	0.2	setosa
2	4.7	3.2	1.3	0.2	setosa
3	4.6	3.1	1.5	0.2	setosa
4	5.0	3.6	1.4	0.2	setosa

Iris - Components

	sepal_length	sepal_width	petal_length	petal_width
0	0.521066	-0.269347	0.580413	0.564857
1	0.377418	0.923296	0.024492	0.066942
2	-0.719566	0.244382	0.142126	0.634273
3	-0.261286	0.123510	0.801449	-0.523597

Iris - Transforming

Y =

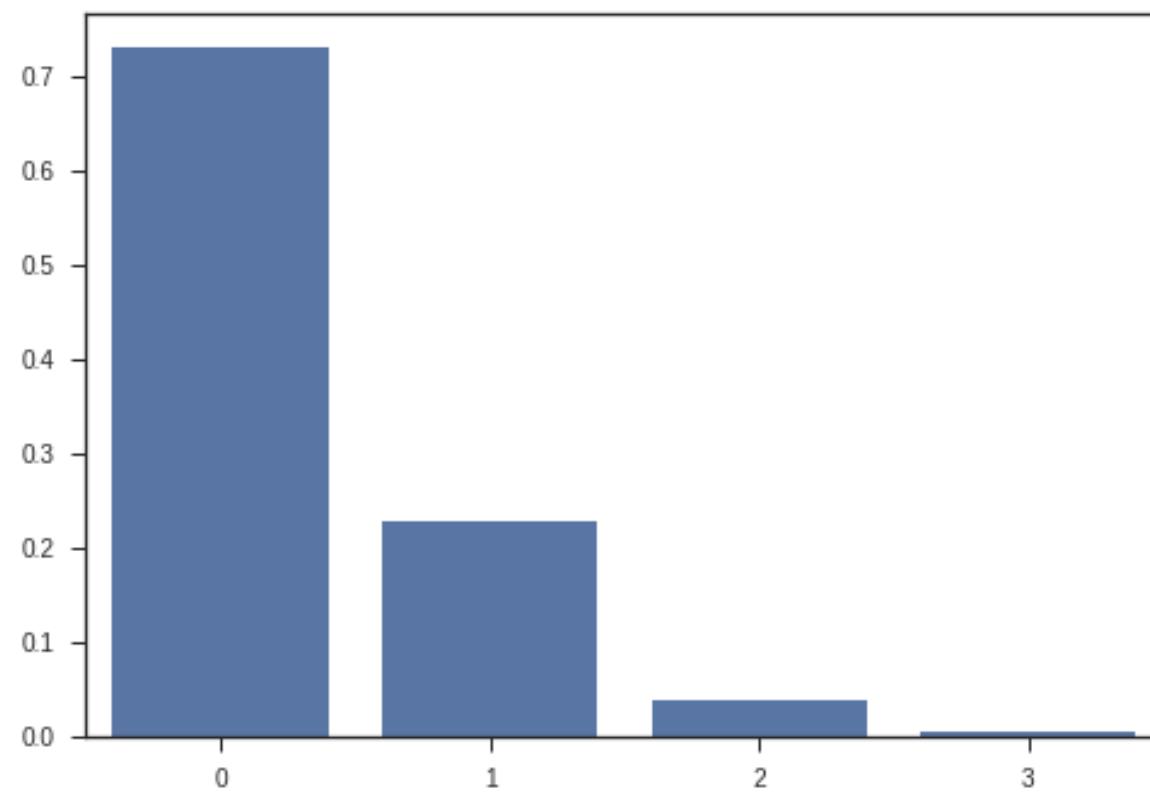
	sepal_length	sepal_width	petal_length	petal_width
0	5.1	3.5	1.4	0.2
1	4.9	3.0	1.4	0.2
2	4.7	3.2	1.3	0.2
3	4.6	3.1	1.5	0.2
4	5.0	3.6	1.4	0.2



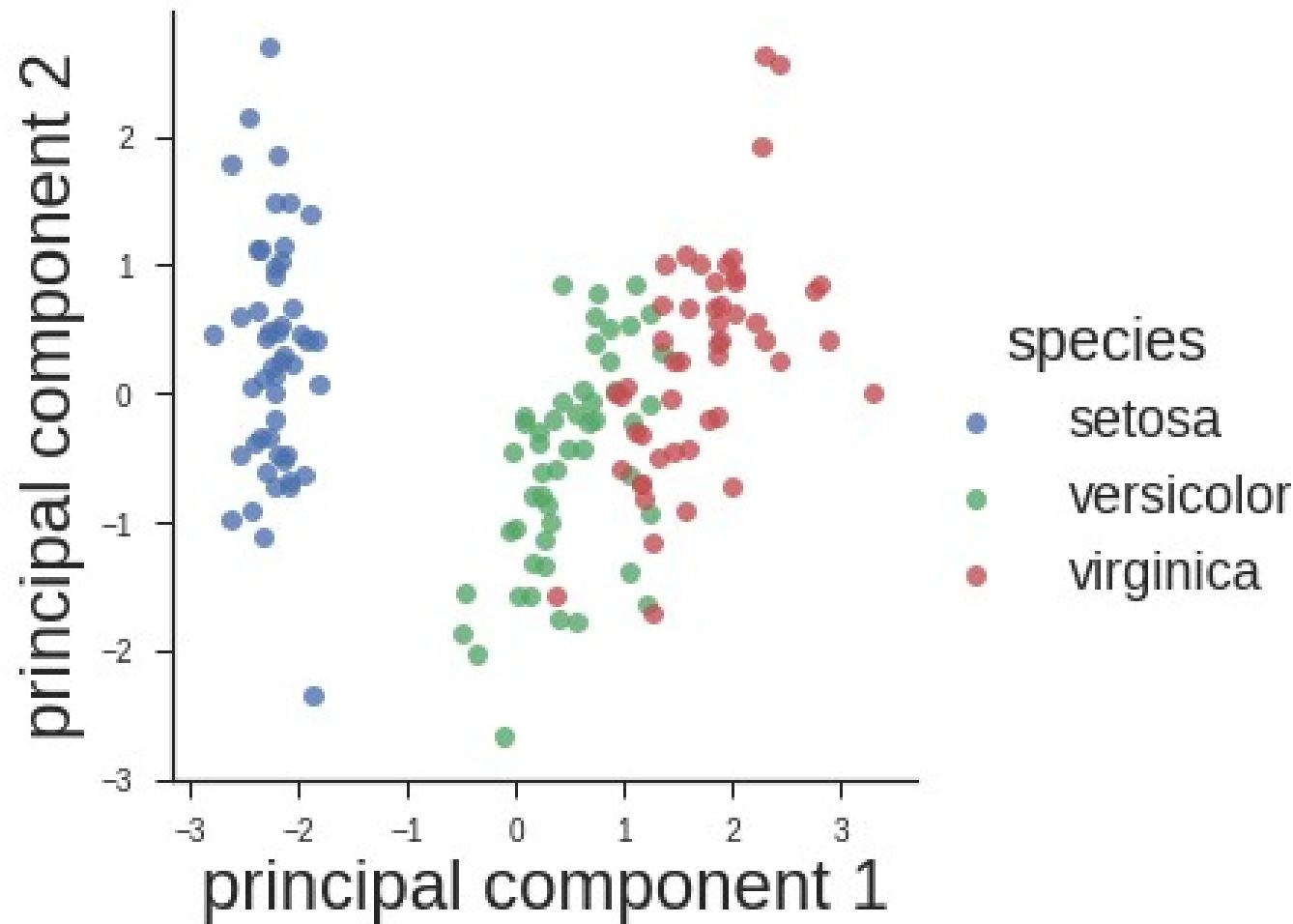
	0	1	2	3
sepal_length	0.521066	0.377418	-0.719566	-0.261286
sepal_width	-0.269347	0.923296	0.244382	0.123510
petal_length	0.580413	0.024492	0.142126	0.801449
petal_width	0.564857	0.066942	0.634273	-0.523597

(transposed matrices)

Iris - Variance per component



Iris - Lower dimensionality



Anomalias em Alta Dimensionalidade

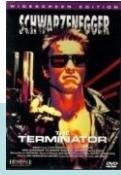
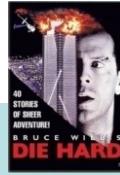
- Grafos
- Texto

SVD decomposition

- Singular Value Decomposition
- Usado tradicionalmente para auxiliar cálculos em matrizes (ex: matriz inversa)
- Também usado para diminuir dimensionalidade, detecção de ruído e compressão de imagens
- Muito parecido com PCA – Mesma fundamentação teórica, pequenas diferenças no cálculo

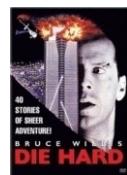
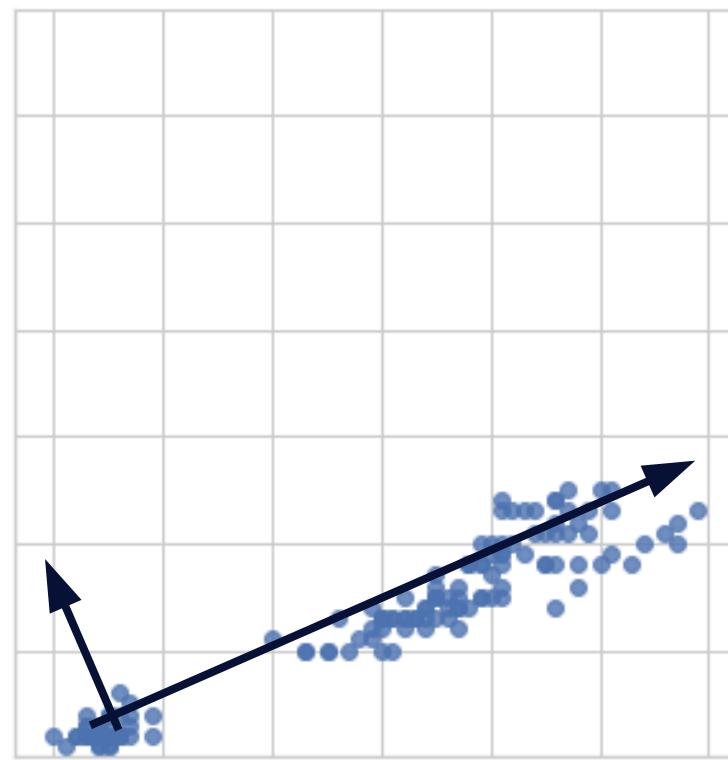
Fatoração de Matrizes

(sistemas de recomendação)

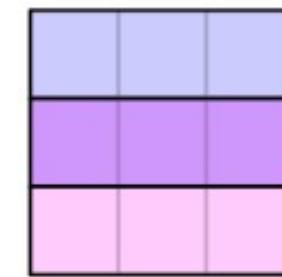
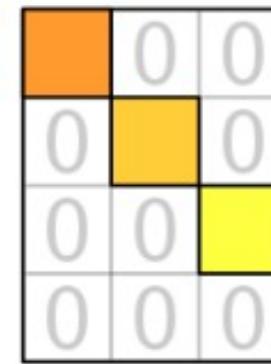
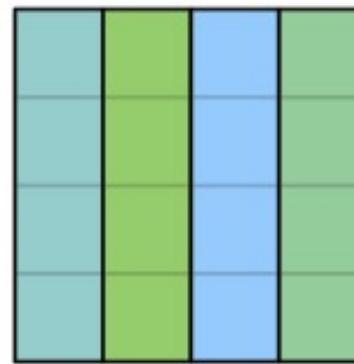
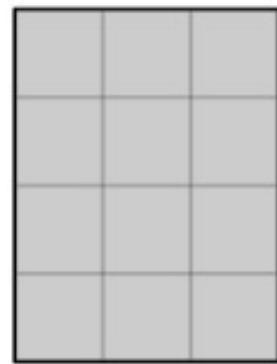
M					
Alice	5	4	1	5	
Bob	4	4	2		1

Exemplo: Dimensões são Pessoas X Filmes.
Valores são intensidade de associação (nota).

Rotação



Processo SVD



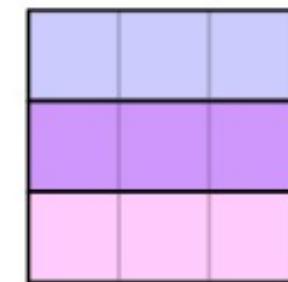
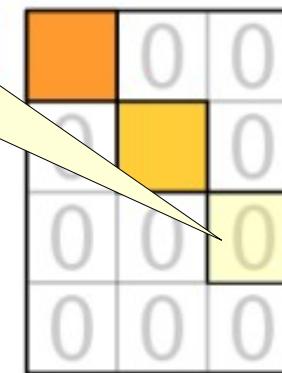
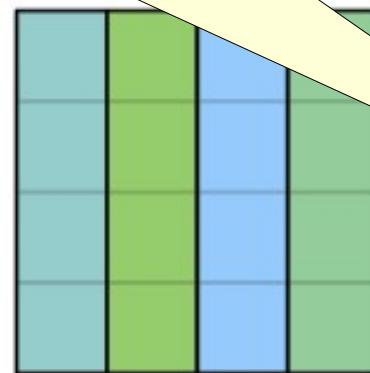
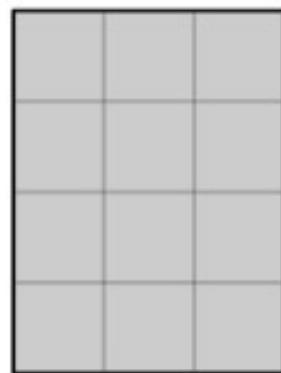
$$M = U \Sigma V^*$$

Matriz
original

Eigenvalues,
“importância”
das novas
dimensões

SVD - Recomposição

Substituir componentes
nenos expressivos por 0



$$\mathbf{M}' = \mathbf{U} \Sigma' \mathbf{V}^*$$

Recalcular nova matriz

Fatoração de Matrizes

- SVD:

$$M_k = U_k \times \Sigma_k \times V_k^T$$

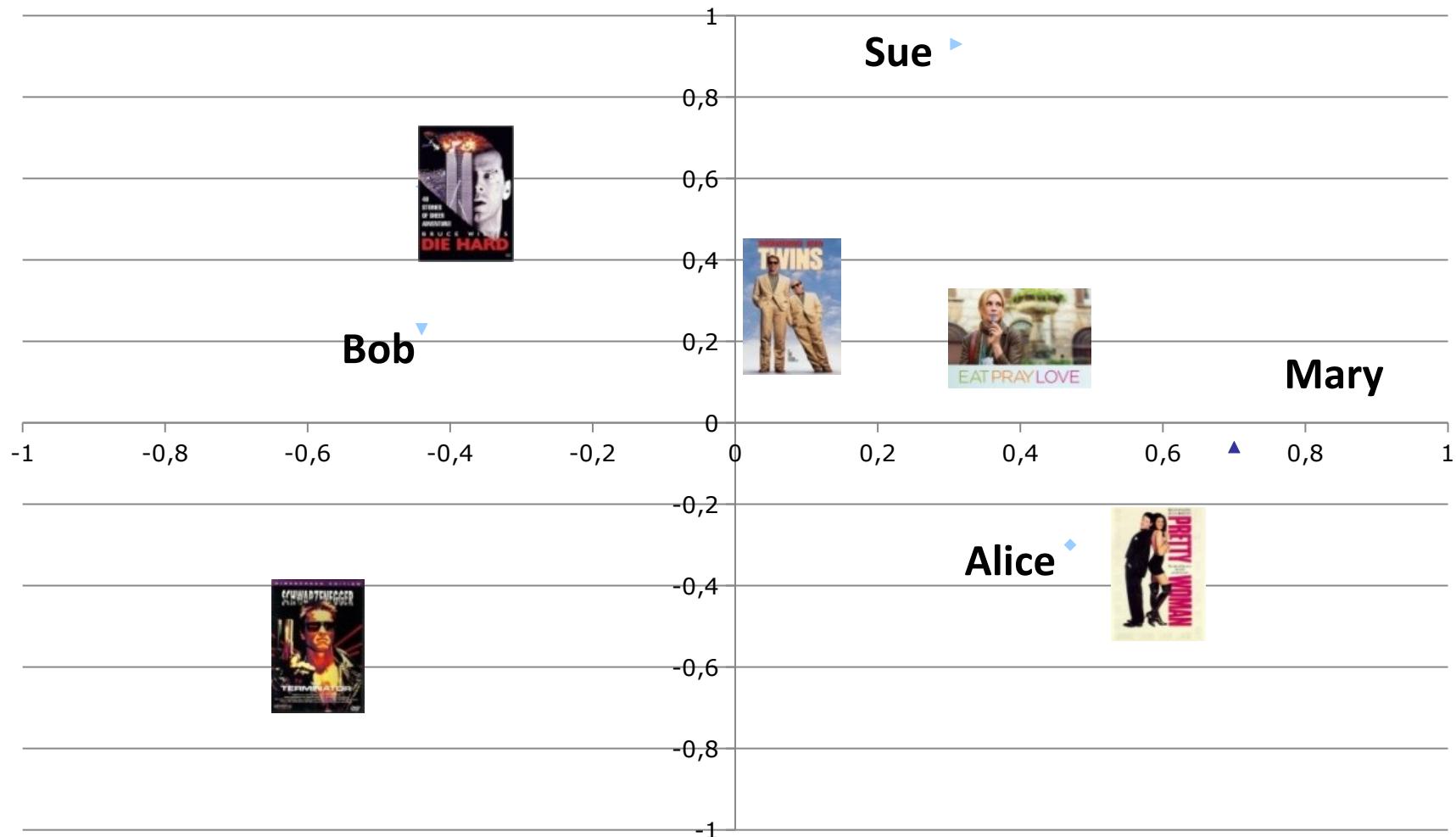
U_k	Dim1	Dim2
Alice	0.47	-0.30
Bob	-0.44	0.23
Mary	0.70	-0.06
Sue	0.31	0.93

V_k^T					
Dim1	-0.44	-0.57	0.06	0.38	0.57
Dim2	0.58	-0.66	0.26	0.18	-0.36

- Prediction: $\hat{r}_{ui} = \bar{r}_u + U_k(Alice) \times \Sigma_k \times V_k^T(EPL)$
 $= 3 + 0.84 = 3.84$

Σ_k	Dim1	Dim2
Dim1	5.63	0
Dim2	0	3.23

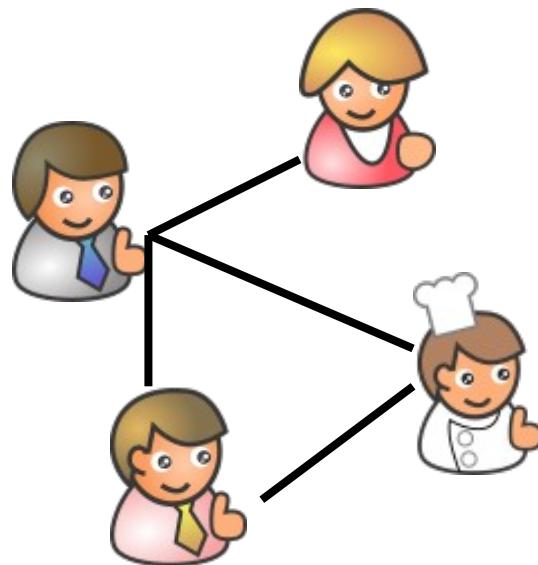
A picture says ...



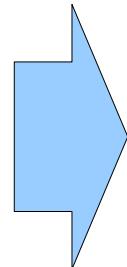
Grafos

- Anomalias estruturais
- Anomalias de Evolução (foco aqui)
 - Ideia: Prever o que seria uma evolução normal do grafo. Calcular distância entre novo grafo e grafo previsto. Distância é uma medida de anormalidade.
 - Mais um exemplo de aplicação de PCA/SVD

Grafo Social



Rede Social



Four small icons of the people from the graph are aligned vertically with the rows of the matrix:

- Row 1: Man in grey suit
- Row 2: Woman in yellow dress
- Row 3: Man in white chef's uniform
- Row 4: Woman in pink dress

0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0

Matriz de Adjacência

Anomalias em Evolução de Grafos

- A: Matriz de Adjacência do grafo incial
- B: Matriz de adjacência do grafo evoluído
- A': Aplica SVD sobre A para obter as “previsões” de evolução
- Calcular distância entre B e A'. Por exemplo, usando alguma norma sobre a diferença: $|B - A'|$
- Exemplo: Norma Frobenius

$$\|A\|_F = \sqrt{\sum_{i=1}^m \sum_{j=1}^n |a_{ij}|^2}$$

Texto

- Anomalia Local (exemplo: correção gramatical)
- Anomalia de Evolução (foco aqui)

Análise de Semântica Latente

- Usa SVD para reduzir a dimensionalidade dos documentos
- Dimensões passam a representar tópicos que agregam termos usados no mesmo contexto
- Estratégia para Detecção de Anomalias:
Monitorar a evolução dos tópicos ao longo do tempo

SVD sobre Texto

Matriz Termos X Documentos

C	d_1	d_2	d_3	d_4	d_5	d_6
ship	1	0	1	0	0	0
boat	0	1	0	0	0	0
ocean	1	1	0	0	0	0
wood	1	0	0	1	1	0
tree	0	0	0	1	0	1

Documentos

Termos

SVD sobre Texto

Matriz Termos X Documentos

C	d_1	d_2	d_3	d_4	d_5	d_6
ship	1	0	1	0	0	0
boat	0	1	0	0	0	0
ocean	1	1	0	0	0	0
wood	1	0	0	1	1	0
tree		0	0	1	0	1

Ao diminuir a dimensionalidade SVD agrupa termos que coocorrem com frequência nos documentos

C_2	d_1	d_2	d_3	d_4	d_5	d_6
ship	0.85	0.52	0.28	0.13	0.21	-0.08
boat	0.36	0.36	0.16	-0.20	-0.02	-0.18
ocean	1.01	0.72	0.36	-0.04	0.16	-0.21
wood	0.97	0.12	0.20	1.03	0.62	0.41
tree	0.12	-0.39	-0.08	0.90	0.41	0.49
U	1	2	3	4	5	
ship	-0.44	-0.30	0.57	0.58	0.25	
boat	-0.13	-0.33	-0.59	0.00	0.73	
ocean	-0.48	-0.51	-0.37	0.00	-0.61	\times
wood	-0.70	0.35	0.15	-0.58	0.16	
tree	-0.26	0.65	-0.41	0.58	-0.09	
Σ_2	1	2	3	4	5	
1	2.16	0.00	0.00	0.00	0.00	
2	0.00	1.59	0.00	0.00	0.00	
3	0.00	0.00	0.00	0.00	0.00	\times
4	0.00	0.00	0.00	0.00	0.00	
5	0.00	0.00	0.00	0.00	0.00	
V^T	d_1	d_2	d_3	d_4	d_5	d_6
1	-0.75	-0.28	-0.20	-0.45	-0.33	-0.12
2	-0.29	-0.53	-0.19	0.63	0.22	0.41
3	0.28	-0.75	0.45	-0.20	0.12	-0.33
4	0.00	0.00	0.58	0.00	-0.58	0.58
5	-0.53	0.29	0.63	0.19	0.41	-0.22

Reducing the
dimensionality to 2

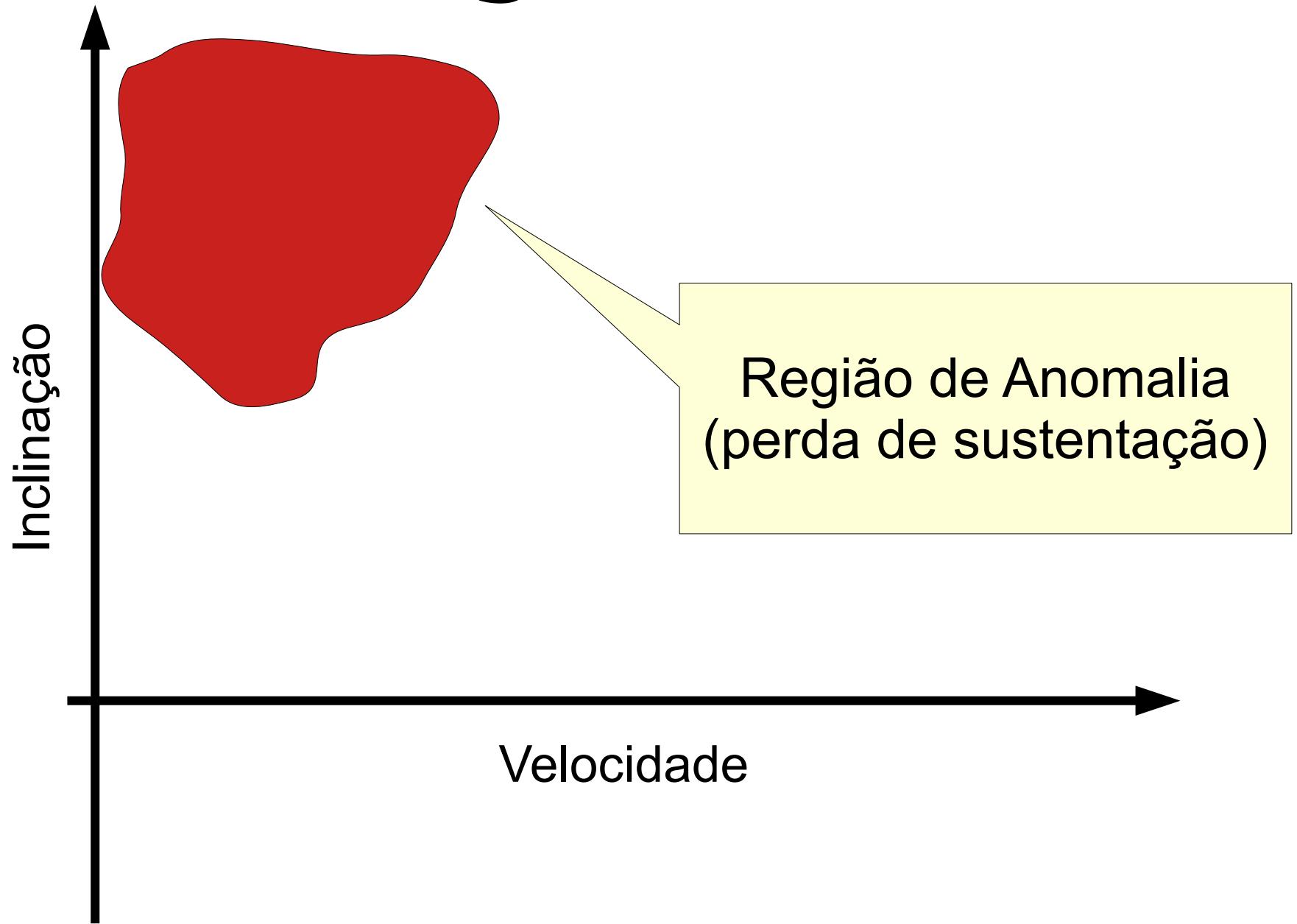
Detecção de Anomalias em Texto

- Correção: treine um modelo probabilístico da língua (e.g. n-gramas) e classifique como anomalia tudo que tiver probabilidade baixa.
- Evolução de tópicos: Modelagem de tópicos (SVD) sobre janelas de texto. Algum algoritmo multidimensional de detecção de anomalias para identificar janelas anômalas.

Cuidado!

- Detecção de anomalias é uma área desafiadora
- Não existe receita para um bom modelo. É preciso entender o problema e os algoritmos.
- Especialmente difícil em aplicações críticas
- Interação entre software (modelo) e hardware (sensores)

Boeing 737 Max



2010 Flash Crash



Referências

- Anomaly Detection: A Survey, 2011. ARUN CHANDOLA, ARINDAM BANERJEE, and VIPIN KUMAR - ACM Computing Surveys
- A Survey on Unsupervised Outlier Detection in High-Dimensional Numerical Data, 2012. Arthur Zimek, Erich Schubert and Hans-Peter Kriegel

Obrigado

- Email: luizelso@gmail.com,
gomesjr@dainf.ct.utfpr.edu.br
- Programa de Pós (PPGCA):
ppgca.dainf.ct.utfpr.edu.br