

# Classes de Métodos Online

Diferentes abordagens para detectar eventos em tempo real

Eduardo Ogasawara

[eduardo.ogasawara@cefet-rj.br](mailto:eduardo.ogasawara@cefet-rj.br)

<https://eic.cefet-rj.br/~eogasawara>

# Introdução aos Métodos Online

Considere uma série temporal observada ao longo do tempo, onde  $x_t$  representa cada observação no instante  $t$ . Os métodos de detecção online diferem principalmente pela forma como definem o que é "típico" e como identificam mudanças.

## Série Temporal

Fluxo contínuo de observações ao longo do tempo

## Modelagem

Diferentes formas de representar tipicidade e mudança

## Cinco Classes

Principais categorias de métodos de detecção

# Detektore Estatísticos Sequenciais

Detektore estatísticos online funcionam como acumuladores de evidência. Cada nova observação contribui para a estatística, e a detecção ocorre quando essa evidência ultrapassa um limiar pré-definido.

Define-se uma estatística acumulativa  $S_t$  que soma as contribuições de cada observação através de uma função  $g$ . Um evento é detectado quando  $S_t$  ultrapassa o limiar  $h$ .

01

## Estatística Acumulada

Soma crescente ao longo do tempo

02

## Evidência Crescente

Cada observação adiciona informação

03

## Decisão por Limiar

Detecção quando excede threshold

# Modelos Probabilísticos Online

Nos métodos probabilísticos, eventos são interpretados como mudanças nos parâmetros do modelo probabilístico. A detecção online acompanha a evolução desses parâmetros ao longo do tempo.

## Distribuição Temporal

Observações seguem  $F_{\theta_t}$  com parâmetros variáveis

## Parâmetros Dinâmicos

$\theta_t$  evolui conforme o processo temporal

## Inferência Incremental

Atualização contínua do modelo

# Aprendizado de Máquina Online

## Modelo Adaptativo

Sistema preditivo que se ajusta continuamente aos dados

O erro de previsão  $e_t$  é calculado como a diferença absoluta entre a observação real  $x_t$  e a previsão do modelo.

## Detecção por Erro

Em aprendizado de máquina online, eventos são identificados quando o modelo perde capacidade preditiva. O erro de previsão funciona como sinal de mudança no processo.

- Modelo preditivo adaptativo
- Erro como indicador de evento
- Limiar dependente do tempo

# Métodos Baseados em Distância

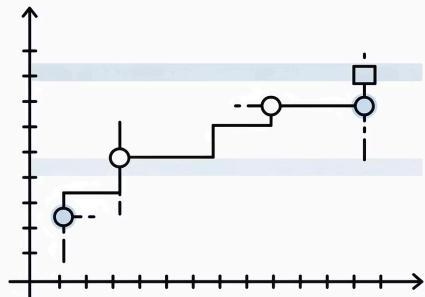
Métodos baseados em distância detectam eventos quando uma subsequência se torna muito diferente do histórico. A noção de "evento" é associada ao isolamento no espaço temporal.



A distância mínima  $D_t$  é definida como a menor distância entre a janela temporal atual e o conjunto de subsequências passadas, usando uma função de distância específica.

# CUSUM Sequencial

O CUSUM acumula desvios persistentes do modelo. Quando esses desvios se tornam suficientemente grandes, o método sinaliza uma mudança estrutural no processo.



## Soma Cumulativa

Acumulação de resíduos ao longo do tempo



## Mudanças Persistentes

Detecção de desvios contínuos



## Sensibilidade

Controlada pelo parâmetro  $k$

A estatística CUSUM  $C_t^+$  é calculada como o máximo entre zero e a soma do valor anterior, o resíduo atual e o parâmetro de sensibilidade negativo.

# Média Móvel Exponencial (EWMA)

## Suavização Adaptativa

O EWMA reduz o ruído da série e enfatiza tendências recentes. Ele é especialmente útil para detectar mudanças graduais no comportamento do processo.

A média exponencial  $z_t$  combina a observação atual  $x_t$  com a média anterior  $z_{t-1}$ , ponderadas pelo fator de suavização  $\lambda$ .



### **1** Suavização

Redução de ruído nas observações

### **2**

### **Peso Recente**

Maior importância para dados atuais

### **3**

### **Mudanças Suaves**

Detecção de transições graduais

# Page-Hinkley

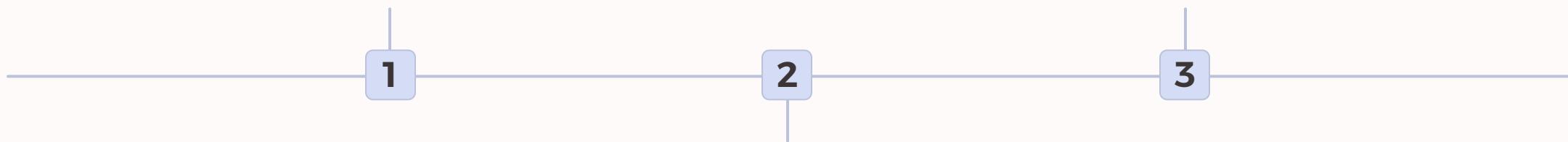
O método Page-Hinkley detecta mudanças na média do processo. Ele acumula desvios em relação à média histórica e sinaliza eventos quando esses desvios se tornam persistentes.

## Monitoramento

Acompanhamento contínuo da média do processo

## Detecção

Identificação de mudanças significativas na média



## Acumulação

Soma de desvios persistentes ao longo do tempo

# **Detectores Adaptativos**

Detectores adaptativos ajustam seus parâmetros continuamente. Isso permite separar mudanças graduais do processo (drift) de rupturas abruptas (eventos).

## **Atualização Contínua**

Parâmetros ajustados ao longo do tempo

## **Erro como Indicador**

Sinal de instabilidade no processo

## **Distinção de Eventos**

Separação entre drift e mudanças abruptas

# Estrutura Unificada de Detecção

Apesar das diferenças metodológicas, a maioria dos detectores online segue a mesma lógica: calcular uma estatística e compará-la a um limiar adaptativo.

A regra geral estabelece que um evento é detectado quando o score  $S_t$  excede o limiar  $\tau_t$  no instante  $t$ .

01

## Cálculo do Score

Estatística da janela temporal

02

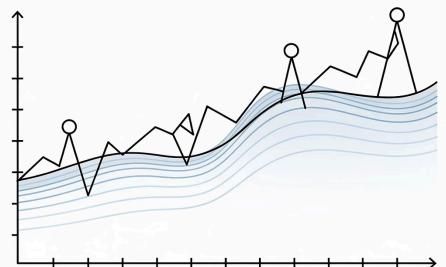
## Comparação

Score versus limiar adaptativo

03

## Decisão

Detecção quando  $S_t > \tau_t$



# Anomalias Online

Anomalias online correspondem a desvios pontuais em relação ao comportamento esperado. Elas não alteram necessariamente o modelo, apenas violam a tipicidade local.

## Desvios Instantâneos

Violações pontuais da tipicidade esperada

## Resíduos do Modelo

Diferença  $r_t = x_t - \hat{x}_t$

## Tipicidade Adaptativa

Referência local e dinâmica

# Change Points Online

Change points representam mudanças abruptas no processo gerador da série. No paradigma online, essas rupturas são detectadas com atraso e sob informação incompleta.

## Rupturas Estruturais

Mudanças fundamentais no processo temporal

Um change point é definido quando  $\theta_t \neq \theta_{t-1}$ , indicando alteração nos parâmetros do modelo

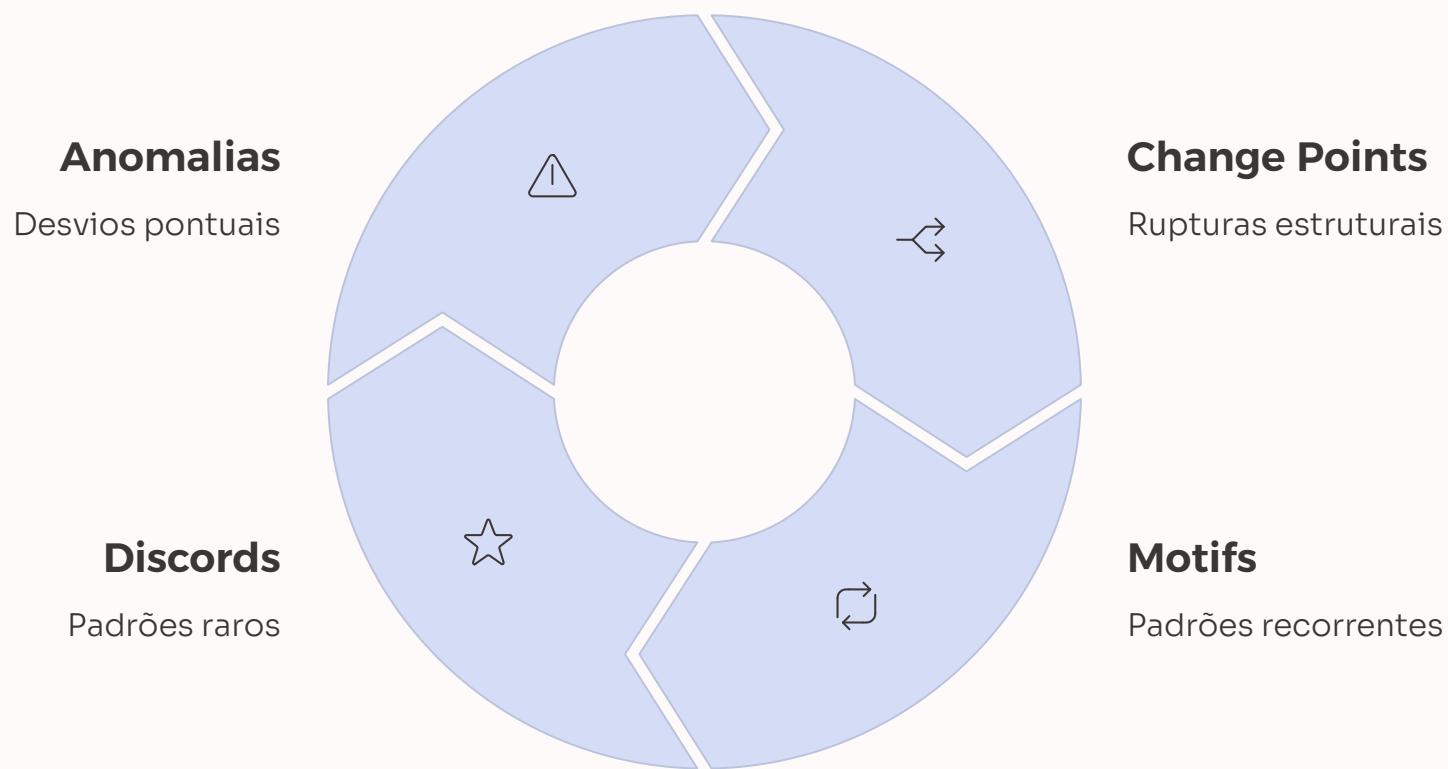
## Detecção Parcial

Identificação sob informação incompleta com atraso inerente ao paradigma online

Associadas a mudanças significativas nos parâmetros do modelo gerador

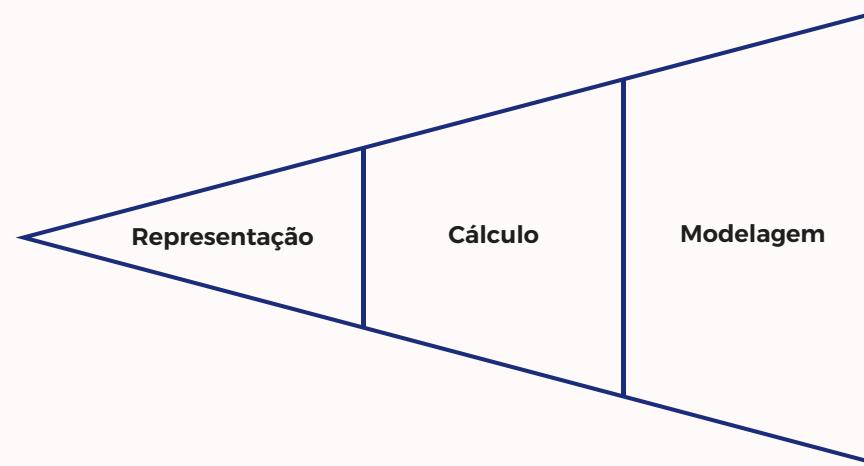
# Sistema Unificado de Eventos

Anomalias, change points, motifs e discords podem ser tratados dentro de uma mesma estrutura matemática. A diferença está na forma do score e no critério de decisão.



# Pipeline de Detecção Online

A detecção online pode ser vista como um pipeline modular: dados → modelo → estatística → decisão. Essa arquitetura evidencia o caráter modular dos sistemas online.



Cada etapa do pipeline contribui para a transformação incremental dos dados brutos em decisões sobre eventos temporais.

# Latência versus Precisão

Em sistemas online, reduzir a latência geralmente aumenta o número de falsos positivos. Assim, existe um compromisso fundamental entre rapidez e precisão.

A latência  $\Delta t$  é definida como a diferença entre o instante detectado  $\hat{\tau}$  e o instante real do evento  $\tau$ .

---

## Latência

Atraso entre evento real e detecção

## Precisão

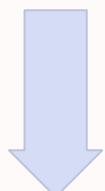
Qualidade e acurácia das detecções

## Trade-off

Compromisso inevitável entre ambos

# Complexidade Computacional

A viabilidade dos detectores online depende da complexidade computacional. Em streaming, o algoritmo precisa operar com custo aproximadamente constante a cada nova observação.



## Métodos Ingênuos

Abordagens tradicionais são computacionalmente inviáveis para streaming



## Abordagem Incremental

Processamento necessário para viabilidade em tempo real



## Custo Constante

Complexidade  $O(1)$  por passo temporal garante escalabilidade

# Arquitetura Unificada de Eventos Temporais

A detecção online organiza a teoria de eventos temporais em uma arquitetura coerente. Tipicidade, eventos e modelos passam a ser componentes de um mesmo sistema integrado.

## Tipicidade como Base

Fundamento conceitual do sistema

## Eventos como Desvios

Violações da tipicidade estabelecida

## Integração Teórica

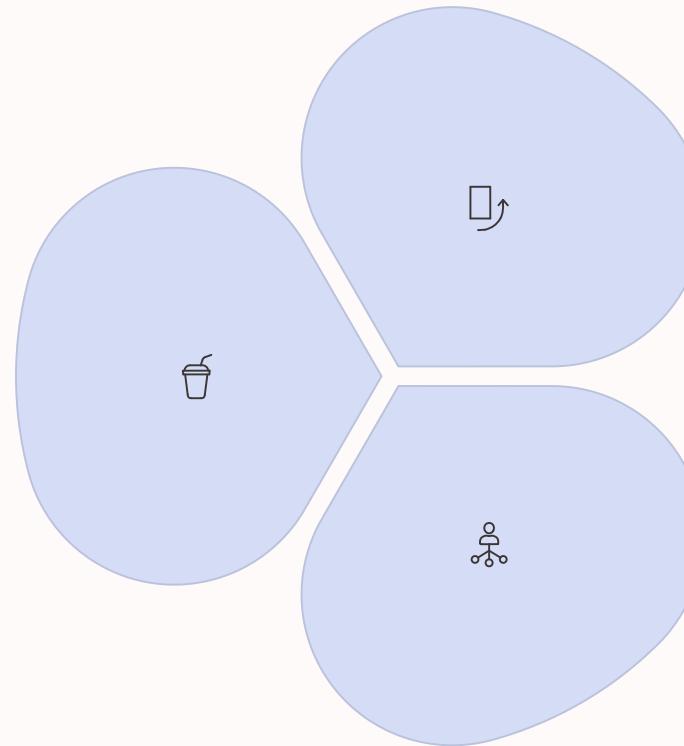
União entre teoria e sistemas práticos

# Eventos como Dinâmica Temporal

A síntese final é que eventos em séries temporais não são objetos estáticos, mas fenômenos dinâmicos. A detecção online transforma a teoria de eventos em uma teoria do tempo em movimento.

## Tipicidade Adaptativa

Referência dinâmica e evolutiva



## Eventos como Processos

Fenômenos temporais contínuos

## Integração Estatística-ML

União de paradigmas complementares

Esta visão unificada estabelece uma nova compreensão dos eventos temporais como manifestações da dinâmica inerente aos processos observados ao longo do tempo.

# Referências Bibliográficas

Uma coleção cuidadosamente selecionada de obras fundamentais que abordam análise de séries temporais e mineração de dados.



## Event Detection in Time Series

Ogasawara, E.; Salles, R.; Porto, F.; Pacitti, E.

(2025). Publicação recente da Springer Nature Switzerland que explora técnicas avançadas de detecção de eventos em séries temporais.

## Time Series Analysis: With Applications in R

Cryer, J. D.; Chan, K.-S. (2008). Obra clássica da Springer que combina fundamentação teórica sólida com implementações práticas.

## Data Mining: Concepts and Techniques

Han, J.; Pei, J.; Tong, H. (2022). Quarta edição publicada pela Morgan Kaufmann que consolida conceitos fundamentais e técnicas avançadas de mineração de dados.