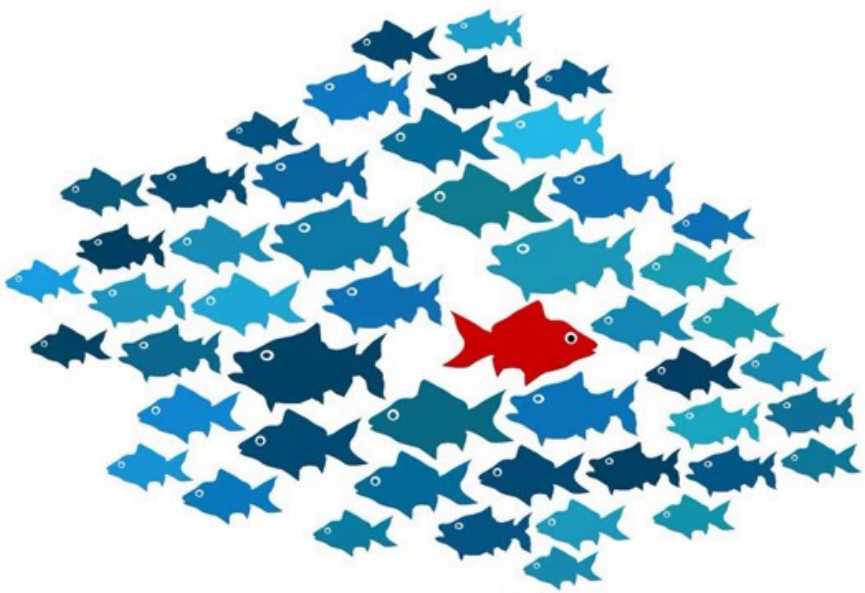
Обнаружение аномалий

Виктор Китов

v.v.kitov@yandex.ru



Аномалии (выбросы)

- Аномалия (выброс, outlier) - объект, нетипичный для общего распределения объектов.
- Применения обнаружения аномалий
  - очистка данных (убрать ошибочные наблюдения)
  - обнаружение нетипичных объектов:
    - мошеннические финансовые транзакции
    - хакерские атаки в сети
    - мониторинг исправности устройств

Методы обнаружения аномалий

- Виды постановок задач:
  - **Детекция новизны (novelty detection):** обучающая выборка не содержит аномалий.
  - **Детекция выбросов (outlier detection):** обучающая выборка содержит аномалии.
- Методы оценивают степень нетипичности:

$$x \text{ - выброс} \iff outlierness(x) > threshold$$

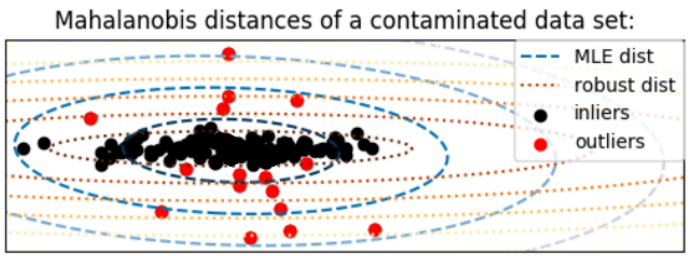
- Это задача обучения без учителя
  - если с учителем, то это классификация несбалансированных классов
- Оценка - по размеченной валидации, используя ROC, AUC.
  - но не используем для обучения-выбросов мало, переобучимся

Содержание

Статистическое обнаружение аномалий

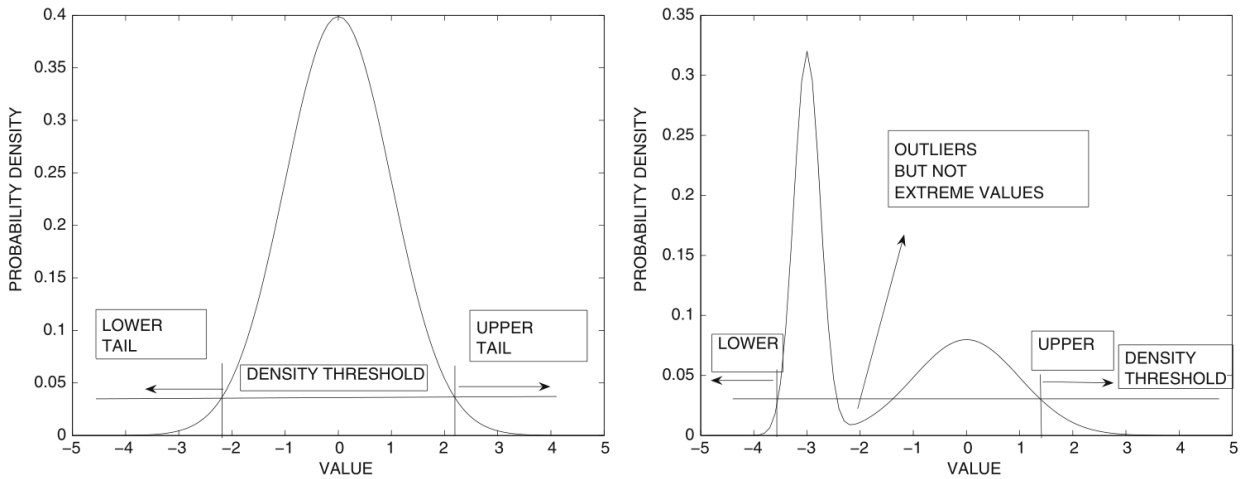
- Выбросы - точки с $p(x) < threshold$.
- Предположим $p(x) \sim \mathcal{N}(x|\mu, \Sigma) \propto e^{-\frac{1}{2}(x-\mu)^T\Sigma^{-1}(x-\mu)}$.
- После получения $\widehat{\mu}, \widehat{\Sigma}$ устойчивым к выбросам способом найдем расстояние Махаланобиса:

$$outlierness(x) = \sqrt{(x-\widehat{\mu})^T\widehat{\Sigma}^{-1}(x-\widehat{\mu})}$$



Статистическое обнаружение аномалий

- Выбросы не обязательно на границе распределений:



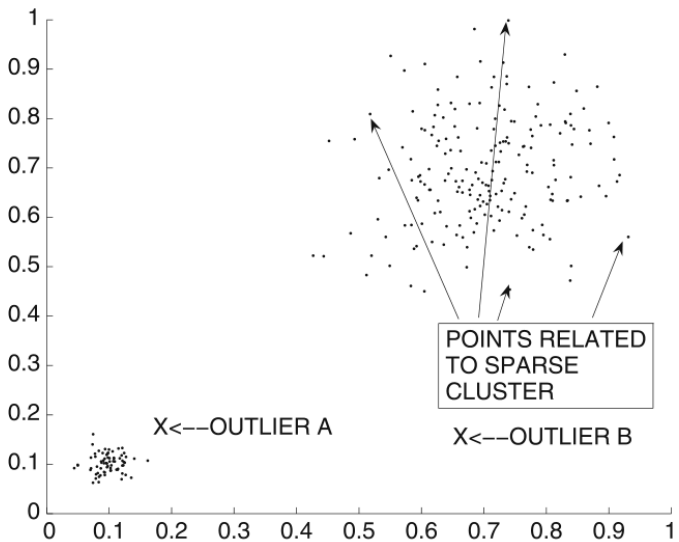
(a) Symmetric distribution (b) Asymmetric distribution

- $p(x)$ можно оценить параметрически, смесью или ядерной оценкой плотности (KDE)
  - лучше не включать x в оценку, особенно для KDE.

Содержание

Обнаружение аномалий по расстоянию

простой способ: x-outlier $\Longleftrightarrow d_K(x) > threshold$



- выброс A либо пропущен, либо все точки разреженного кластера - выбросы.
- Local outlier factor (LOF) приспосабливается к изменяемой плотности.

Метод local outlier factor

- Идея: смотреть на относительное расстояние:

$$outlierness(x) = \frac{\rho\left(x, x_{NN_K(x)}\right)}{\rho\left(x_{NN_K(x)}, x_{NN_K(x_{NN_K}(x))}\right)}$$

где $NN_K(x)$-индекс K-го ближайшего соседа x.

Метод local outlier factor

- Идея: смотреть на относительное расстояние:

$$outlierness(x) = \frac{\rho\left(x, x_{NN_K(x)}\right)}{\rho\left(x_{NN_K(x)}, x_{NN_K(x_{NN_K}(x))}\right)}$$

где $NN_K(x)$-индекс K-го ближайшего соседа x.

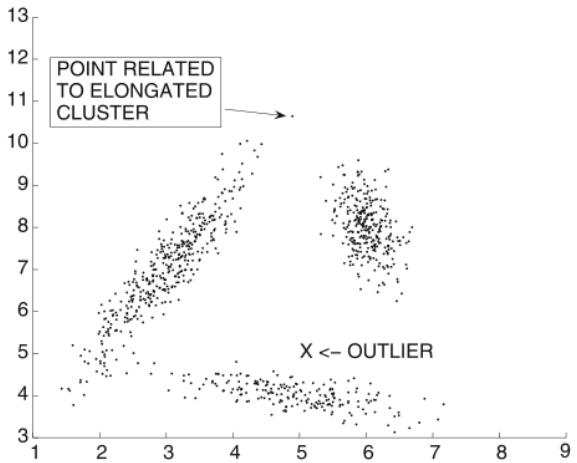
- Метод LOF (сглаженный вариант)

$$outlierness(x) = \frac{1}{K}\sum_{i\in NN_K(x)}\frac{AR_K(x)}{AR_K(x_i)}$$

где $AR_K(x)$ - оценка локальной плотности вокруг x:

$$AR_K(x) = \frac{1}{K}\sum_{i\in NN_K(x)}\rho(x, x_i)$$

Учет локального распределения точек



- У учетом локального распределения выброс м. быть не самым далеким объектом.
- Подходы, учитывающие локальное распределение:
  - смесь Гауссиан, выброс-точка с малым $p(x)$ либо принадлежащая компоненте с большим Σ.
  - метод локального кластера (local cluster)
  - метод локальной окрестности (local neighborhood)

Метод локального кластера

1. Кластеризуем точки на K кластеров:
2. Для каждого кластера находим μ_k и Σ_k.
3. Для объекта x:
   1. находим ближайший кластер:

$$\widehat{c} = \arg\min_c \sqrt{(x-\mu_c)^T \Sigma_c^{-1} (x-\mu_c)}$$

   2. степень нетипичности:

$$outlierness(x) = \sqrt{(x-\mu_{\widehat{c}})^T \Sigma_{\widehat{c}}^{-1} (x-\mu_{\widehat{c}})}$$

Метод локальной окрестности

1. Инициализируем $L_K(x) = \{x\}$
2. Для $k = 1, 2, ...K$:
   1. $x_k = \arg\min_z \rho(z, L_K(x))$
   2. $L_K(x) := L_K(x) \cup \{x_k\}$
3. Исключим x: $L_K(x) := L_K(x) \backslash \{x\}$
4. Используя $L_K(x)$ рассчитаем $\mu(x)$ и $\Sigma(x)$
5. Степень нетипичности:

$$outlierness(x) = \sqrt{(x - \mu(x))^T \Sigma(x)^{-1} (x - \mu(x))}$$

Комментарий: вычислительно сложнее м-да локального кластера, зато лучше таргетирует распределение вокруг x.

Содержание

Одноклассовый метод опорных векторов

Найдем подпирающую границу данных $\langle w, x_n \rangle + w_0 \geq \rho$ с макс. ρ:

$$\begin{cases} \frac{1}{2}\|w\|^2 - \rho \to \min_{w,w_0,\rho}, \\ \langle w, x_n \rangle + w_0 \geq \rho \qquad\qquad n = \overline{1,N} \end{cases}$$

Одноклассовый метод опорных векторов

Найдем подпирающую границу данных $\langle w, x_n \rangle + w_0 \geq \rho$ с макс. ρ:

$$\begin{cases} \frac{1}{2}\|w\|^2 - \rho \to \min_{w,w_0,\rho}, \\ \langle w, x_n \rangle + w_0 \geq \rho \qquad\qquad n = \overline{1,N} \end{cases}$$

Одноклассовый метод опорных векторов (one-class SVM) оставляет "нарушителей", внося штраф $\xi_n \geq 0$:

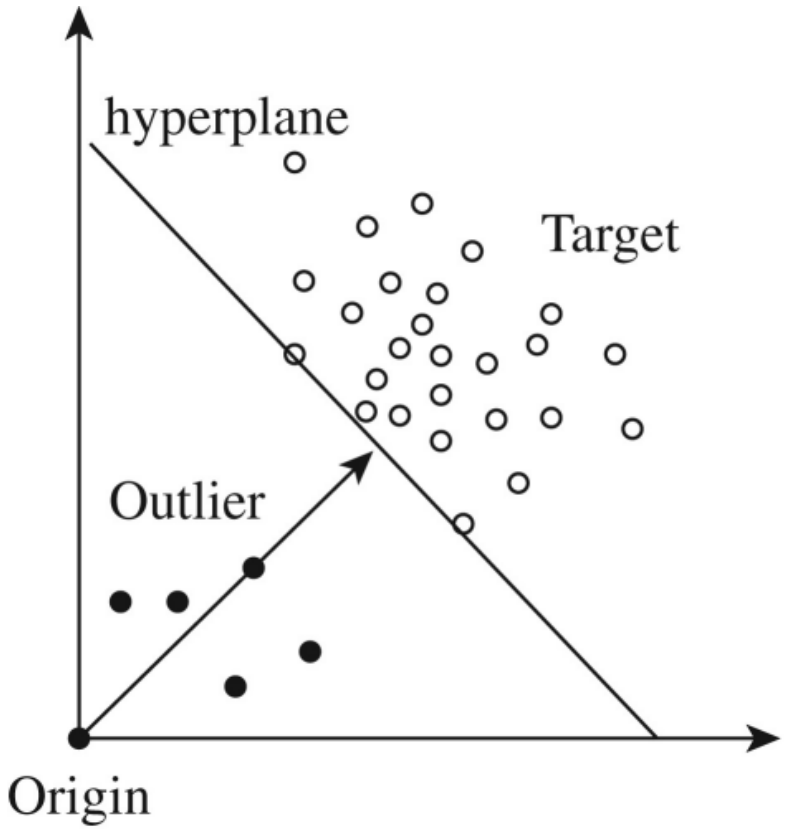
$$\begin{cases} \frac{1}{2}\|w\|^2 + \frac{1}{\nu N}\sum_{n=1}^{N}\xi_n - \rho \to \min_{w,\rho,\xi_1,\dots\xi_N} \\ \langle w, x_i \rangle + w_0 \geq \rho - \xi_n,\ n = \overline{1,N}. \\ \xi_n \geq 0,\ n = \overline{1,N}. \end{cases}$$

$\langle w, x_i \rangle + w_0 < \rho \ <=>\ x_i -$ выброс, $\nu \downarrow \Rightarrow$#выбросов$\downarrow$, доля выбросов в выборке$\to \nu$ при $N \to \infty$

$$outlierness(x) = \rho - \langle w, x \rangle + w_0$$

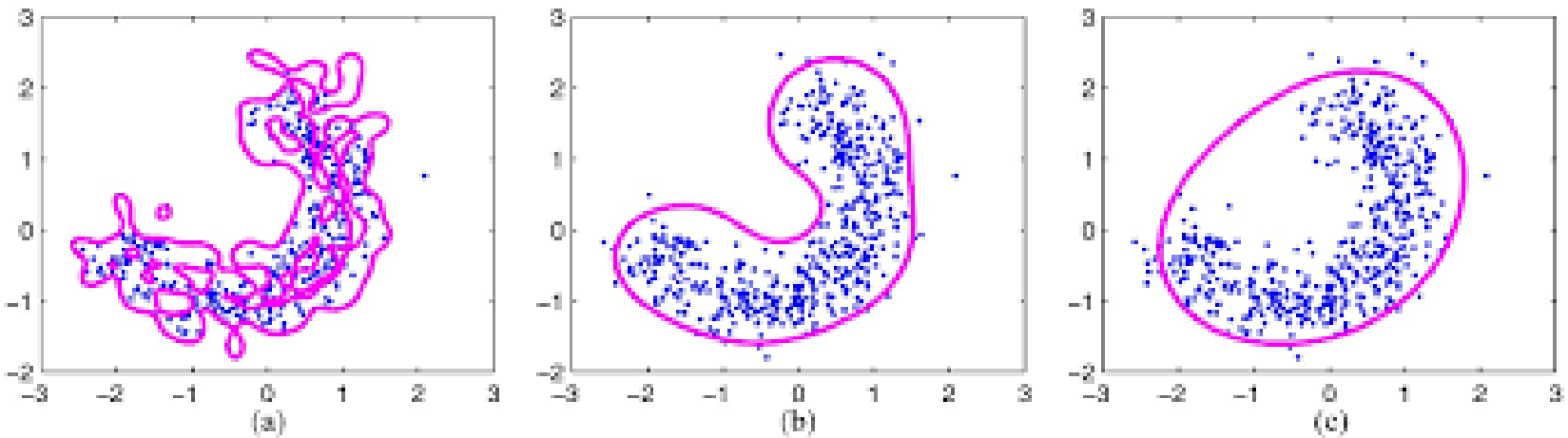
Интуиция

Выбросы - объекты, слишком близкие к началу координат



Ядерное обобщение с RBF ядром

Одноклассовый SVM с RBF ядром ($\sigma \uparrow$)



Содержание

Изолирующий лес

- Алгоритм построения изолирующего дерева:

```
инициализировать корень со всеми наблюдениями

пока существуют узлы с ≥ 2 несовпадающими наблюдениями:
    выбрать такой узел
    выбрать случайный неконстантный признак f
    выбрать случайный порог t ∈ [f_min, f_max)
    разбить узел на 2 подузла по правилу f ≤ t
```

Изолирующий лес

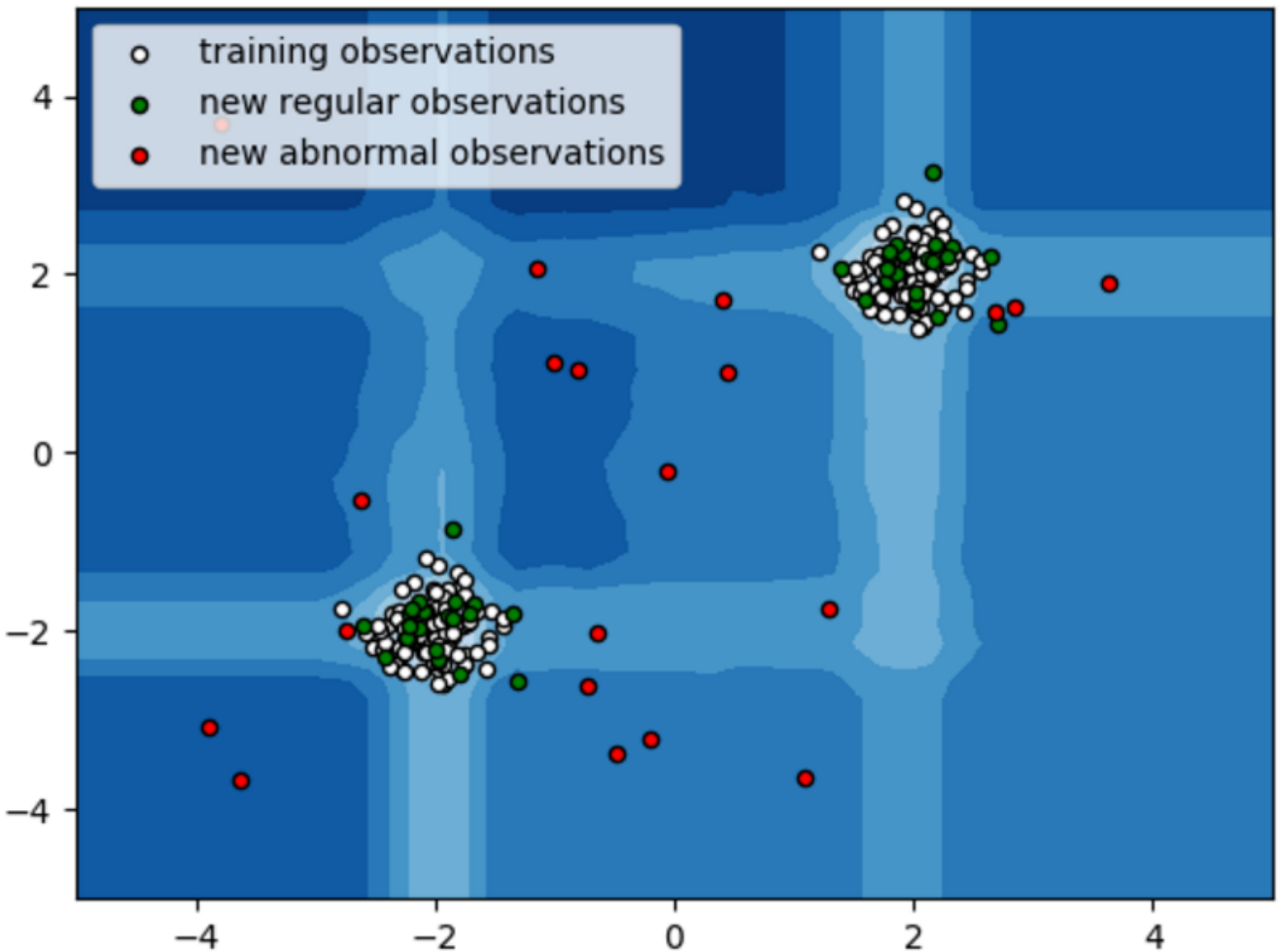
- Алгоритм построения изолирующего дерева:

```
инициализировать корень со всеми наблюдениями

пока существуют узлы с ≥ 2 несовпадающими наблюдениями:
    выбрать такой узел
    выбрать случайный неконстантный признак f
    выбрать случайный порог t ∈ [f_min, f_max)
    разбить узел на 2 подузла по правилу f ≤ t
```

  - Типичность объекта≈глубина листа с этим объектом
    - выбросы легче отделить
    - показатель слишком зависит от дерева
- Изолирующий лес (isolation forest) - ансамбль M независимых изолирующих деревьев.
  - типичность объекта=средняя глубина соотв. листа по деревьям.
  - нетипичность = - типичность.

Пример работы изолирующего леса



Заключение

- Детекция выбросов - задача обучения без учителя
  - с учителем - классификация несбалансированных классов
- Важно адаптировать метод к
  - изменяющейся плотности данных
  - локальному распределению данных
- Оценка - по размеченной валидации, используя ROC, AUC.
- Подходы:
  - основанные на плотности $p_\theta(x) < threshold$, θ-робастная оценка.
  - основанные на расстоянии
    - Local outlier factor (LOF)
    - метод локальных центроидов
    - метод локальных окрестностей
  - Линейный: одноклассовый метод опорных векторов +ядерное обобщение
  - Правиловый: изолирующий лес

Сравнение методов

Сравнение методов (sklearn)