LIRIS

UMR 5205 CNRS

Détection d'anomalies

Haytham Elghazel

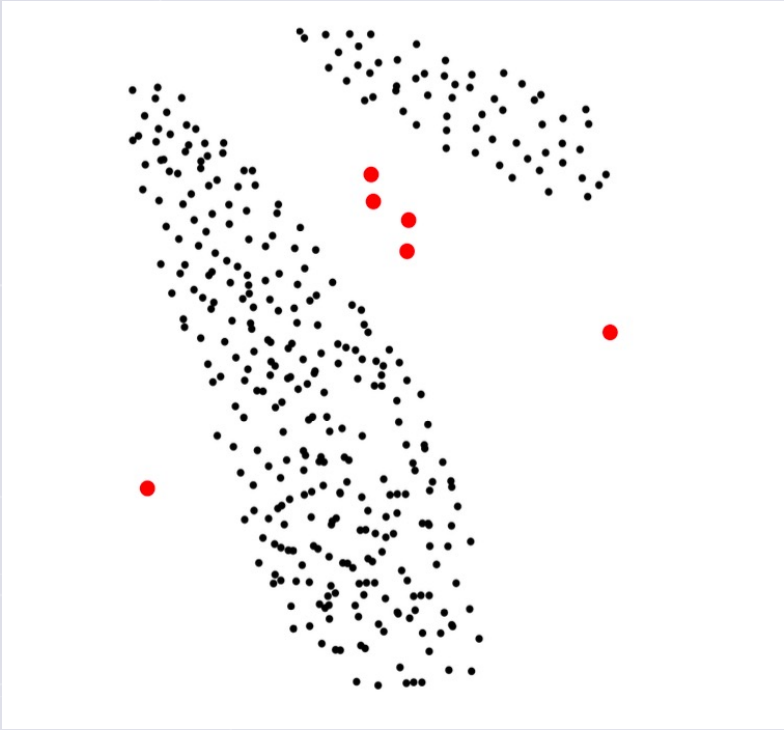
Laboratoire d'InfoRmatique en Image et Systèmes d'information

Pôle Data Science, Equipe DM2L

cnrs INSA Université Claude Bernard Lyon 1 Université Lumière Lyon 2 École Centrale Lyon

Détection d'anomalies

Identifier les instances ayant un comportement non conforme



Applications : Network intrusions, fraude de carte de crédit, surveillance, assurance

Détection d'anomalies

- Supprimer ou modifier les observations atypiques à un modèle sans justification serait totalement contraire à l'éthique.

- L'objectif est avant tout de les identifier car ce sont celles, les plus susceptibles d'être la conséquence d'une erreur (à confirmer) de mesure, de libellé, ou encore une anomalie, défaillance ou tentative de fraude, d'intrusion, selon le contexte.

Détection d'anomalies

- La **détection d'anomalies** contient deux familles d'approches :
  - **Détection d'outliers (Outlier detection) :** Les données d'apprentissage contiennent des outliers et qui sont des observations qui se trouvent loin des autres. Il s'agit d'apprendre à détecter les anomalies dans le jeu de données initial en cherchant des régions denses (où les données sont le plus concentrées) tout en ignorant les anomalies.
  - **Détection de nouveautés (Novelty detection) :** Ici le jeu de données d'apprentissage n'est pas pollué par des anomalies. Il s'agit de détecter des anomalies dans les données futures non observées (nouvelles données). Les outliers sont ainsi appelés nouveautés.

Plusieurs approches

- **Approches supervisées**
  - Des labels à la fois pour les instances normales et anomalies
  - Les anomalies appartiennent à la classe rare
  - Données déséquilibrées

- **Approches non supervisées**
  - Pas de labels fournis
  - Base d'apprentissage = données normales + anomalies
  - Les anomalies sont très rares

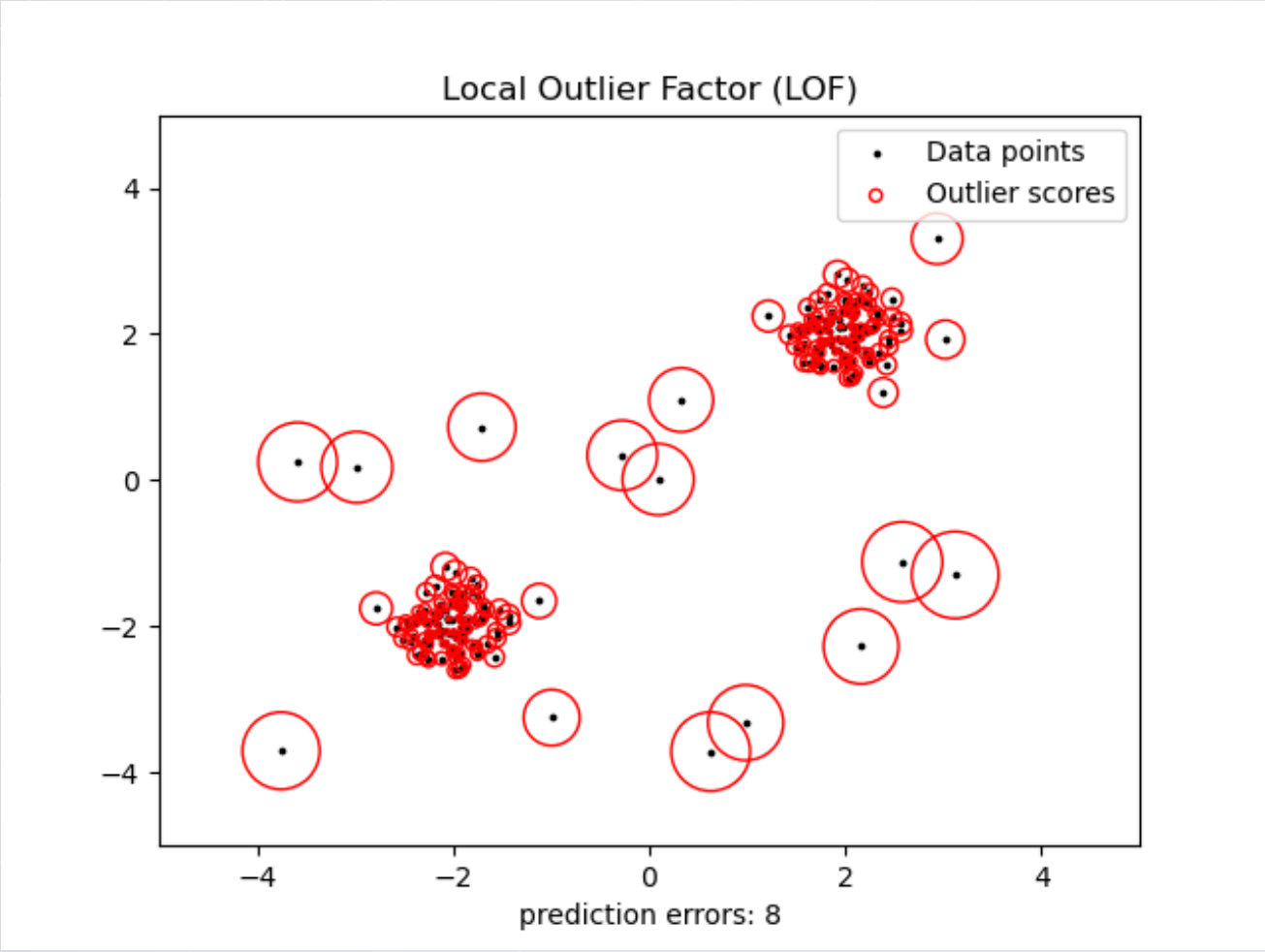
Approches non supervisées

- **Approches basées sur le voisinage**
  - L'anomalie ou l'isolement d'une observation est apprécié par la proximité des points de son voisinage
    - **Exemple :** Local Outlier Factor (LOF)
    - LOF compare la densité locale des observations. S'il existe une différence entre le point observé et ses voisins, le point est considéré comme une anomalie. Cette méthode est basée sur les k plus proches voisins : la densité locale d'une observation est évaluée en considérant les k plus proche observations de son voisinage.

Local Outlier Factor

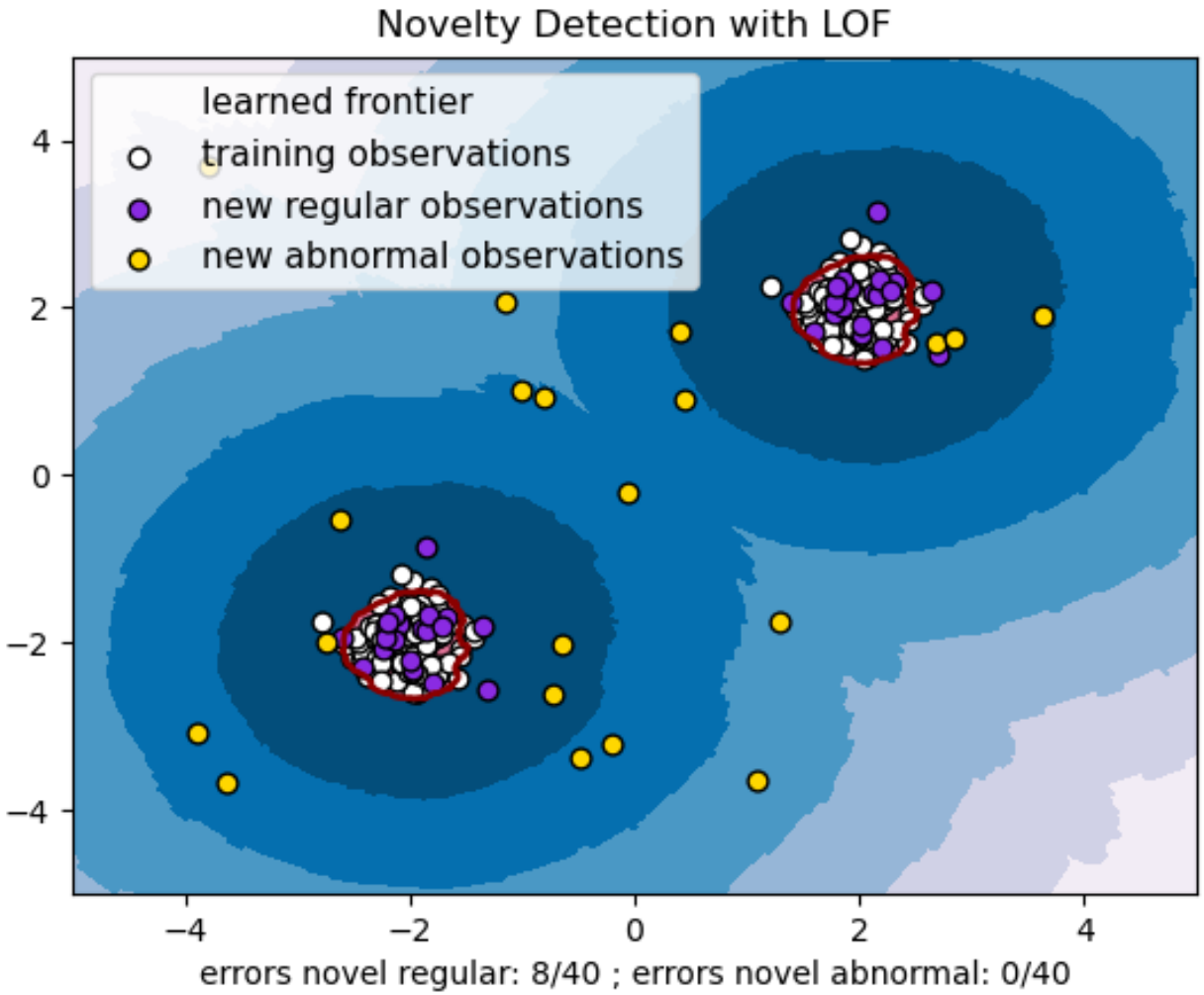
- On définit pour chaque point **x**, $\mathbf{D_k(x)}$ sa distance par rapport à son $\mathbf{k^{ème}}$ plus proche voisin et $\mathbf{N_k(x)}$ l'ensemble de ses **k** plus proches voisins.
- On définit la distance d'accessibilité $\mathbf{R_k(x,y)}$ de **x** par rapport à **y** comme étant le **max(d(x,y) et $\mathbf{D_k(y)}$)**.
- On définit la distance d'accessibilité moyenne $\mathbf{AR_k(x)}$ de **x** comme étant égale à la moyenne des distances d'accessibilité de **x** avec tous les points de son voisinage $\mathbf{N_k(x)}$
- On définit la densité d'accessibilité locale $\mathbf{f_k(x)}$ comme étant l'inverse de $\mathbf{AR_k(x)}$.
- **Une instance normale est sensée avoir une densité locale similaire à ses voisins, alors qu'une instance anormale est sensée avoir un beaucoup plus petite to have densité locale**
- On définit **LOF(x)** par la moyenne du rapport $\mathbf{f_k(y)/f_k(x)}$ pour tous les **y** dans $\mathbf{N_k(x)}$.
- Le LOF mesure l'écart local d'un point par rapport à ses k voisins les plus proches
- Si ce score est proche de 1, nous pouvons en conclure que l'observation est comparable à ses voisins. Si le score est inférieur à 1, nous pouvons dire que l'observation se trouve dans une région dense. Dans les deux cas, l'observation n'est pas considérée comme un outlier.
- Un score est largement supérieur à 1 indique qu'on à faire à un outlier.

Local Outlier Factor



- Utilisée pour la détection de nouveautés ou d'outliers.
- LOF est une méthode est très puissante en dimension modérée.

Local Outlier Factor



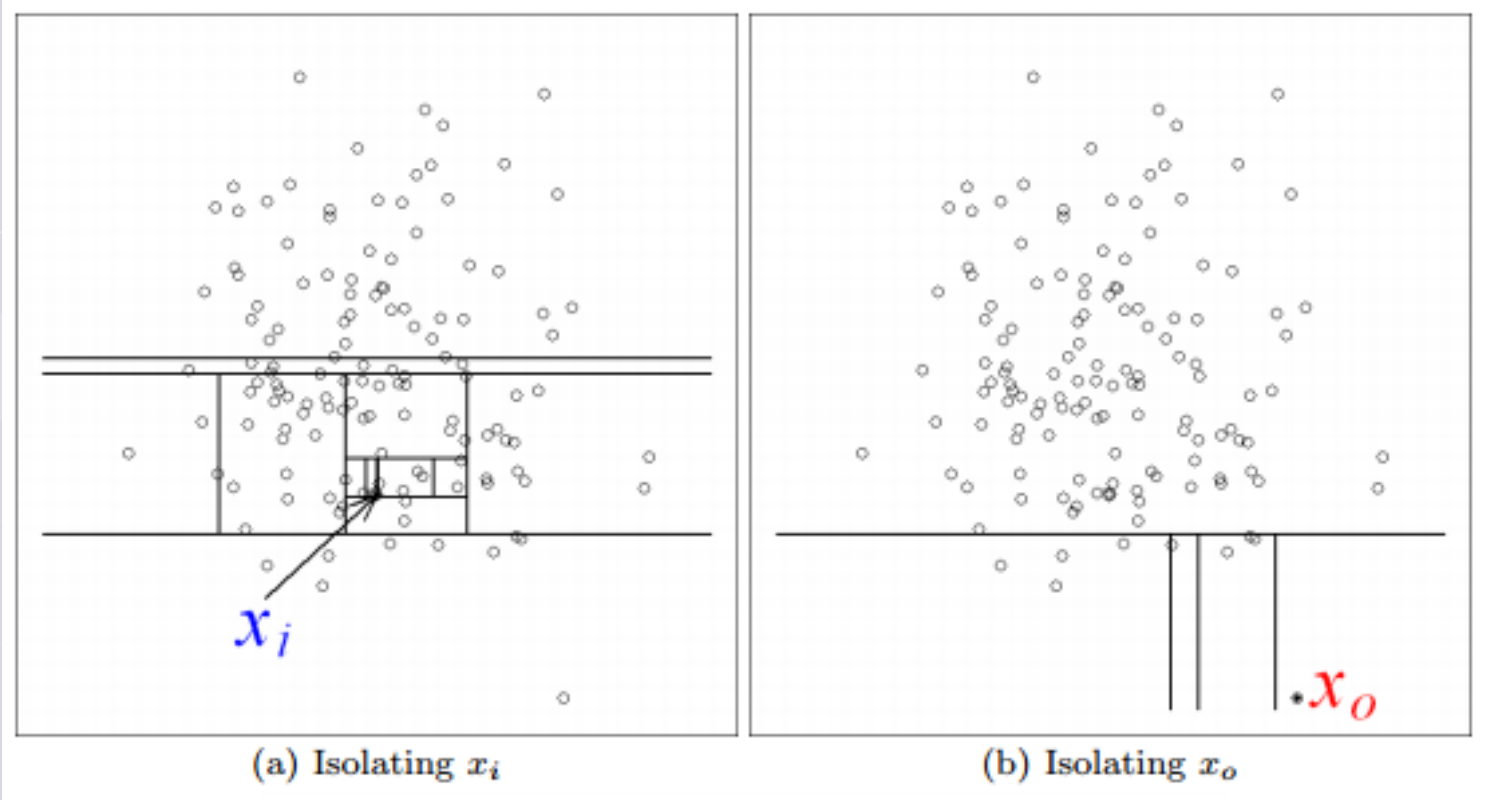
Approches non supervisées

- **One class SVM : Pour la détection de nouveauté.**
  - L'objectif est de séparer toutes les observations, de l'origine, dans l'espace de représentation en maximisant la marge, à savoir la distance entre l'hyperplan et l'origine.

- **Isolation Forest (Forêt d'isolation) : Pour la détection d'outliers.**

Isolation Forest

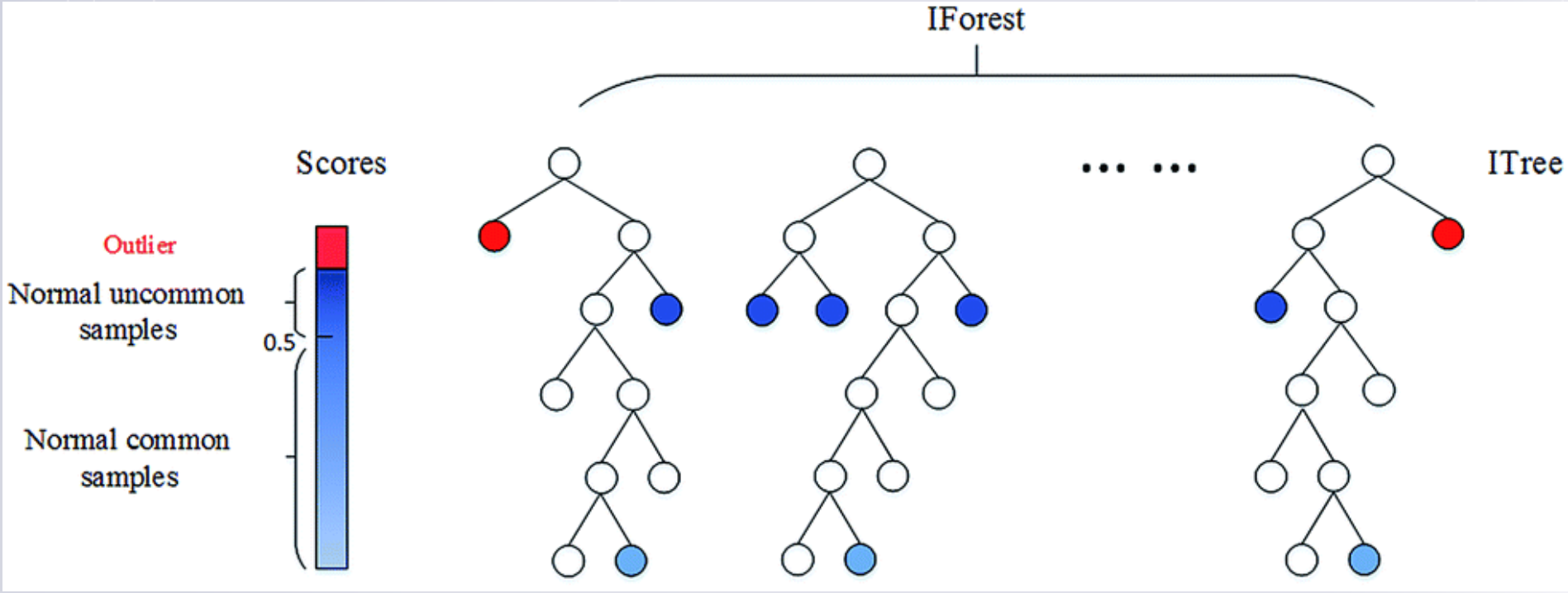
Principe : Les anomalies sont rares et différentes. Elles sont donc susceptibles au mécanisme d'isolation



(a) Isolating x_i (b) Isolating x_o

Isolation Forest

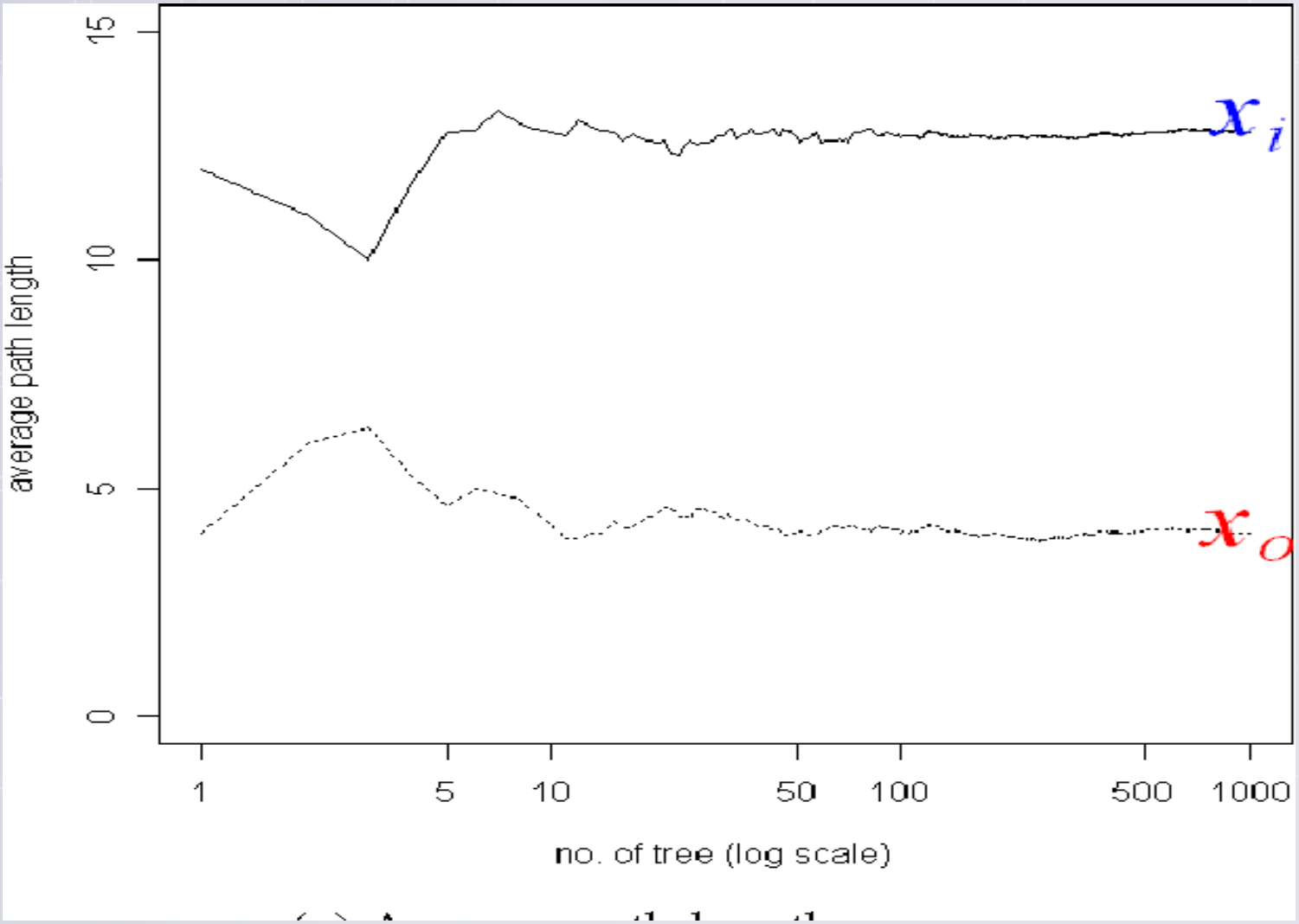
Principe : Les anomalies sont rares et différentes. Elles sont donc susceptibles au mécanisme d'isolation



Isolation Forest

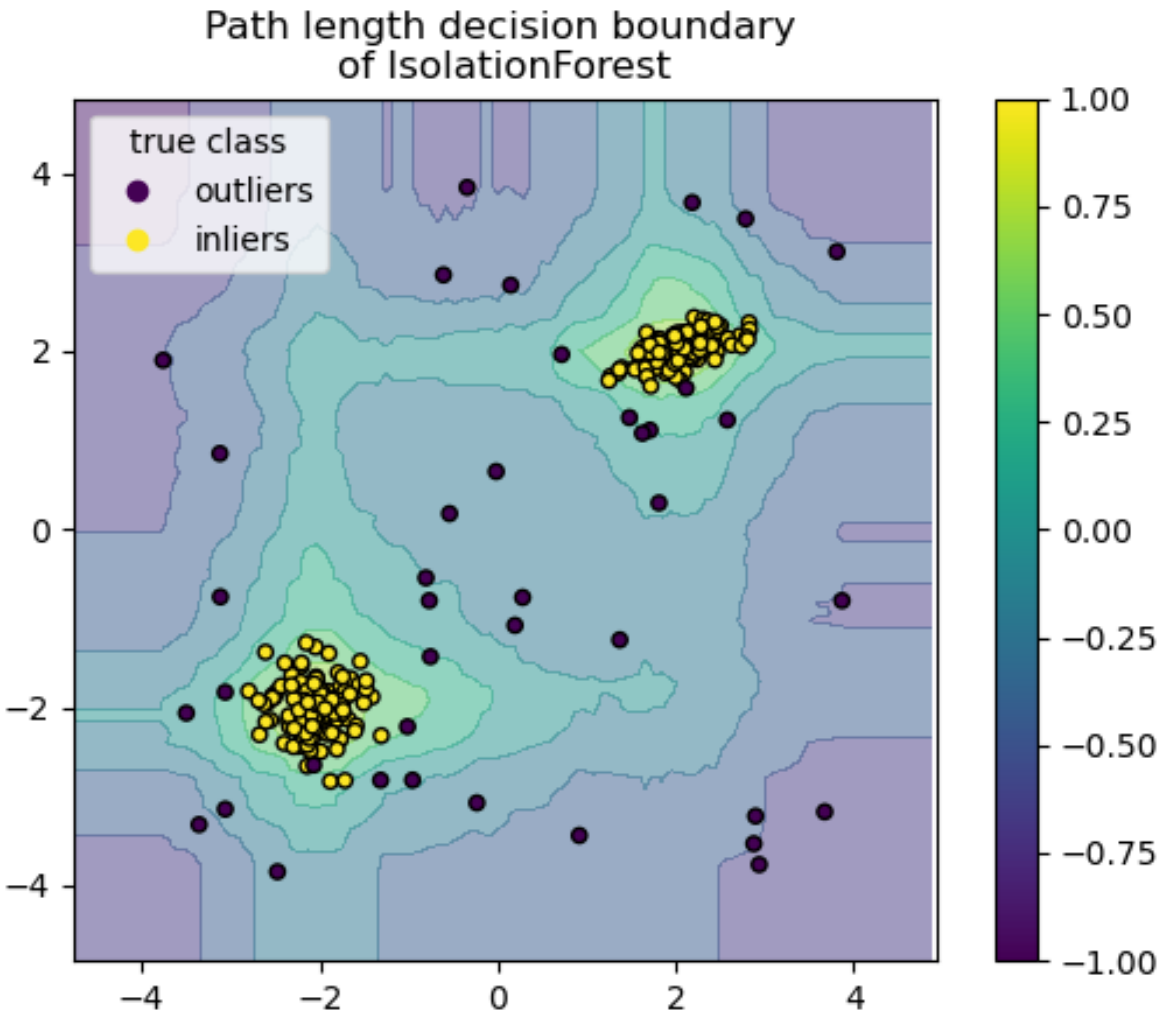
- **Le principe repose sur la construction d'un ensemble d'arbres complètement aléatoires : *isolation tree*.**
- **Chaque arbre est construit sur un échantillon aléatoire des instances**
- **Division opérée dans chaque nœud via un tirage aléatoire d'une variable et**
  - un seuil aléatoire pour une **variable quantitative**
  - une répartition aléatoire des modalités en deux groupes pour une **variable qualitative**
  - La construction de l'arbre jusqu'à l'obtention d'une observation par feuille.
- **Le score de l'isolement ou de l'anomalie d'une observation est obtenue par la *longueur du chemin atteignant cette observation*. Plus celui-ci est court, plus l'observation est considérée isolée ou atypique.**

Isolation Forest



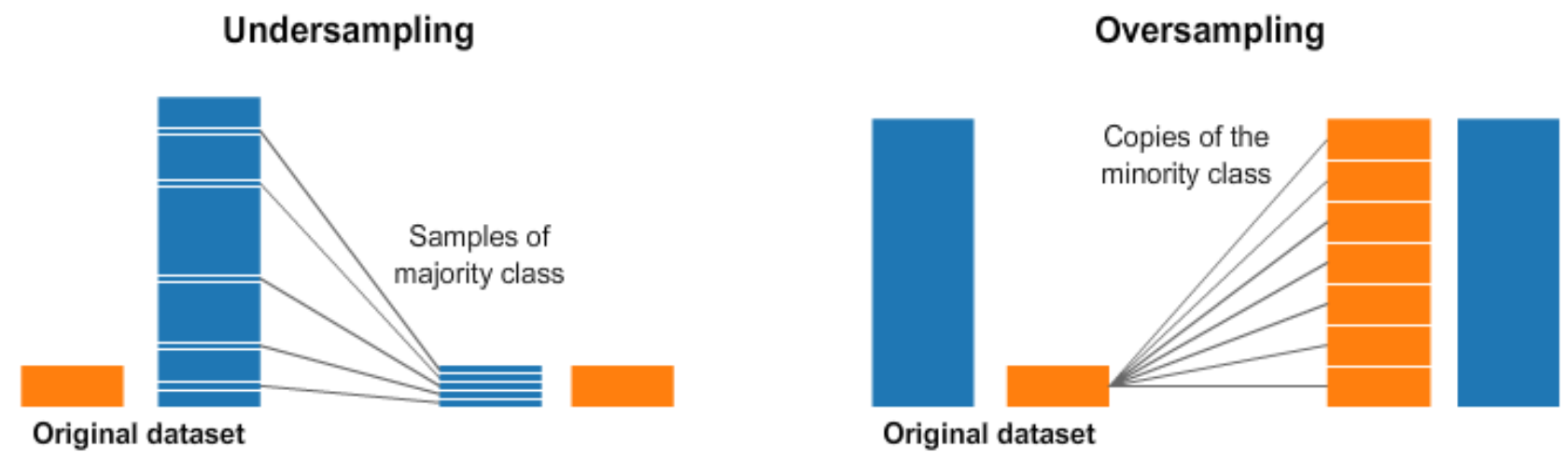
Convergence rapide

Isolation Forest



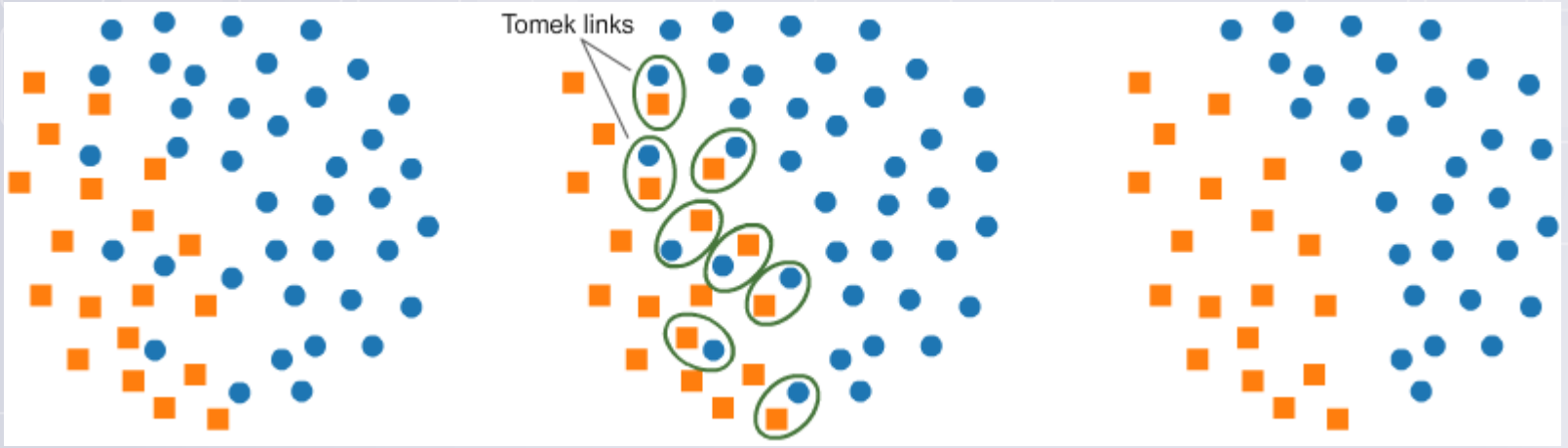
Approches supervisées

- **Approches d'apprentissage sur des données déséquilibrées**
- **Adaptation des approches supervisées existantes :**
  - ***Undersampling*** : sous échantillonnage **(Bibliothèque `imblearn`)**
  - ***Oversampling*** : sur échantillonnage **(Bibliothèque `imblearn`)**
  - ***Balancing :*** Pondération des classes
  - **Random Undersampling et Random Oversampling**

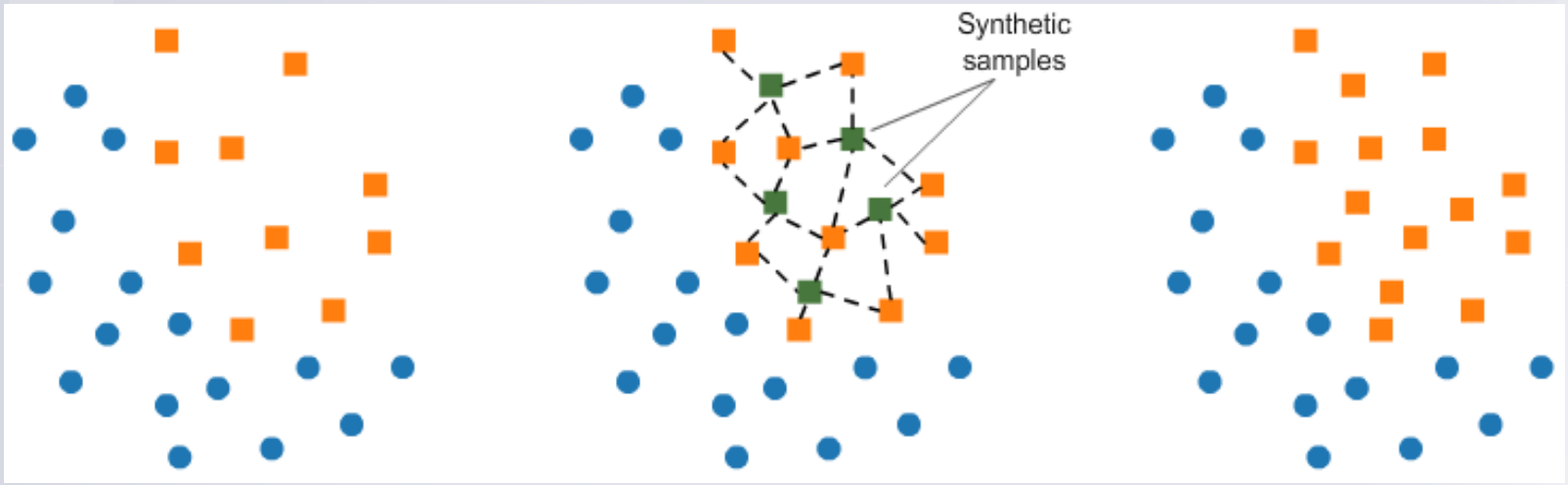


Approches supervisées

- **Tomek Links :** une approche d'undersampling



- **Synthetic Minority Oversampling Technique (SMOTE) :** une approche d'oversampling



Approches supervisées

- **Attention : Bien choisir la métrique d'évaluation**
  - *Accuracy déconseillée*
  - *AUC-ROC déconseillée*
  - *Plutôt utiliser le F1-score ou l'AUC-PR (`average_precision_score`): l'aire sous la courbe formée par les points de coordonnées (Rappel+, Précision+) en fonction du seuil (`precision_recall_curve`).*
- **Attention : Ne pas évaluer votre modèle sur un échantillon équilibré**
- **Les anomalies se produisant souvent de manière complètement nouvelle, le modèle ne pourra pas détecter les nouvelles anomalies sur lesquelles il n'a pas été entraîné.**