MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Πανεπιστήμιο Κύπρου - Τεχνητή Νοημοσύνη

MAI612 - ΜΗΧΑΝΙΚΗ ΜΑΘΗΣΗ

Διάλεξη 14: Ανίχνευση Ανωμαλιών

Βασίλης Βασιλειάδης, PhD

Χειμερινό Εξάμηνο 2022/23

CYENS CENTRE OF EXCELLENCE

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Επανάληψη

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Μείωση των διαστάσεων

- Τι είναι η μείωση των διάστασεων: μετασχηματισμός των δεδομένων υψηλής διάστασης σε χώρο χαμηλής διάστασης
- Γιατί η μείωση της διάστασης:
  - Οπτικοποίηση δεδομένων
  - Συμπίεση δεδομένων
    - Μπορεί να βοηθήσει αλγορίθμους ΜΜ (εποπτευόμενη μάθηση, ομαδοποίηση)
- Ανάλυση κύριων συστατικών
  - Γραμμική μετατροπή σε ένα νέο σύστημα συντεταγμένων
  - Μεγιστοποίηση της διακύμανσης των δεδομένων χαμηλής διάστασης = ελαχιστοποίηση του σφάλματος ανακατασκευής
  - Βρίσκει n ορθογώνια διανύσματα το καθένα με βάση το πόσο εξηγεί τη διακύμανση στα δεδομένα
    - Αυτά είναι τα κύρια συστατικά ή ιδιοδιανύσματα
  - Προβολή = κωδικοποίηση σε χαμηλές διαστάσεις
  - Ανακατασκευή = αποκωδικοποίηση από χαμηλές διαστάσεις σε υψηλές διαστάσεις
  - Μπορούμε να επιλέξουμε τον αριθμό των συστατικών με βάση την επιθυμητή αναλογία εξηγημένης διακύμανσης (συνήθως 90-99 %)

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Μείωση της διάστασης

- Το PCA λειτουργεί καλά σε διάφορα προβλήματα, αλλά είναι μια γραμμική μέθοδος
- Οι μέθοδοι μείωσης της μη γραμμικής διάστασης αντιμετωπίζουν αυτή την έλλειψη
  - Ο πυρήνας PCA χρησιμοποιεί το τέχνασμα του πυρήνα
  - Οι αυτόματοι κωδικοποιητές είναι ΝΔ εκπαιδευμένα να κωδικοποιούν και να ανακατασκευάζουν την είσοδο
- Πολλαπλές προσεγγίσεις μάθησης = μη γραμμικές μέθοδοι μείωσης της διάστασης που θεωρούν ρητά ότι τα δεδομένα βρίσκονται σε δομές χαμηλής διάστασης ενσωματωμένες σε χώρο υψηλής διάστασης
  - Isomap: αντί της Ευκλείδειας απόστασης, θεωρεί την γεωδεσική απόσταση
    - Γεωδεσική απόσταση γ: απόσταση στην πολλαπλότητα
    - Παράδειγμα Swiss roll: ο Isomap μπορεί να το ξεδιπλώσει
    - Επιτρέπει καλύτερη παρεμβολή καθώς τα παρεμβαλλόμενα σημεία που αναμένεται να βρίσκονται στην πολλαπλή
  - T-SNE
    - χρησιμοποιημένος για οπτικοποίηση
    - στοχαστική μέθοδος που διατηρεί τις τοπικές ομοιότητες
    - μπορεί να δώσει διαφορετικά αποτελέσματα για διαφορετικές αρχικοποιήσεις

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Διάλεξη 14: Ανίχνευση ανωμαλίας

Μαθησιακά αποτελέσματα

Θα μάθετε για:

1. Το πρόβλημα της ανίχνευσης ανωμαλίας και η διαφορά της με τη δυαδική ταξινόμηση
2. Η έννοια της εκτίμησης της πυκνότητας και ο τρόπος χρήσης της για την ανίχνευση ανωμαλιών
3. Πώς να χωρέσει τις παραμέτρους μιας πυκνότητας πιθανότητας Gaussian
4. Δημιουργία μοντέλου ανίχνευσης ανωμαλιών με τη χρήση εκτίμησης πυκνότητας πυρήνα, SVM μιας κατηγορίας, δασών απομόνωσης και αυτοκωδικοποιητών
5. Πώς να αξιολογήσετε τα συστήματα ανίχνευσης ανωμαλιών

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Ανίχνευση ανωμαλίας

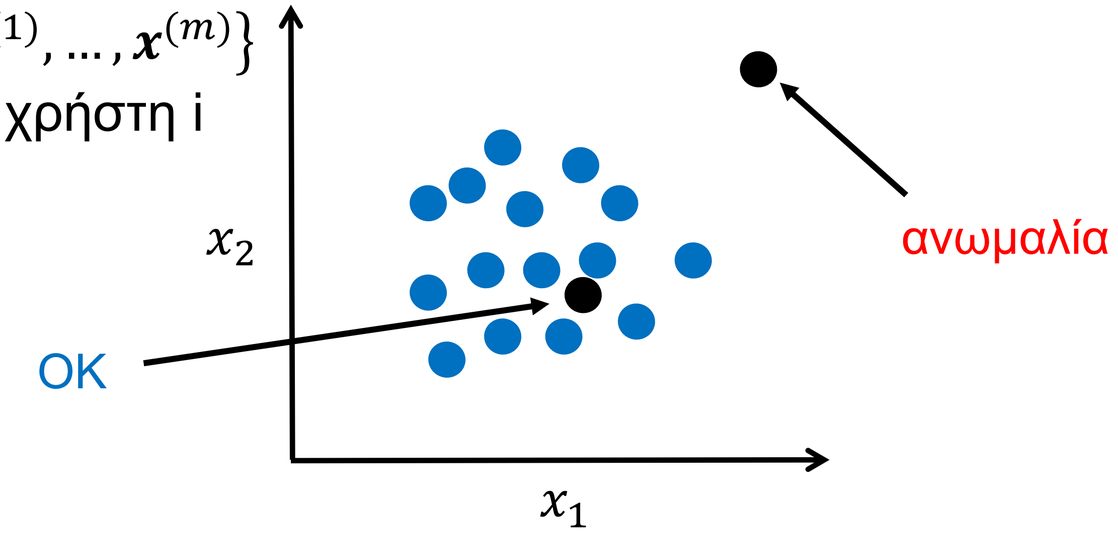
Οι αλγόριθμοι ανίχνευσης ανωμαλίας εξετάζουν ένα μη επισημασμένο σύνολο δεδομένων φυσιολογικών συμβάντων και εγείρουν συναγερμό όταν συμβαίνει ένα ασυνήθιστο ή ανώμαλο συμβάν.

Παράδειγμα ανίχνευσης απάτης:

Δεδομένου ενός συνόλου δεδομένων $D = \{\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(m)}\}$

$\boldsymbol{x}^{(i)}$ χαρακτηριστικά των δραστηριοτήτων του χρήστη i

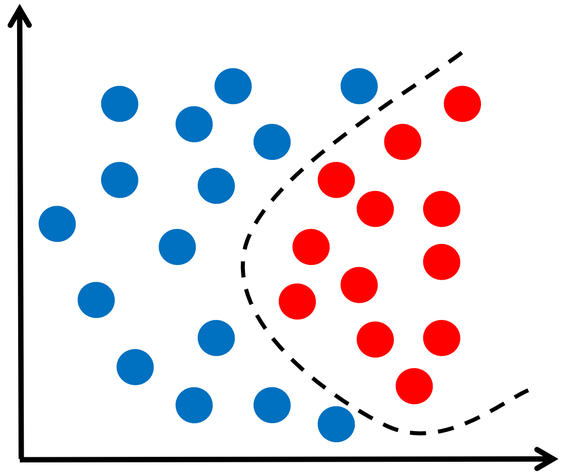
Χαρακτηριστικά γνωρίσματα:
x_1 = αριθμός συναλλαγών
x_2 = ταχύτητα πληκτρολόγησης



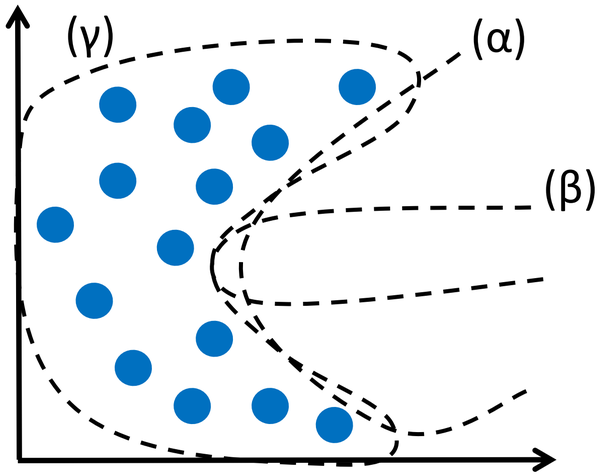
Νέος χρήστης: $\boldsymbol{x}^{(new)}$

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Εποπτευόμενη δυαδική ταξινόμηση έναντι ανίχνευσης ανωμαλίας



- Διαθεσιμότητα μεγάλου αριθμού θετικών και αρνητικών παραδειγμάτων
- Ο αλγόριθμος κατανοεί πώς να δομήσει το όριο απόφασης
- Μελλοντικά αρνητικά παραδείγματα πιθανόν να είναι παρόμοια με αυτά στο σύνολο κατάρτισης



- Εάν δεν υπάρχουν αρνητικά παραδείγματα κατά τη διάρκεια της κατάρτισης, πώς θα πρέπει να είναι το όριο απόφασης;

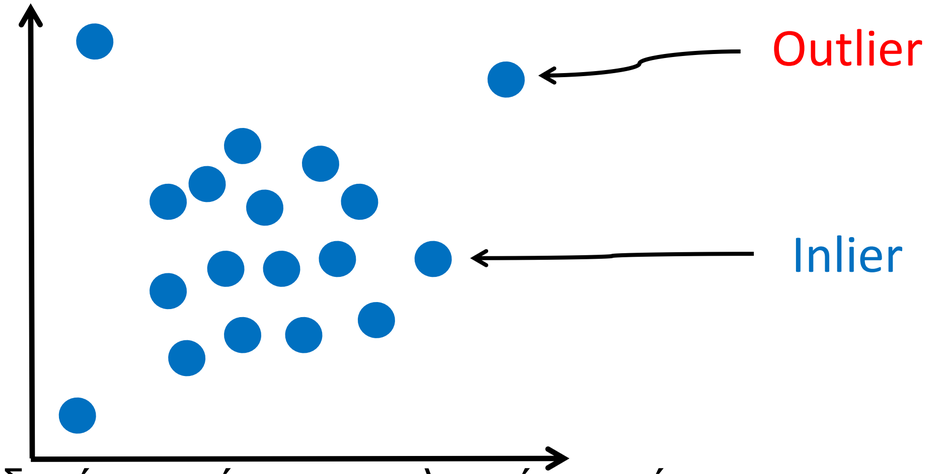
- Για παράδειγμα:
  1. Εντοπισμός απάτης
  2. Παρακολούθηση μηχανών

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

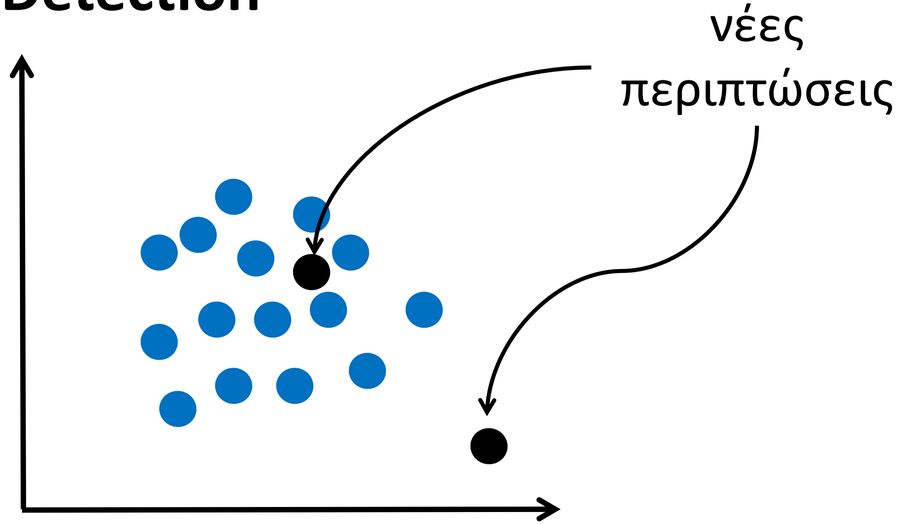
Ανίχνευση ανωμαλίας

Outlier Detection



- Δεδομένα κατάρτισης μολυσμένα από ακραίες τιμές (περιστάσεις μακριά από τις άλλες)
- Κατάλληλες περιοχές με τα πιο συγκεντρωμένα δεδομένα
- Ας υποθέσουμε ότι οι ακραίες τιμές δεν είναι συγκεντρωμένες

Novelty Detection



- Δεν υπάρχουν ακραίες τιμές στα δεδομένα κατάρτισης
- Ενδιαφέρεστε να εντοπίσετε αν μια **νέα** περίπτωση είναι ακραία (καινοτόμος)
- Οι καινοτομίες θα μπορούσαν να συγκεντρωθούν εφόσον βρίσκονται σε μια περιοχή **χαμηλής πυκνότητας** των δεδομένων κατάρτισης

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Εκτίμηση πυκνότητας

Τυχαία μεταβλητή x από δειγματοληψία από **άγνωστη** κατανομή πιθανοτήτων $p(x)$

- x είναι ένα χαρακτηριστικό

Πυκνότητα πιθανοτήτων: σχέση μεταξύ των αποτελεσμάτων (τιμές) x και της πιθανότητας

- Ορισμένα αποτελέσματα μιας τυχαίας μεταβλητής θα έχουν χαμηλή πυκνότητα πιθανότητας, άλλα θα έχουν υψηλή πυκνότητα πιθανότητας

Κατανομή πιθανοτήτων: το σχήμα της πυκνότητας πιθανότητας σε όλο το πεδίο x

- Π.χ., στολή, Gaussian, εκθετική

Ο υπολογισμός των πιθανοτήτων για συγκεκριμένα αποτελέσματα x πραγματοποιείται από **συνάρτηση πυκνότητας πιθανότητας** (PDF)

Χρήσιμο να γνωρίζουμε το PDF για ένα δείγμα δεδομένων, προκειμένου να γνωρίζουμε αν μια δεδομένη παρατήρηση είναι απίθανη, έτσι ώστε να θεωρείται μια ακραία ή ανωμαλία

(Πιθανότητα) Εκτίμηση πυκνότητας: χρησιμοποιούμε τις παρατηρήσεις από το δείγμα μας (δεδομένα) για να εκτιμήσουμε την πυκνότητα των πιθανοτήτων πέρα από το δείγμα.

ΠΗΓΗ

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

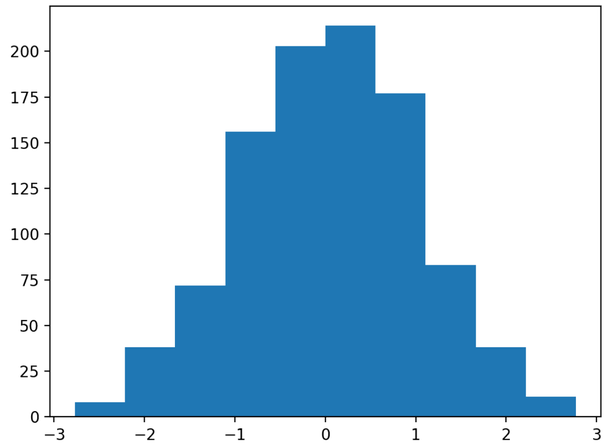
Εκτίμηση πυκνότητας: Ιστόγραμμα

Ιστόγραμμα: σχεδιάστε ότι ομαδοποιεί τις παρατηρήσεις σε κάδους και μετρώντας τον αριθμό των γεγονότων που πέφτουν στον κάδο

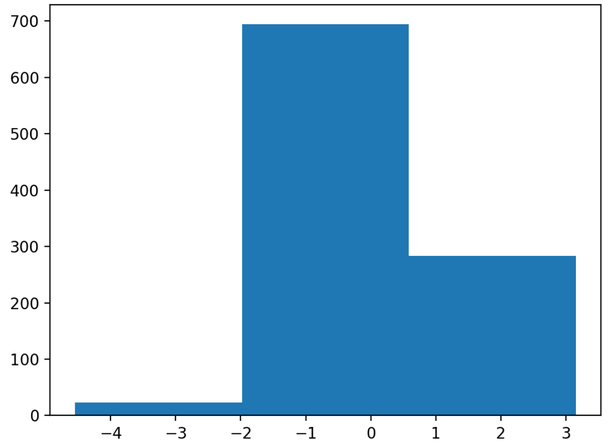
Οι μετρήσεις (ή συχνότητες) σε κάθε κάδο απεικονίζονται ως γράφημα μπαρ με κάδους στον άξονα x και συχνότητα στον άξονα y

Η επιλογή του αριθμού των κάδων είναι σημαντική:
- ελέγχει τη χονδρότητα της κατανομής
- πόσο καλά απεικονίζεται η πυκνότητα των παρατηρήσεων

Το σχήμα του ιστογράμματος συχνά ταιριάζει με γνωστές κατανομές πιθανοτήτων



10 κάδοι



3 κάδοι

ΠΗΓΗ

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Παραμετρική εκτίμηση πυκνότητας

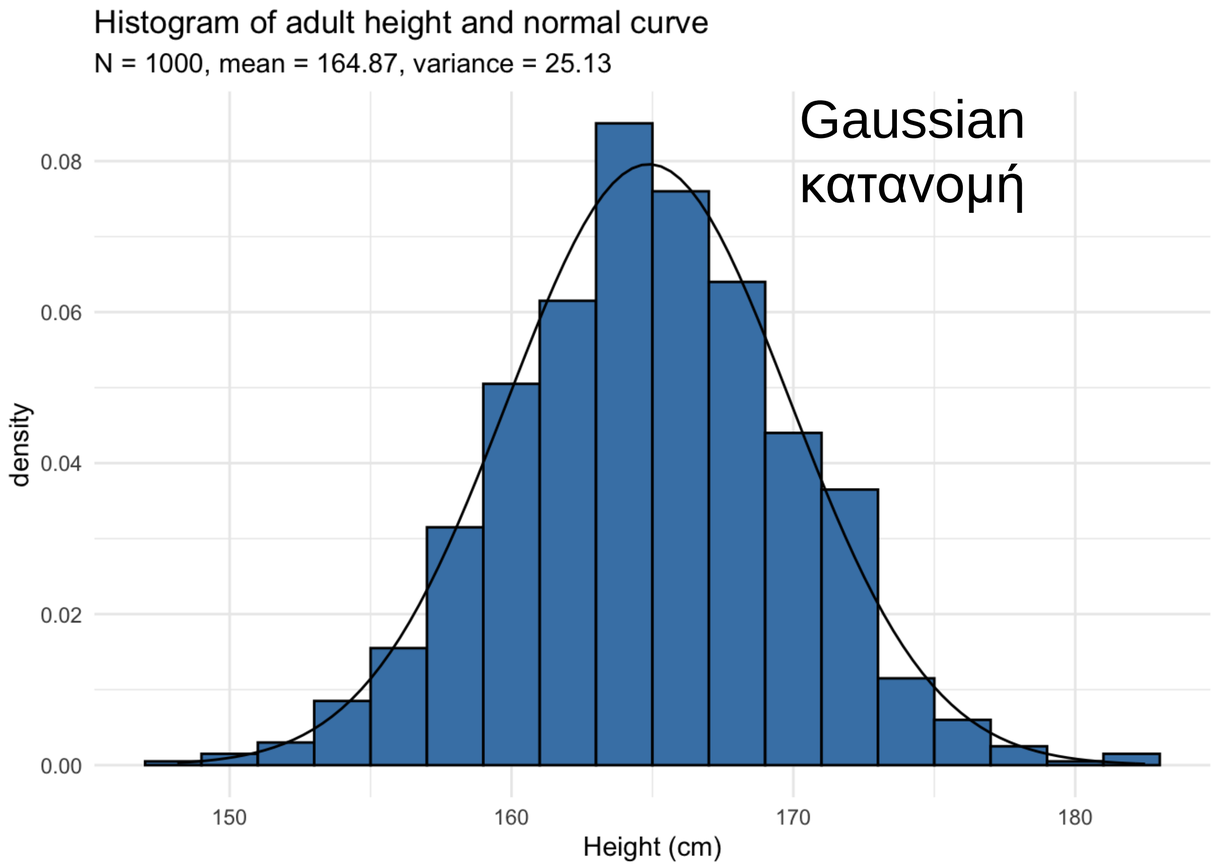
Για παράδειγμα:

Πάρτε 1000 τυχαίους ανθρώπους και μετρήστε το ύψος τους

Δημιουργήστε ένα ιστόγραμμα των δεδομένων

Τα δειγματοληπτικά σημεία ακολουθούν μια **κατανομή Gauss**

Έχει παραμέτρους: μέση και διακύμανση
- Η μέση τιμή: 164.87
- Η διακύμανση: 25.13



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Gaussian κατανομή

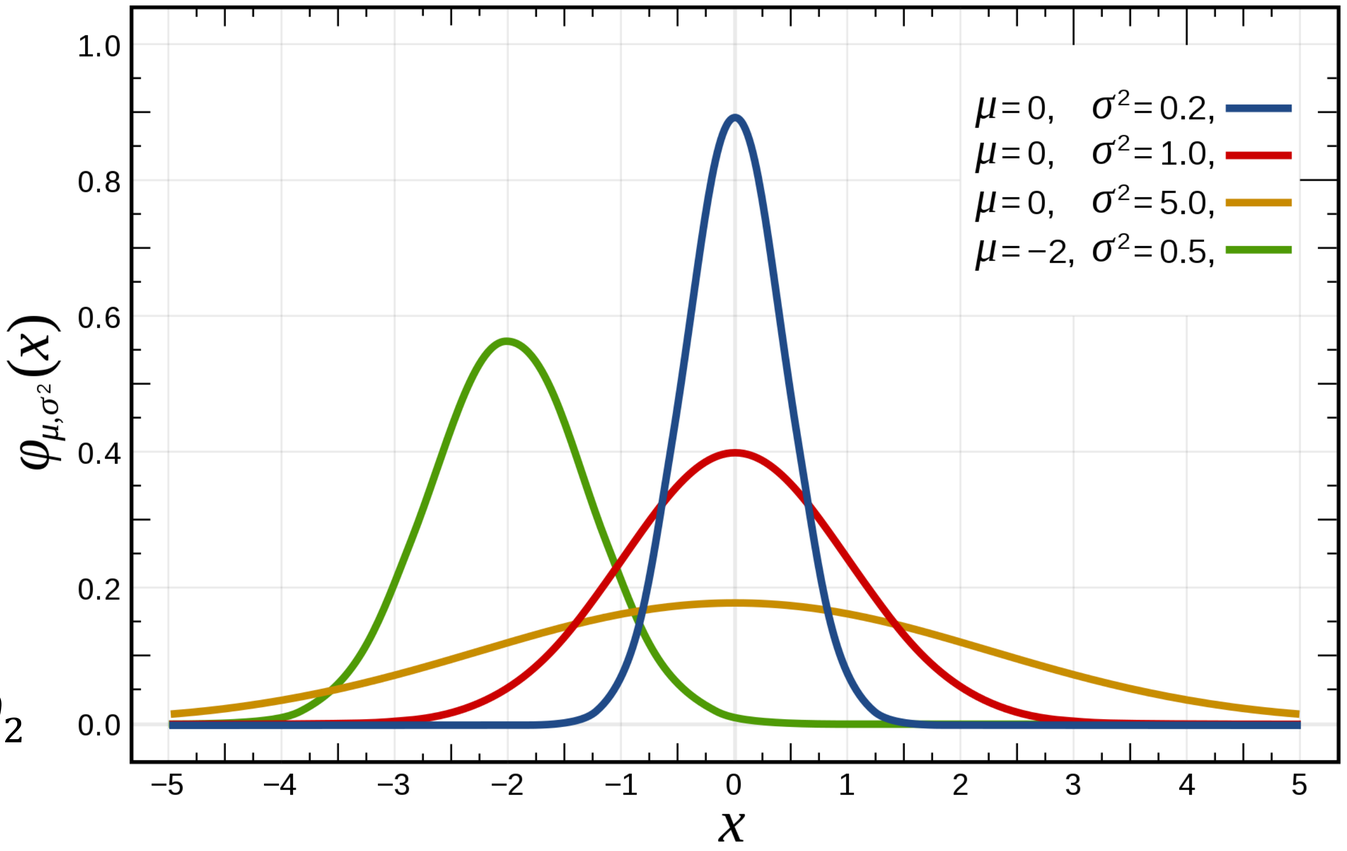
$$x \sim N(\mu, \sigma^2)$$

$$f_{\boldsymbol{\theta}}(x) \quad where \quad \boldsymbol{\theta} = (\mu, \sigma^2)$$

$$f_{\mu,\sigma^2}(x) = \frac{1}{\sigma\sqrt{2\pi}} exp\left(\frac{-(x-\mu)^2}{2\sigma^2}\right)$$

$$f_{\boldsymbol{\theta}}(x) = \frac{1}{\theta_2\sqrt{2\pi}} exp\left(\frac{-(x-\theta_1)^2}{2\theta_2^2}\right)$$

Γραμμική παλινδρόμηση: $f_{\boldsymbol{\theta}}(x) = \theta_1 x + \theta_2$



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Τοποθέτηση παραμέτρου

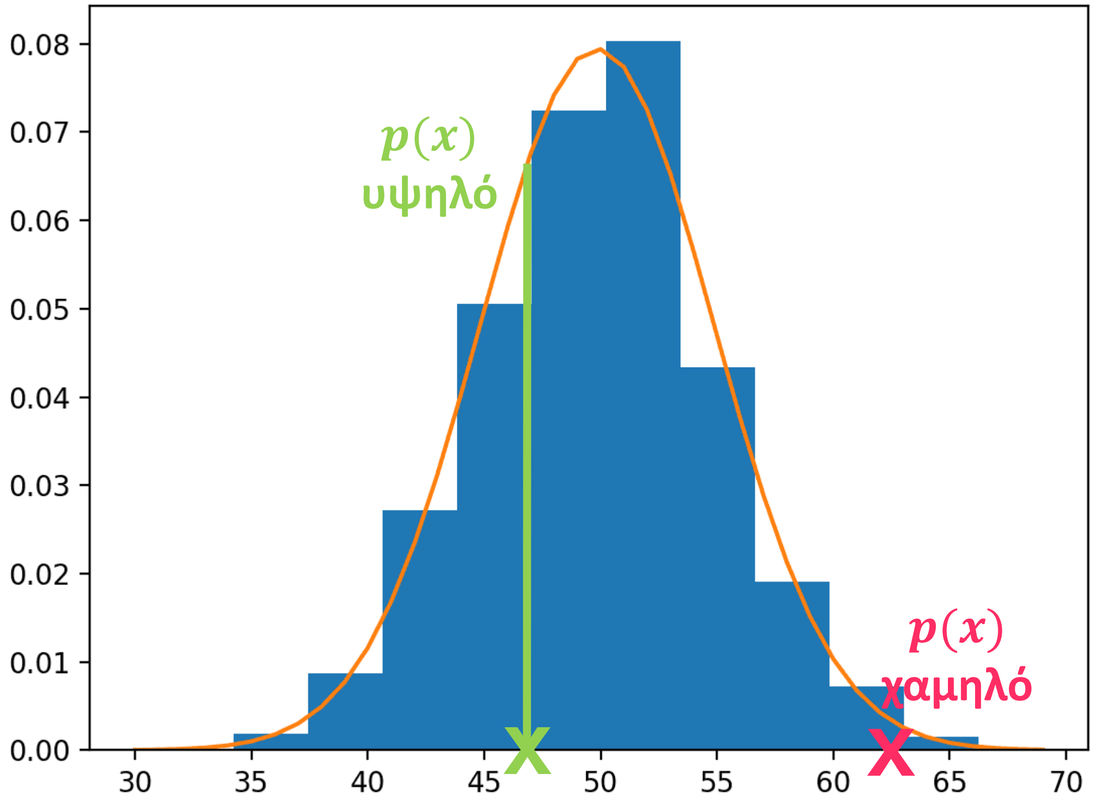
Πώς υπολογίζουμε τις παραμέτρους αυτού του μοντέλου;

Σύνολο δεδομένων: $D = \{\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(m)}\}$

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x^{(i)}$$

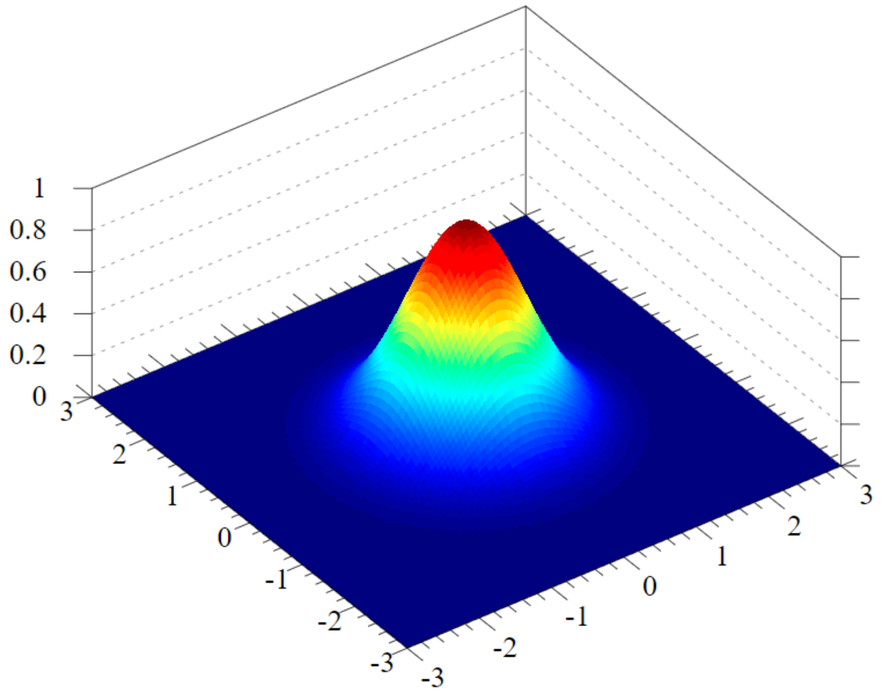
$$\sigma^2 = \frac{1}{m}\sum_{i=1}^{m} \left(x^{(i)} - \mu\right)^2$$

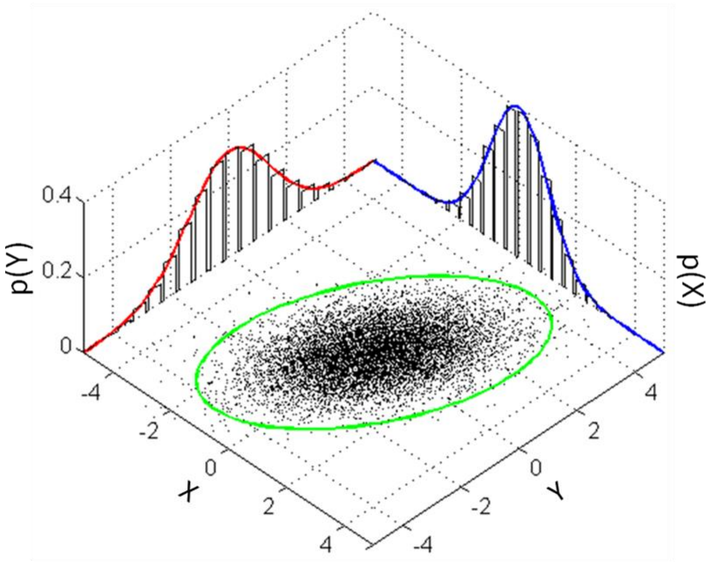
$$p(x) = f_{\mu,\sigma^2}(x) = \frac{1}{\sigma\sqrt{2\pi}} exp\left(\frac{-(x-\mu)^2}{2\sigma^2}\right)$$

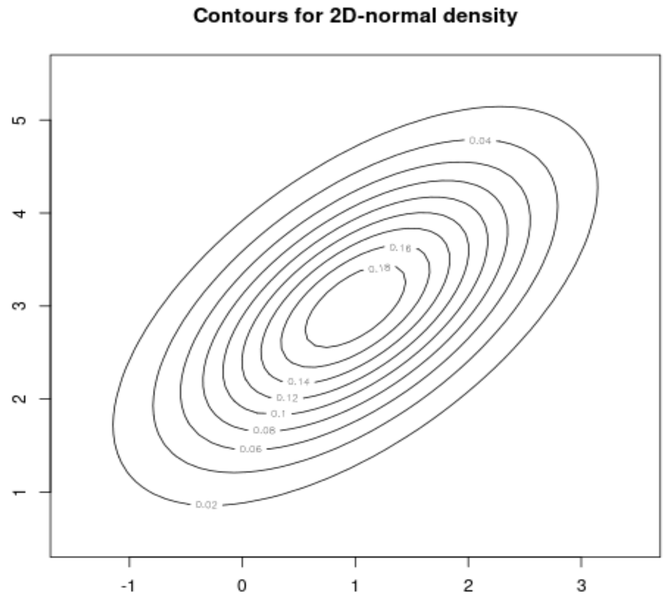


This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Πολυδιάστατες κατανομές Gaussian







This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

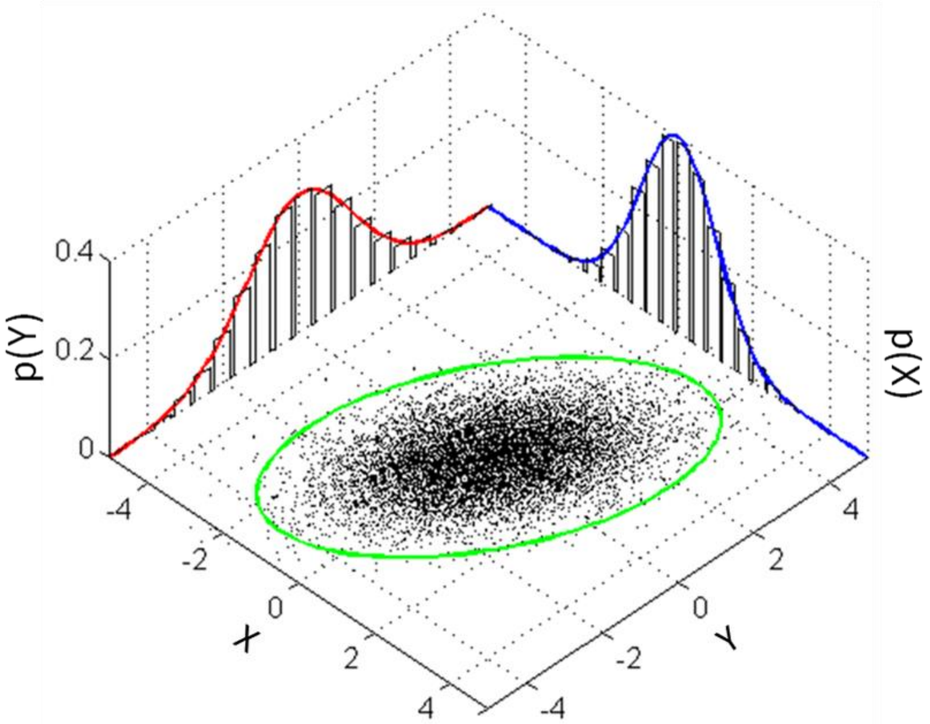
Εκτίμηση πυκνότητας σε πολυδιάστατη περίπτωση

Δεδομένα εκμάθησης: $D = \{\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(m)}\}$
Κάθε $\boldsymbol{x}^{(i)} \in \mathbb{R}^n$ (έχει n χαρακτηριστικά)

$$p(\boldsymbol{x}) = p(x_1; \mu_1, \sigma_1^2) * p(x_2; \mu_2, \sigma_2^2) * \cdots * p(x_n; \mu_n, \sigma_n^2)$$

Πολλαπλασιαζόμαστε επειδή η πιθανότητα να πάρουμε x_1 μια συγκεκριμένη αξία και να x_2 πάρουμε μια συγκεκριμένη αξία γίνεται χαμηλότερη.

$$p(\boldsymbol{x}) = \prod_{j=1}^{n} p(x_j; \mu_j, \sigma_j^2)$$



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

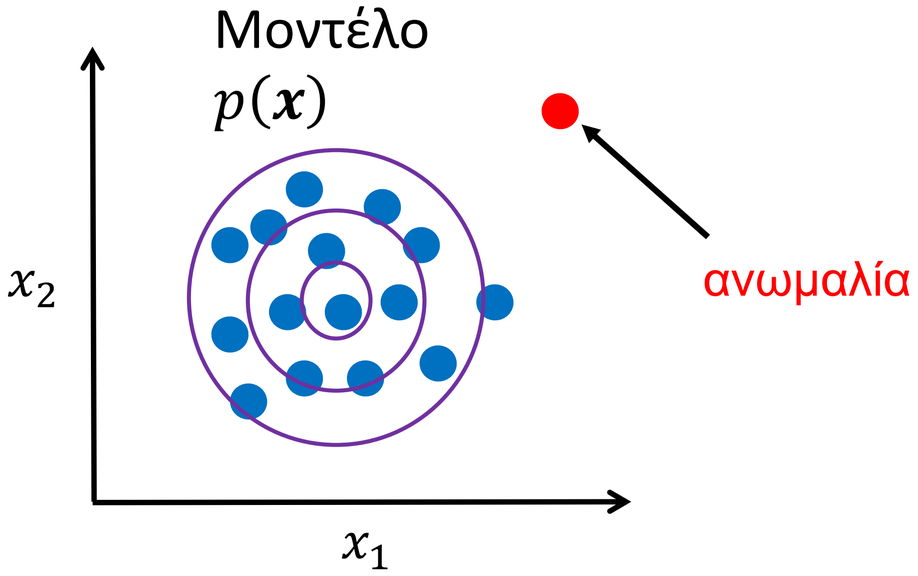
Ανίχνευση ανωμαλίας με τη χρήση εκτίμησης πυκνότητας

Σύνολο δεδομένων $D = \{\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(m)}\}$

Είναι το $\boldsymbol{x}^{(new)}$ ανωμαλία;

$p(\boldsymbol{x}^{(new)}) < \varepsilon$ ανωμαλία

$p(\boldsymbol{x}^{(new)}) \geq \varepsilon$ κανονικό



Για να μοντελοποιήσουμε θα $p(x)$ χρησιμοποιήσουμε μια διανομή Gaussian

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Αλγόριθμος ανίχνευσης ανωμαλίας

Δεδομένο σύνολο δεδομένων $D = \{\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(m)}\}$

1. Επιλέξτε n χαρακτηριστικά που μπορεί να είναι ενδεικτικά παραδείγματα ανωμαλιών

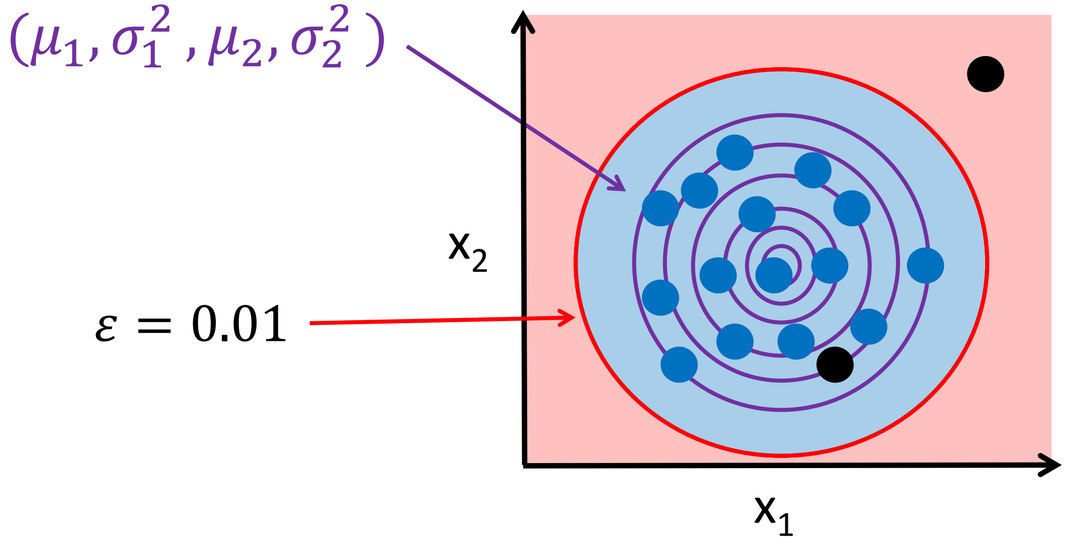
2. Κατάλληλες παράμετροι $\mu_1, \dots, \mu_n, \sigma_1^2, \dots, \sigma_n^2$

$$\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)} \quad \sigma_j^2 = \frac{1}{m}\sum_{i=1}^{m}\left(x_j^{(i)} - \mu_j\right)^2$$

3. Λαμβάνοντας υπόψη το νέο παράδειγμα $\boldsymbol{x}$, υπολογίστε $p(\boldsymbol{x})$

$$p(\boldsymbol{x}) = \prod_{j=1}^{n} p\left(x_j; \mu_j, \sigma_j^2\right) = \prod_{j=1}^{n} \frac{1}{\sigma_j \sqrt{2\pi}} exp\left(\frac{-(x_j-\mu_j)^2}{2\sigma_j^2}\right)$$

4. Εάν$p(\boldsymbol{x}) < \varepsilon$: x είναι ανωμαλία



$$p(\boldsymbol{x}) = f_{\mu_1\sigma_1^2}(x_1) f_{\mu_2\sigma_2^2}(x_2)$$

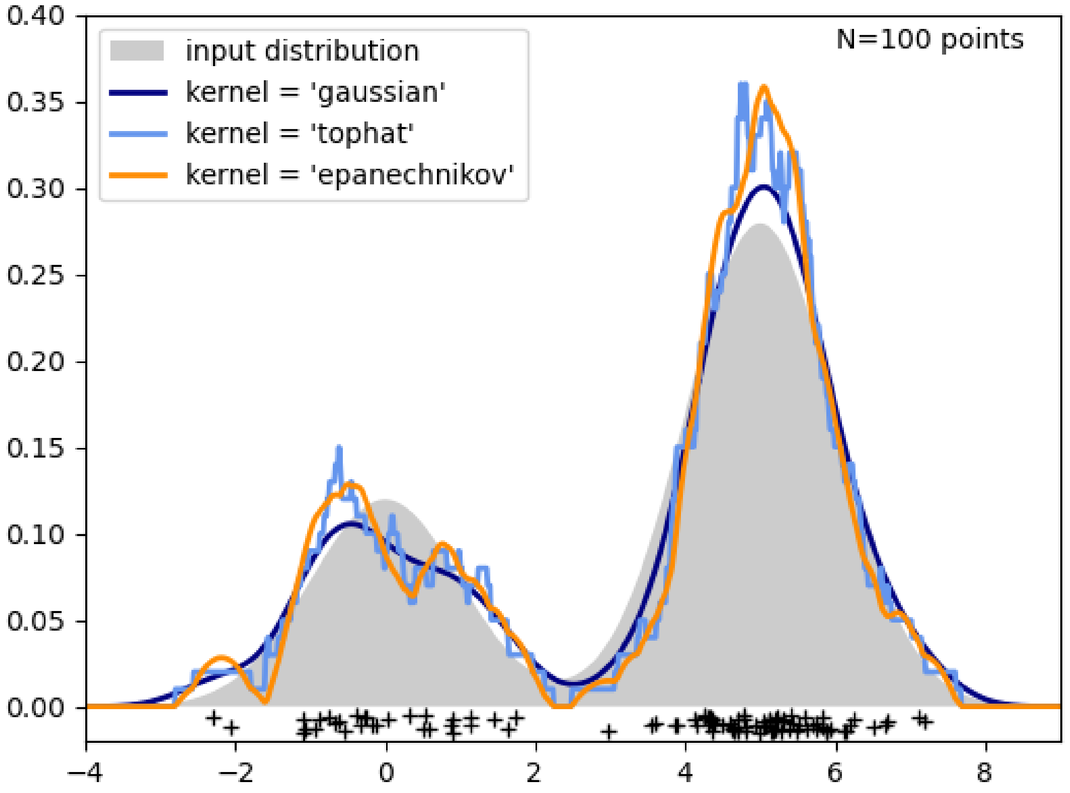
$p(\boldsymbol{x}) = 0.001 < \varepsilon$ ανωμαλία

$p(\boldsymbol{x}) = 0.041 \geq \varepsilon$ κανονικό

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Μη παραμετρική εκτίμηση πυκνότητας

- Τι γίνεται αν τα δεδομένα δεν είναι Gaussian κατανεμημένα;
- 100 βαθμοί που προέρχονται από διτροπική κατανομή
- Η παραμετρική εκτίμηση πυκνότητας δεν θα εκτιμήσει την κατανομή των δεδομένων καλά
  - Ο Gaussian θα βρίσκεται στη μέση των σημείων
- Χρησιμοποιήστε **την εκτίμηση πυκνότητας πυρήνα**



Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

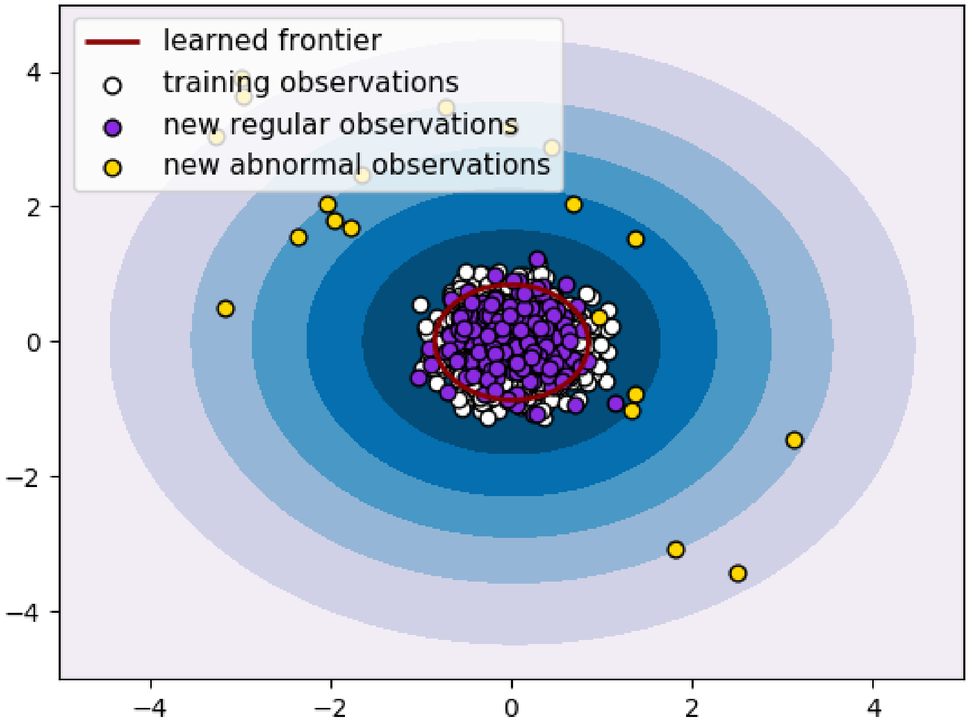
Ταξινόμηση μιας κατηγορίας

- Κοινή προσέγγιση για την ανίχνευση ανωμαλιών
- Αντί να υπολογίσουμε την πυκνότητα,ορίζουμε ένα **μοντέλο** διάκρισης για να μάθουμε ένα συντηρητικό όριο απόφασης που περιλαμβάνει τα φυσιολογικά σημεία (σημεία της θετικής τάξης)
- Τυπικές επιλογές:
  - One-class SVM
  - Isolation forests

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

One-class SVM

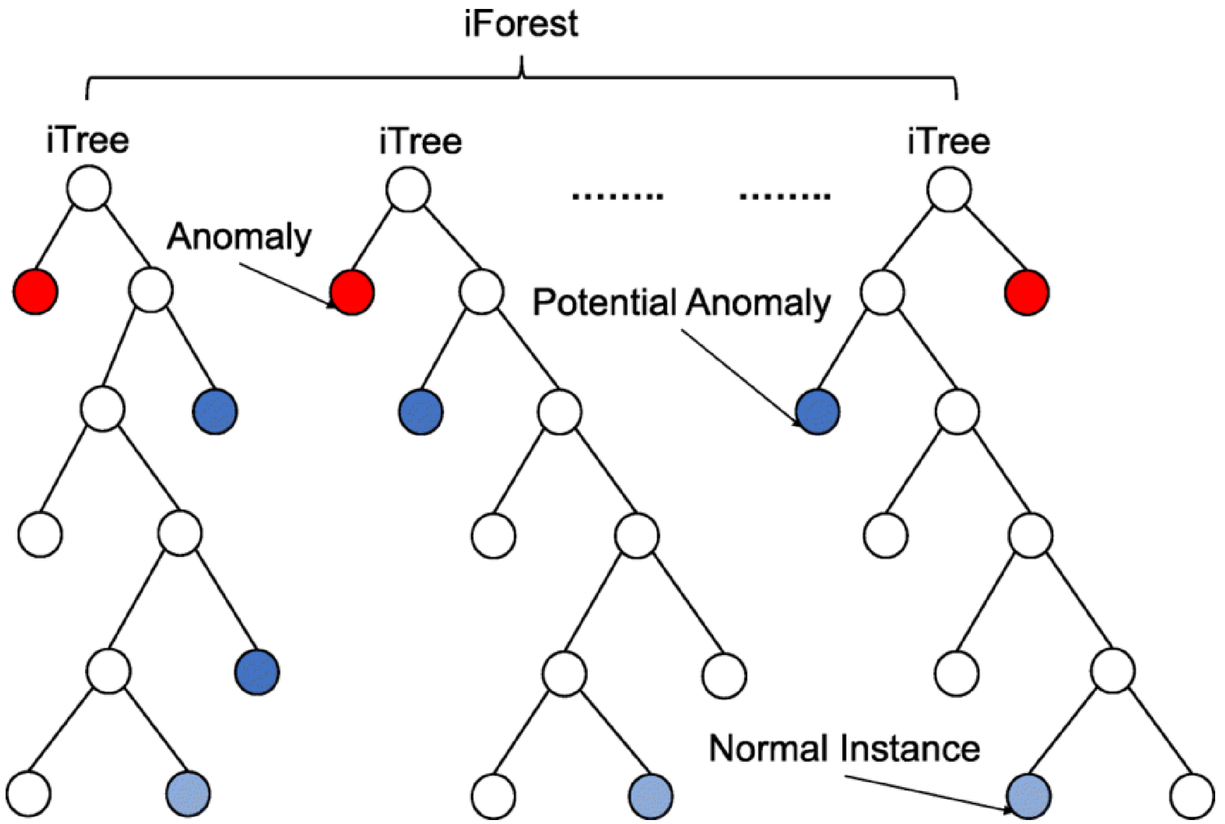
- Προσπαθήστε να περιλάβετε όλες τις περιπτώσεις της κανονικής τάξης χρησιμοποιώντας ένα **hypersphere**
- Δημιουργήστε το μικρότερο δυνατό hypersphere
- Τα πάντα έξω από την υπερσφαίρα θεωρούνται ανωμαλία



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

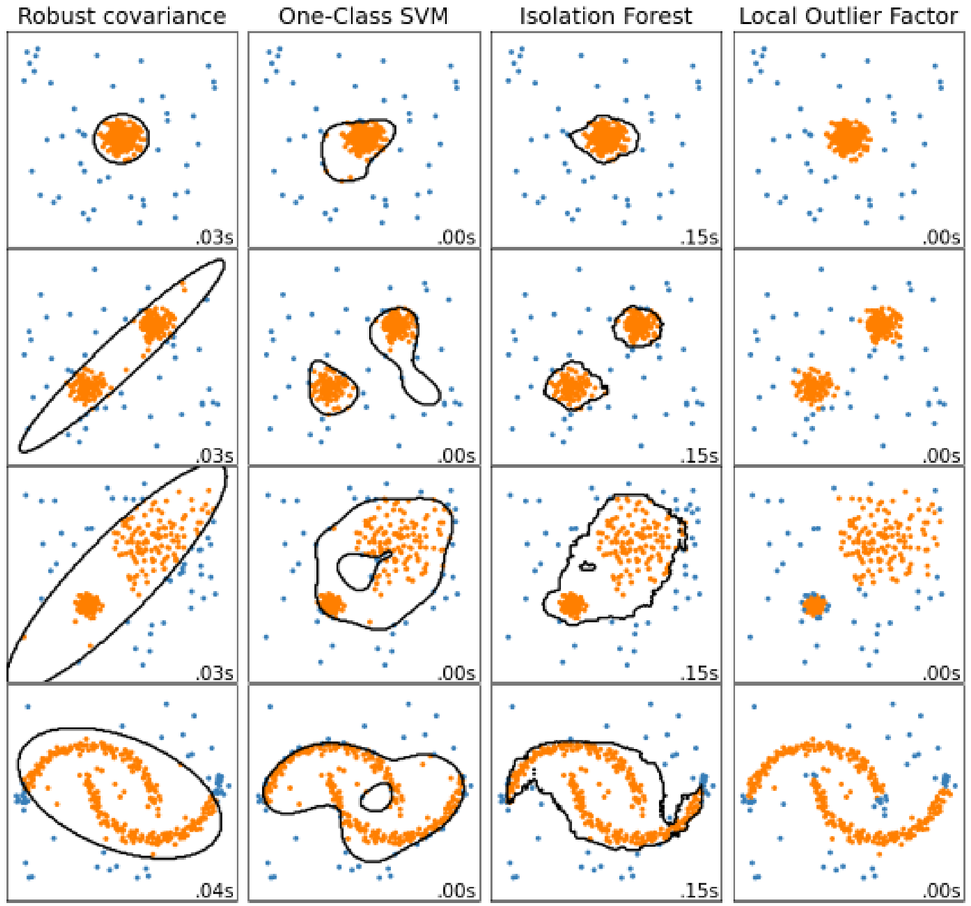
Isolation forests

- Όπως τα τυχαία δάση
- Ανωμαλίες = παρατηρήσεις με σύντομα μέσα μήκη διαδρομής
- Οι ακραίες τιμές/οι ανωμαλίες είναι πιο εύκολο να απομονωθούν (σύντομα μήκη διαδρομής)
- Inliers/Κανονικές περιπτώσεις είναι πιο δύσκολο να απομονωθούν (μακρύτερα μήκη διαδρομής)



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

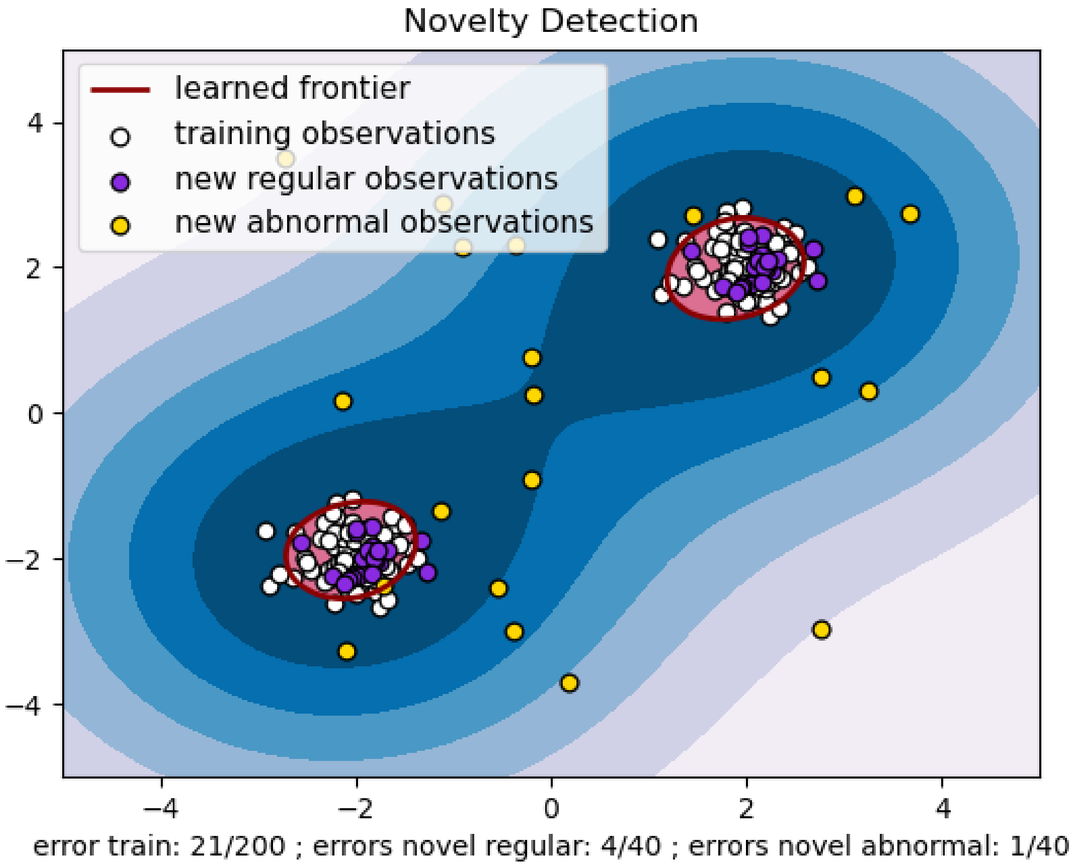
Outlier detection στο scikit-learn

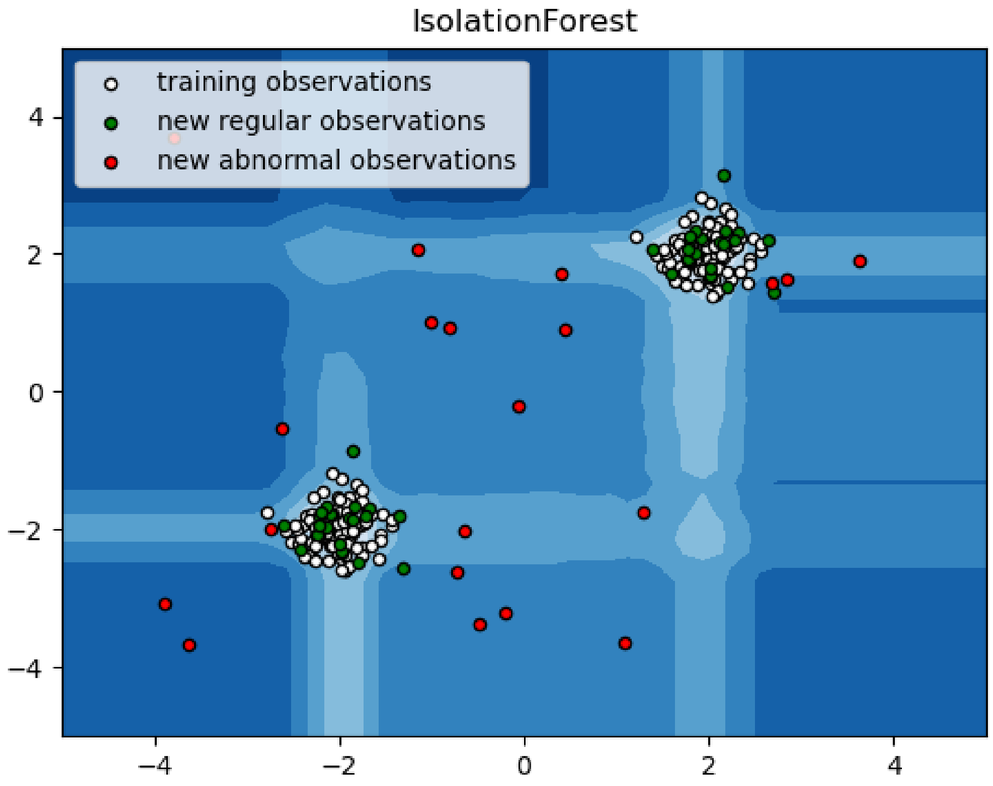


Τυπικά πρέπει να ορίσετε κάποια εξωτερική παράμετρο κλάσματος

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Novelty detection στο scikit-learn

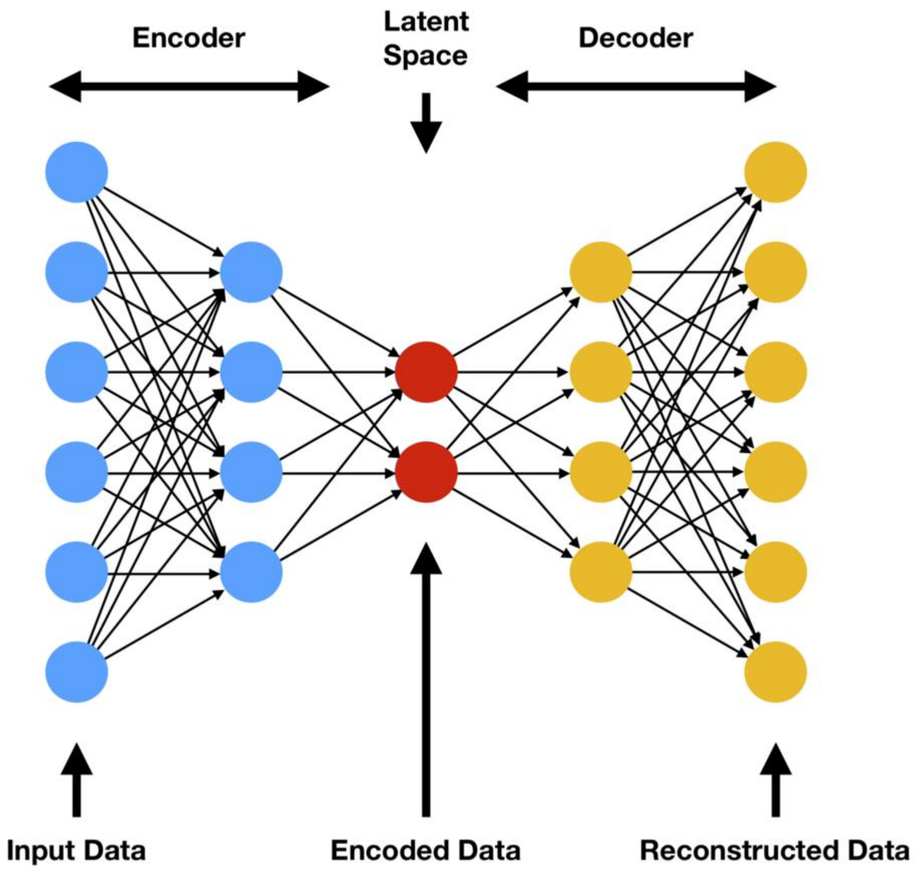




Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action
No 2020-EU-IA-0087, co-financed by the EU CEF Telecom
under GA nr. INEA/CEF/ICT/A2020/2267423

Anomaly Detection με χρήση Autoencoders



- Οι αυτόματοι κωδικοποιητές παρέχουν έναν τρόπο εύρεσης κανονικότητας στα δεδομένα, συμπιέζοντας την είσοδο και ανακατασκευάζοντας την.
- Είναι εκπαιδευμένοι να ελαχιστοποιούν το σφάλμα ανακατασκευής για ένα δεδομένο σύνολο δεδομένων.
- Βασική ιδέα πίσω από τη χρήση ενός αυτόματου κωδικοποιητή για την ανίχνευση ανωμαλιών: τα κανονικά δεδομένα θα έχουν χαμηλό σφάλμα ανακατασκευής, ενώ **τα ανώμαλα δεδομένα θα έχουν υψηλότερο σφάλμα ανακατασκευής**.

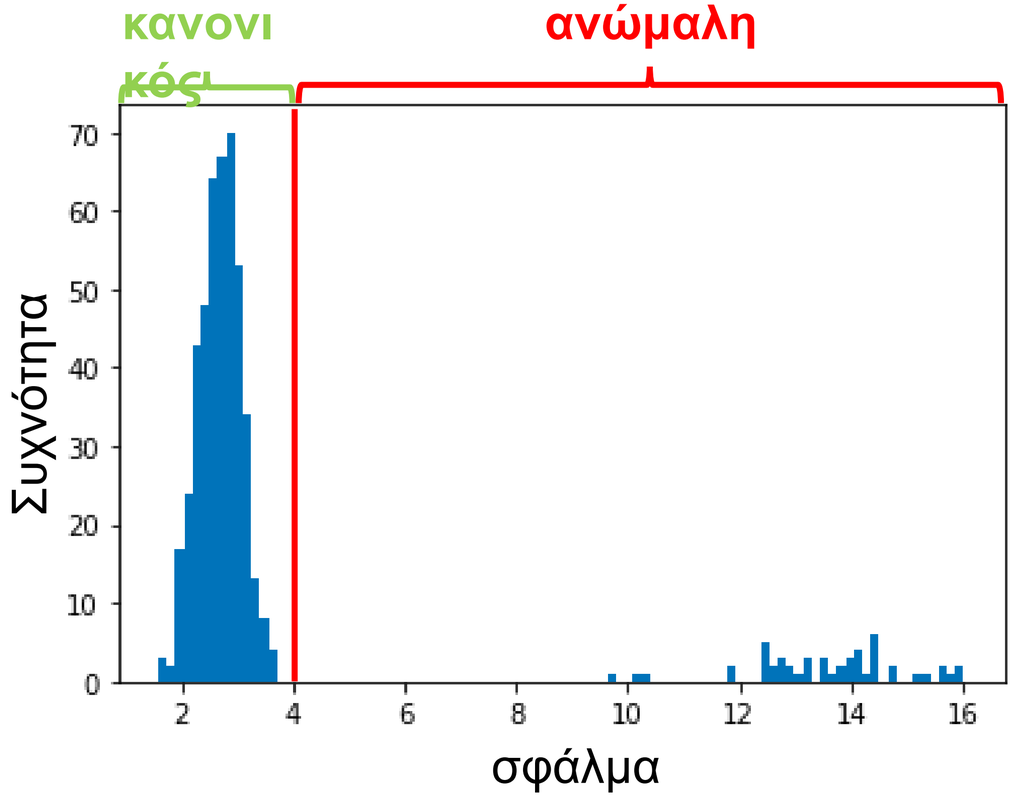
Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Anomaly Detection με χρήση Autoencoders

Διαδικασία:

- Δεδομένου ενός συνόλου δεδομένων $D = \{\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(m)}\}$
- Εκπαιδεύστε έναν Autoencoder για να κωδικοποιήσετε και να ανακατασκευάσετε κάθε διάνυσμα εισόδου $\boldsymbol{x}^{(i)}$
- Μετά την εκπαίδευση, χρησιμοποιήστε ένα ιστόγραμμα για να απεικονίσετε τη συχνότητα των σφαλμάτων
- Καθορισμός του κατώτατου ορίου απόφασης βάσει του ιστογράμματος (π.χ., 4)
- Μελλοντικά δεδομένα που έχουν σφάλμα ανακατασκευής:
  - μικρότερα από το όριο ταξινομούνται ως **κανονικά**
  - μεγαλύτερα από το όριο ταξινομούνται ως **μη φυσιολογικά**



This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Παράδειγμα anomaly detection

Εντοπισμός απάτης στις συναλλαγές: Ένας απατεώνας συνήθως θα προσπαθήσει να κάνει κατάχρηση της κάρτας όσο το δυνατόν περισσότερο σε σύντομο χρονικό διάστημα πριν από τον εντοπισμό και την αναστολή της κάρτας.

Merchant id	Merchant category code	Merchant city	Time	Transaction method	Transaction type	Amount
K2203	BC	LIMASSOL	9:02	Magnetic	Retail	100.10
L3425	GD	NICOSIA	9:10	Magnetic	Retail	40.10
F3928	VS	NICOSIA	10:20	Chip	Retail	5.10
W9843	TY	PAPHOS	13:20	Magnetic	Internet	200.00

Σημασία της μηχανικής χαρακτηριστικών:

travel_speed = distance between cities / time difference between two adjacent transactions
travel_speed = 85 km / 8 min = 10.625 km/min = 637.5 km/h !!

Προσαρμόστηκε από εδώ

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Αξιολόγηση ενός συστήματος ανίχνευσης ανωμαλιών

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Αξιολόγηση ενός συστήματος ανίχνευσης ανωμαλιών

- Κατά την ανάπτυξη ενός συστήματος ανίχνευσης ανωμαλίας (π.χ. χαρακτηριστικά, μοντέλα, αλγόριθμοι) το να έχει έναν τρόπο να αξιολογήσει την απόδοσή του θα κάνει τις αποφάσεις πολύ ευκολότερες.
- Ας υποθέσουμε ότι έχουμε μια μικρή ποσότητα δεδομένων με ετικέτα
  - Y=1: ανώμαλη
  - Y=0: κανονική
- Το σύνολο εκπαίδευσης θα πρέπει να έχει μόνο κανονική (μη ανώμαλη· Y=0) δεδομένα: $\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}, \dots, \boldsymbol{x}^{(m)}$
- Η διασταυρούμενη επικύρωση και τα σύνολα δοκιμών θα πρέπει να περιέχουν δεδομένα με επισήμανση:
  - $\left(x_{cv}^{(1)}, y_{cv}^{(1)}\right), \dots, \left(x_{cv}^{(m_{cv})}, y_{cv}^{(m_{cv})}\right)$ $\left(x_{test}^{(1)}, y_{test}^{(1)}\right), \dots, \left(x_{test}^{(m_{test})}, y_{test}^{(m_{test})}\right)$
  - Συνήθως κανονικά παραδείγματα (y=0)
  - Μερικά ανώμαλα παραδείγματα (y=1)

Slides based on Andrew Ng's Machine Learning course - Coursera

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Παράδειγμα παρακολούθησης κινητήρα

10000 Καλοί (κανονικοί) κινητήρες
20 Ελαττωματικοί (ανώμαλοι) κινητήρες

Ακόμα μη εποπτευόμενη μάθηση επειδή το σύνολο εκμάθησης περιέχει μη επισημασμένα παραδείγματα

Δεδομένα εκμάθησης: 6000 καλοί κινητήρες
CV: 2000 καλοί κινητήρες (y=0) 10 ανώμαλοι (y=1) → συντονισμός υπερπαραμέτρων
Δοκιμή: 2000 καλοί κινητήρες (y=0) 10 ανώμαλοι (y=1) → αξιολόγηση

Η εναλλακτική λύση: Κανένα σύνολο δοκιμής → Χρησιμοποιήστε μόνο εάν πολύ λίγα επισημασμένα ανώμαλα παραδείγματα

Δεδομένα εκμάθησης: 6000 καλοί κινητήρες
CV: 4000 καλοί κινητήρες (y=0) 20 ανώμαλοι (y=1) → συντονιστείτε υπερπαράμετροι, αλλά υψηλότερο κίνδυνο υπερπροσαρμογής

Διαφάνειες βασισμένες στο μάθημα Machine Learning του Andrew Ng — Coursera

Co-financed by the European Union Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

Αξιολόγηση του συστήματος ανίχνευσης ανωμαλιών

- Μοντέλο προσαρμογής (π.χ.,$p(\boldsymbol{x})$) σε σύνολο εκπαίδευσης $\boldsymbol{x}^{(1)}, \boldsymbol{x}^{(2)}, \ldots, \boldsymbol{x}^{(m)}$

- Σε ένα παράδειγμα διασταυρούμενης επικύρωσης/δοκιμής$\boldsymbol{x}$, πρόβλεψη
  - y=1 σε περίπτωση ανωμαλίας (π.χ., εάν $p(\boldsymbol{x}) < \varepsilon$)
  - y=0 εάν είναι φυσιολογικό (π.χ., εάν $p(\boldsymbol{x}) \leq \varepsilon$)

- Όπως η δυαδική ταξινόμηση, έτσι και οι πιθανές μετρήσεις αξιολόγησης:
  - Αληθώς θετικά, ψευδώς θετικά, ψευδώς αρνητικά, αναλογία αληθώς αρνητικών
  - Ακρίβεια/ανάκληση
  - F1-score
  - Βαθμολογία AUC

- Χρήση cross validation για τον συντονισμό των υπερπαραμέτρων

Διαφάνειες βασισμένες στο μάθημα Machine Learning του Andrew Ng — Coursera

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423

MAI4CAREU

Master programmes in Artificial Intelligence 4 Careers in Europe

Σας ευχαριστούμε

Co-financed by the European Union
Connecting Europe Facility

This Master is run under the context of Action No 2020-EU-IA-0087, co-financed by the EU CEF Telecom under GA nr. INEA/CEF/ICT/A2020/2267423