

Podstawy uczenia maszynowego

Część 1

Dr Mateusz Radzimski

Czego się nauczyszmy?

- Kilku podstawowych algorytmów ML
- Sposób przygotowania danych, trenowania, ewaluacji uczenia maszynowego
- Poznamy trochę teorii i intuicji. Niektóre detale techniczne pominiemy.
- Poznamy jak zaimplementować takie modele w Pythonie przy użyciu bibliotek:
 - Pandas, numpy, sci-kit learn, matplotlib
 - Poznamy również kilka „klasycznych” zbiorów danych

Uczenie maszynowe (ang. machine learning, ML)

- Dziedzina Sztucznej Inteligencji (AI)
- Wykorzystanie metod statystycznych, algorytmów, sieci neuronowych itd.
- Zdolność uczenia się, ale bez konieczności posiadania bezpośrednich instrukcji
- Uczenie się na podstawie danych wejściowych: poprzez odnajdywanie wzorców lub generalizację przypadków

ML i inne *buzzwords*

Sztuczna Inteligencja (AI) - cena maszyn polegająca na postrzeganiu, syntezie, wnioskowaniu (np. rozpoznawanie obrazów, rozpoznawanie i rozumienie języka mówionego, synteza mowy, itd.)

Data Science / Data Scientist - dziedzina wykorzystująca metody statystyczne, uczenie maszynowe, eksplorację i analizę danych, techniki wizualizacji w celu zrozumienia danych dla potrzeb biznesowych. Data Scientist to osoba wykonująca pracę w tej dziedzinie, tworząca modele ML.

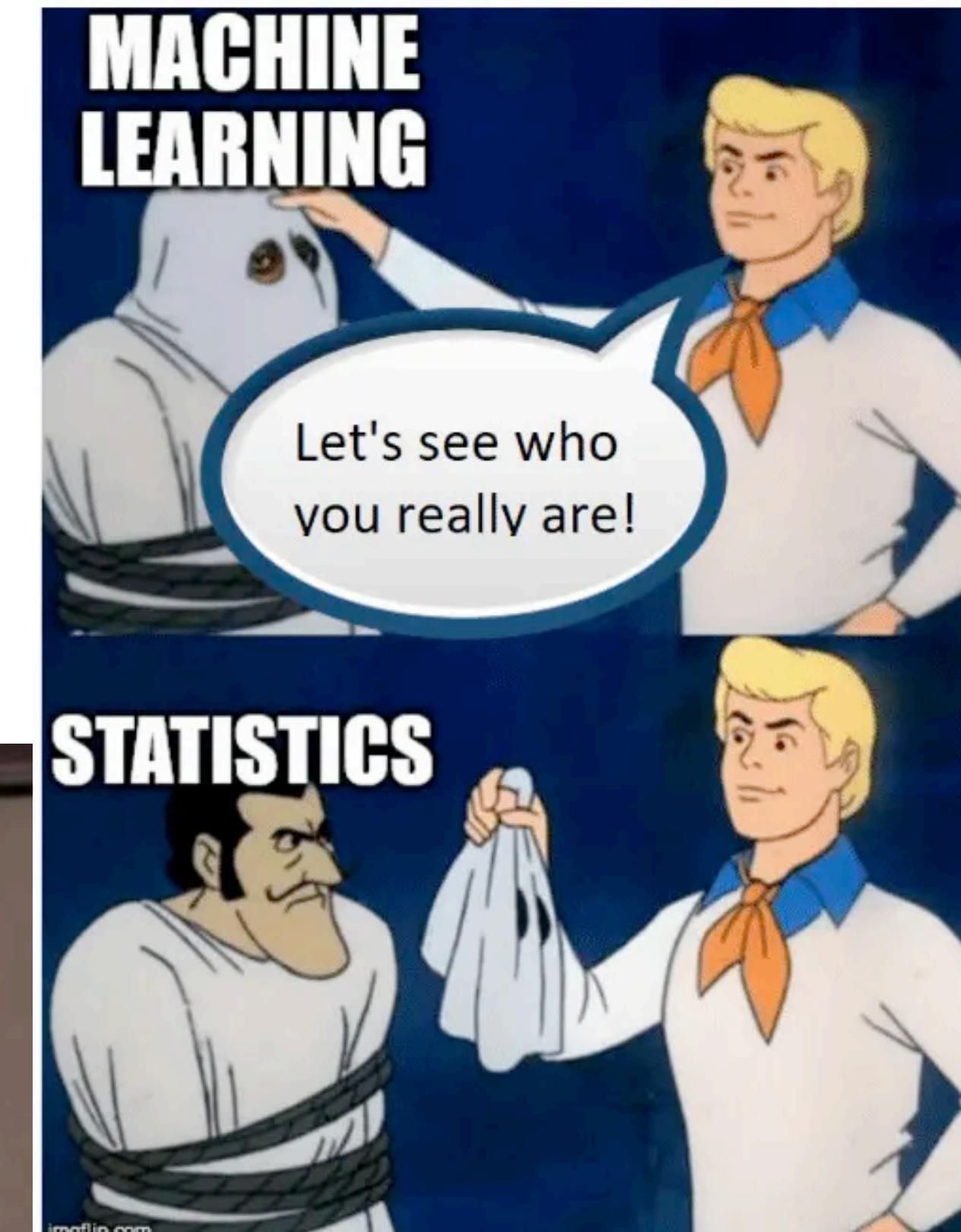
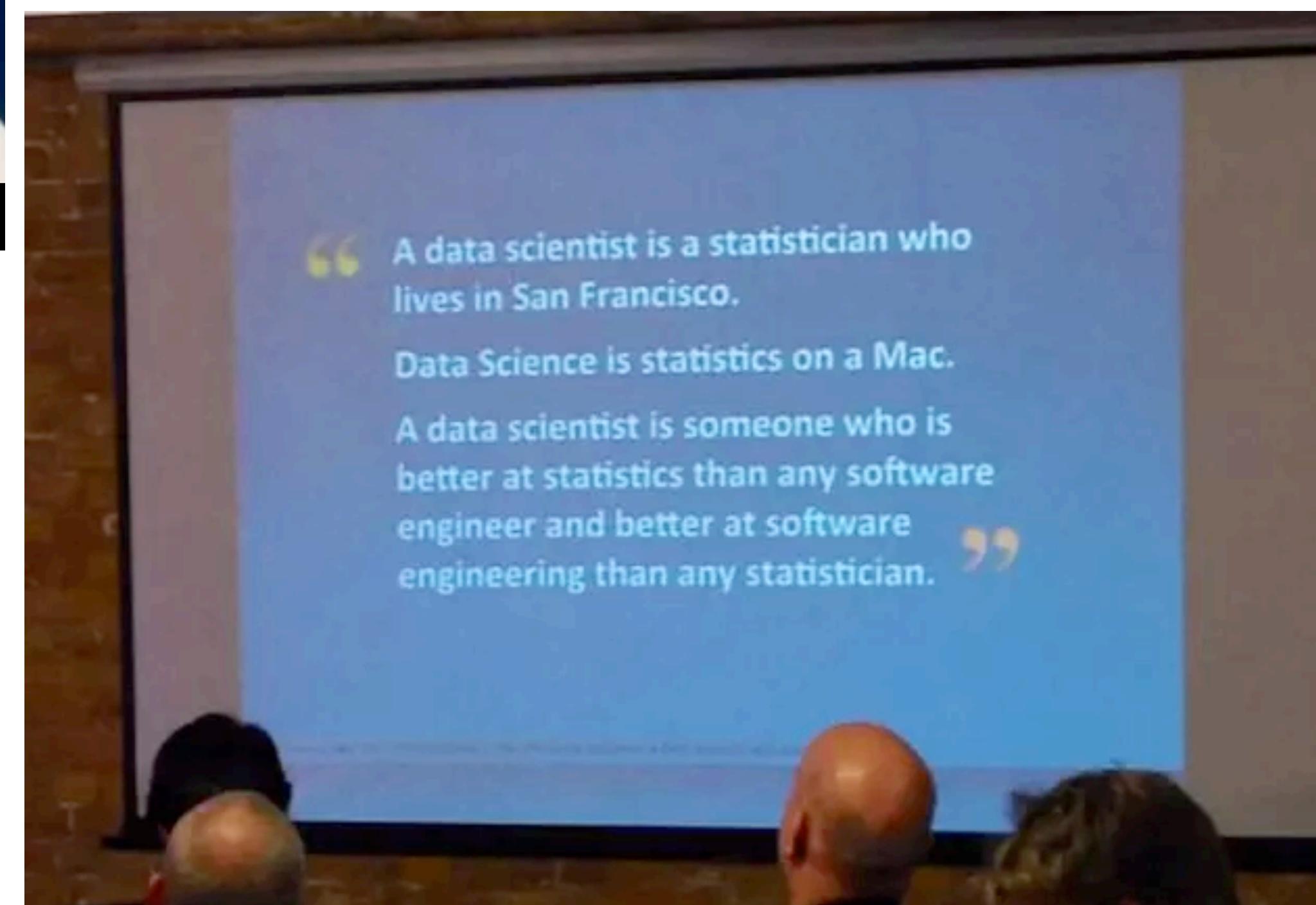
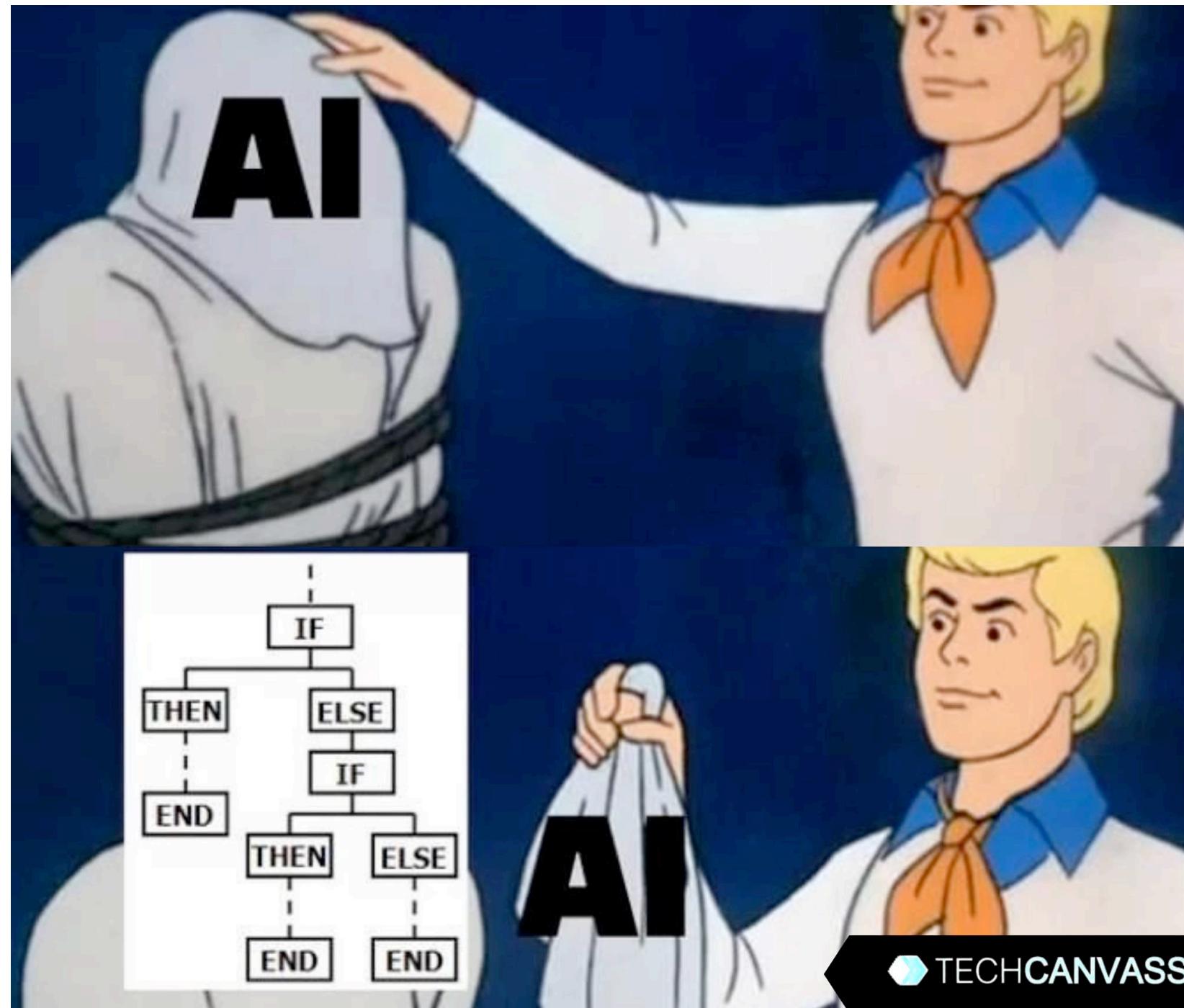
Machine Learning - uczenie maszynowe (patrz poprzedni slajd)

Deep Learning - uczenie maszynowe wykorzystujące tzw. głębokie sieci neuronowe (architektury sieci neuronowych wykorzystujące więcej niż jedną warstwę ukrytą, np. RNN, CNN, GAN, Transformer, GNN, itd.)

Machine Learning Engineer - osoba potrafiąca wykorzystać model uczenia maszynowego (stworzonego przez Data Scientista) w procesie biznesowym. Inżynier posiadający doświadczenie zarówno w dziedzinie inżynierii oprogramowania jak również w dziedzinie uczenia maszynowego

MLOps - zbiór praktyk i technologii związanych z wdrażaniem i utrzymaniem modeli uczenia maszynowego w środowiskach produkcyjnych

ML i inne *buzzwordy*



Dlaczego warto?

W ostatnich latach jesteśmy świadkami wielu przełomów z wykorzystaniem technologii uczenia maszynowego

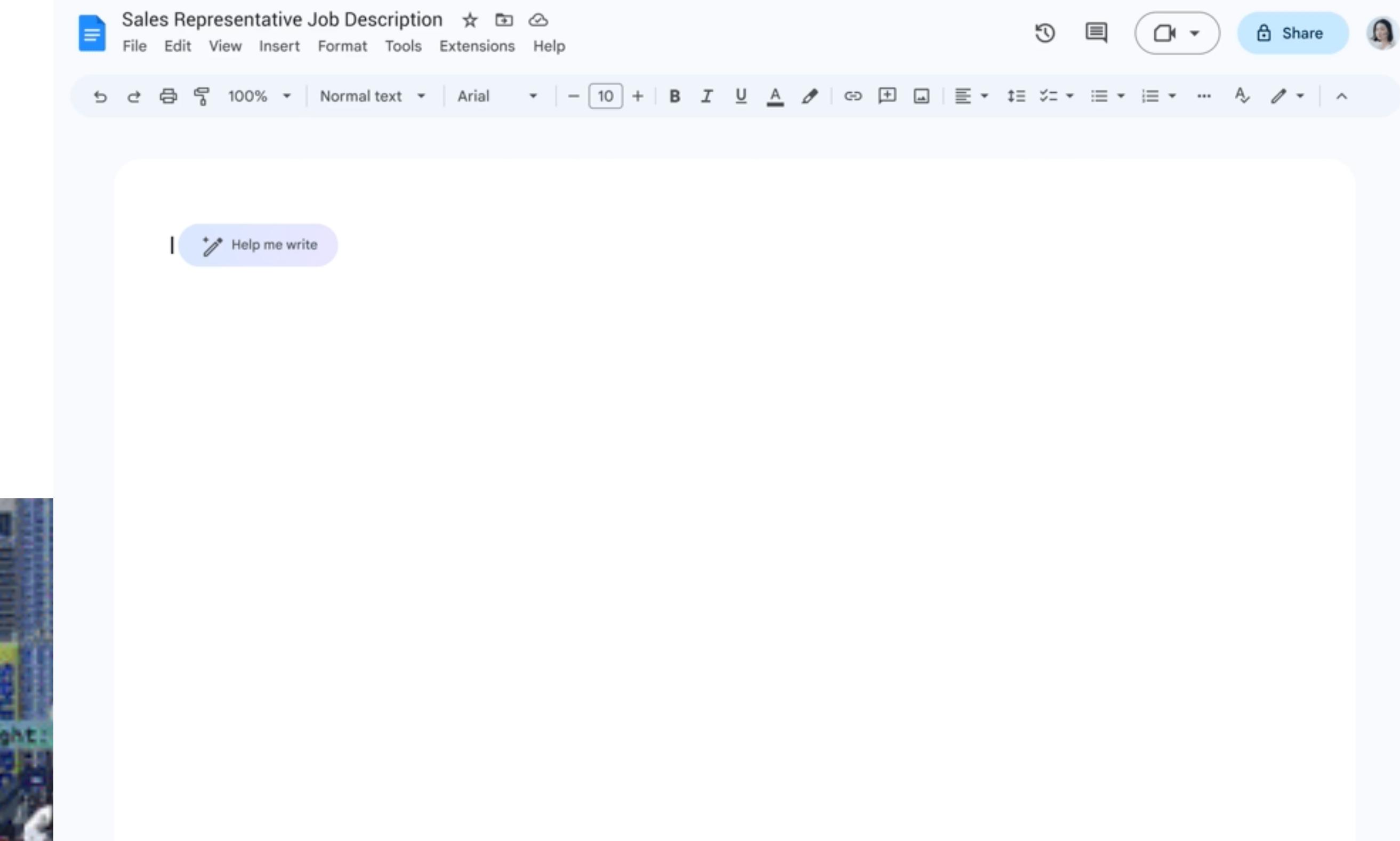
- Lepsze systemy rozpoznawania mowy (głębokie sieci neuronowe) —> rozwój wirtualnych asystentów, lepsze komendy głosowe w smartfonach
- Rozpoznawanie obrazów w czasie rzeczywistym —> Prototypy autonomicznych samochodów
- Algorytmy generatywne, „AI art”: DALL·E, Midjourney, Stable Diffusion
- LLM (duże modele językowe, ang. Large Language Models) —> chatbots, such as: ChatGPT, LLaMa, BingChat
- I wiele innych

Midjourney

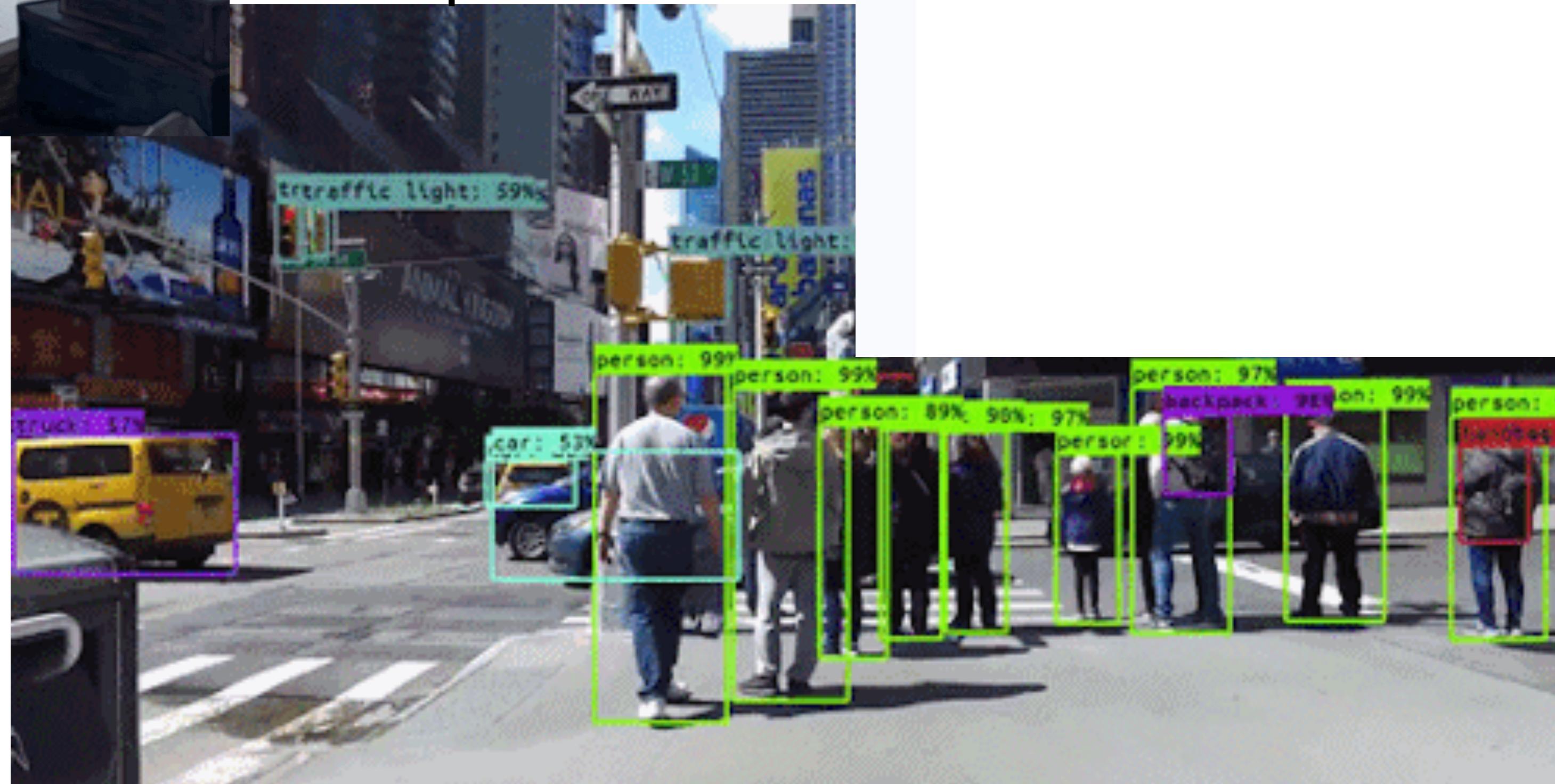
Prompt: Thanos a businessman



Dlaczego warto?



YOLO + OpenCV



Uczenie maszynowe - rodzaje

- Uczenie nadzorowane (supervised learning)
- Uczenie nienadzorowane (unsupervised learning)
- Uczenie przez wzmacnianie (reinforcement learning)

W praktyce, rodzaje te stosujemy w zależności od problemu.

Istnieje jeszcze kilka innych rodzajów, które są pochodnymi powyższych, np. semi-supervised learning.

Uczenie nadzorowane (supervised)

Cechy:

- Posiadamy zbiór uczący (training data), który zawiera dane wejściowe wraz z pożądaną odpowiedzią / etykietą (labels; labeled data).
- Celem jest przewidywanie odpowiedzi na podstawie nowych danych wejściowych.

Rezultatem uczenia jest „model”, który dokonuje predykcji (prediction, inference).
Predykcją może być np.:

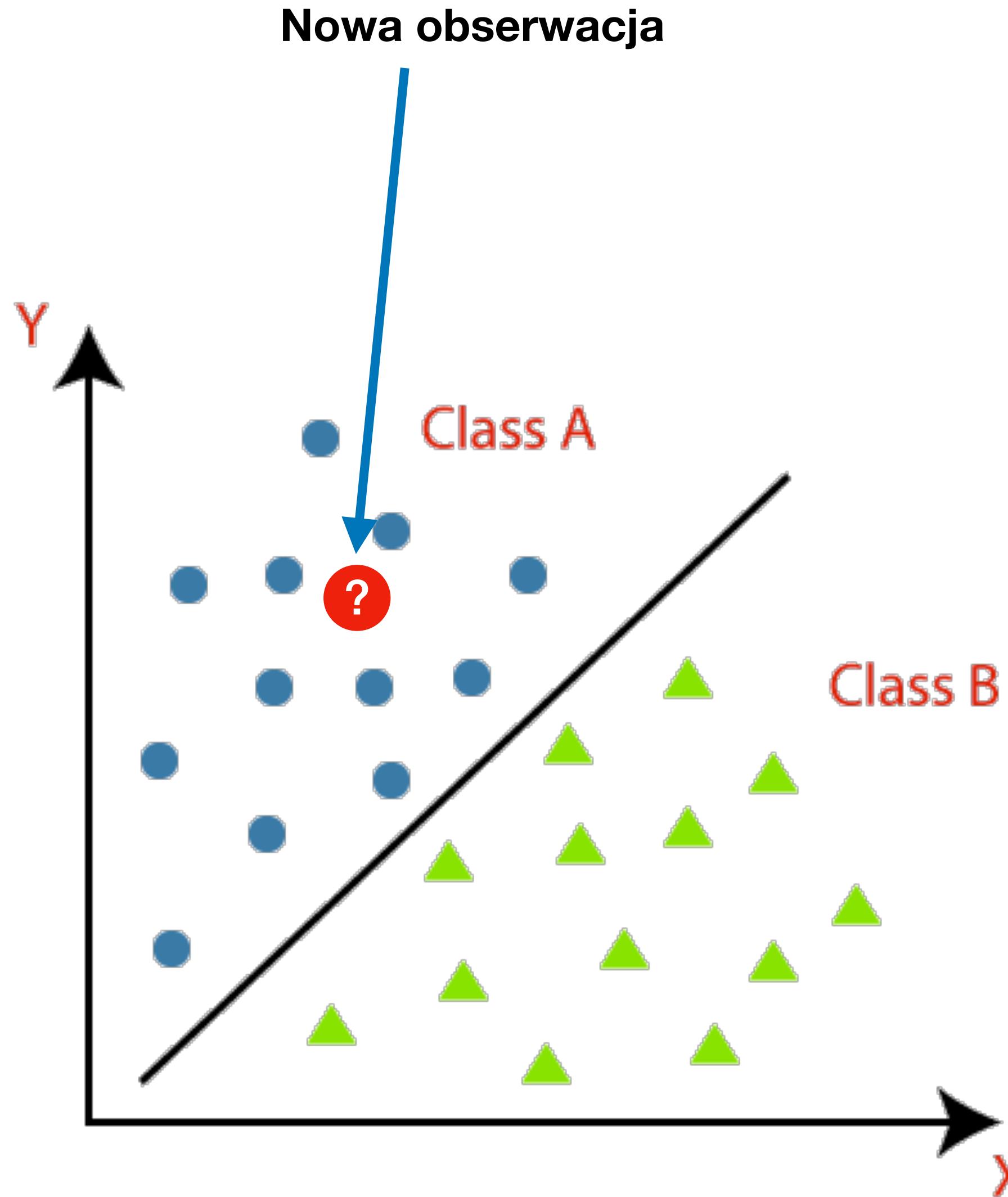
- Klasyfikacja: zaklasyfikowanie nowej obserwacji do jednej z kategorii dyskretnych (classification task)
- Regresja: uzyskanie wartości liczbowej (ciągłej) (regression)

Uczenie nadzorowane - przykłady klasyfikacji

- Klasyfikacja sentymenu - określenie czy dany tekst ma wydźwięk pozytywny lub negatywny
- Filtr spamu - klasyfikacja email do jednej z dwóch grup: spam, nie-spam
- Rozpoznawanie cyfr: klasyfikacja do jednej z 10 grup (0...10)



Uczenie nadzorowane - ilustracja klasyfikacji

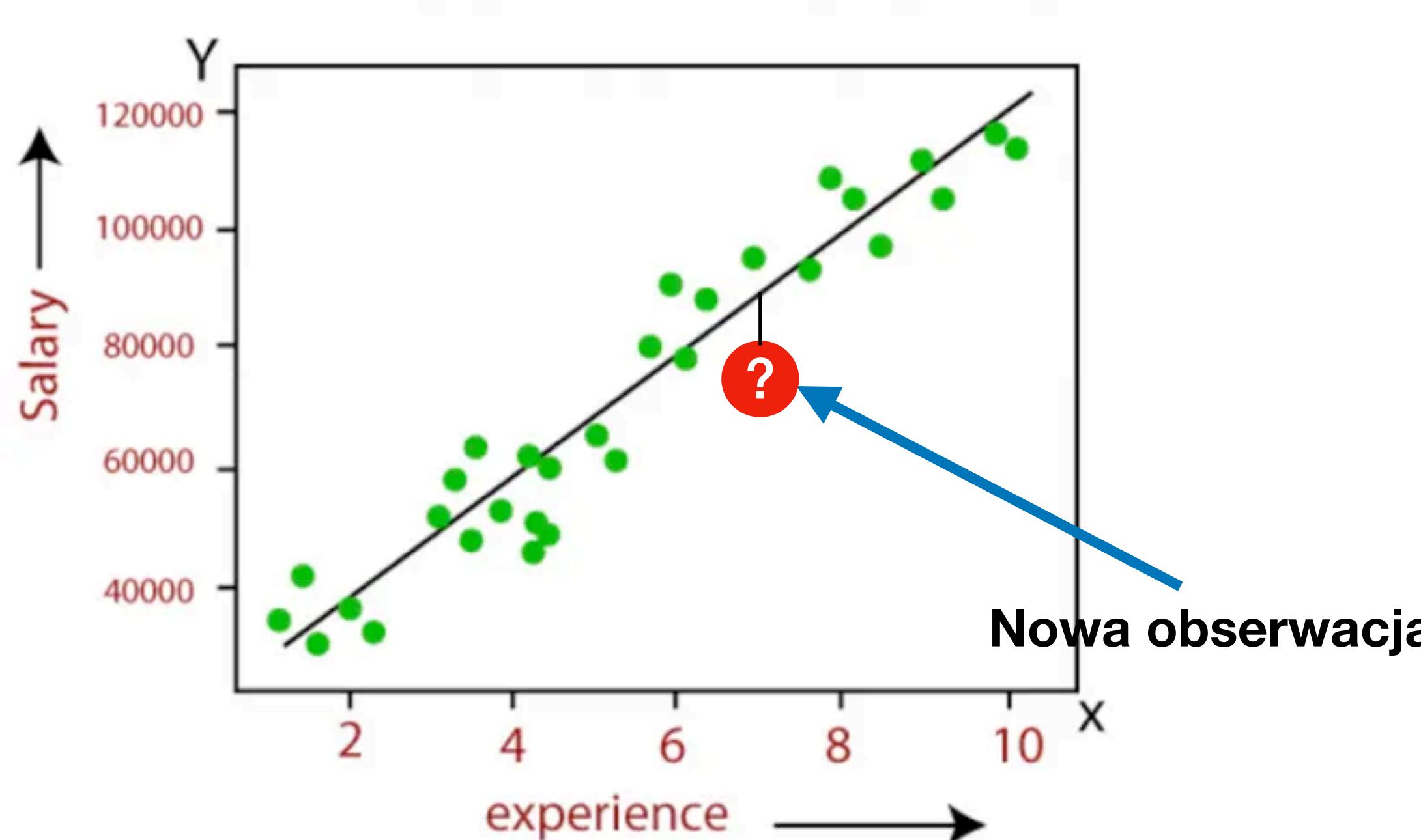


- Zbiór uczący zawierający 25 elementów
- 2 klasy: niebieskie kropki i zielone trójkąty
- Zbiór jest 2-wymiarowy
- Nasz algorytm uczenia maszynowego nauczył się oddzielać kropki od trójkątów
- Modelem jest płaszczyzna oddzielająca dwie klasy od siebie
- Płaszczyzna ta jest w stanie oddzielić (=zaklasyfikować) nową obserwację, której dotychczas nie widzieliśmy

Uczenie nadzorowane - przykłady regresji

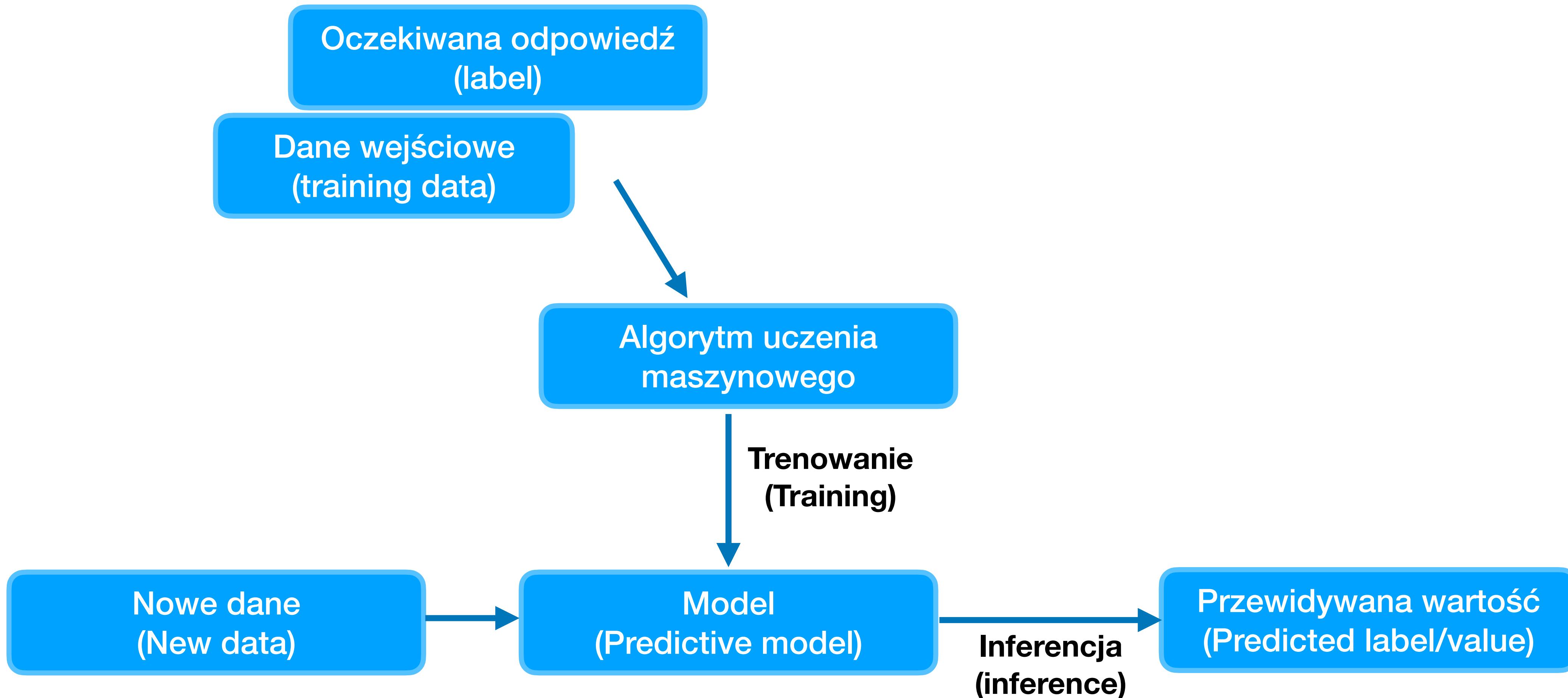
- Przewidywanie cen nieruchomości na podstawie danych takich, jak: ilość pokoi, metraż, lokalizacja, piętro, odległość od przystanku autobusowego, itd.
- Przewidywanie wielkości sprzedaży w oparciu o dane historyczne
- Przewidywanie zapotrzebowania na energię elektryczną w zależności od pogody, godziny, dnia tygodnia
- Przewidywanie wpływu sytuacji makroekonomicznej na wyniki finansowe firmy
- Przewidywanie serii czasowych

Uczenie nadzorowane - przykłady regresji



- Zielone kropki to obserwacje: punkty danych
- Oś X to tzw. zmienna niezależna (feature variable or explanatory variable)
- Oś Y to tzw. zmienna zależna (target variable or response variable)
- Modelem jest prosta minimalizującą odległość między każdym z tych punków i tą prostą
- Najczęściej odległość ta jest wyrażona jako suma kwadratów odległości (o tym później)

Uczenie nadzorowane - schemat uczenia



Uczenie nienadzorowane (unsupervised learning)

Cechy:

- Nasz zbiór danych nie posiada etykiet lub oczekiwanej wartości
- Ingerencja człowieka jest minimalna; nie wymagamy przygotowania danych lub „nadzoru” nad uczeniem
- Nie znamy dobrze struktury danych; naszym celem jest odkrycie pewnych cech tej struktury

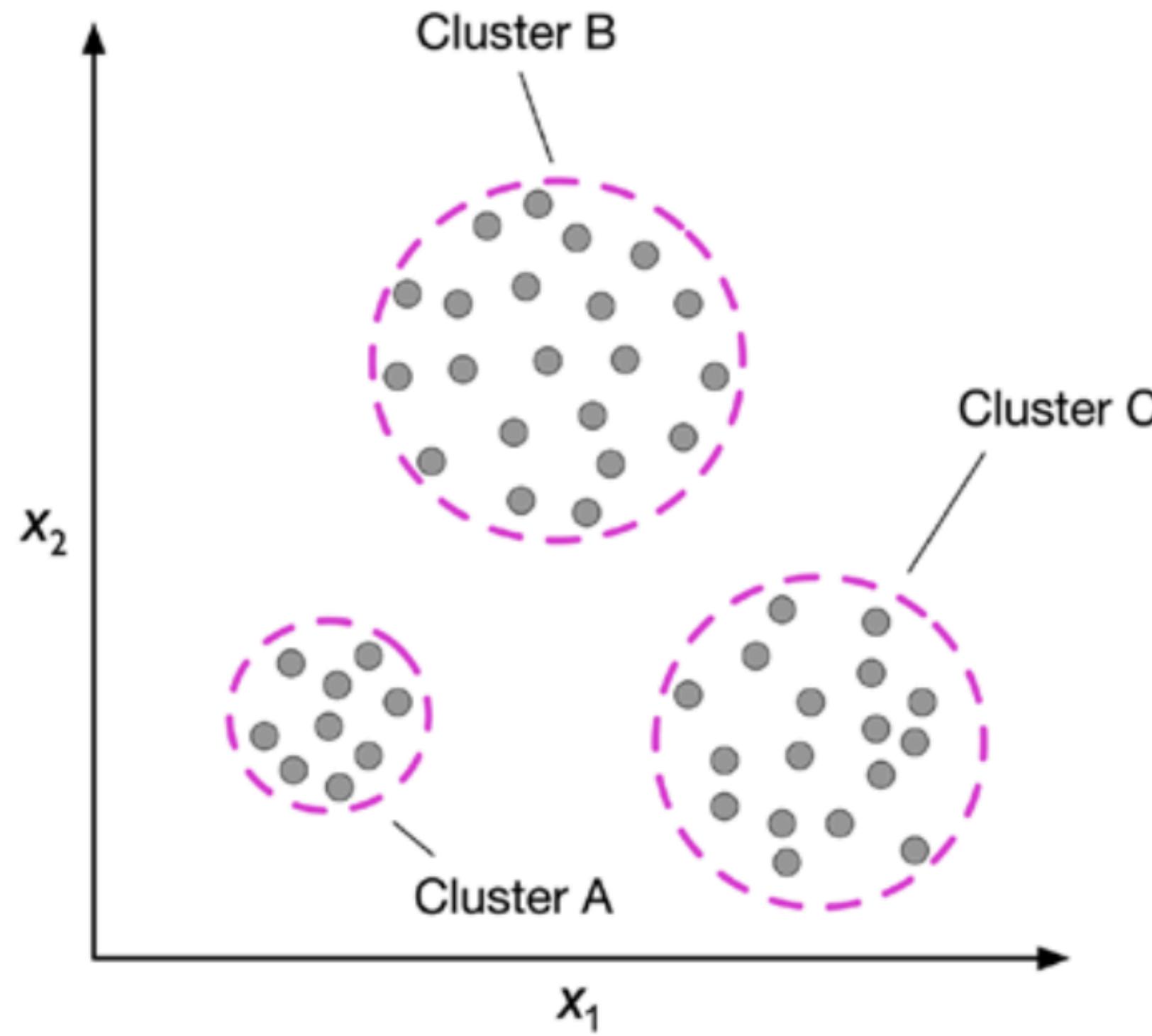
Uczenie nienadzorowane (unsupervised learning)

Rodzaje:

- Analiza skupień (clustering)
- Analiza składowych głównych (PCA - Principal Component Analysis)
- Metody redukcji wymiarowości (dimensionality reduction) (t-SNE, UMAP)
- Reguły asocjacyjne (association rule learning)

Uczenie nienadzorowane

- analiza skupień



Organizacja informacji i odkrywanie grup (clusters) danych bez wcześniejszej wiedzy o ich istnieniu. Np. Identyfikacja grup klientów pod kątem marketingowym.

Przykłady algorytmów:

- k-Means
- DBSCAN

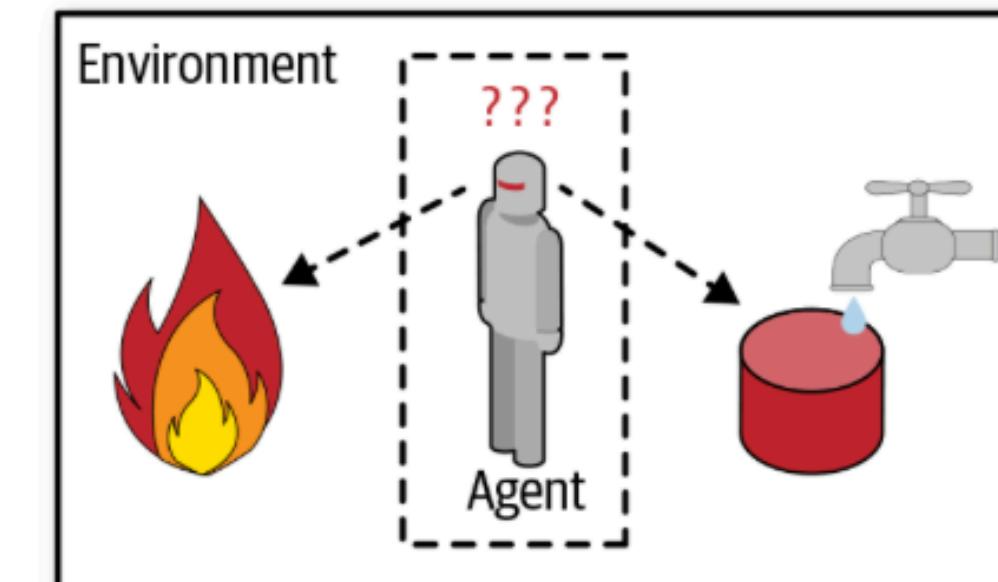
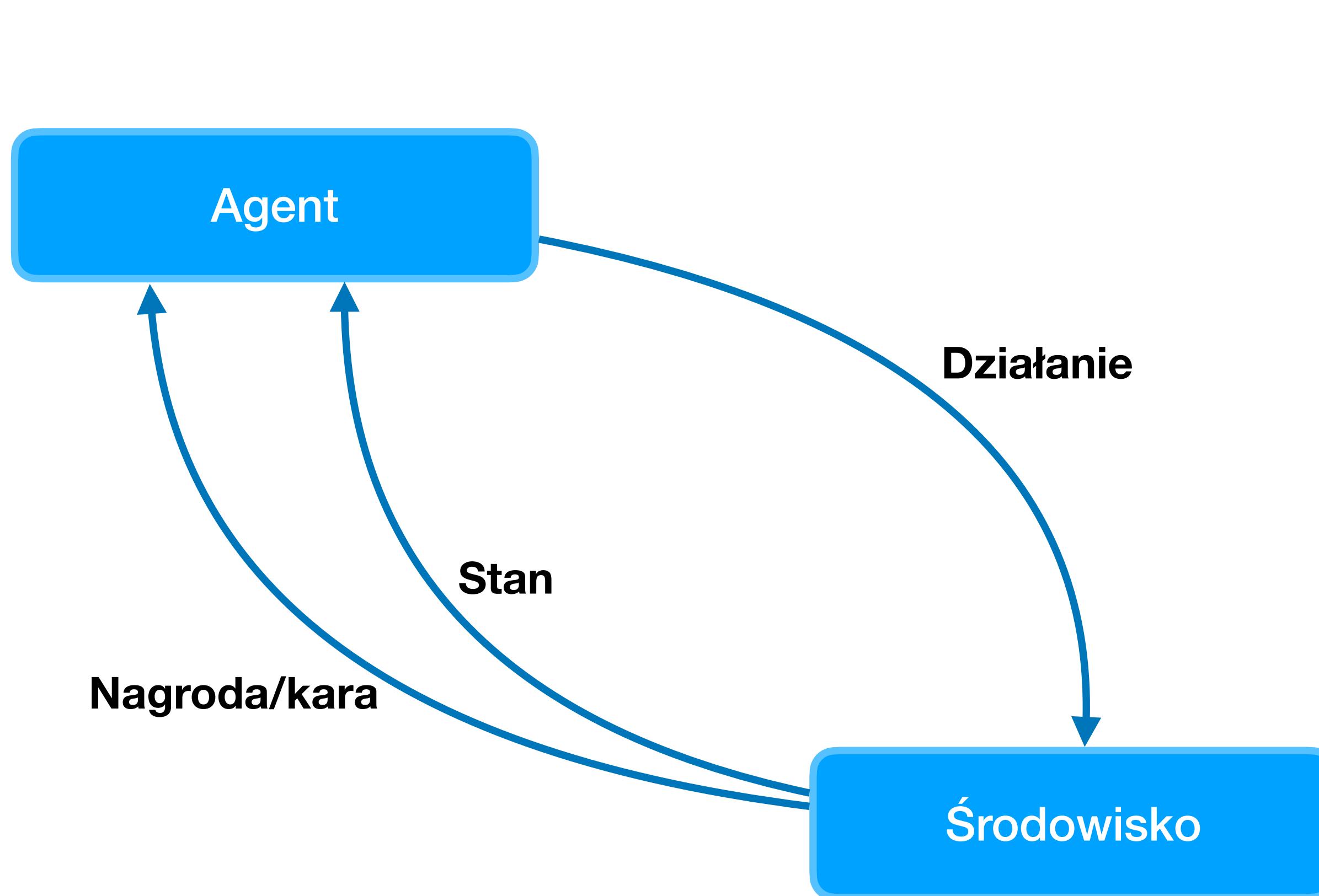
Analiza skupień może być również użyta w celu eliminowania danych nietypowych/odstających (outliers)

Uczenie przez wzmacnianie (reinforcement learning)

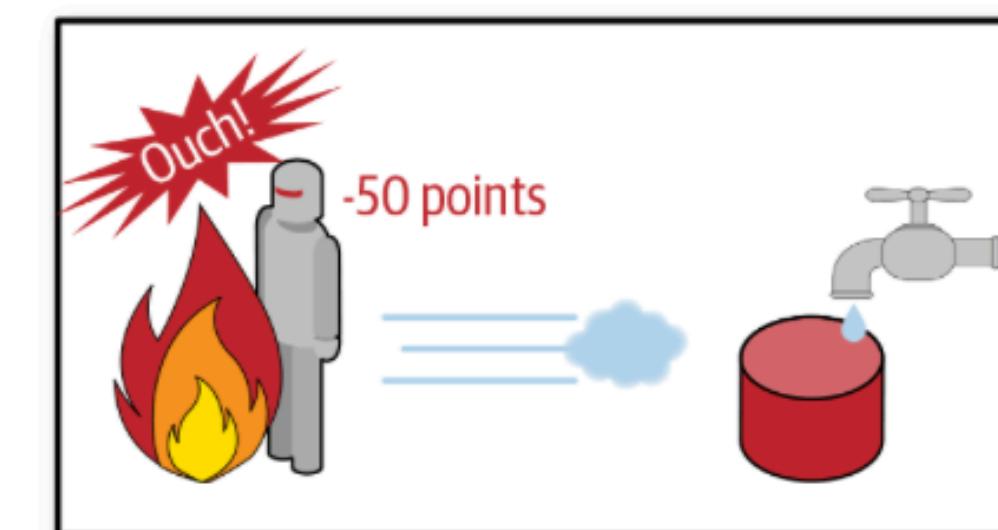
Istnieje cała grupa metod uczenia przez wzmacnianie. Ich głównym założeniem jest:

- Uczenie poprzez interakcje ze środowiskiem.
- Agent za swoje działania otrzymuje nagrody (positive rewards) lub kary (negative rewards). Nagrodą może być osiągnięcie celu lub poprawne wykonanie pewnego kroku.
- Agent dąży do maksymalizacji nagród.

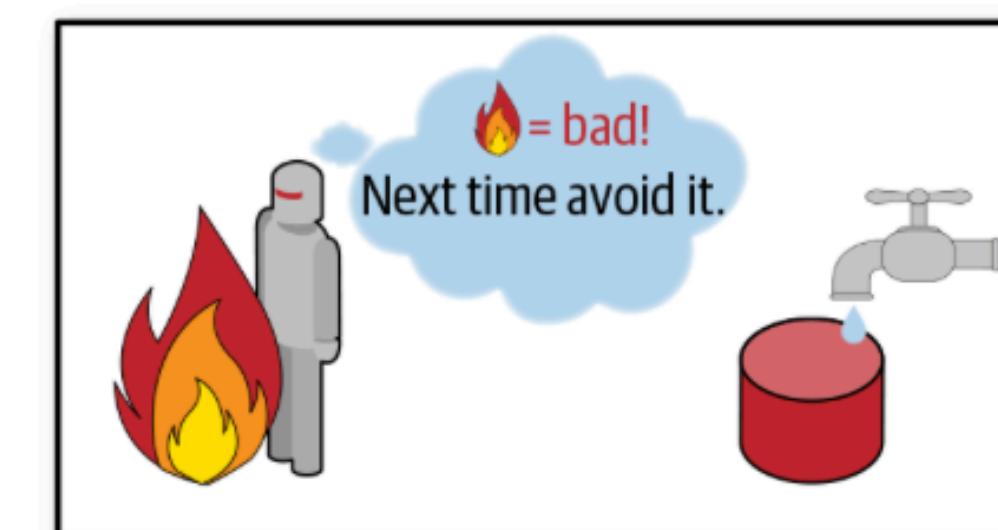
Uczenie przez wzmacnianie (reinforcement learning)



- 1 Observe
- 2 Select action using policy



- 3 Action!
- 4 Get reward or penalty



- 5 Update policy (learning step)
- 6 Iterate until an optimal policy is found

Regresja liniowa

Zanim zaczniemy

- Zbiór danych (dataset) „Advertising”
 - Zawiera dane sprzedaży pewnego produktu
 - na 200 różnych rynkach...
 - wraz z budżetami przeznaczonymi na...
 - 3 różne kanały marketingowe:
 - TV, radio, prasa

Przyjrzymy się relacji między budżetem na TV i wielkością sprzedaży

Notebook: 01 - Loading Data with Pandas

Pandas Data Frames

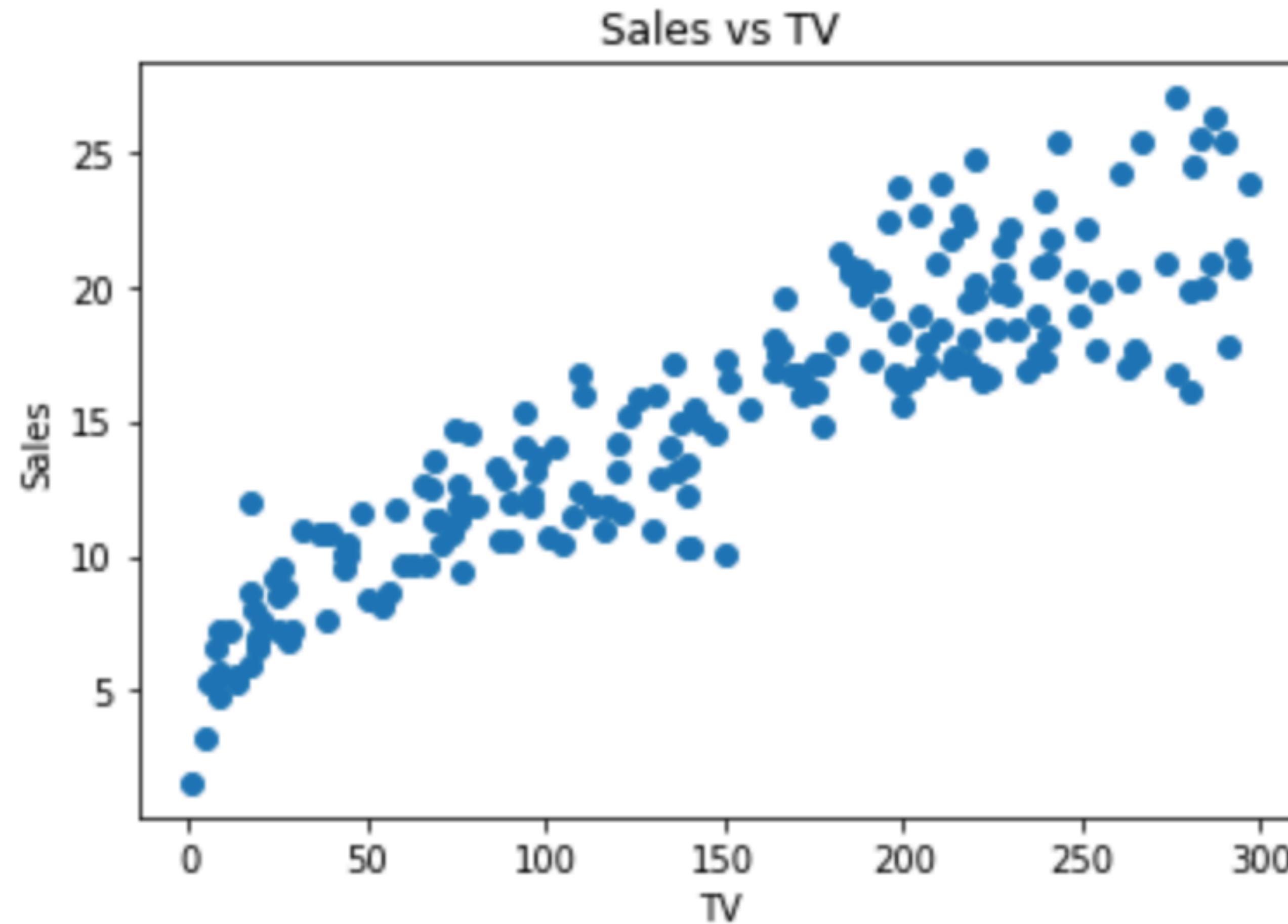
```
df = pd.read_csv('advertising.csv')  
#just print the data frame  
df
```

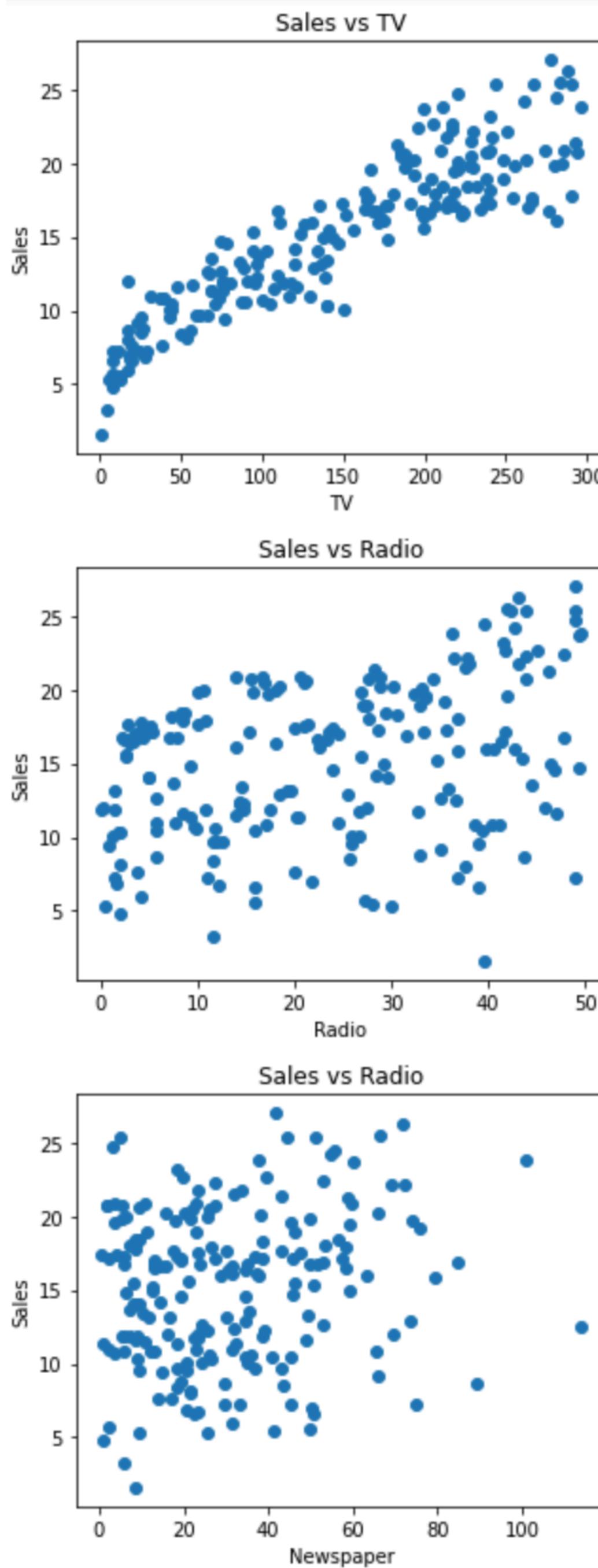
Obserwacja

	TV	Radio	Newspaper	Sales
0	230.1	37.8	69.2	22.1
1	44.5	39.3	45.1	10.4
2	17.2	45.9	69.3	12.0
3	151.5	41.3	58.5	16.5
4	180.8	10.8	58.4	17.9
...
195	38.2	3.7	13.8	7.6
196	94.2	4.9	8.1	14.0
197	177.0	9.3	6.4	14.8
198	283.6	42.0	66.2	25.5
199	232.1	8.6	8.7	18.4

200 rows × 4 columns

```
#scatter plots  
plot.scatter(df[ "TV" ], df[ "Sales" ])  
plot.xlabel( "TV" )  
plot.ylabel( "Sales" )  
plot.title( "Sales vs TV" )
```





A diagram at the top right shows three curved arrows originating from the words "TV", "Radio", and "Newspaper" and pointing to the word "Sales".

	TV	Radio	Newspaper	Sales
0	230.1	37.8	69.2	22.1
1	44.5	39.3	45.1	10.4
2	17.2	45.9	69.3	12.0
3	151.5	41.3	58.5	16.5
4	180.8	10.8	58.4	17.9
...
195	38.2	3.7	13.8	7.6
196	94.2	4.9	8.1	14.0
197	177.0	9.3	6.4	14.8
198	283.6	42.0	66.2	25.5
199	232.1	8.6	8.7	18.4

200 rows × 4 columns

Regresja liniowa - założenia

Prosta regresja liniowa (univariate or simple linear regression) polega na przewidywaniu odpowiedzi Y (zmiennej zależnej) na podstawie pojedynczej zmiennej niezależnej X. Regresja liniowa zakłada, że pomiędzy X i Y istnieje zależność liniowa, tzn taka którą da się opisać funkcją liniową:

$$Y \approx \beta_0 + \beta_1 X$$

β_0, β_1 nazywane są parametrami modelu. Trenowanie modelu polega na estymacji tych parametrów, a następnie na postawie wartości x przewidzenie \hat{y}

$$\hat{y} = \hat{\beta}_0 + \hat{\beta}_1 x$$

$\hat{y}, \hat{\beta}_0, \hat{\beta}_1$ - daszek nad tymi symbolami oznacza estymowaną wartość (nieznaną)

Regresja liniowa - estymacja parametrów

Parametry β_0, β_1 są nieznane, więc aby dokonać predykcji należy najpierw je wyznaczyć.

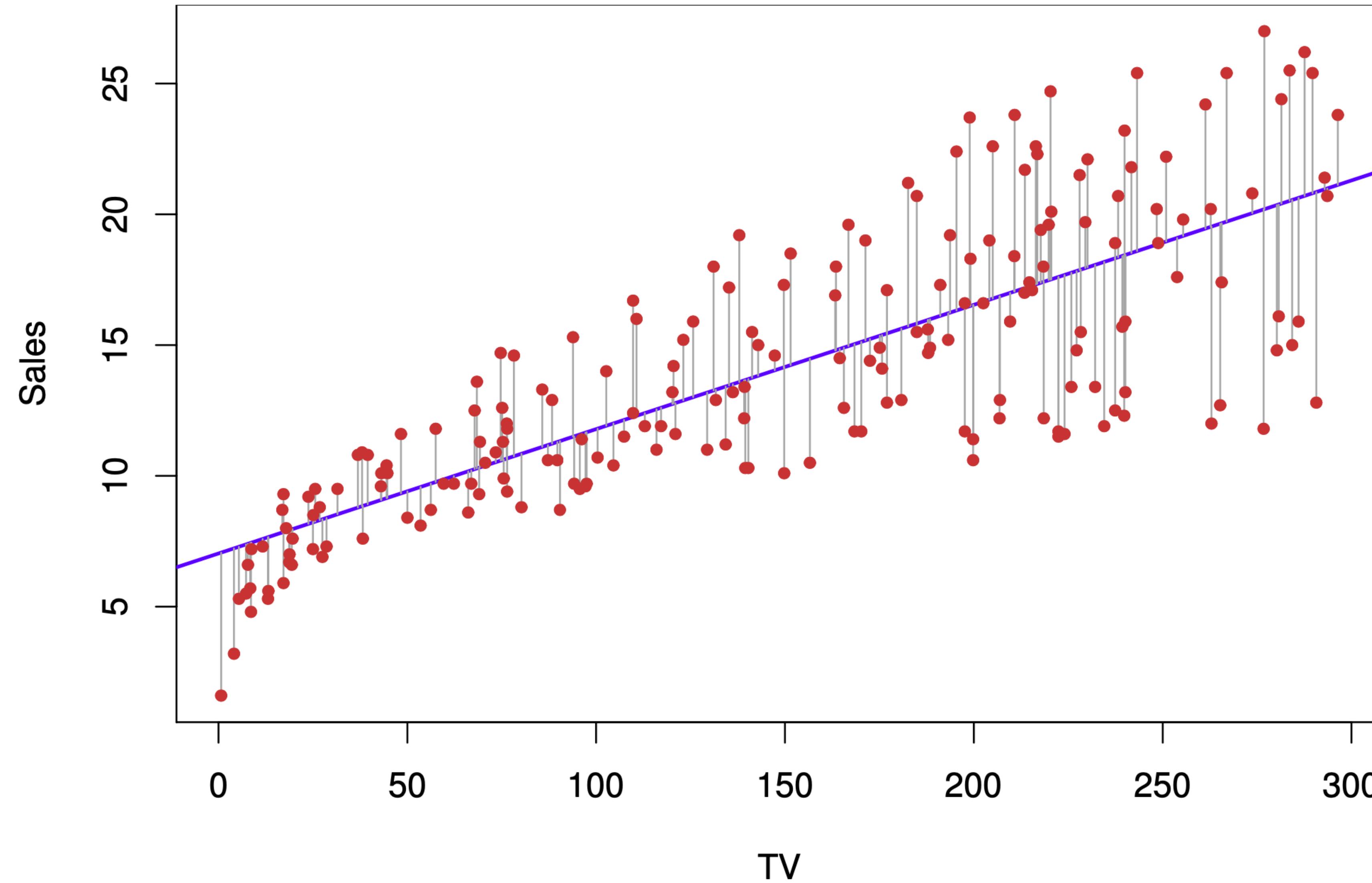
Używamy do tego naszego zbioru n obserwacji (punktów):

$$(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$$

Celem jest takie wyznaczenie parametrów β_0, β_1 aby równanie było spełnione dla wszystkich obserwacji:

$$y_i \approx \hat{\beta}_0 + \hat{\beta}_1 x_i \text{ for } i = 1 \dots n$$

Regresja liniowa - intuicja



Chcemy aby prosta
 $y_i \approx \hat{\beta}_0 + \hat{\beta}_1 x_i$ była jak
najbliżej wszystkich
punktów.

Co to znaczy „jak
najbliżej”?

Regresja liniowa - funkcja straty (loss function)

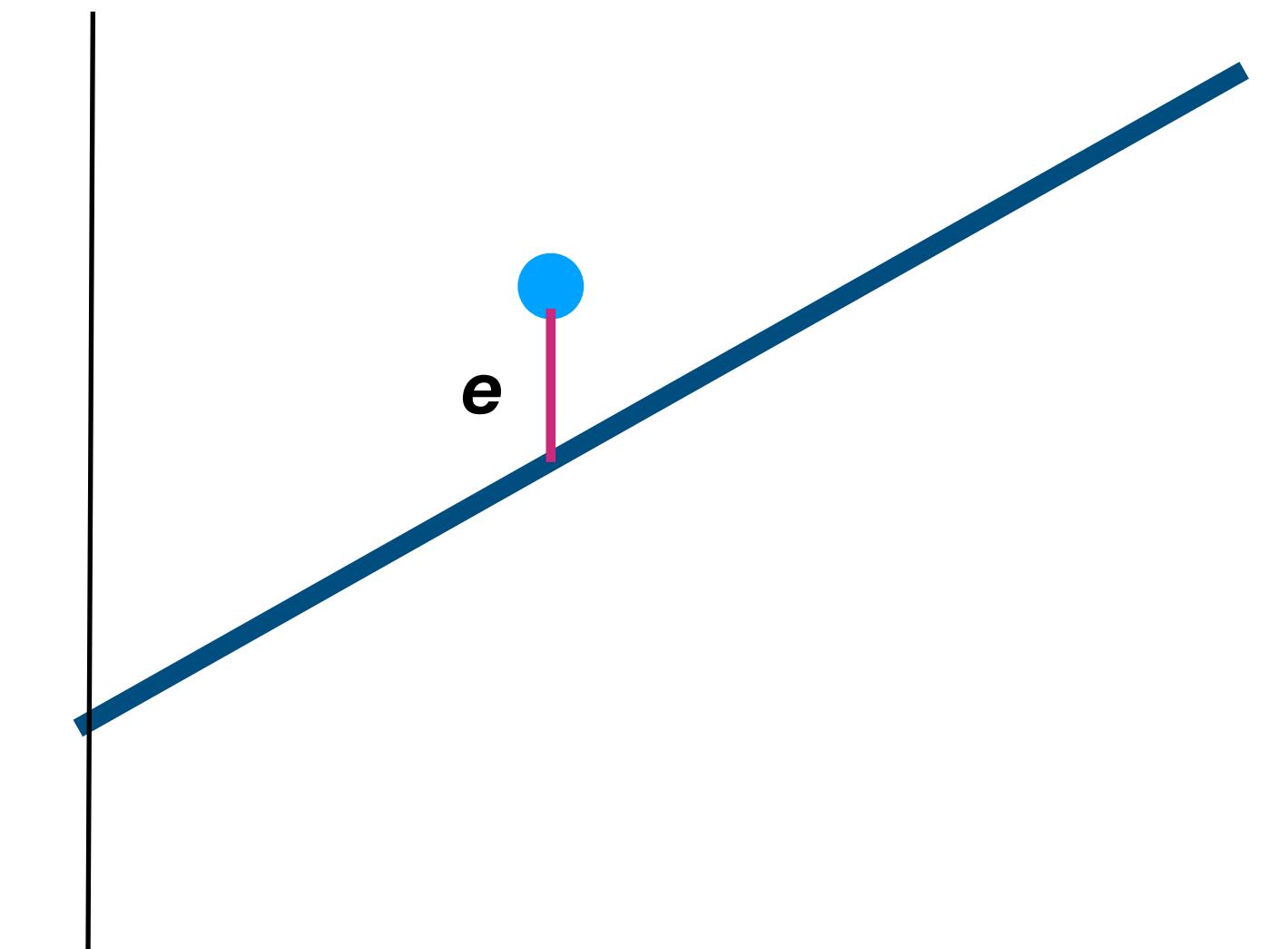
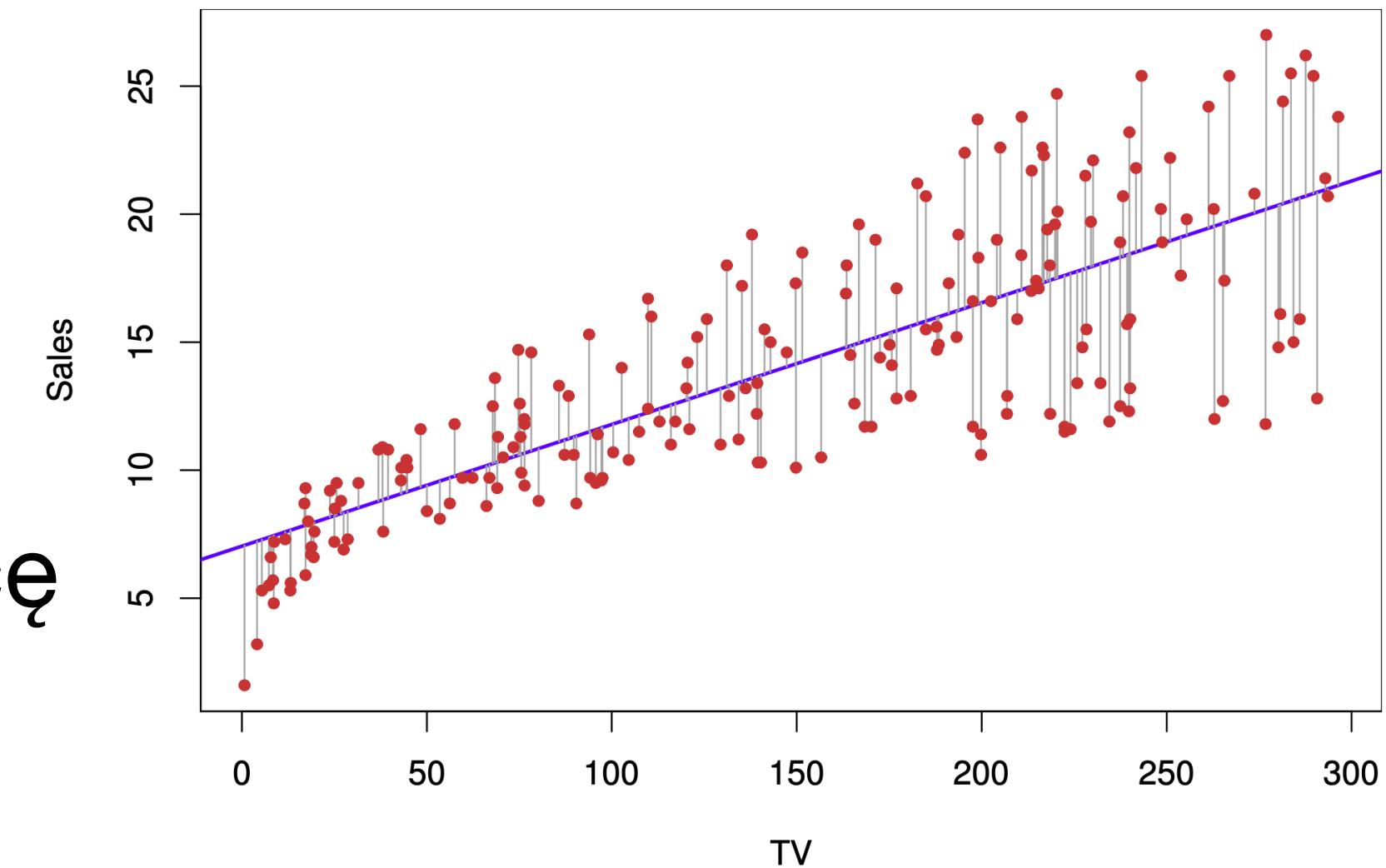
Jeśli $\hat{y}_i \approx \hat{\beta}_0 + \hat{\beta}_1 x_i$ opisuje przewidywana wartość Y w oparciu o i-tą wartość X, to zdefiniujmy:

$e_i = y_i - \hat{y}_i$ jako wartość resztową (residual), czyli różnicę między obserwacją (y_i) a wartością przewidzianą (\hat{y}_i)

Sumą kwadratów wszystkich wartości resztowych będzie:

$$RSS = e_1^2 + e_2^2 + \dots + e_n^2$$

(Residual sum of squares)



Chwila, co?

- To jest moment w którym definiujemy naszą „funkcję celu” (objective function).
- Funkcja celu pomaga nam ocenić jak dobra jest nasza regresja: tj. im suma błędów jest większą tym regresja jest gorsza (prosta jest „daleko od punktów”).
- Naszym celem jest zatem optymalizacja funkcji celu aby suma była jako najmniejsza -> będziemy dążyli aby funkcja dążyła do minimum.
- Dlaczego podnosimy do kwadratu? Podziękujcie Gaussowi!
 - Na serio: funkcja kwadratowa ma ciekawe własności: większe liczby (błąd) podniesione do kwadratu dają jeszcze większą wartość (i na odwrót)
 - Penalizujemy w ten sposób duże odchylenia a faworyzujemy małe



Regresja liniowa - RSS

Find $\min_{\hat{\beta}_0, \hat{\beta}_1} Q(\hat{\beta}_0, \hat{\beta}_1) = \min RSS$

$$RSS = e_1^2 + e_2^2 + \dots + e_n^2 = (y_1 - \hat{\beta}_0 - \hat{\beta}_1 x_1)^2 + (y_2 - \hat{\beta}_0 - \hat{\beta}_1 x_2)^2 + \dots + (y_n - \hat{\beta}_0 - \hat{\beta}_1 x_n)^2$$

Dla regresji prostej łatwo można policzyć tzw. rozwiązanie analityczne. Rozwiążując to równanie dla parametrów $\hat{\beta}_0, \hat{\beta}_1$ otrzymamy:

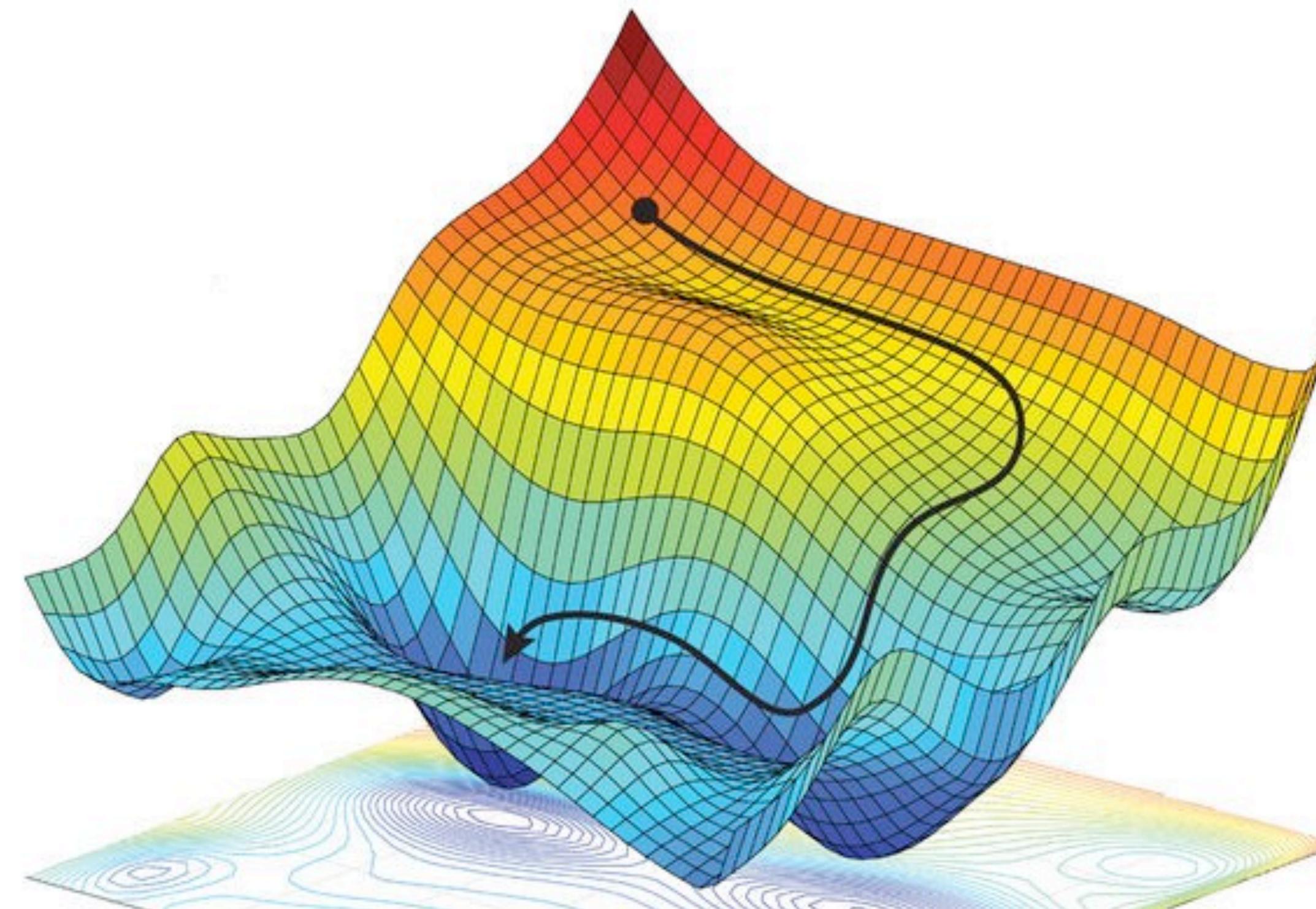
$$\hat{\beta}_1 = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sum_{i=1}^n (x_i - \bar{x})^2}$$

$$\hat{\beta}_0 = \bar{y} - \hat{\beta}_1 \bar{x}$$

Gdzie: $\bar{y} = \frac{1}{n} \sum_{i=1}^n y_i$ oraz $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$ (po prostu są to średnie z X i Y)

Regresja liniowa - poszukiwanie minimum

Rozwiążanie analityczne jest Ok dla regresji prostej (z jedną zmienną). Przeważnie do poszukiwania minimum funkcji celu używamy metody gradientu prostego.



Regresja liniowa - poszukiwanie minimum

Funkcja celu ma najczęściej postać MSE, tj. $\frac{RSS}{n}$

Find $\min_{\hat{\beta}_0, \hat{\beta}_1} Q(\hat{\beta}_0, \hat{\beta}_1) = \min MSE$

$$MSE = \frac{e_1^2 + e_2^2 + \dots + e_n^2}{n} = \frac{1}{n} \sum_{i=0}^n (y_i - \hat{y}_i)^2 = \frac{1}{n} \sum_{i=0}^n (y_i - (\hat{\beta}_1 x_i + \hat{\beta}_0))$$

Obliczamy pochodne cząstkowe (partial derivative) dla $\hat{\beta}_0, \hat{\beta}_1$:

$$D_{\hat{\beta}_1} = \frac{1}{n} \sum_{i=0}^n 2(y_i - (\hat{\beta}_1 x_i + \hat{\beta}_0))(-x_i) = \frac{-2}{n} \sum_{i=0}^n x_i(y_i - \hat{y}_i)$$

$$\text{Tak samo dla } \hat{\beta}_0: D_{\hat{\beta}_0} = \frac{-2}{n} \sum_{i=0}^n (y_i - \hat{y}_i)$$

Regresja liniowa - poszukiwanie minimum

Jak znaleźć $\hat{\beta}_0, \hat{\beta}_1$?

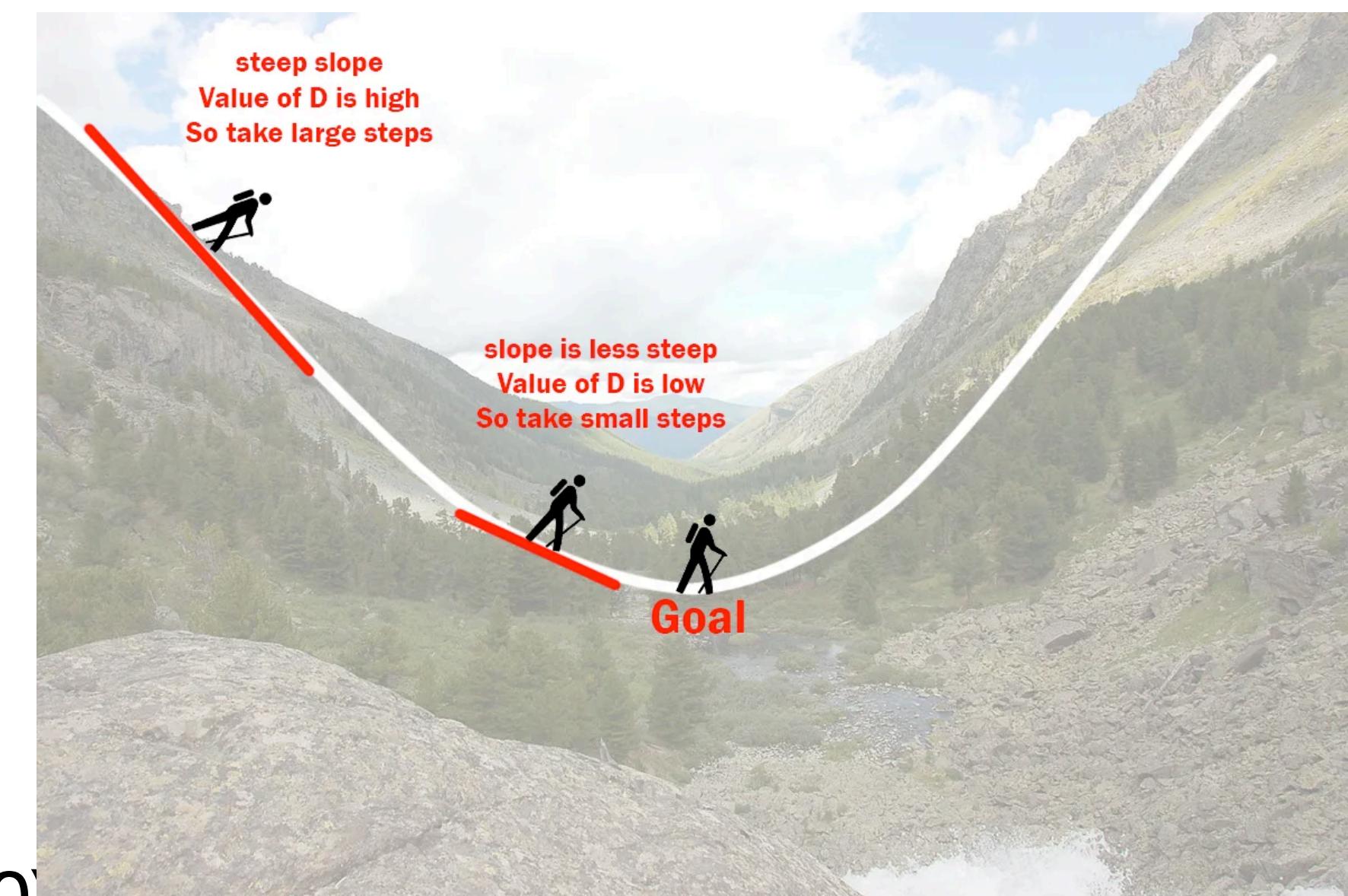
Zaczynamy od jakiejś dowolnej wartości $\hat{\beta}_0, \hat{\beta}_1$ (0, 0). Ustalamy współczynnik α (learning rate) - to będzie „długość naszego kroku”, czyli jak szybko będziemy zmieniać wartości $\hat{\beta}_0, \hat{\beta}_1$

Uaktualniamy wartości $\hat{\beta}_0, \hat{\beta}_1$:

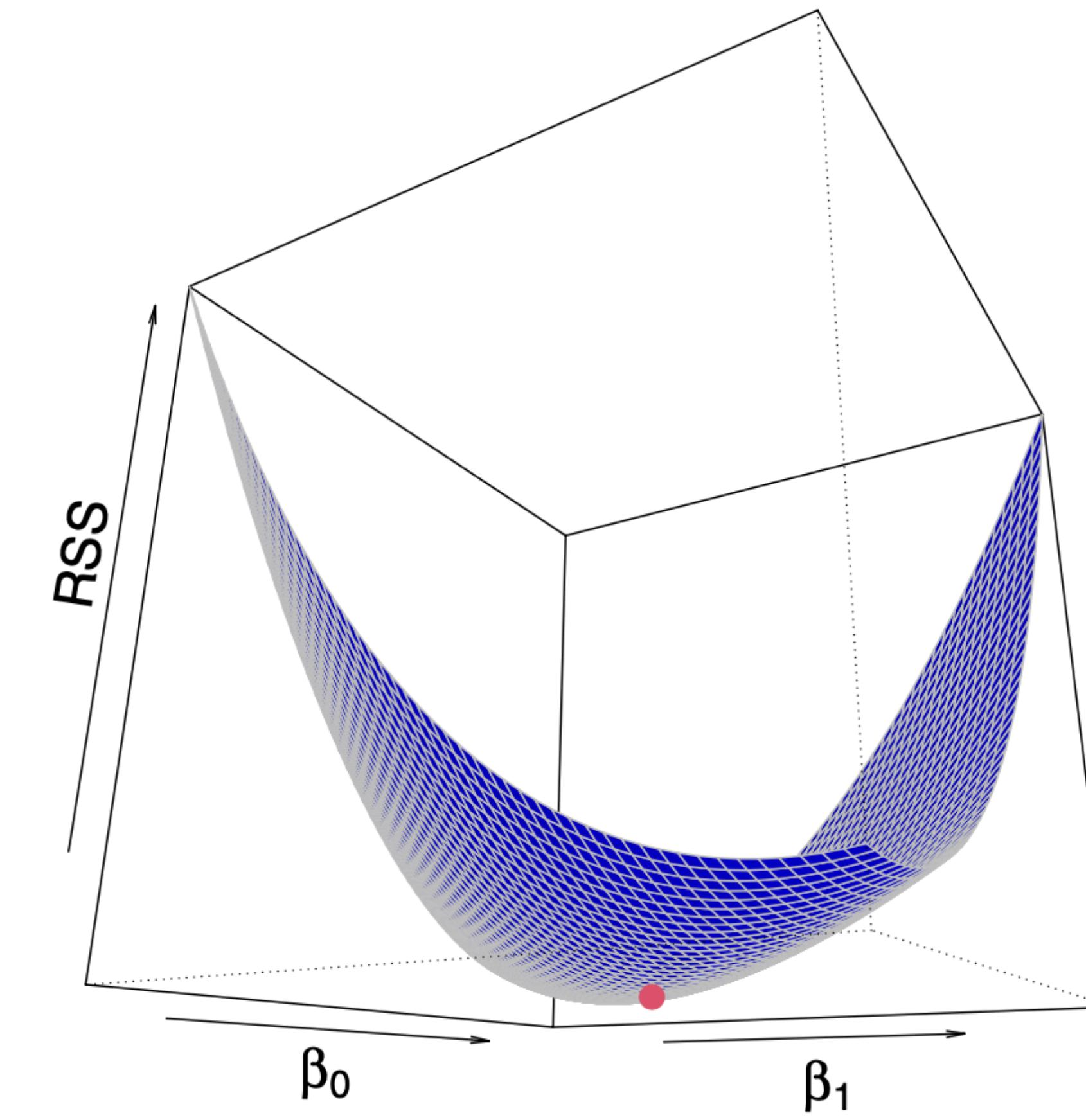
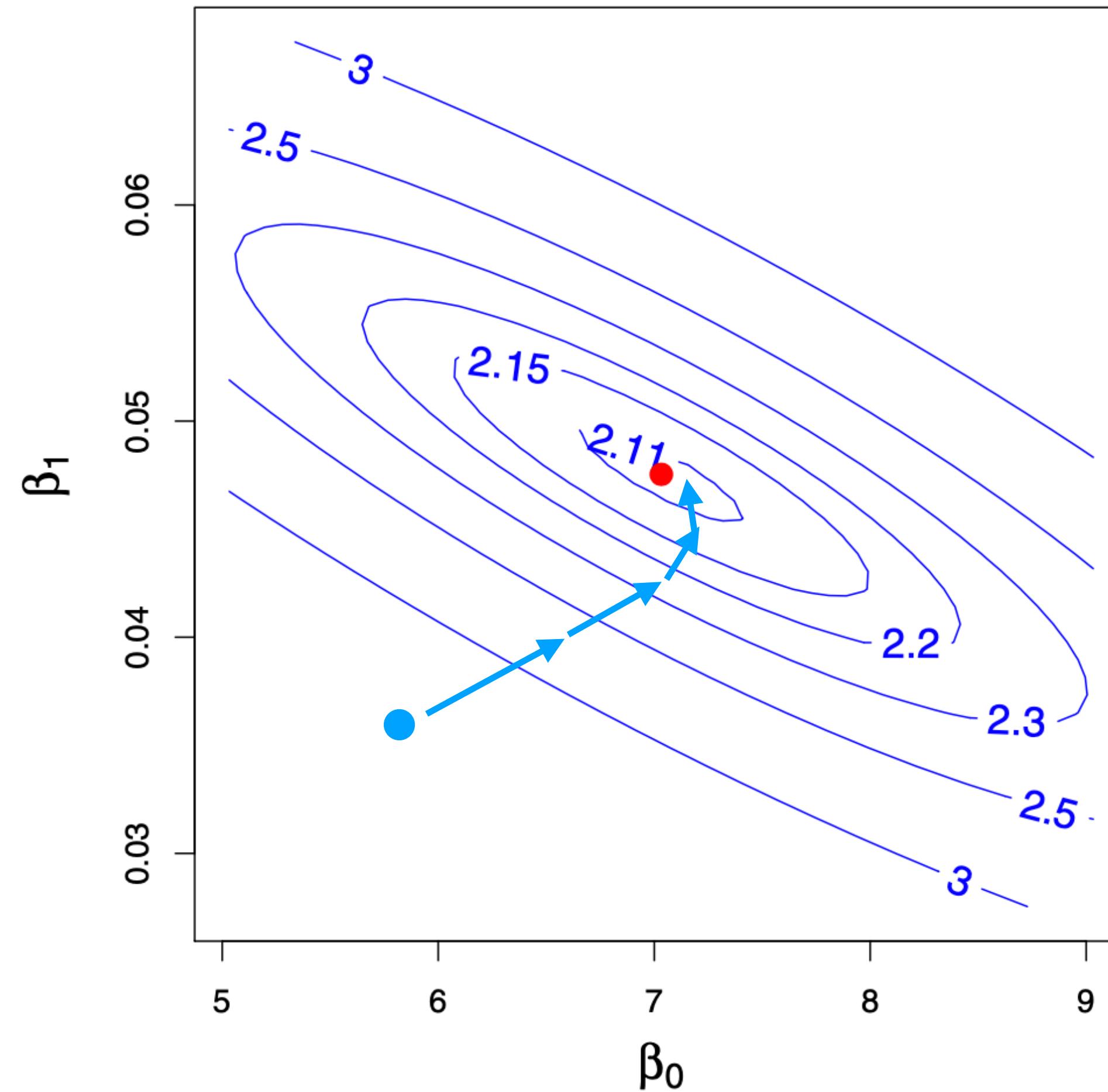
$$\hat{\beta}_1 = \hat{\beta}_1 - \alpha D_{\hat{\beta}_1}$$

$$\hat{\beta}_0 = \hat{\beta}_0 - \alpha D_{\hat{\beta}_0}$$

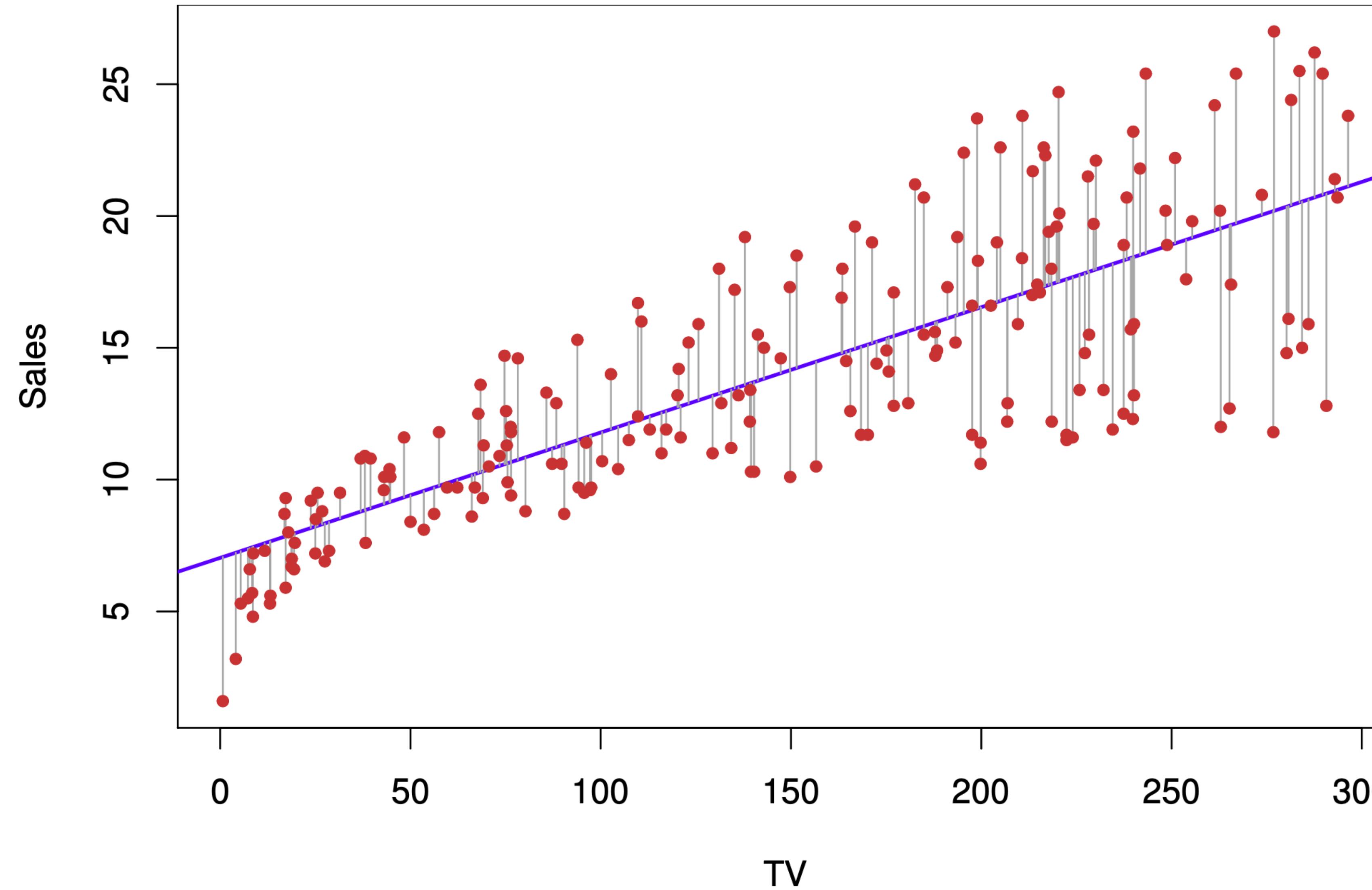
Kontynuujemy aż nasza funkcja straty jest bardzo mała (bliska 0)



Regresja liniowa - minimalizacja RSS metoda gradientu prostego



Regresja liniowa - RSS



Wizualizacja prostej
regresji liniowej (linear
regression fit)

$$\hat{\beta}_0 = 6,97$$

$$\hat{\beta}_1 = 0,055$$

Czyli: każde kolejne
1000\$ wydane na
reklamę w TV to
 $1000 \cdot 0,055 = 55$
dodatkowych jednostek
sprzedaży

Ewaluacja parametrów

- Założenie regresji liniowej jest takie, że istnieje zależność pomiędzy X i Y. Jak to sprawdzić?
 - Hipoteza zerowa: $H_0: \beta_1 = 0$
 - Hipoteza alternatywna: $H_1 : \beta_1 \neq 0$
- β_1 powinno być dalekie od zera ale jak bardzo?
 - 2x odchylenie standardowe (SE, Standard Error)
 - P-value: niska wartość wskazuje, że jest to bardzo mało prawdopodobne, że zależność Y od X jest przypadkowa zakładając, że Y i X w przeciwności od siebie nie zależą. Przyjęto się, że wartości 0.05 albo 0.01 wystarczają, żeby odrzucić hipotezę zerową.

Ewaluacja modelu

- Kiedy udowodniliśmy, że istnieje zależność Y od X, warto jeszcze sprawdzić jak dobry jest nasz model. Popularne metryki:
 - RSE (Residual Standard Error) - odchylenie standardowe składnika resztowego
$$RSE = \sqrt{\frac{1}{n - 2} RSS}$$
 - $MSE = \frac{1}{N} \sum_{i=1}^n (y_i - \hat{y})^2$ & $RMSE = \sqrt{MSE}$
 - R^2 - współczynnik determinacji - liczba z przedziału $<0,1>$. Określa jaka część zmienności/wariancji Y jest wyjaśniona przez korelacje z X. R^2 bliskie 1 oznacza, że większość wariancji wyjaśniona jest zależnością liniową.

Notebook:

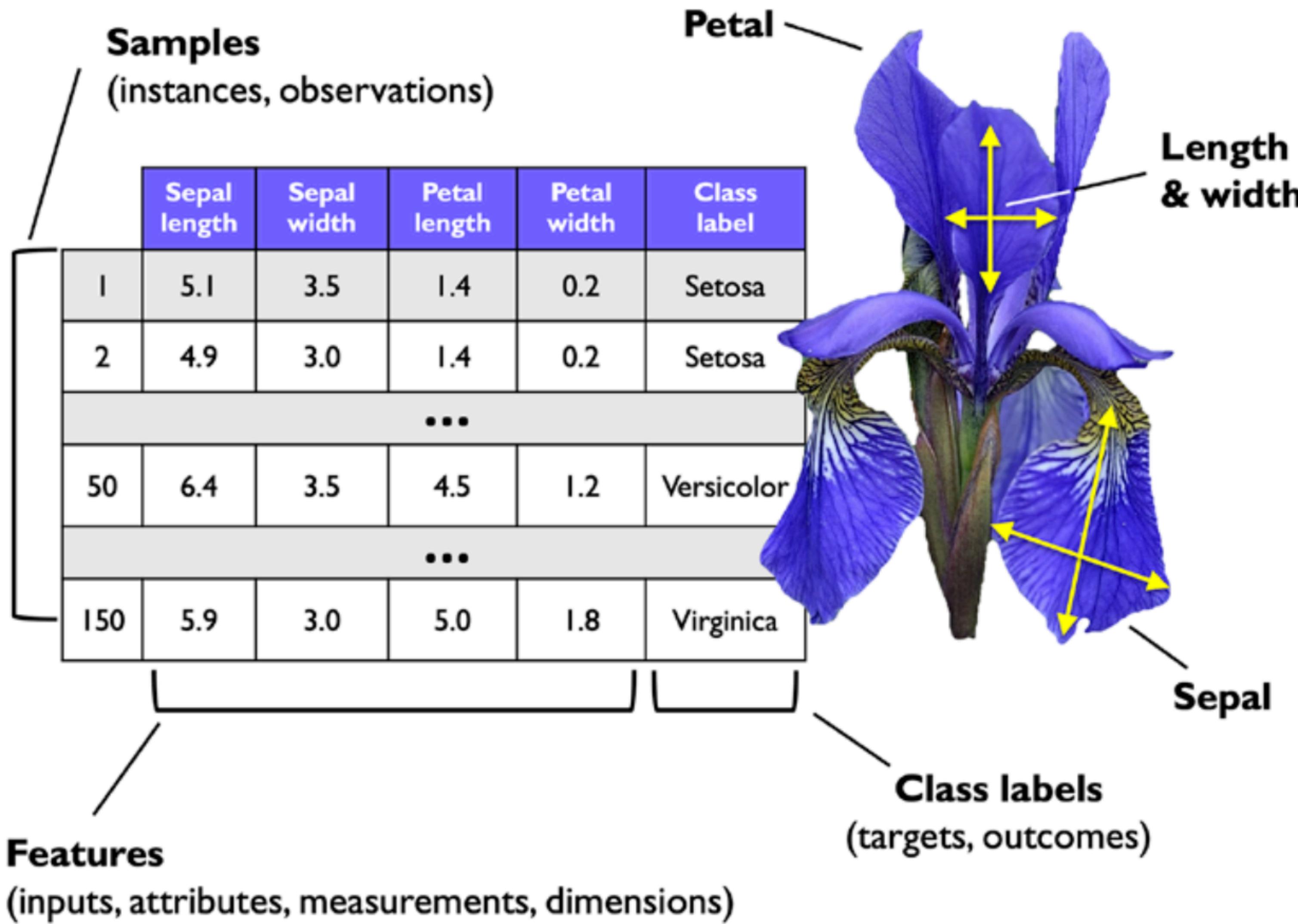
02 - Simple Linear Regression

Regresja logistyczna

To jest algorytm zaliczany do
algorytmów klasyfikacji
(a nie regresji)



Iris dataset

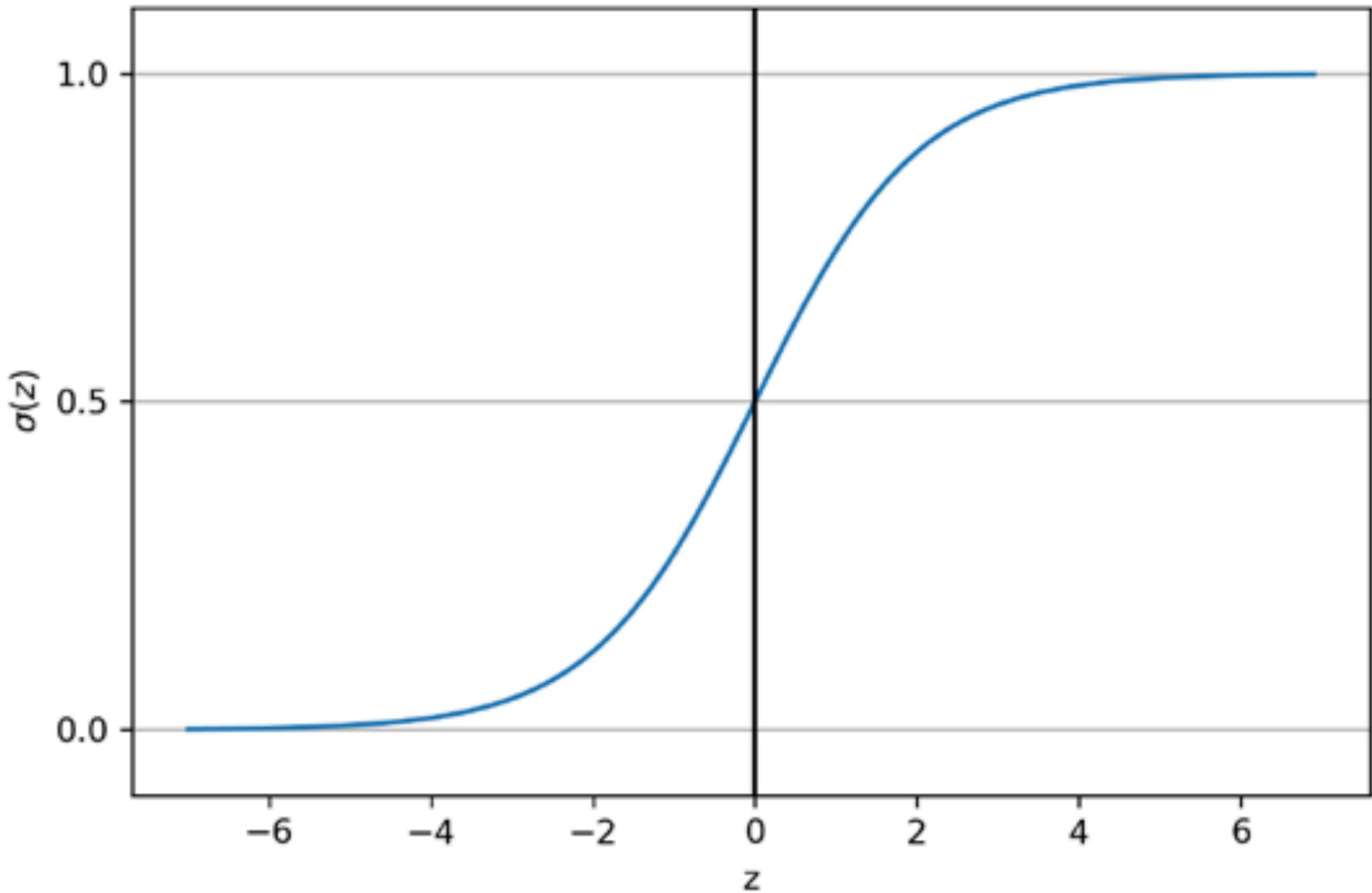


Iris dataset

- Iris setosa - kosaciec szczecinowy
- Iris virginica -
- Iris versicolor - kosaciec różnobarwny



Funkcja logistyczna



Szansa zdarzenia (logit function):

$$\frac{p}{(1 - p)}$$

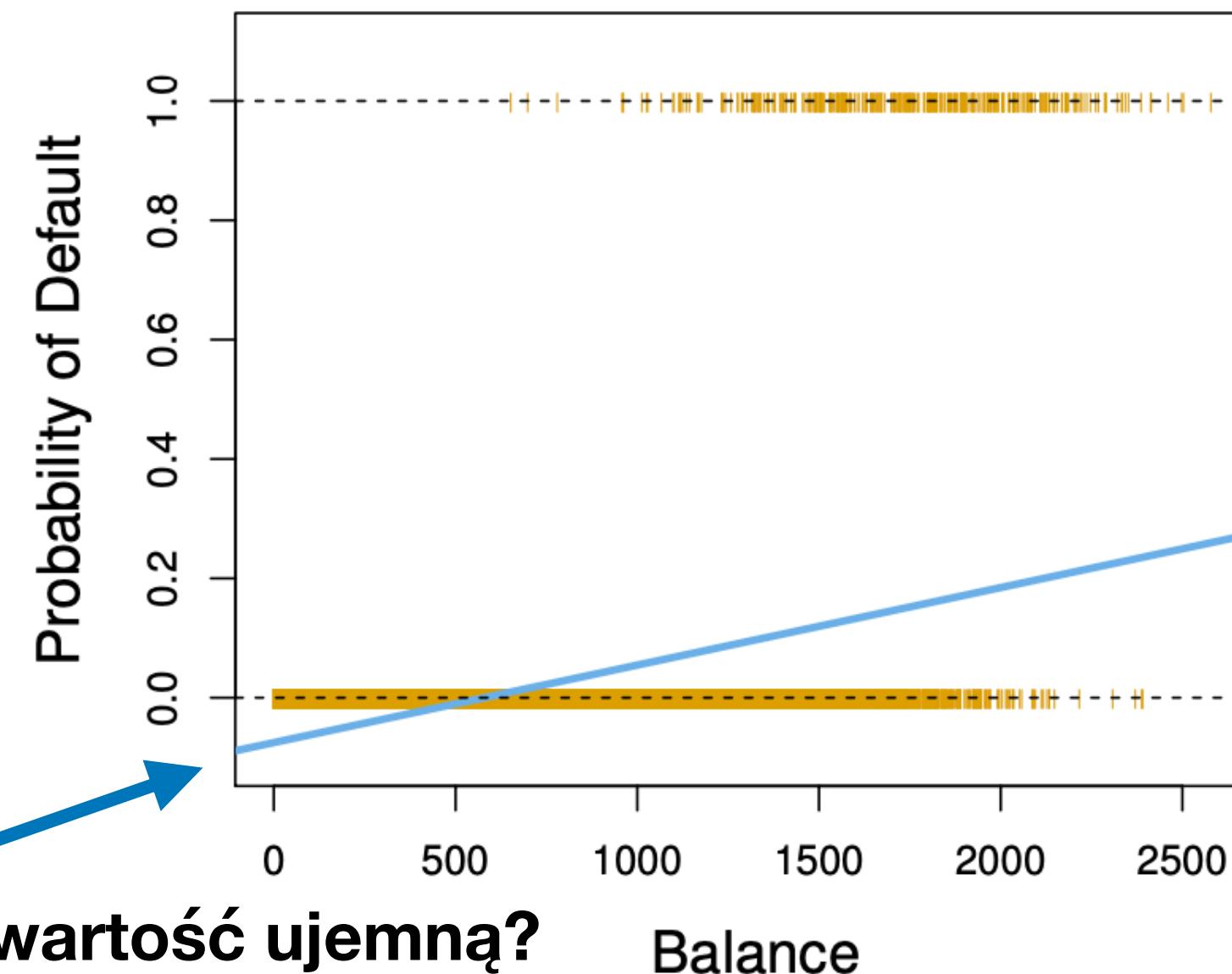
Funkcja logistyczna jest jej odwrotnością:

$$\sigma(z) = \frac{1}{1 + e^{-z}}$$

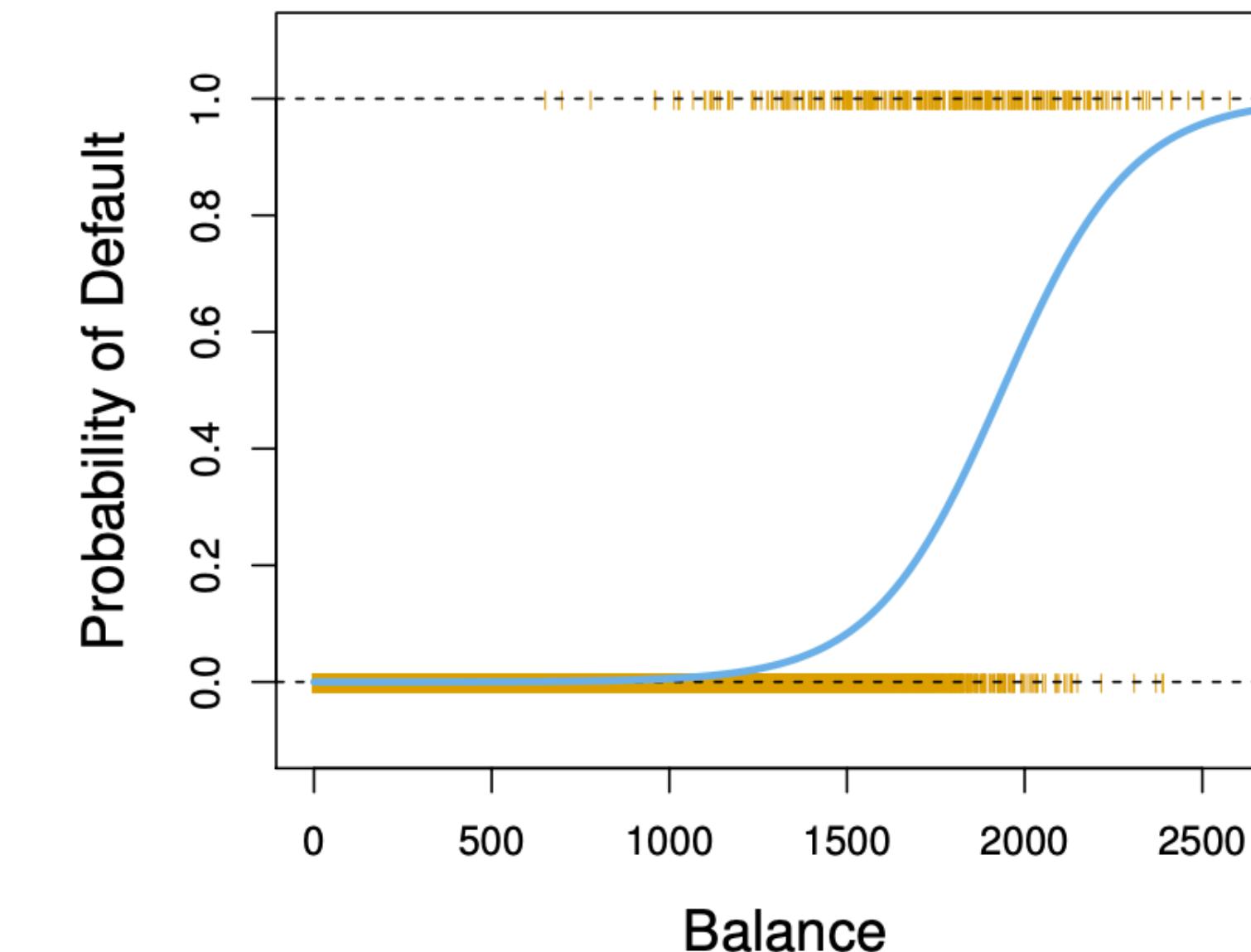
Przyjmuje wartości z przedziału (0,1)

Dlaczego regresja logistyczna?

Regresja liniowa nie ma „sensu” w zadaniach klasyfikacyjnych, gdzie chcemy najlepiej „odseparować” klasy



Jak zinterpretować wartość ujemną?



Klasyfikacja - dane wejściowe

	Id	SepalLengthCm	SepalWidthCm	PetalLengthCm	PetalWidthCm	Species
0	1	5.1	3.5	1.4	0.2	Iris-setosa
1	2	4.9	3.0	1.4	0.2	Iris-setosa
2	3	4.7	3.2	1.3	0.2	Iris-setosa
3	4	4.6	3.1	1.5	0.2	Iris-setosa
4	5	5.0	3.6	1.4	0.2	Iris-setosa
...
145	146	6.7	3.0	5.2	2.3	Iris-virginica
146	147	6.3	2.5	5.0	1.9	Iris-virginica
147	148	6.5	3.0	5.2	2.0	Iris-virginica
148	149	6.2	3.4	5.4	2.3	Iris-virginica
149	150	5.9	3.0	5.1	1.8	Iris-virginica

150 rows × 6 columns

04 - Logistic regression - vis

Zbiór uczący i zbiór testowy

Aby w ogóle móc dokonać ewaluacji algorytmów klasyfikujących, musimy podzielić nasz zbiór danych uczących na 2 części:

- Zbiór używany do uczenia algorytmu (train set)
- Zbiór używany do testowania/walidacji (test set)

Np. 80% train set i 20% test set. Trenowanie wykonujemy na zbiorze trenującym a następnie dokonujemy walidacji modelu na zbiorze testowym w celu porównania wyników.

Zbiór uczący i zbiór testowy

Dlaczego rozdzielamy zbiory?

- Unikamy w ten sposób sytuacji, w której model „widział” już daną obserwację i najprawdopodobniej zaklasyfikuje ją właściwie („nauczy się ich na pamięć”)

Jak wybrać zbiór testowy?

- Najczęściej można wybrać po prostu losowe obserwacje. Czasami jednak chcemy się upewnić, że klasy są jednakowo reprezentowane, wtedy warto o to zadbać zachowując takie same proporcje klas w zbiorze testowym i treningowym (stratified validation)

Sprawdzian krzyżowy - Cross-validation

4-fold validation ($k=4$)



Nie musimy ograniczać się do walidacji tylko jednokrotnej.

ε_1 Dzięki walidacji krzyżowej możemy sprawdzić nasz algorytm na wszystkich przypadkach.

ε_2 Wyniki uzyskane w każdej walidacji uśredniamy.

Ewaluacja



actual predicted



0	2	2
----------	---	---

1	0	0
----------	---	---

2	1	1
----------	---	---

3	0	0
----------	---	---

4	0	0
----------	---	---

5	0	0
----------	---	---

6	2	2
----------	---	---

7	2	2
----------	---	---

8	2	2
----------	---	---

9	1	1
----------	---	---

Polega na porównaniu wyniku rzeczywistej obserwacji z wynikiem przewidzianym przez model.

Jak porównywać takie wyniki?

Macierz błędu (confusion matrix)

		Predicted condition	
		Positive (PP)	Negative (PN)
Total population $= P + N$	Positive (P)	True positive (TP)	False negative (FN)
Actual condition	Negative (N)	False positive (FP)	True negative (TN)

czułość (*ang. recall, sensitivity, true positive rate*)

$$TPR = \frac{TP}{P} = \frac{TP}{TP+FN}$$

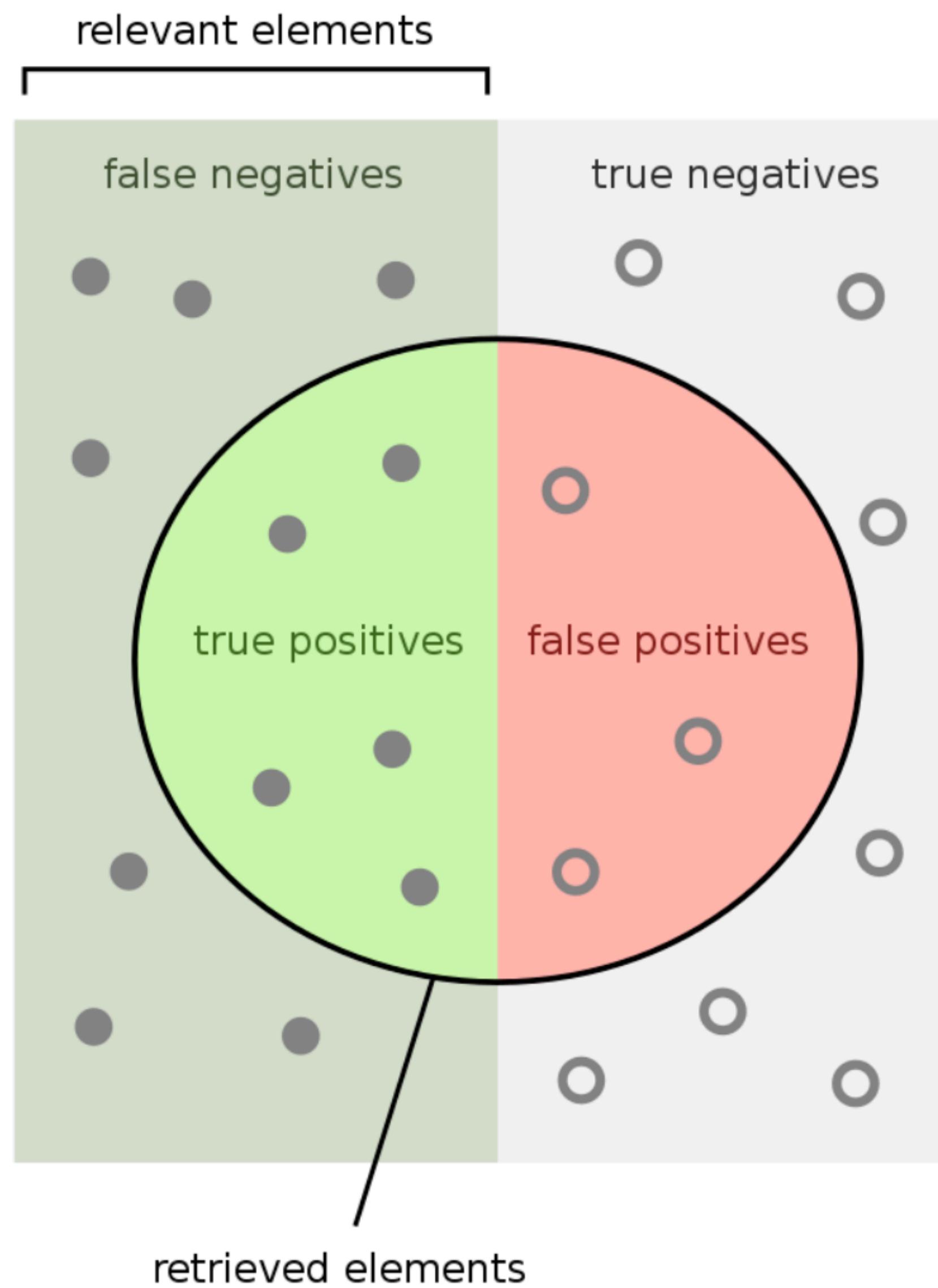
precyzja (*ang. precision, positive predictive value*)

$$PPV = \frac{TP}{TP+FP}$$

F1-score

$$F_1 - score = \frac{2TP}{2TP+FP+FN}$$

Macierz błędu (confusion matrix)



How many retrieved items are relevant?

Precision =

How many relevant items are retrieved?

Recall =

Macierz błędu (confusion matrix)

		Przewidziane	
		Jabłko	Gruszka
Prawdziwe	Jabłko	10	2
	Gruszka	5	10

$$\text{Precyzja} = 10/15 = 0,66$$

$$\text{Czułość} = 10/12 = 0,83$$

Macierz błędu (confusion matrix)

Przykład

	setosa	versicolor	virginica
setosa	10	0	0
versicolor	0	10	0
virginica	0	1	9

Materiały

- Linear regression with Andrew Ng - seria nagrani na YouTube
- Książki:
 - The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Second Edition (wersja elektroniczna dostępna za darmo)
 - Effective Pandas: Patterns for Data Manipulation

