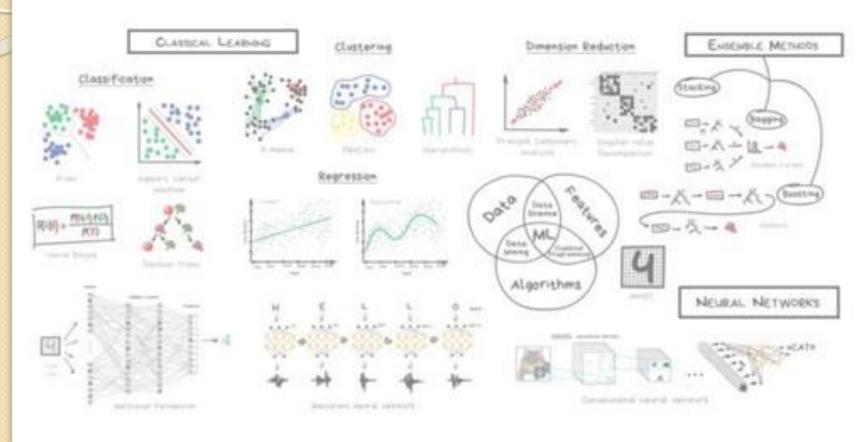
### МАШИНЕ НАВЧАННЯ

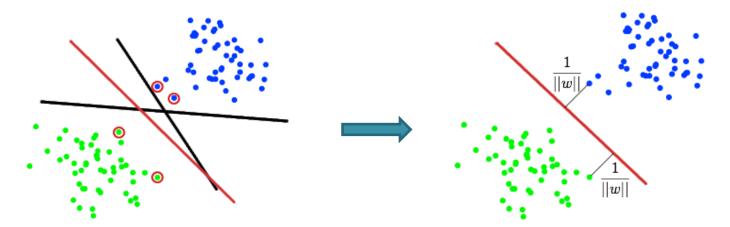
### Класичне навчання. Навчання з вчителем



Лекція №**6** 

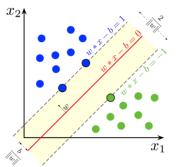
### Методи класифікації Метод опорних векторів (**SVM**)

Найбільш популярний метод класичної класифікації. Ним класифікували вже **все**: типи рослин, лиця на фотографіях, документи за тематиками. Багато років він був головною відповіддю на питання «який би мені взяти класифікатор».



Ідея SVM — провести полосу пряму між категоріями таким чином, що відстані від неї до граничного об'єкта кожного класу була максимальною.

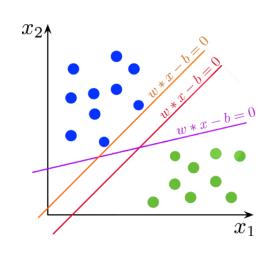




Розглянемо задачу бінарної класифікації, в якій об'єктам з  $X=\mathbb{R}^n$  (об'єкти описуються n числовими признаками) відповідає один з двох класів  $Y=\{-1,+1\}$ . Нехай задана навчальна вибірка пар "об'єкт-відповідь":  $(x_i,yi), i=1\dots \ell$ . Необхідно побудувати алгоритм класифікації  $a(x):X\to Y$ .

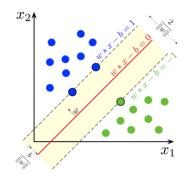
### Розділяюча гіперплощина

У просторі  $\mathbb{R}^n$  рівняння  $\langle w, x \rangle - b = 0$  при заданих w та b визначає гіперплощину, що розділяє  $\mathbb{R}^n$  на два класи:  $\mathsf{C}_1$  та  $\mathsf{C}_2$ :

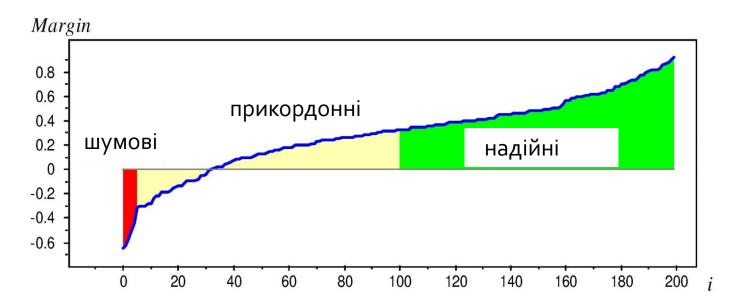


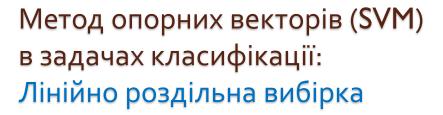
$$\begin{cases} \langle w, x \rangle - b > 0, & \forall x \in C_1 \\ \langle w, x \rangle - b < 0, & \forall x \in C_2 \end{cases}$$
 або 
$$\begin{cases} \langle w, x \rangle - b < 0, & \forall x \in C_1 \\ \langle w, x \rangle - b > 0, & \forall x \in C_2 \end{cases}$$
  $w$  — вектор нормалі до гіперплощини  $\frac{b}{\|w\|}$  — відстань від гіперплощини до початку координат

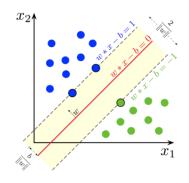
# Метод опорних векторів (SVM) в задачах класифікації: Лінійно роздільна вибірка



**Відступ (Margin)** — характеристика, яка оцінює, наскільки об'єкт «занурений у свій клас, наскільки типовим представником свого класу він є. Чим менше значення відступа  $M_i$ , тим ближче об'єкт  $x_i$  підходе до границі класів і тим вище стає ймовірність помилки. Відступ  $M_i$  від'ємний лише тоді, коли алгоритм класифікації  $a(x_i)$  допускає помилку на об'єкті  $x_i$ .







Для лінійного класифікатора відступ визначається рівнянням:

$$M_i(w, b) = y_i(\langle x_i, w \rangle - b)$$

Для **лінійно роздільної вибірки** існує така гіперплощина, відступ від якої до кожного об'єкта є позитивним:

$$\exists w, b: Mi(w, b) = yi(\langle x_i, w \rangle - b) > 0, \qquad i = 1 \dots \ell$$

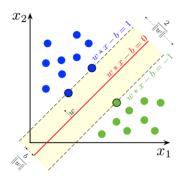
Задача: поюудувати таку розділяючу гіперплощину, щоб об'єкти навчальної вибірки знаходились на найбільшій відстані від неї.

#### Нормування

При множенні w та b на константу  $C \neq 0$  рівняння  $\langle x_i, Cw \rangle - Cb = 0$  визначає ту ж саму гіперплощину, що й  $\langle x_i, w \rangle - b = 0$  .

Для зручності проведемо нормування: оберемо константу C таким чином, щоб  $\min M_i(w,b)=1$ .

### Лінійно роздільна вибірка



В кожному з двох класів нзайдеться хоча б один "граничний" об'єкт навчальної вибірки, відступ якого дорівнює цьому мінімуму: в іншому випадку можна було б змістити гіперплощину в бік класу з більшим відступом, тим самим збільшити мінімальну відстанб від гіперплощини до об'єктів навчальної вибірки.

Позначимо "граничний" об'єкт з класа +1 як  $x_+$  , а з класа -1 як  $x_-$  .

$$x_+$$
:  $\langle x, w \rangle - b = +1$ 

$$x_-$$
:  $\langle x, w \rangle - b = -1$ 

$$M_{+}(w, b) = (+1)(\langle x_{+}, w \rangle - b) = 1$$

$$M_{-}(w,b) = (-1)(\langle x_{-},w\rangle - b) = 1$$

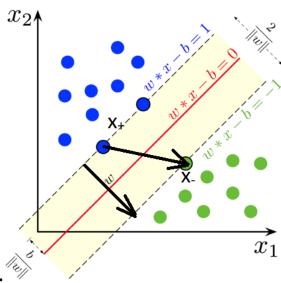
Нормування дозволяє обмежити розділяючу полосу між класами:

$$x: \{-1 < \langle x, w \rangle - b < 1\}$$

Всередині якої не может лежати жоден об'єкт Навчальної вибікри.

Ширина полоси це проекція вектора  $(x_+ - x_-)$  на w:

$$\frac{\langle x_+ - x_-, w \rangle}{\|w\|} = \frac{M_+ + M_-}{\|w\|} = \frac{2}{\|w\|} \to \max \Longrightarrow \|w\| \to \min.$$

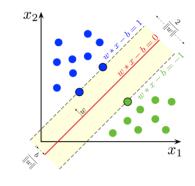


$$||w|| = \langle w, w \rangle -$$
 скалярний добуток

### Лінійно роздільна вибірка

Максимальність ширини розділяючої полоси

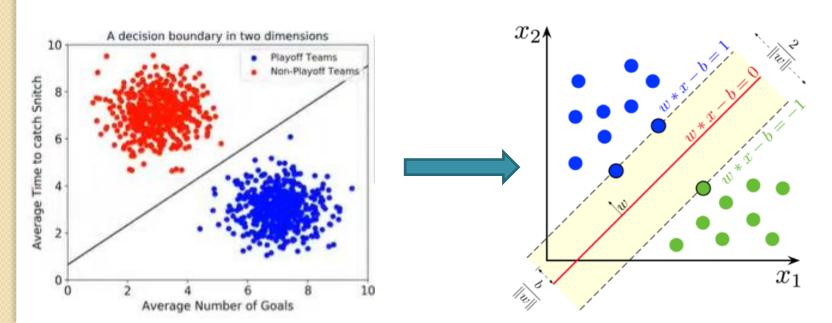
$$\frac{2}{\|w\|} \to \max \Longrightarrow \|w\| \to \min.$$

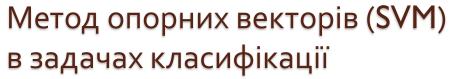


$$||w|| = \langle w, w \rangle -$$
 скалярний добуток

Постановка задачи оптимизации в терминах квадратичного программирования:

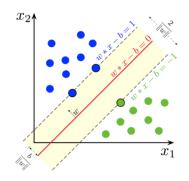
$$\begin{cases} ||w|| \to \min_{w,b} \\ M_i(w,b) \ge 1, \quad i = 1 \dots \ell \end{cases}$$





### Умови Каруша-Кунна-Таккера

задача нелінійного програмування з обмеженнями:

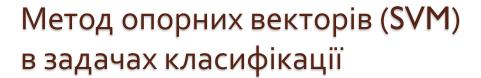


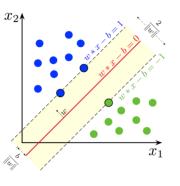
$$\begin{cases} f(x) \to \min_{x \in X} \\ g_i(x) \le 0, & i = 1 \dots m \\ h_j(x) = 0, & j = 1 \dots k \end{cases}$$

Якщо x — точка локального мінімума при накладених обмеженнях, то існують такі множники  $\mu_i$ ,  $i=1\dots m$  та  $\lambda_j$ ,  $j=1\dots k$ , що для функції Лагранжа  $\mathcal{L}(x;\mu,\lambda)$  виконуються умови:

$$\begin{cases} \frac{d\mathcal{L}}{dx} = 0, \mathcal{L}(x; \mu, \lambda) = f(x) + \sum_{i=1}^{m} \mu_{i} g_{i}(x) + \sum_{j=1}^{k} \lambda_{j} h_{j}(x) \\ g_{i}(x) \leq 0, \qquad h_{j}(x) = 0 \qquad \text{(вихідні обмеження)} \\ \mu_{i} \geq 0 \qquad \qquad \text{(двійкові обмеження)} \\ \mu_{i} g_{i}(x) = 0 \qquad \text{(доповнюючі обмеження)} \end{cases}$$

При цьому шукана точка є сідловою точкою функції Лагранжа: мінімумом по x та максимумом по двійковим змінним  $\mu$ .





Для нашої задачі оптимізації:

$$\begin{cases} ||w|| \to \min_{w,b} \\ M_i(w,b) \ge 1, \quad i = 1 \dots \ell \end{cases}$$

За теоремою ККТ маємо Лагранжиан

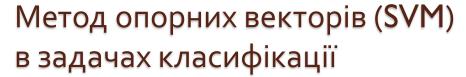
$$\mathcal{L}(w, b, \lambda_1, \dots, \lambda_{\ell}) = \frac{1}{2} \|w\| - \sum_{i=1}^{\ell} \lambda_i \{ y_i(\langle x_i, w \rangle - b) - 1 \}$$

Похідні від Лагранжиану за параметрами

$$\begin{cases} \frac{\partial \mathcal{L}(w,b,\lambda_1,\ldots,\lambda_\ell)}{\partial w} = 0; \\ \frac{\partial \mathcal{L}(w,b,\lambda_1,\ldots,\lambda_\ell)}{\partial b} = 0; \\ \lambda_i \geq 0; \\ \lambda_i = 0 \text{ ago } \{y_i(\langle x_i,w\rangle - b) - 1\} = 0 \end{cases}$$

3 перших двох рівнянь знаходимо:

$$\begin{cases} w = \sum_{i=1}^{\ell} \lambda_i y_i x_i; \\ \sum_{i=1}^{\ell} \lambda_i y_i = 0 \end{cases}$$

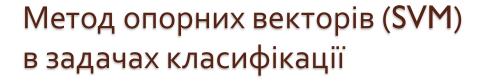


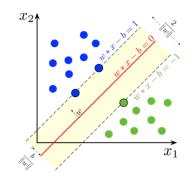
Підставляючи отримані обмеження в функцію Лагранжа отримуємо постановку двійкової задачі, яка залежить лише від двійкових змінних  $\lambda$ :

$$\begin{cases}
\mathcal{L}(\lambda) = \sum_{i=1}^{\ell} \lambda_i - \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j y_i y_j \langle x_i, x_j \rangle \\
0 \le \lambda_i \le C, & i = 1 \dots \ell \\
\sum_{i=1}^{\ell} \lambda_i y_i = 0
\end{cases}$$

$$\mathcal{L}(\lambda) = \sum_{i=1}^{\ell} \lambda_i - \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j y_i y_j \langle x_i, x_j \rangle = \begin{cases}
(H)_{ij} = y_i y_j \langle x_i, x_j \rangle \\
= \sum_{i=1}^{\ell} \lambda_i - \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j (H)_{ij} = \lambda + \frac{1}{2} \lambda^T H \lambda
\end{cases}$$

Це задача квадратичного програмування:





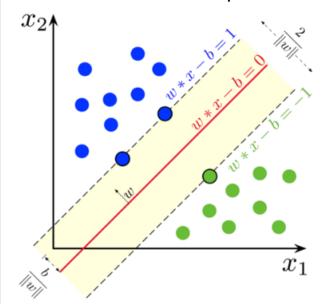
Метод градієнтного спуску:

$$\mathcal{L}(\lambda) = \lambda + \frac{1}{2} \lambda^T H \lambda$$

Невідомі параметри Лагранжа:

$$\boldsymbol{\lambda}^{t+1} = \boldsymbol{\lambda}^t + \eta \, \frac{\partial \mathcal{L}}{\partial \boldsymbol{\lambda}}$$

Навчальна вибірка



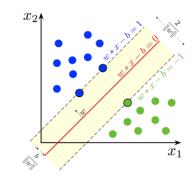
За отриманими  $\lambda_i$  розв'язок прямої задачі:

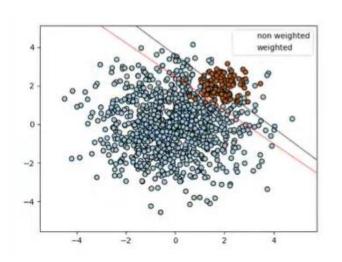
$$\begin{cases} w = \sum_{i=1}^{\ell} \lambda_i y_i x_i; \\ b = \begin{cases} \overline{(\langle w, x_i \rangle - y_i)} \\ med(\langle w, x_i \rangle - y_i) \end{cases} \forall i: \lambda_i > 0, M_i = 1 \end{cases}$$

Лінійний класифікатор

$$a(x) = sign\left(\sum_{i=1}^{\ell} \lambda_i y_i \langle x_i, x \rangle - b\right)$$

# Метод опорних векторів (SVM) в задачах класифікації: Лінійно не роздільна вибірка





В даних можуть бути певні викиди, що приводить до нечітких меж між класами. Необхідно послабити обмеження, дозволяючи де-яким об'єктам попадати в середину розділяючої полоси та на "територію" іншого класу.

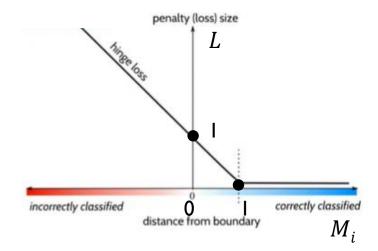
### Відступ

$$M_i(w,b) = yi(\langle x_i, w \rangle - b)$$

Функція втрат (Loss function)

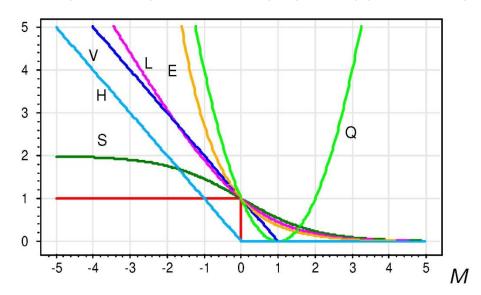
$$L = \max(0, 1 - Mi)$$

Інакше всі помилки рівноправні



# Неперервні апроксимації порогової функції втрат

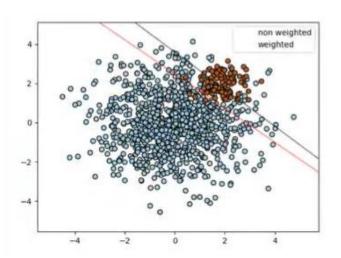
Часто використовувані неперервні функції втрат L(M)

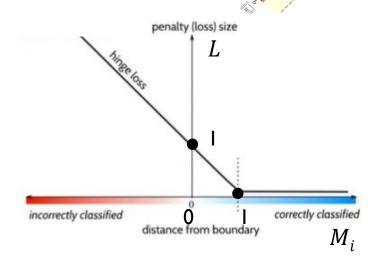


$$V(M) = (1 - M)_{+}$$
 $H(M) = (-M)_{+}$ 
 $L(M) = \log_{2}(1 + e^{-M})$ 
 $Q(M) = (1 - M)^{2}$ 
 $S(M) = 2(1 + e^{M})^{-1}$ 
 $E(M) = e^{-M}$ 
 $[M < 0]$ 

- кусочно-лінійна (SVM);
- кусочно-лінійна (Hebb's rule);
- логарифмічна (LR);
  - квадратична (FLD);
  - сигмоїдна (ANN);
  - експоненціальна (AdaBoost);
  - порогова функція втрат

### Лінійно не роздільна вибірка



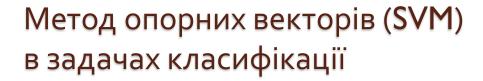


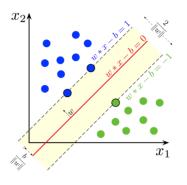
• Для кожного об'єкта віднімемо від відступа позитивну величину  $\xi_i$ , яле будемо вимагати, що ці уведені поправки були мінімальними. Це приведе до задачі, що має назву SVM з м'яким відступом (англ. soft-margin SVM):

$$\begin{cases} \frac{1}{2} ||w|| + C \sum_{i=1}^{\ell} \xi_i \to \min_{w,b,\xi} \\ M_i(w,b) \ge 1 - \xi_i, & i = 1 \dots \ell \\ \xi_i \ge 0, & i = 1 \dots \ell \end{cases}$$

• Еквівалентна задача безумовної мінімізації:

$$\frac{1}{2}||w|| + C\sum_{i=1}^{\ell} (1 - M_i(w, b))_+ \to \min_{w, b}$$





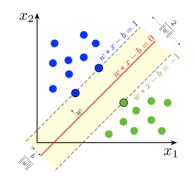
За теоремою Каруша—Куна—Таккера, поставлена задача мінімізації еквівалентна двійковій задачі пошуку сідлової точки функції Лагранжа:

$$\mathcal{L}(w,b,\xi;\lambda,\eta) = \frac{1}{2}\|w\| - \sum\nolimits_{i=1}^{\ell} \lambda_i (M_i(w,b) - 1) - \sum\nolimits_{i=1}^{\ell} \xi_i \left(\lambda_i + \eta_i - C\right)$$

 $\lambda_i$  — змінні, двійкові до обмежень  $M_i \geq 1 - \xi_i$   $\eta_i$  — змінні, двійкові до обмежень  $\xi_i \geq 0$ 

Необхідні умови існування сідлової точки функції Лагранжа:

$$\begin{cases} \frac{d\mathcal{L}}{dw} = 0, & \frac{d\mathcal{L}}{db} = 0, \\ \xi_i \geq 0, & \lambda_i \geq 0, \\ \lambda_i M_i(w,b) = 0 \implies \lambda_i = 0 \text{ afo } M_i(w,b) = 1 - \xi_i, \\ \eta_i \xi_i = 0 \implies \eta_i = 0 \text{ afo } \xi_i = 0, \end{cases} \qquad i = 1 \dots \ell$$



Відступ (margin) об'єкта  $x_i$  від розділяючої гіперплощини :

$$M_i(w, b) = y_i(\langle x_i, w \rangle - b)$$

Функція Лагранжа:

$$\mathcal{L}(w, b, \xi; \lambda, \eta) = \frac{1}{2} \|w\| - \sum_{i=1}^{\ell} \lambda_i (M_i(w, b) - 1) - \sum_{i=1}^{\ell} \xi_i (\lambda_i + \eta_i - C)$$

Необхідні умови існування сідлової точки фугкції Лагранжа:

$$\begin{cases} \frac{d\mathcal{L}}{dw} = w - \sum_{i=1}^{\ell} \lambda_i y_i x_i = 0 \implies w = \sum_{i=1}^{\ell} \lambda_i y_i x_i \\ \frac{d\mathcal{L}}{db} = \sum_{i=1}^{\ell} \lambda_i y_i = 0 \implies \sum_{i=1}^{\ell} \lambda_i y_i = 0 \\ \frac{d\mathcal{L}}{d\xi_i} = -\lambda_i - \eta_i + C = 0 \implies \eta_i + \lambda_i = C, \qquad i = 1 \dots \ell \end{cases}$$

Зауважимо, що  $\eta_i \geq 0$ ,  $\lambda_i \geq 0$ , C > 0, тому, з останнього обмеження отримуємо  $0 \leq \eta_i \leq C$ ,  $0 \leq \lambda_i \leq C$ .

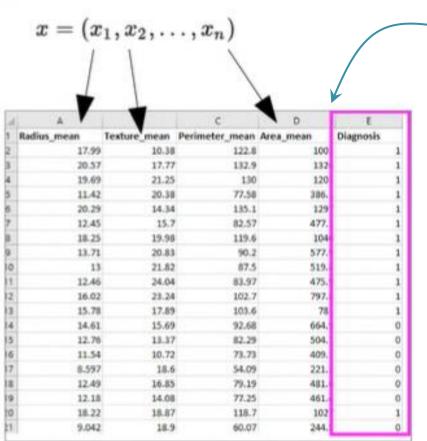
Система умов Каруша-Куна-Таккера:

$$\begin{cases} w = \sum_{i=1}^{\ell} \lambda_i y_i x_i; \sum_{i=1}^{\ell} \lambda_i y_i = 0; & Mi(w, b) \ge 1 - \xi_i \\ \xi_i \ge 0, & \eta_i \ge 0, & \lambda_i \ge 0, & \eta_i + \lambda_i = C \\ \lambda_i M_i(w, b) = 0 \implies \lambda_i = 0 \text{ afo } M_i(w, b) = 1 - \xi_i, & i = 1 \dots \ell \\ \eta_i \xi_i = 0 \implies \eta_i = 0 \text{ afo } \xi_i = 0, & i = 1 \dots \ell \end{cases}$$

Діапазон значень  $\lambda_i$  які відповідають обмеженням на величину відступа дозволяють поділити об'єкти навчальної вибірки на три типи:

- 1.  $\lambda_i = 0 \implies \eta_i = C; \; \xi_i = 0; \; M_i \ge 1$  периферійні (неінформативні) об'єкти: вони знаходяться в своєму класі, класифікуються вірно та не впливають на вибір розділяючої гіперплощини;
- 2.  $0 < \lambda_i < C \implies 0 < \eta_i < C; \ \xi_i = 0; \ M_i = 1$  опорні граничні об'єкти: знаходяться чітко на границі розділяючої полоси на стороні свого класу;
- $\lambda_i = C \implies \eta_i = 0; \; \xi_i > 0; 0 < M_i < 1$  об'єкти-порушники: знаходяться всередині розділяючої полоси;
- 4.  $\lambda_i = C \implies \eta_i = 0; \; \xi_i > 0; \; M_i < 0$  помилки: не вірно класифіковані об'єкти, які знаходяться на боці не свого класу

Перехід до більш зручного опису



$$x_{n+1} = 1; w_0 = -b$$

$$[\langle x_i, w \rangle - b]_{i=1} \xrightarrow{n} [\langle x_i, w \rangle]_{i=1} \xrightarrow{n+1}$$

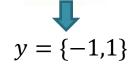
Відступ

$$M_i(w) = yi\langle x_i, w \rangle$$

Задача оптимізації

$$\frac{1}{2}||w|| + C\sum_{i=1}^{\ell} (1 - M_i(w))_+ \to \min_{w}$$

Розв'язується методом градієнтного спуску



### Метод градієнтного спуску в задачах машинного навчання

Функціонал якості  $f(w) \to \min_{w}$ 

$$f(w) = \frac{1}{2} \|w\| + C \frac{1}{\ell} \sum_{i=1}^{\ell} (1 - M_i(w))_+$$

Для всіх об'єктів навчальної вибірки

$$f(w) = \frac{1}{\ell} \sum_{i=1}^{\ell} \left[ \frac{1}{2} \|w\| + C(1 - y_i \langle w, x_i \rangle)_+ \right]$$

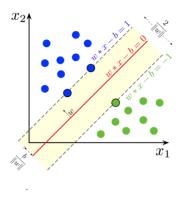
Розрахунок наступного значення ваг w за методом градієнтного спуску:

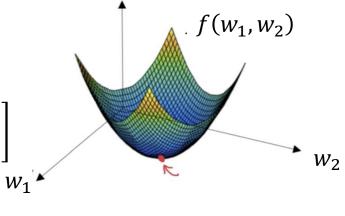
$$w_i = w_i - \eta \frac{1}{\ell} \nabla f(w)$$

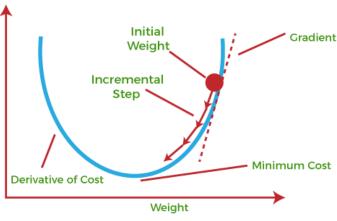
 $\eta$  — крок навчання



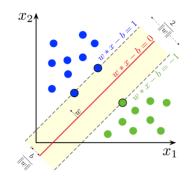
$$\nabla f(w) = \frac{df}{dw} = \frac{1}{\ell} \sum_{i=1}^{\ell} \begin{cases} w, & if \max(1 - y_i \langle w, x_i \rangle)_+ = 0 \\ w - Cy_i x_i, & otherwise \end{cases}$$









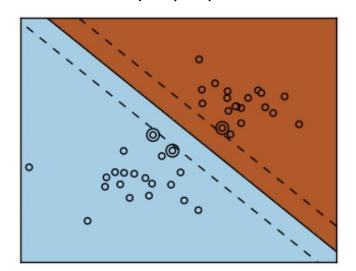


Розрахунок наступного значення ваг w за методом градієнтного спуску

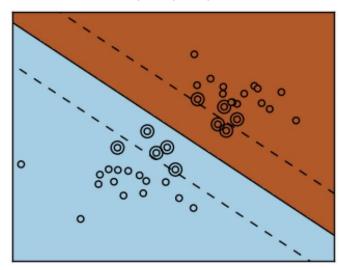
$$w_i = w_i - \eta \frac{1}{\ell} \sum_{i=1}^{\ell} \begin{cases} w, & if \max(1 - y_i \langle w, x_i \rangle)_+ = 0 \\ w - Cy_i x_i, & otherwise \end{cases}$$

Вплив параметра  ${\mathcal C}$ 

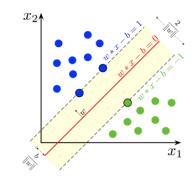
Велике значення параметра C слабка регуляризація



Мале значення параметра C сильна регуляризація



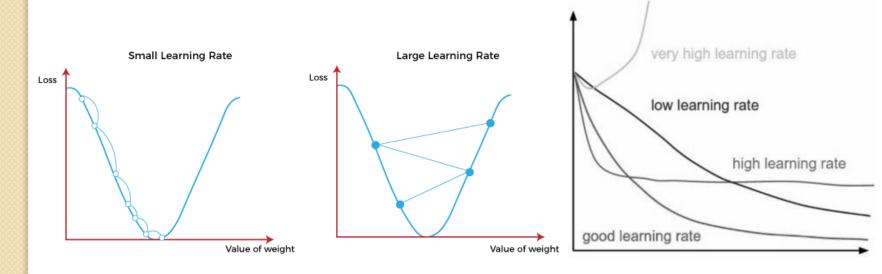




Розрахунок наступного значення вагw за методом градієнтного спуску

$$w_i = w_i - \eta \frac{1}{\ell} \sum_{i=1}^{\ell} \begin{cases} w, & if \max(1 - y_i \langle w, x_i \rangle)_+ = 0 \\ w - Cy_i x_i, & otherwise \end{cases}$$

Вплив швидкості навчання  $\eta$ 



#### Нелінійне узагальнення (kernel trick)

- Для лінійно нероздільної вибірки  $X = \mathbb{R}^n$  існує спрямляючий простір  $\mathcal{H}$  (більшої розмірності) з функцією переходу  $\psi : X \to \mathcal{H}$
- Скалярний добуток  $\langle x_1, x_2 \rangle$  у прострорі X замінінюється скалярним добутком  $\langle \psi(x_1), \psi(x_2) \rangle$  у гільбертовому просторі  $\mathcal H$  з визначеним скалярним добутком.
- Це надає можливість замінити скалярний добуток у просторі X на <u>ядро</u> функцію, що є скалярним добутком у де-якому просторі  $\mathcal{H}$ . Замість підбору  $\psi$  можна підбирати безпосередньо ядро  $K(x_i, x_j) = \langle \psi(x_1), \psi(x_2) \rangle$ .

Постановка задачі з застосуванням ядер приймає вигляд

$$\begin{cases} -\mathcal{L}(\lambda) = -\sum_{i=1}^{\ell} \lambda_i + \frac{1}{2} \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \lambda_i \lambda_j y_i y_j K(x_i, x_j) \to \min_{\lambda} \\ 0 \le \lambda_i \le C, & i = 1 \dots \ell \\ \sum_{i=1}^{\ell} \lambda_i y_i = 0 \end{cases}$$

Лінійний класифікатор з ознаками  $f_i(x) = K(x, x_i)$ :

$$a(x) = sign\left(\sum_{i=1}^{\ell} \lambda_i y_i K(x, x_i)\right)$$

#### Приклади ядер

1. Квадратичне ядро dim  $\mathcal{H} = \frac{1}{2}n(n+1)$ :

$$K(x, x') = \langle x, x' \rangle^2$$

2. Поліноміальне ядро,  $\dim \mathcal{H} = \mathcal{C}_{n+d-1}^d$ :

$$K(x, x') = \langle x, x' \rangle^d$$

Поліноміальне ядро:

$$K(x, x') = (\langle x, x' \rangle + 1)^d$$

Сигноідне ядро:

$$K(x, x') = th(k_1 \langle x, x' \rangle - k_0), \qquad k_0, k_1 > 0$$

5. Гаусове ядро (RBF ядро):

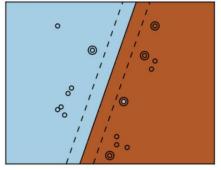
$$K(x, x') = \exp(-\gamma ||x - x'||^2)$$

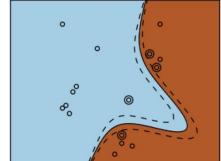
линейное

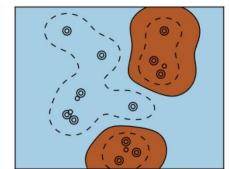
$$\langle x, x' \rangle$$

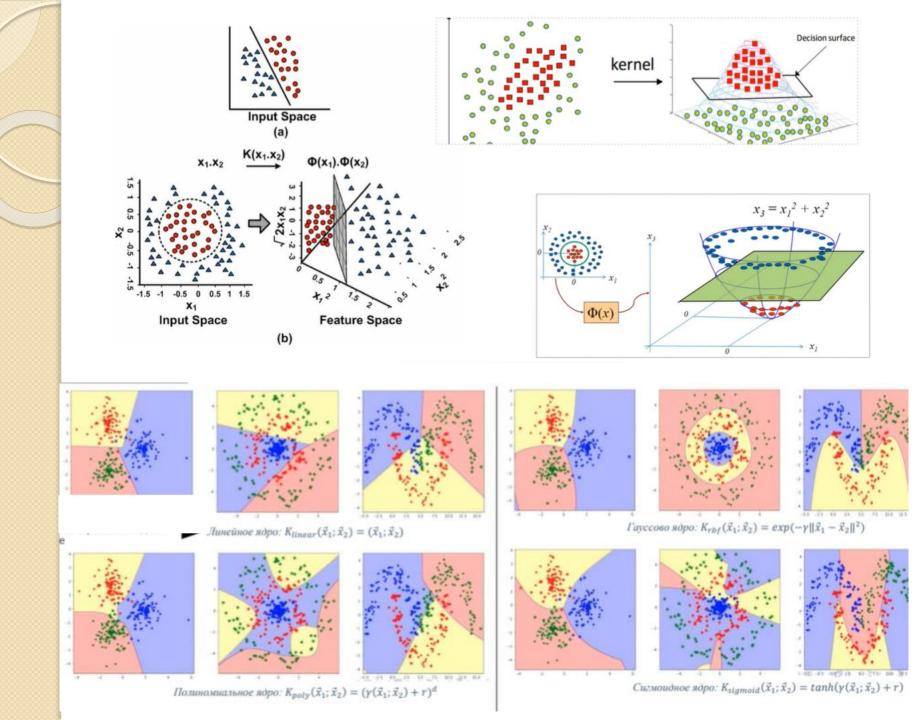
полиномиальное

полиномиальное гауссовское (RBF) 
$$\left(\langle x,x'\rangle+1\right)^d,\ d{=}3$$
  $\exp\left(-\gamma\|x-x'\|^2\right)$ 









### Переваги та недоліки **SVM**

#### Переваги класичного SVM:

- Завдання опуклого квадратичного програмування добре вивчене і має єдине рішення.
- Метод опорних векторів еквівалентний двошарової нейронної мережі, де число нейронів на прихованому шарі визначається автоматично як число опорних векторів.
- Принцип оптимальної роздільної гіперплощини призводить до максимізації ширини смуги, що розділяє, а отже, до більш впевненої класифікації.

#### Недоліки класичного SVM:

- Нестійкість до шуму: викиди у вихідних даних стають опорними об'єктамипорушниками та безпосередньо впливають на побудову роздільної гіперплощини.
- Не описані загальні методи побудови ядер та спрямовуючих просторів, що найбільш підходять для конкретного завдання.
- Немає відбору ознак.
- Необхідно підбирати константу С за допомогою крос-валідації.

### Дякую за увагу