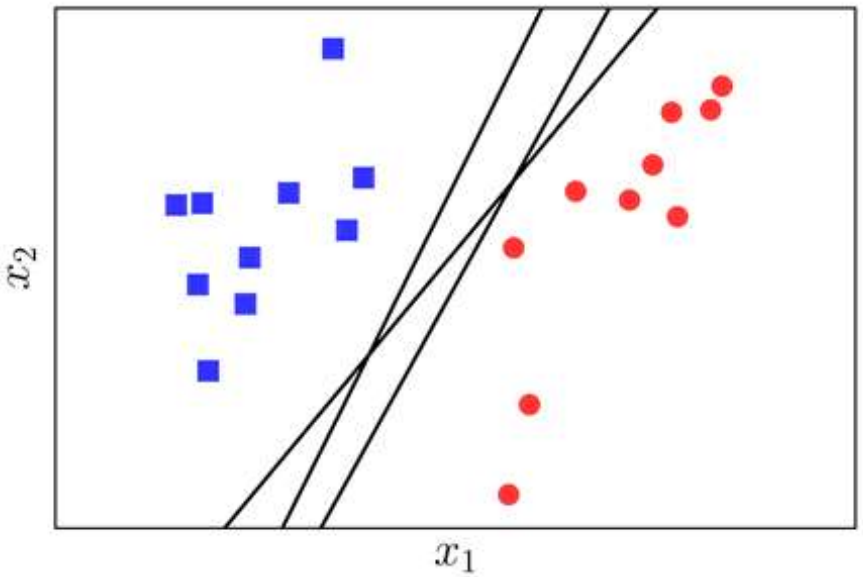
CSE: Faculty of Computer Science and Engineering
Thuyloi University

Máy véc tơ hỗ trợ
(Support vector machine, SVM)

TS. Nguyễn Thị Kim Ngân

Giới thiệu

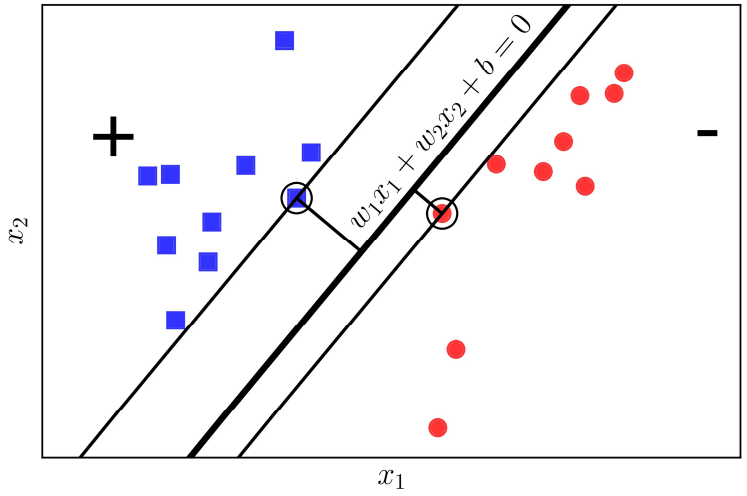
- Bài toán trong PLA: Tìm một siêu phẳng phân chia dữ liệu thành 2 lớp:
  - Tất cả điểm dữ liệu có nhãn 1 thuộc về cùng một phía của siêu phẳng
  - Các điểm dữ liệu khác thuộc về phía còn lại của siêu phẳng
- Thuật toán PLA có thể tìm ra vô số siêu phẳng

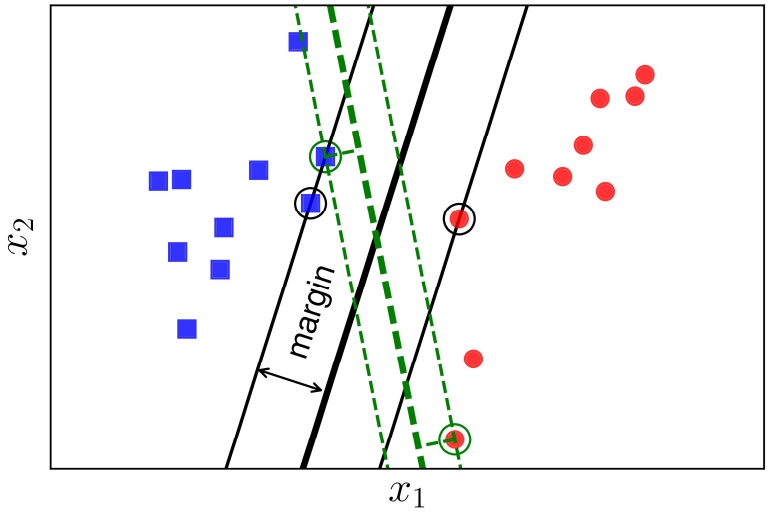


Trong số các siêu phẳng tìm được, siêu phẳng nào là tốt nhất?

Giới thiệu

- Cần tìm một tiêu chuẩn để đo sự *công bằng* của hai class



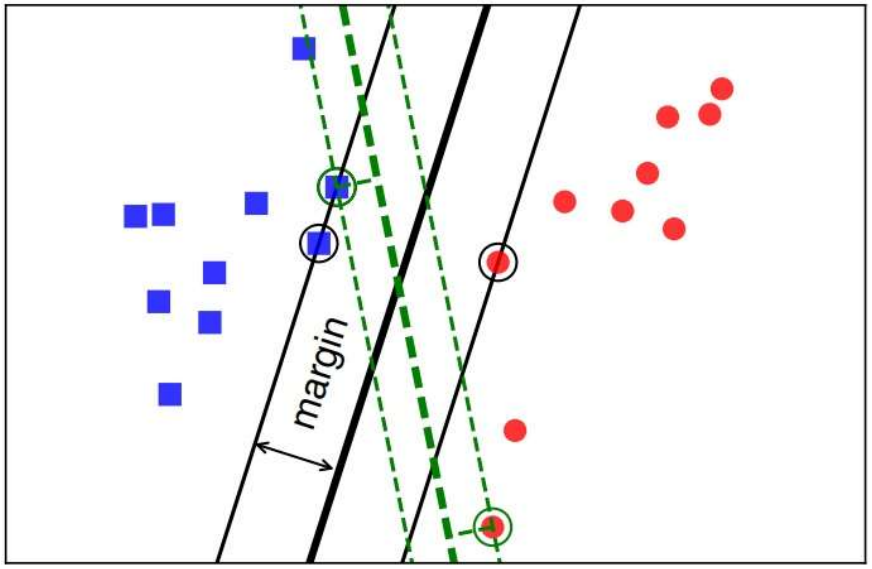


- **Ý tưởng của SVM**: Margin của một siêu phẳng được định nghĩa là khoảng cách từ các điểm gần nhất của lớp đó tới mặt phân chia. Margin của hai lớp phải bằng nhau và lớn nhất có thể

Support Vector Machine

- Cần tìm một đường phân chia sao cho:
  - Khoảng cách từ điểm gần nhất của mỗi lớp tới đường phân chia là như nhau (*margin*, *lề*).
  - Margin này phải là cực đại

- **Bài toán tối ưu trong *Support Vector Machine* (SVM) là tìm đường phân chia sao cho *margin* là lớn nhất** (*Maximum Margin Classifier*)



Độ đo khoảng cách

Khoảng cách từ một điểm tới một siêu mặt phẳng

- Trong không gian 2 chiều, khoảng cách từ một điểm có toạ độ (x_0, y_0) tới *đường thẳng* có phương trình $w_1x + w_2y + b = 0$ được xác định bởi:

$$\frac{|w_1x_0 + w_2y_0 + b|}{\sqrt{w_1^2 + w_2^2}}$$

- Trong không gian ba chiều, khoảng cách từ một điểm có toạ độ (x_0, y_0, z_0) tới một *mặt phẳng* có phương trình $w_1x + w_2y + w_3z + b = 0$ được xác định bởi:

$$\frac{|w_1x_0 + w_2y_0 + w_3z_0 + b|}{\sqrt{w_1^2 + w_2^2 + w_3^2}}$$

Độ đo khoảng cách

Trong không gian d chiều

Khoảng cách từ một điểm $(x_{10}, x_{20}, \ldots, x_{d0})$

tới siêu mặt phẳng $w_1x_1 + w_2x_2 + \cdots + w_dx_d + b = 0$

$$\frac{|w_1x_{10} + w_2x_{20} + \cdots + w_dx_{d0} + b|}{\sqrt{w_1^2 + w_2^2 + \cdots + w_d^2}} = \frac{|\mathbf{w}^T\mathbf{x}_0 + b|}{\|\mathbf{w}\|_2}$$

Trong đó, $x_0 = [x_{10}, x_{20}, \ldots, x_{d0}]^T$, $w = [w_0, w_1, \ldots, w_d]^T$

Dấu của biểu thức

$$\frac{|w_1 x_{10} + w_2 x_{20} + \cdots + w_d x_{d0} + b|}{\sqrt{w_1^2 + w_2^2 + \cdots + w_d^2}} = \frac{|\mathbf{w}^T \mathbf{x}_0 + b|}{\|\mathbf{w}\|_2}$$

- Nếu bỏ dấu trị tuyệt đối ở tử số, ta biết được điểm đó nằm về phía nào của *mặt phẳng* đang xét:
  - Những điểm mang dấu dương nằm về cùng 1 phía
  - Những điểm mang dấu âm nằm về phía còn lại
  - Những điểm nằm trên *măt phẳng* làm cho tử số có giá trị bằng 0, tức khoảng cách bằng 0

Xây dựng bài toán tối ưu cho SVM

- Giả sử rằng các cặp dữ liệu của *training set* là $(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \ldots, (\mathbf{x}_N, y_N)$ với:
  - vector $\mathbf{x}_i \in \mathbf{R}^d$ thể hiện *đầu vào* của một điểm dữ liệu
  - y_i là *nhãn* của điểm dữ liệu đó
  - d là số chiều của dữ liệu
  - N là số điểm dữ liệu
- Giả sử rằng *nhãn* của mỗi điểm dữ liệu được xác định bởi $y_i = 1$ (class 1) hoặc $y_i = -1$ (class 2) giống như trong PLA

Xây dựng bài toán tối ưu cho SVM

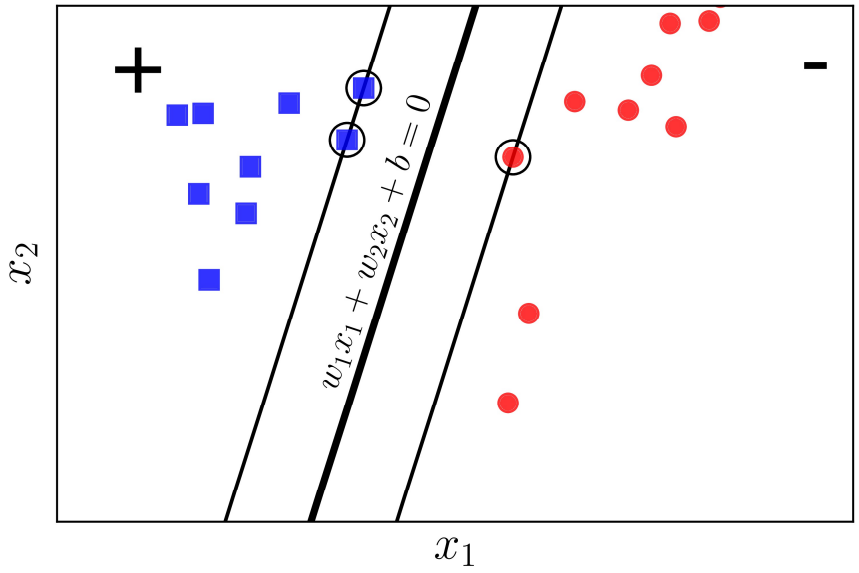
Xét trong không gian hai chiều

- Các điểm vuông xanh thuộc class 1
- Các điểm tròn đỏ thuộc class -1
- Mặt phẳng phân chia giữa hai classes là

$$\mathbf{w}^T\mathbf{x} + b = w_1x_1 + w_2x_2 + b = 0$$

- Class 1 nằm về *phía dương*, class -1 nằm về *phía âm* của mặt phân chia

Ta cần đi tìm các hệ số w và b



Xây dựng bài toán tối ưu cho SVM

- Với cặp dữ liệu $(\mathbf{x}_n, y_n)$ bất kỳ, khoảng cách từ điểm đó tới mặt phân chia là:

$$\frac{y_n(\mathbf{w}^T\mathbf{x}_n + b)}{||\mathbf{w}||_2}$$

- Vì y_n luôn cùng dấu với *phía* của $\mathbf{x}_n$, nên y_n cùng dấu với $(\mathbf{w}^T\mathbf{x}_n + b)$, tử số luôn là 1 số không âm.
- Với mặt phân chia như trên, *margin* được tính là khoảng cách gần nhất từ 1 điểm tới mặt đó: $(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \ldots, (\mathbf{x}_N, y_N)$

$$\text{margin} = \min_n \frac{y_n(\mathbf{w}^T\mathbf{x}_n + b)}{||\mathbf{w}||_2}$$

điểm nào có khoảng cách đến siêu phẳng là nhỏ nhất thì lấy làm margin

Xây dựng bài toán tối ưu cho SVM

- Bài toán tối ưu trong SVM chính là bài toán tìm **w** và b sao cho *margin* này đạt giá trị lớn nhất:

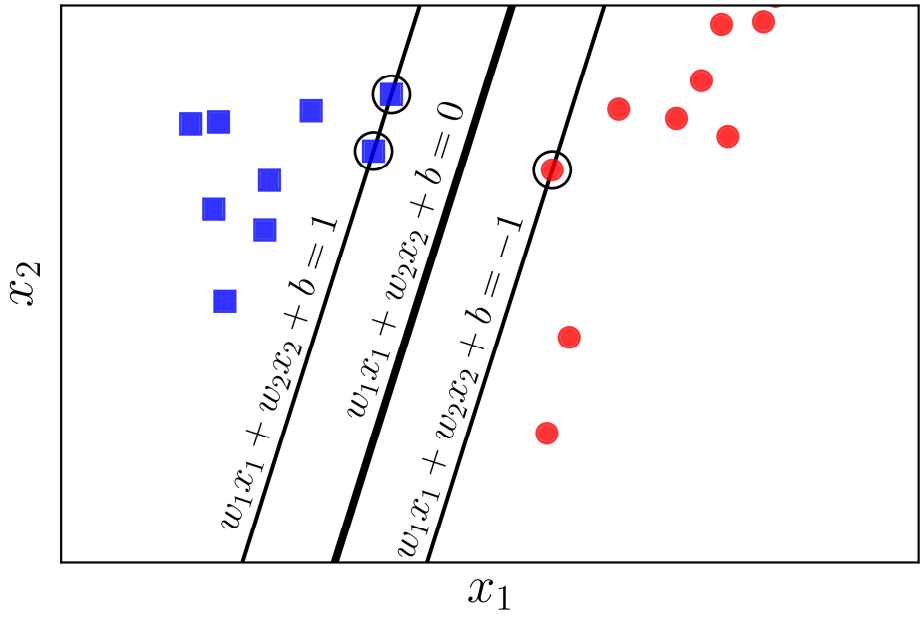
$$(\mathbf{w}, b) = \arg\max_{\mathbf{w},b} \left\{ \min_n \frac{y_n(\mathbf{w}^T\mathbf{x}_n + b)}{||\mathbf{w}||_2} \right\} = \arg\max_{\mathbf{w},b} \left\{ \frac{1}{||\mathbf{w}||_2} \min_n y_n(\mathbf{w}^T\mathbf{x}_n + b) \right\}$$

- Việc giải trực tiếp bài toán này sẽ rất phức tạp, nhưng ta có cách để đưa nó về bài toán đơn giản hơn
- Nhận xét quan trọng nhất là nếu ta thay vector hệ số **w** bởi $k\mathbf{w}$ và b bởi kb trong đó k là một hằng số dương thì mặt phân chia không thay đổi, tức khoảng cách từ từng điểm đến mặt phân chia không đổi, tức *margin* không đổi

Xây dựng bài toán tối ưu cho SVM

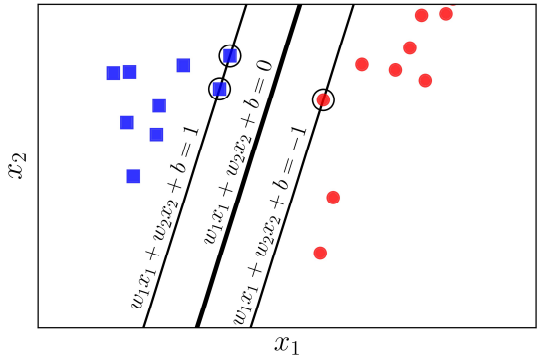
- Dựa trên nhận xét, ta có thể giả sử: $y_n(\mathbf{w}^T\mathbf{x}_n + b) = 1$

với những điểm nằm gần mặt phân chia nhất như Hình:



Xây dựng bài toán tối ưu cho SVM

- Như vậy, với mọi n, ta có: $y_n(\mathbf{w}^T\mathbf{x}_n + b) \geq 1$



- Vậy bài toán tối ưu

$$(\mathbf{w}, b) = \arg\max_{\mathbf{w},b} \left\{ \min_n \frac{y_n(\mathbf{w}^T\mathbf{x}_n + b)}{||\mathbf{w}||_2} \right\} = \arg\max_{\mathbf{w},b} \left\{ \frac{1}{||\mathbf{w}||_2} \min_n y_n(\mathbf{w}^T\mathbf{x}_n + b) \right\}$$

Có thể đưa về bài toán tối ưu có ràng buộc sau đây:

$$(\mathbf{w}, b) = \arg\max_{\mathbf{w},b} \frac{1}{||\mathbf{w}||_2}$$

$$\text{subject to:} \quad y_n(\mathbf{w}^T\mathbf{x}_n + b) \geq 1, \forall n = 1, 2, \ldots, N$$

Xây dựng bài toán tối ưu cho SVM

$$(\mathbf{w}, b) = \arg\max_{\mathbf{w},b} \frac{1}{||\mathbf{w}||_2}$$

$$\text{subject to:} \quad y_n(\mathbf{w}^T\mathbf{x}_n + b) \geq 1, \forall n = 1, 2, \ldots, N$$

- Bằng phép lấy nghịch đảo, bài toán trên chuyển thành:

$$(\mathbf{w}, b) = \arg\min_{\mathbf{w},b} \frac{1}{2}\|\mathbf{w}\|_2^2$$

$$\text{thoả mãn: } 1 - y_n(\mathbf{w}^T\mathbf{x}_n + b) \leq 0, \forall n = 1, 2, \ldots, N$$

Xây dựng bài toán tối ưu cho SVM

$$(\mathbf{w}, b) = \arg\min_{\mathbf{w},b} \frac{1}{2}\|\mathbf{w}\|_2^2$$

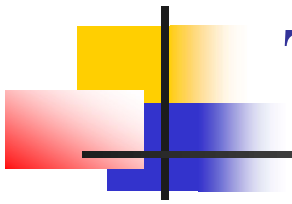
$$\text{thoả mãn: } 1 - y_n(\mathbf{w}^T\mathbf{x}_n + b) \leq 0, \forall n = 1, 2, \ldots, N$$

- Bài toán tối ưu này là bài toán lồi, và là một quadratic programming (phương trình bậc 2)
- Suy ra nghiệm cho SVM là *duy nhất*
- Để giải bài toán này, người ta thường giải bài toán đối ngẫu Lagrange

Xác định lớp cho một điểm dữ liệu mới

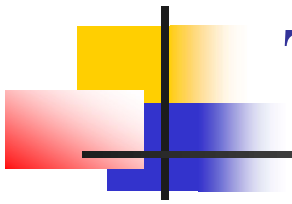
- Sau khi đã tìm được mặt phân cách $w^T x + b = 0$
- Nhãn của bất kỳ một điểm được xác định bằng $class(x) = sgn(w^T x + b)$

nếu có gt > thì gán nhãn là 1 còn k thì gán nhãn -1



Tóm tắt

- Với bài toán binary classification mà 2 classes là *linearly separable*, có vô số các siêu mặt phẳng giúp phân biệt hai classes:
  - Với mỗi mặt phân cách, ta có một *classifier*
  - Khoảng cách gần nhất từ 1 điểm dữ liệu tới mặt phân cách ấy được gọi là *margin* của classifier đó.
- Support Vector Machine là bài toán đi tìm mặt phân cách sao cho *margin* tìm được là lớn nhất, đồng nghĩa với việc các điểm dữ liệu *an toàn nhất* so với mặt phân cách
- Bài toán tối ưu trong SVM là một bài toán hoàn toàn lồi (*strictly convex)* bậc 2. Nghiệm của bài toán này là duy nhất



Tóm tắt

- Mặc dù có thể trực tiếp giải SVM qua bài toán tối ưu gốc này, thông thường người ta thường giải bài toán đối ngẫu.
- Bài toán đối ngẫu cũng là một QP nhưng nghiệm là *sparse* nên có những phương pháp giải hiệu quả hơn.
- Với các bài toán mà dữ liệu *gần linearly separable* hoặc *nonlinear separable*, có những cải tiến khác của SVM để thích nghi với dữ liệu đó.