Máquinas de Vectores de Soporte (SVM)

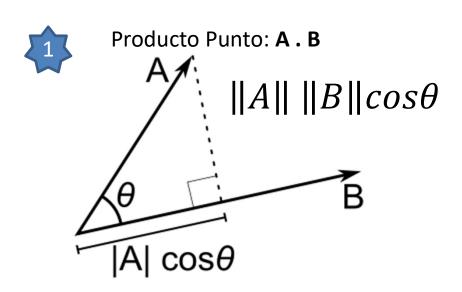
Agenda

- Antecedentes
 - Conceptos geométricos
 - Algoritmo simple de clasificación
 - Aprendizaje estadístico
- Máquinas de Vectores de Soporte
 - Retrato Generalizado.
 - SVM.
 - Lineal
 - No-lineal
 - Con Ruido
- Discusión



B. Schölkopf, A. Smola (2002). *Learning with Kernels: SVM, Regularization, Optimization, and Beyond*. MIT Press.

Repaso de algunos conceptos geométricos





Vector unitario

$$\widehat{x} = \frac{x}{\|x\|}$$



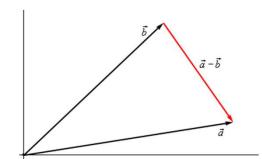
Distancia entre vectores

$$d = ||a - b||$$



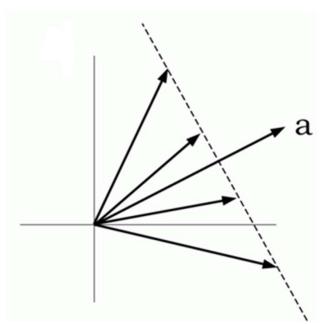
Magnitud de un vector x

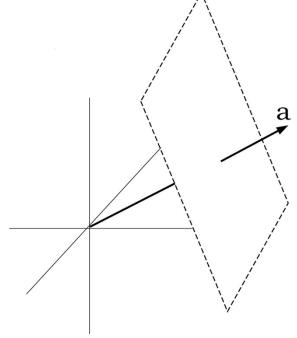
$$||x|| = \sqrt{\langle x, x \rangle} = \sqrt{x_1^2 + x_2^2 + \dots + x_N^2}$$



Definición geométrica de un Hiperplano

 $\{x \in H | \langle w, x \rangle + b = 0\}$ $x \in H, b \in \mathbb{R}$

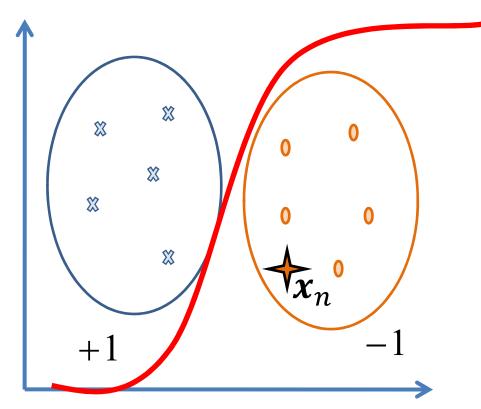




Dado un problema de clasificación binaria ...

$$(x_1, y_1), (x_2, y_2), ..., (x_m, y_m)$$

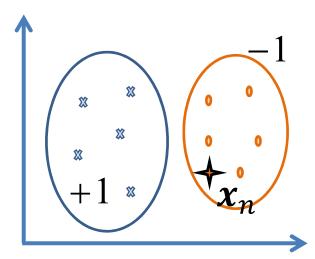
 $x \in \mathbb{R}^N, y \in \{\pm 1\}$



¿Cómo podemos asignar cada nuevo patrón a la clase a la que pertenece?

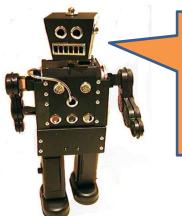


Encontremos una superficie de decisión!!



$$(x_1, y_1), (x_2, y_2),..., (x_m, y_m)$$

 $x \in \mathbb{R}^N, y \in \{\pm 1\}$



Para elegir la clase de (x_n, y_n) , necesitamos una medida de similitud con \mathcal{X} , y designar la clase respecto a las muestras más similares.

$$k: \mathcal{X} \times \mathcal{X} \to \mathbb{R}$$

$$(x_i, x_j) \to k(x_i, x_j)$$

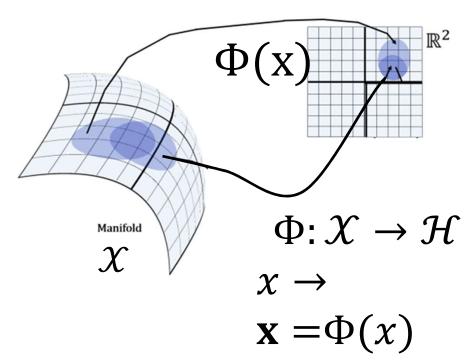
$$k(x_i, x_j) = k(x_j, x_i)$$

Función Kernel

$$\langle x_i, x_j
angle = \sum_{s=1}^N x_s^i \cdot x_s^j$$
 $||x||$ El producto punto es una función kernel

La función de similitud solo funciona en un espacio Hilbert

Espacio de Características



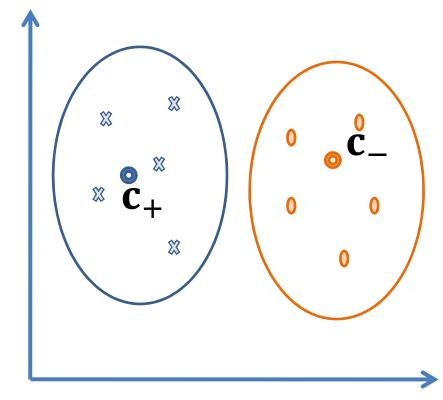
- 1. Medida de Similitud en \mathcal{H} $k(x_i, x_j) = \langle x_i, x_j \rangle = \langle \Phi(x_i), \Phi(x_j) \rangle$
- 2. Análisis Geométrico usando algebra lineal y geometría analítica.
- 3. El producto punto, es un caso especial de Φ . Por lo que es posible realizar un análisis no-lineal.

Un algoritmo simple para clasificación binaria (2)

Paso 1: Calcular las medias de las dos clases

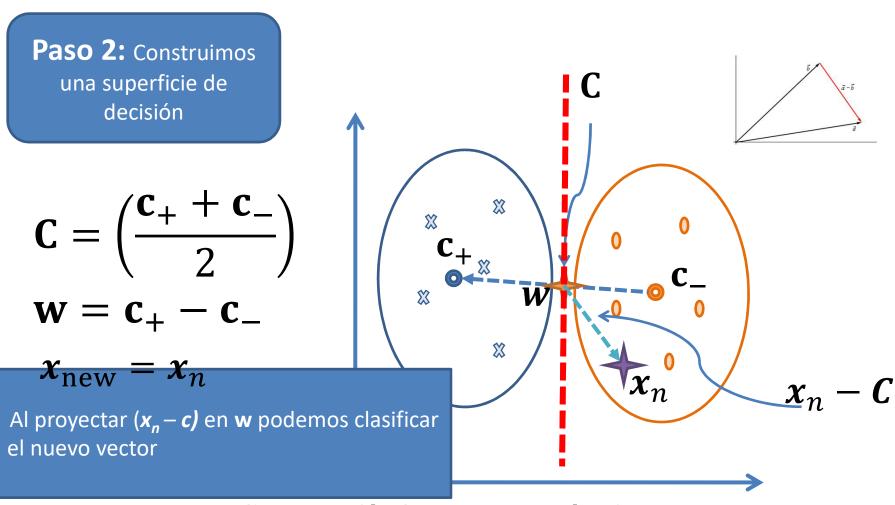
$$c_{+} = \frac{1}{m_{+}} \sum_{\{i \mid y_{i} = +1\}} x_{i}$$

$$c_{-} = \frac{1}{m_{-}} \sum_{\{i \mid y_{i} = -1\}} x_{i}$$



 $m_+, m_- \#$ de elementos de la clase + 1 y - 1 respectivamente

Un algoritmo simple para clasificación binaria (3)



Construcción formulada en términos del producto punto

Un algoritmo simple para clasificación binaria (4)

Paso 3: Para un x_n calculamos la clase al proyectar x_n - c en w

$$y = sgn(\langle \mathbf{x}_n - \mathbf{C}, \mathbf{w} \rangle)$$

¿Cómo?

Un algoritmo simple para clasificación binaria (4)

Paso 3: Para un x_n calculamos la clase al proyectar x_n - c en w

$$y = sgn(\langle \mathbf{x}_{n} - \mathbf{C}, \mathbf{w} \rangle)$$

$$= sgn(\langle \mathbf{x}_{n}, \mathbf{w} \rangle - \langle \mathbf{C}, \mathbf{w} \rangle)$$

$$= sgn(\langle \mathbf{x}_{n}, (\mathbf{c}_{+} - \mathbf{c}_{-}) \rangle - \langle \mathbf{C}, (\mathbf{c}_{+} - \mathbf{c}_{-}) \rangle)$$

$$= sgn(\langle \mathbf{x}_{n}, \mathbf{c}_{+} \rangle - \langle \mathbf{x}_{n}, \mathbf{c}_{-} \rangle - \langle \mathbf{C}, (\mathbf{c}_{+} - \mathbf{c}_{-}) \rangle)$$

$$= sgn(\langle \mathbf{x}_{n}, \mathbf{c}_{+} \rangle - \langle \mathbf{x}_{n}, \mathbf{c}_{-} \rangle - \langle (\frac{\mathbf{c}_{+} + \mathbf{c}_{-}}{2}), (\mathbf{c}_{+} - \mathbf{c}_{-}) \rangle)$$

$$= sgn(\langle \mathbf{x}_{n}, \mathbf{c}_{+} \rangle - \langle \mathbf{x}_{n}, \mathbf{c}_{-} \rangle - \langle (\frac{\mathbf{c}_{+} + \mathbf{c}_{-}}{2}), (\mathbf{c}_{+} - \mathbf{c}_{-}) \rangle)$$

Un algoritmo simple para clasificación binaria (4)

Paso 3: Para un x_n calculamos la clase al proyectar x_n - c en w

$$y_n = sgn(\langle \mathbf{x}_n, \mathbf{c}_+ \rangle - \langle \mathbf{x}_n, \mathbf{c}_- \rangle + b)$$

$$= sgn\left(\langle \mathbf{x}_{n}, \mathbf{c}_{+} \rangle - \langle \mathbf{x}_{n}, \mathbf{c}_{-} \rangle - \left\langle \left(\frac{\mathbf{c}_{+}}{2} + \frac{\mathbf{c}_{-}}{2}\right), (\mathbf{c}_{+} - \mathbf{c}_{-})\right\rangle\right)$$

$$b = -\left\langle \left(\frac{\mathbf{c}_{+}}{2} + \frac{\mathbf{c}_{-}}{2}\right), (\mathbf{c}_{+} - \mathbf{c}_{-})\right\rangle$$

$$b = -\frac{1}{2}\langle \mathbf{c}_{+}, \mathbf{c}_{+} \rangle - \frac{1}{2}\langle \mathbf{c}_{-}, \mathbf{c}_{+} \rangle + \frac{1}{2}\langle \mathbf{c}_{+}, \mathbf{c}_{-} \rangle + \frac{1}{2}\langle \mathbf{c}_{-}, \mathbf{c}_{-} \rangle$$

$$b = -\frac{1}{2}\langle \mathbf{c}_{+}, \mathbf{c}_{+} \rangle + \frac{1}{2}\langle \mathbf{c}_{-}, \mathbf{c}_{-} \rangle$$
Si las medias de cada clase tienen la misma norma, $b \to 0$

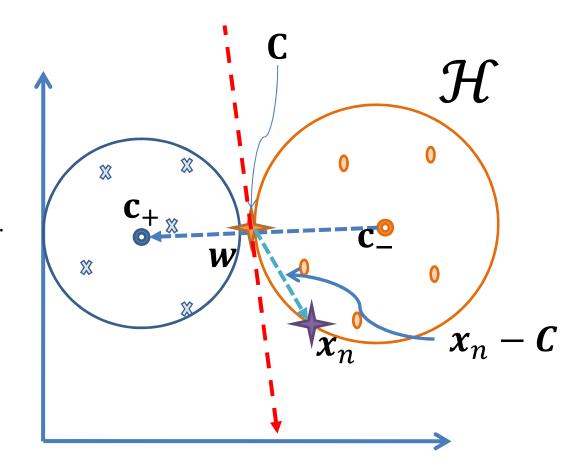
Límite de Decisión

$$y_n = sgn(\langle \mathbf{x}_n, \mathbf{c}_+ \rangle - \langle \mathbf{x}_n, \mathbf{c}_- \rangle + b)$$

Esta función también define un Hiperplano:

$$\{x \in H | \langle w, x \rangle + b = 0\}$$
$$x \in H, b \in \mathbb{R}$$

Un nuevo vector \mathbf{x}_n es clasificado como +1 o -1 si: El vector $\mathbf{x}_n - C$ que conecta a C con \mathbf{x}_n , tiene un ángulo $\leq \frac{\pi}{2}$ con \mathbf{w}_i . En la función del hiperplano, lo anterior corresponde a un cambio de signo.



Reescribamos el problema, es decir, **c** y w en términos de $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m$ y k.

$$y_n = sgn(\langle \mathbf{x}_n, \mathbf{c}_+ \rangle - \langle \mathbf{x}_n, \mathbf{c}_- \rangle + b)$$

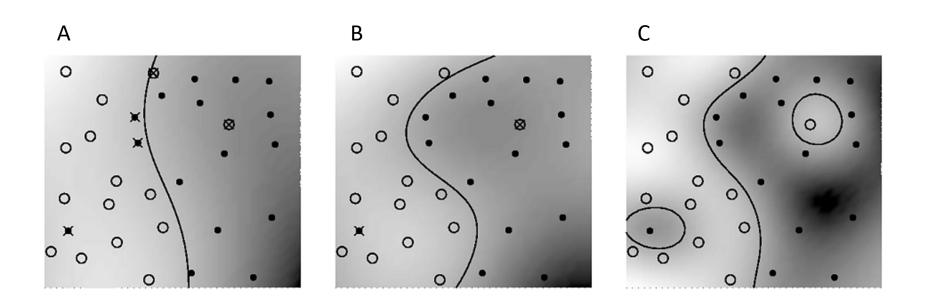
$$y_{n} = sgn\left(\frac{1}{m_{+}}\sum_{\{i|y_{i}=+1\}}\langle \mathbf{x}_{n}, \mathbf{x}_{i}\rangle - \frac{1}{m_{-}}\sum_{\{i|y_{i}=-1\}}\langle \mathbf{x}_{n}, \mathbf{x}_{i}\rangle + b\right)$$

$$y_{n} = sgn\left(\frac{1}{m_{+}}\sum_{\{i|y_{i}=+1\}}k(\mathbf{x}_{n}, \mathbf{x}_{i}) - \frac{1}{m_{-}}\sum_{\{i|y_{i}=-1\}}k(\mathbf{x}_{n}, \mathbf{x}_{i}) + b\right)$$

$$b = \frac{1}{2}\left(\frac{1}{m_{-}^{2}}\sum_{\{(i,j)|y_{i}=y_{j}=-1\}}k(\mathbf{x}_{i}, \mathbf{x}_{j}) - \frac{1}{m_{+}^{2}}\sum_{\{(i,j)|y_{i}=y_{j}=+1\}}k(\mathbf{x}_{i}, \mathbf{x}_{j})\right)$$

Observe que, si las medias de las clases tienen la misma distancia al origen $b \rightarrow 0$.

Tres clasificadores en 2-D



Buscamos $f: \mathcal{X} \to \{\pm 1\}$

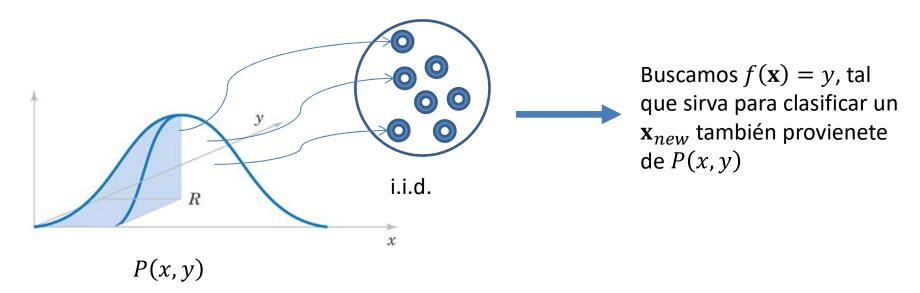
En lugar de graficar f_1 , f_2 y f_3 , solo se muestran las superficies de decisión.

Pregunta: ¿Cuál clasificador es mejor con los datos de entrenamiento? ¿Cuál será mejor con datos nuevos?

Objetivos del Aprendizaje Estadístico (SL)

Incorporar estos argumentos "intuitivos" en un marco formal, a través de las propiedades de f.

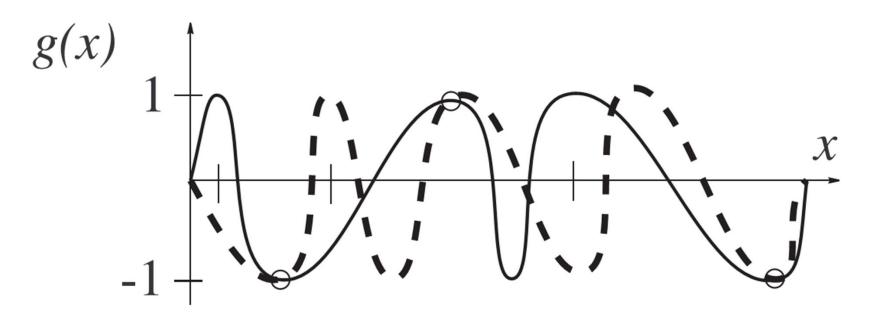
Dados (\mathbf{x}_i, y_i) provenientes de P(x, y)



La precisión de <u>clasificación</u> de f es medida con la <u>función</u> <u>de pérdida</u> (i.e. riesgo, error, etc.) *cero-uno*:

$$c(\mathbf{x}, y, f(\mathbf{x})) = \frac{1}{2}|f(\mathbf{x}) - y|$$
 ¿Qué valores toma esta Función de pérdida?

Pero, ¿qué pasa si solo minimizamos la función de pérdida?



¿Qué función es preferible?, ¿Por qué?, ¿Es suficiente minimizar el error?

No es suficiente minimizar en promedio el Riesgo Empírico

Minimizar el Riesgo empírico (ERM)

$$R_{emp}[f] = \frac{1}{m} \sum_{i=1}^{m} \frac{1}{2} |f(\mathbf{x}) - y| \qquad c(\mathbf{x}, y, f(\mathbf{x})) = \frac{1}{2} |f(\mathbf{x}) - y|$$

No implica minimizar el <u>riesgo verdadero</u> sobre una muestra de prueba también proveniente de P(x, y)

$$R[f] = \frac{1}{m} \int \frac{1}{2} |f(x) - y| dP(x, y)$$

$$R[f] \text{ no se puede evaluar}$$

La ERM obtiene f óptima cuando el problema esta **bien planteado**(well-posed)

- Un problema esta bien-planteado si la solución:
 - Existe
 - Es única
 - Es consistente. Es decir, conforme la cantidad de datos n → ∞ los parámetros θ de f convergen.



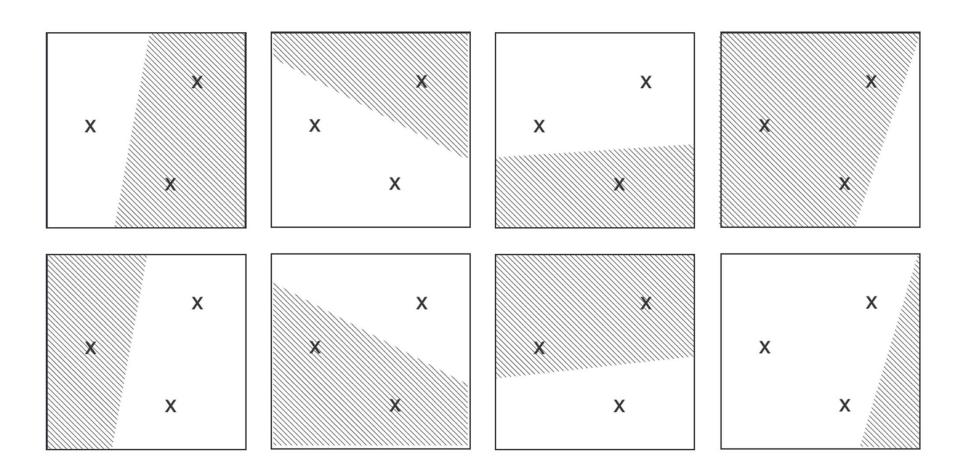
Riesgo Estructural

- SL o Teoría de Vapnik-Chervonenkis (VC) establecen que:
 - Se debe restringir la <u>CAPACIDAD</u> de f de acuerdo a los datos disponibles.
- SL provee <u>LIMITES</u> sobre los errores de prueba los cuales dependen:
 - $-R_{emp}[f]$ Capacidad de fMinimización del Riesgo Estructural

La dimensión VC como medida de Capacidad de f

- Para cada $f_i \in F$ los datos son separados de forma específica \therefore el etiquetando también es de forma específica. Además, si $y \in \{\pm 1\}$ existen 2^m diferentes formas de etiquetar los datos.
- La <u>capacidad</u> es una medida del número de puntos que *F* puede separar.
- Si F es muy rica, podrá obtener las 2^m separaciones. En otras palabras, F <u>puede "romper" los m puntos</u>. Sin embargo, usualmente puede representar menos separaciones.
- La dimensión VC es: $VC(F) = \begin{cases} m & \text{máximo } \# m \text{ que } F \text{ puede romper} \\ \infty & \text{Si no existe } m \end{cases}$

$$f_i \in F$$



¿Cuál es la dimensión VC de F?, ¿Por qué?

Apreciad los resultados de la Teoría VC

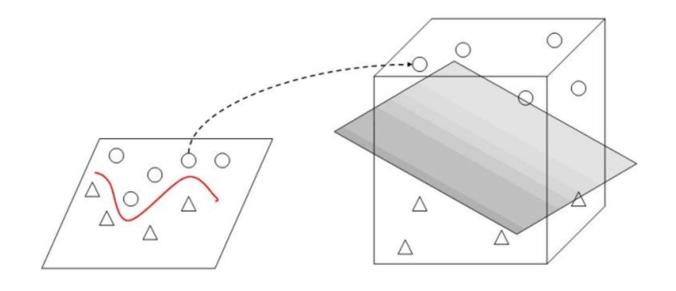
- Si h < m es la dimensión VC de F
 - Entonces, para $f_i \in F | \forall i$
 - Independientemente de P(x, y)
 - Con una probabilidad de al menos $1-\delta$ sobre la muestra de entrenamiento

Entonces:

$$R[f] \le R_{emp}[f] + \phi(h, m, \delta)$$

Tal que ϕ (Término de Confianza o Capacidad) se define como:

$$\phi(h, m, \delta) = \sqrt{\frac{1}{m} \left(h \left(\ln \frac{2m}{h} + 1 \right) + \ln \left(\frac{4}{\delta} \right) \right)}$$



SUPPORT VECTOR MACHINES

Retrato Generalizado (1)

 Propuesto por Vapnik, 1963, asume separación Lineal. Esta basado en 2 supuestos:

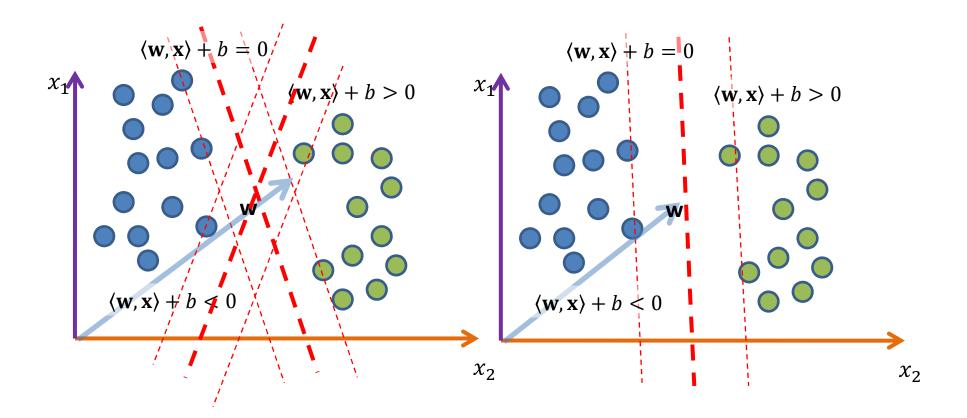
 Entre todos los hiperplanos que separan los datos, existe un único hiperplano óptimo que se distingue por tener el máximo margen de separación entre las clases

Maximizar min.
$$\|\mathbf{x} - \mathbf{x}_i\|$$
 $\mathbf{x} \in \mathcal{H}, \mathbf{b} \in \mathbb{R}$

Sujeto a
$$\mathbf{x} \in \mathcal{H}$$
 $\langle \mathbf{w}, \mathbf{x} \rangle + b = 0, \forall i = i, ..., m.$

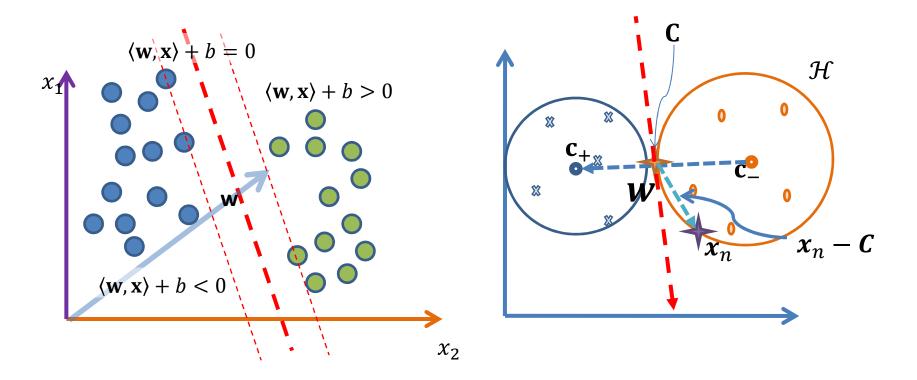
Retrato Generalizado (2)

2. La capacidad de la clase F de hiperplanos, decrece conforme el margen crece.



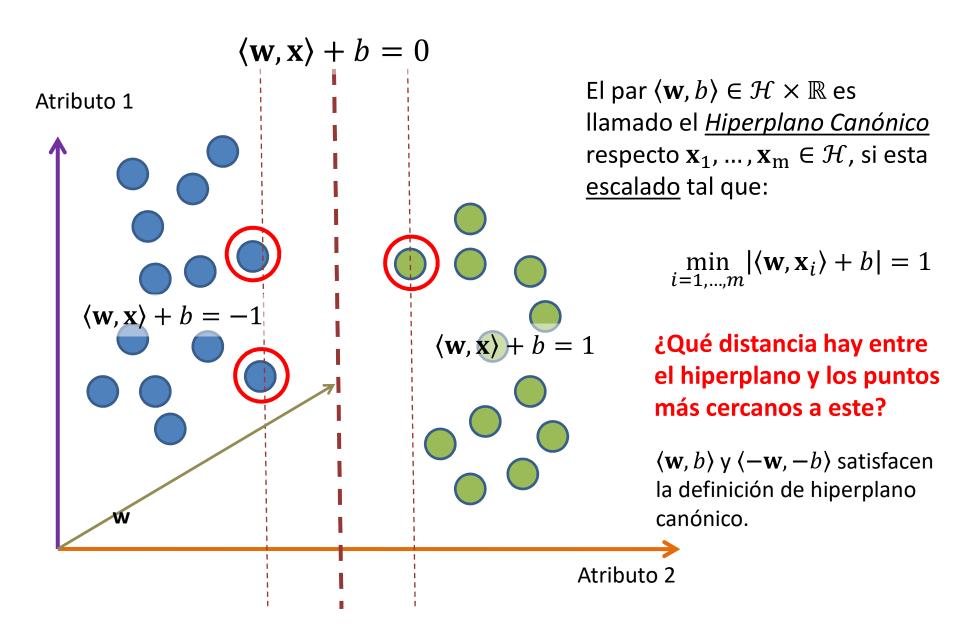
La superficie de decisión es prácticamente la misma que la del algoritmo simple

$$f(\mathbf{x}) = sgn(\langle \mathbf{w}, \mathbf{x} \rangle + b) \qquad y_n = sgn(\langle \mathbf{x}_n, \mathbf{c}_+ \rangle - \langle \mathbf{x}_n, \mathbf{c}_- \rangle + b)$$



La diferencia es como estimamos w.

Definición: Hiperplano canónico



$$\langle \mathbf{w}, b \rangle y \langle -\mathbf{w}, -b \rangle$$

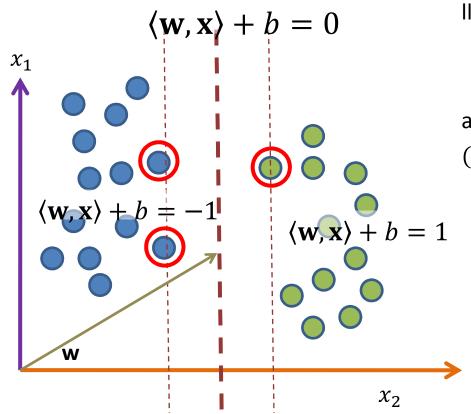
 Estas 2 tuplas forman dos superficies de decisión:

$$f_{\mathbf{w},b} \colon \mathcal{H} \to \{\pm 1\}$$

$$\mathbf{x} \mapsto f(\mathbf{x}) = sgn(\langle \mathbf{w}, \mathbf{x} \rangle + b)$$

• Si para cada $\mathbf{x}_i \exists y_i$, los planos definidos por $f_{\mathbf{w},b}$ realizan asignaciones de clase opuestas.

Definición: Margen geométrico



Dado el hiperplano $\{\mathbf{x} \in \mathcal{H} | \langle \mathbf{w}, \mathbf{x} \rangle + b = 0\}$ Ilamamos

$$\rho_{(\mathbf{w},b)} = \frac{y(\langle \mathbf{w}, \mathbf{x} \rangle + b)}{\|\mathbf{w}\|}$$

al margen geométrico del punto

$$(\mathbf{x}, y) \in \mathcal{H} \times \{\pm 1\}$$
.

Y el valor mínimo

$$P_{(\mathbf{w},b)} = \min_{i=1,\dots,m} \rho_{(\mathbf{w},b)}(\mathbf{x}_i, y_i)$$

es <u>el margen geométrico del conjunto de</u> <u>entrenamiento</u> $(\mathbf{x_i}, y_i)$, $\forall i = 1, ..., m$.

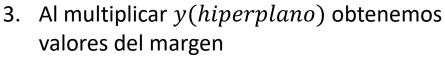
¿Qué distancia hay entre el hiperplano y los puntos más cercanos a este?

¿Qué relación existe entre minimizar w y una buena clasificación?

- 1. Para un punto (\mathbf{x}_i, y_i) bien clasificado, ρ es la distancia al hiperplano. $\rho = 0$ si \mathbf{x} esta sobre el hiperplano.
- 2. Trabajamos con el hiperplano normalizado

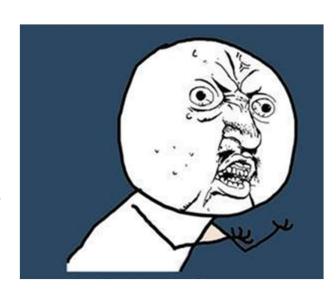
$$\left(\widehat{\mathbf{w}}, \widehat{b}\right) = \left(\frac{\mathbf{w}}{\|\mathbf{w}\|}, \frac{b}{\|\mathbf{w}\|}\right) \operatorname{con} \frac{\mathbf{w}}{\|\mathbf{w}\|} = 1 \text{ y}$$
 solo debemos calcular $y\left(\langle \widehat{\mathbf{w}}, \mathbf{x}_i \rangle + \widehat{b}\right)$.

 $\langle \hat{\mathbf{w}}, \mathbf{x}_i \rangle$ calcula $\mathbf{x}_i \perp$ hiperplano, y al sumar \hat{b} tenemos la distancia al hiperplano.



- + si esta bien clasificado el punto
- de otra forma.

Al minimizar **w** maximizamos la distancia entre las clases, *ergo*, la mejor clasificación posible dado el conjunto de entrenamiento



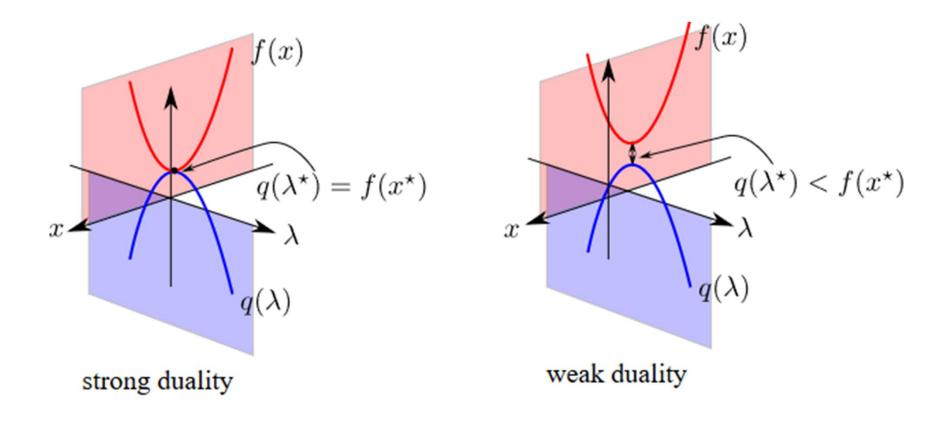
Formulación primal de SVM

$$\operatorname{Min} \tau(w) = \frac{1}{2} \|w\|^2$$

Sujeto a

$$y_i(\langle \vec{x}_i, \vec{w} \rangle + b) \ge 1, \forall i = 1, \dots, m$$

Optimización, Primal y Dualidad.



Hacia la formulación dual de SVM

- τ(w) es la función objetivo
- y_i(<w,x_i>+b)≥1 son las restricción de desigualdad.
- Utilizando los multiplicadores de Lagrange α_i
 ≥0 podemos construir el lagrangeano:

$$L(\vec{w},b,\alpha) = \frac{1}{2} ||w||^2 - \sum_{i=1}^{m} \alpha_i (y_i(\langle \vec{x}_i, \vec{w} \rangle + b) - 1)$$

Hacia la formulación dual de SVM

- 1. <u>Minimizar</u> con respecto a las variables *primales* w y b
- 2. Maximizar con respecto a las variables duales $\alpha_{\rm i}$
- Para obtener la solución debemos derivar L con respecto a las variables primales:

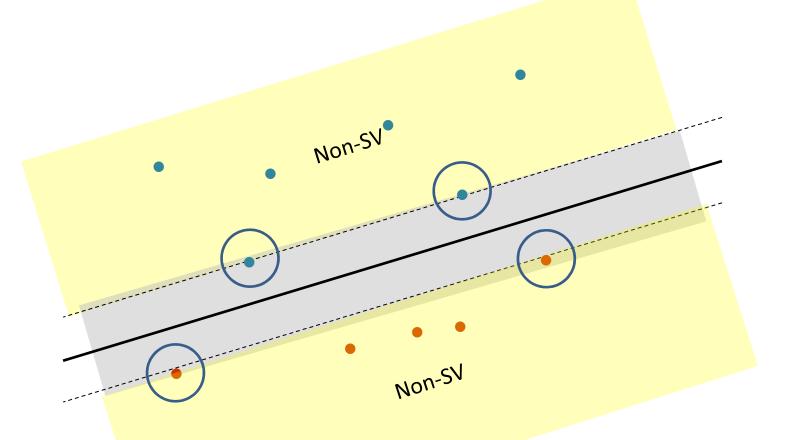
$$\frac{\partial L}{\partial b}(w, b, \alpha) = 0 \qquad \qquad \frac{\partial L}{\partial w}(w, b, \alpha) = 0$$

Condiciones de Optimalidad KKT

$$\frac{\partial L(\mathbf{w}, b, \alpha)}{\partial \mathbf{w}} = \mathbf{w} - \sum_{i=1}^{N} \alpha_i y_i \mathbf{x}_i = 0$$
 Expressados como una combinación lineal del conjunto de entrenamiento
$$\frac{\partial L(\mathbf{w}, b, \alpha)}{\partial b} = \sum_{i=1}^{N} \alpha_i y_i = 0$$

 $KKT \ cond : \alpha_i[y_i(\mathbf{w}\mathbf{x}_i + b) - 1] = 0$ \rightarrow Únicamente los SVs tendrán un ∞_i mayor a cero

¿Qué significado tienen las variables duales?



Indican cuales son los Vectores de Soporte

Formulación Dual de SVM

 Substituyendo las derivadas en el lagrangeano obtenemos la formulación Dual del P.O.:

maximizar
$$f_0(x) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{j=1}^{m} \sum_{i=1}^{m} \alpha_j \alpha_i y_j y_i x_i, x_j$$

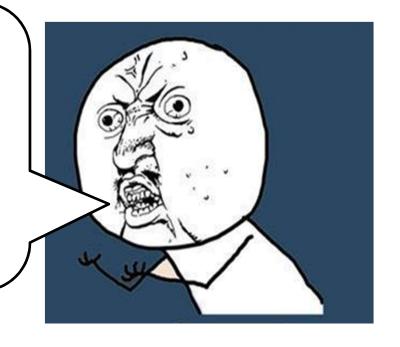
Sujeto a

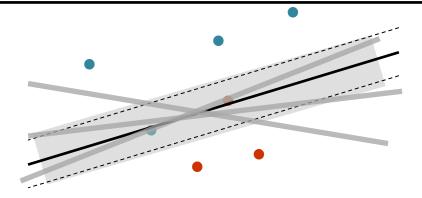
$$\alpha_{i} \geq 0, i = 1, ..., m$$

$$\sum_{i=1}^{m} \alpha_i y_i = 0$$

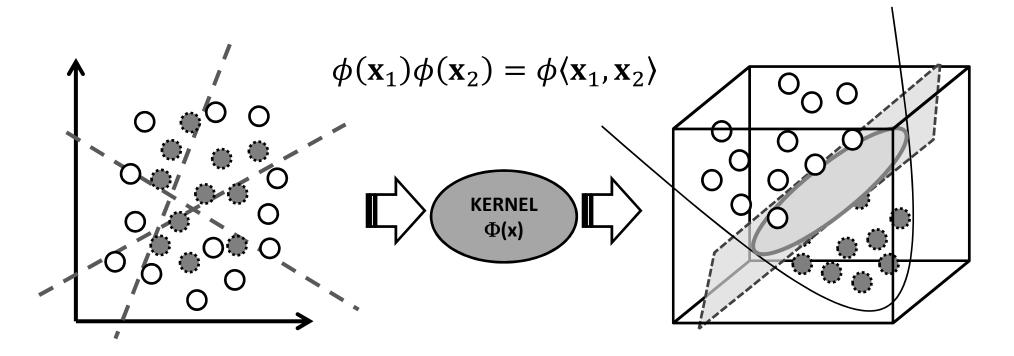
¿Qué sucede si no existe un hiperplano separador?

¿Cómo podemos manejar el ruido y datos etiquetados erróneamente?





Separación No-Lineal: Truco del Kernel



Lineal
$$(K_{lineal})$$
 $K_{lineal}(\mathbf{x}_i, \mathbf{x}_j) = \mathbf{x}_i * \mathbf{x}_j$
Polinomial (K_{pol}) $K_{pol}(\mathbf{x}_i, \mathbf{x}_j) = ((\mathbf{x}_i * \mathbf{x}_j) + r)^d$
Gausiano (K_{Gaus}) $K_{Gaus}(\mathbf{x}_i, \mathbf{x}_j) = exp(-\gamma ||\mathbf{x}_i * \mathbf{x}_j||^2)$

La formulación dual de SVM es preferida debido al número reducido de variables [Schölkopf, 2002]

maximizar
$$f(x) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{j=1}^{m} \sum_{i=1}^{m} \alpha_j \alpha_i y_j y_i x_i, x_j$$

Caso Lineal:

sujeto a

$$\alpha_{i} \geq 0, i = 1,..., m$$

$$\sum_{i=1}^{m} \alpha_i y_i = 0$$

• Caso no-lineal:

maximizar
$$f(x) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{j=1}^{m} \sum_{i=1}^{m} \alpha_j \alpha_i y_j y_i k(x_i, x_j)$$

sujeto a

$$\alpha_{i} \geq 0, i = 1, ..., m$$

$$\sum_{i=1}^{m} \alpha_{i} y_{i} = 0$$

 α : multiplicadores de Lagrange $K(x_i, x_i)$: truco del kernel

Forma primal de C-SVM

minimizar
$$f_0(x) = \frac{1}{2} ||\vec{w}||^2 + \frac{C}{m} \sum_{i=1}^m \xi_i$$

sujeto a

$$y_{i}(\langle \vec{w}, \vec{x} \rangle + b) \geq 1 - \xi, i = 1, ..., m$$

$$\xi_{i} \geq 0, \forall i = 1, ..., m$$

$$\xi_{2}$$

SVM Margen suave forma dual

maximizar
$$f_0(x) = \sum_{i=1}^{m} \alpha_i - \frac{1}{2} \sum_{j=1}^{m} \sum_{i=1}^{m} \alpha_j \alpha_i y_j y_i k(x_i, x_j)$$

sujeto a

$$0 \le \alpha_{i} \le \frac{C}{m}, i = 1, ..., m$$

$$\sum_{i=1}^{m} \alpha_{i} y_{i} = 0$$

$$\sum_{i=1}^{m} \alpha_i y_i = 0$$

C-Support Vector Classification C-SVC/ C-SVM