2022-2023

Aprendizaje Automático

2. Conceptos básicos de aprendizaje automático



(evidal@dsic.upv.es)

Enrique Vidal Ruiz Francisco Casacuberta Nolla (fcn@dsic.upv.es)

Departament de Sistemas Informàtics i Computació (DSIC)

Universitat Politècnica de València (UPV)

- 1 Teoría de la decisión estadística ▷ 2
- 2 Estimación empírica de la probabiliad de error > 7
- 3 Aprendizaje estadístico ⊳ 12
- 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
- 5 La amenaza de la dimensionalidad ▷ 24
- 6 Notación ⊳ 26

- 1 Teoría de la decisión estadística > 2
 - 2 Estimación empírica de la probabiliad de error > 7
 - 3 Aprendizaje estadístico ⊳ 12
 - 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
 - 5 La amenaza de la dimensionalidad ▷ 24
 - 6 Notación ⊳ 26

Planteamiento formal de aprendizaje inductivo

Recordatorio de los elementos que intervienen en el aprendizaje automático:

- Método o algoritmo de aprendizaje, A.
- Clase \mathcal{G} de funciones a aproximar o "aprender". Toda $g \in \mathcal{G}$ es de la forma $g : \mathcal{X} \to \mathcal{Y}$. Para cada tarea, se asume que existe alguna $g \in \mathcal{G}$ que la representa exactamente¹.
- Clase \mathcal{F} funciones con las que se representan los "modelos" resultado del aprendizaje. Toda $f \in \mathcal{F}$ es de la forma: $f: \mathcal{X} \to \mathcal{Y}$.
- Muestra finita de aprendizaje $S \subset \mathcal{X} \times g(\mathcal{X})$.
- Modo de presentación de la muestra. Indica cómo se extraen las muestras S de $\mathcal{X} \times g(\mathcal{X})$.
- Criterio de éxito. Indica qué se espera de A al final del aprendizaje.

^{1.} Esta definición obvia la existencia de una función de representación que asigna a cada objeto real un elemento del espacio de representación, \mathcal{X} . Cuando esto se tiene en cuenta, en general \mathcal{G} no puede ser un espacio de funciones, sino de relaciones de la forma: $g \subset \mathcal{X} \times \mathcal{Y}$.

Teoría de la decisión estadística

- La "función" a aprender, g, es arbitraria (es decir, no se hace ninguna asunción sobre la clase \mathcal{G}).
- El modelo que se aprende, $f: \mathcal{X} \to \mathcal{Y}$, se considera una "función de decisión".
- Para definir un *criterio de éxito* (simplificado, pero útil en la práctica) se asume que, para cada $x \in \mathcal{X}$, la "decisión" f(x) solo puede ser "acertada" o "errónea" (por ej., según f(x) sea idéntica o bastante similar a g(x), o no).
- Toda decisión tiene un *coste*. El planteamiento más simple asume que si la decisión f(x) es *acertada* su coste es 0 y si es *errónea* su coste es 1.
- La función de decisión, f, se basa en la *probabilidad a posteriori*, $P(y \mid x)$, estimada a partir de una muestra de entrenamiento $S \subset \mathcal{X} \times g(\mathcal{X})$.
- El *criterio de éxito* es minimizar la esperanza estadística del coste de las decisiones sobre todos los posibles datos de entrada $x \in \mathcal{X}$. Con la simplificación de coste 0/1, esto equivale a minimizar la probabilidad de error.
- Este planteamiento es la base del marco estadístico en AA y RF.

Septiembre, 2022 DSIC – UPV

^{1.} En este caso, g no es una función propiamente hablando, sino una relación de la forma $g:\subset\mathcal{X}\times\mathcal{Y}$.

Sea $x \in \mathcal{X}$ un dato de *entrada* y sea $y \in \mathcal{Y}$ una *decisión* que se toma para x. $P(y \mid x)$ representa la probabilidad de que la decisión y sea correcta.

Probabilidad de error si se toma la decisión y:

$$P_y(\text{error} \mid x) = 1 - P(y \mid x)$$

Sea $x \in \mathcal{X}$ un dato de *entrada* y sea $y \in \mathcal{Y}$ una *decisión* que se toma para x. $P(y \mid x)$ representa la probabilidad de que la decisión y sea correcta.

Probabilidad de error si se toma la decisión y:

$$P_y(\text{error} \mid x) = 1 - P(y \mid x)$$

Mínima probabilidad de error:

$$\forall x \in \mathcal{X} : P_{\star}(\text{error} \mid x) = \min_{y \in \mathcal{Y}} P_{y}(\text{error} \mid x) = 1 - \max_{y \in \mathcal{Y}} P(y \mid x)$$

Para cada x la probabilidad de error se minimiza si se toma la decisión con mayor $P(y \mid x)$; o sea, la decisión que es "probablemente más acertada".

Sea $x \in \mathcal{X}$ un dato de *entrada* y sea $y \in \mathcal{Y}$ una *decisión* que se toma para x. $P(y \mid x)$ representa la probabilidad de que la decisión y sea correcta.

Probabilidad de error si se toma la decisión y:

$$P_y(\text{error} \mid x) = 1 - P(y \mid x)$$

Mínima probabilidad de error:

$$\forall x \in \mathcal{X} : P_{\star}(\text{error} \mid x) = \min_{y \in \mathcal{Y}} P_{y}(\text{error} \mid x) = 1 - \max_{y \in \mathcal{Y}} P(y \mid x)$$

Para cada x la probabilidad de error se minimiza si se toma la decisión con mayor $P(y \mid x)$; o sea, la decisión que es "probablemente más acertada".

Función de decisión de mínimo riesgo de error o de Bayes:

$$\forall x \in \mathcal{X}: f^{\star}(x) = \underset{y \in \mathcal{Y}}{\operatorname{arg\,max}} P(y \mid x)$$

Sea $x \in \mathcal{X}$ un dato de *entrada* y sea $y \in \mathcal{Y}$ una *decisión* que se toma para x. $P(y \mid x)$ representa la probabilidad de que la decisión y sea correcta.

Probabilidad de error si se toma la decisión y:

$$P_y(\text{error} \mid x) = 1 - P(y \mid x)$$

Mínima probabilidad de error:

$$\forall x \in \mathcal{X} : P_{\star}(\text{error} \mid x) = \min_{y \in \mathcal{Y}} P_{y}(\text{error} \mid x) = 1 - \max_{y \in \mathcal{Y}} P(y \mid x)$$

Para cada x la probabilidad de error se minimiza si se toma la decisión con mayor $P(y \mid x)$; o sea, la decisión que es "probablemente más acertada".

Función de decisión de mínimo riesgo de error o de Bayes:

$$\forall x \in \mathcal{X}: f^{\star}(x) = \underset{y \in \mathcal{Y}}{\operatorname{arg\,max}} P(y \mid x)$$

Esta función garantiza la *minimización del riesgo global o de la esperanza* de error de decisión:

$$P_{\star}(\text{error}) = \int_{x \in \mathcal{X}} p_{\star}(\text{error}, x) dx = \int_{x \in \mathcal{X}} P_{\star}(\text{error} \mid x) p(x) dx$$

Ejercicio (recordatorio de la asignatura SIN)

Un problema clásico de decisión consiste en clasificar flores de la familia Iris en tres clases; setosa, versicolor y virgínica, en base a los tamaños de sus pétalos y sépalos (x).

Para ello se han calculado sendos histogramas de las superficies de los pétalos de una muestra de 50 flores de cada clase. Normalizando estos histogramas, se ha estimado la siguiente distribución de tamaños de pétalos para cada clase (y):

tamaño de los pétalos en cm²

| $P(x \mid y)$ | <1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | >10 |
|---------------|------|------|---|------|------|------|------|------|------|------|------|------|
| SETO | 0.90 | 0.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| VERS | 0 | 0 | 0 | 0.20 | 0.30 | 0.32 | 0.12 | 0.06 | 0 | 0 | 0 | 0 |
| Virg | 0 | 0 | 0 | 0 | 0 | 0 | 0.08 | 0.12 | 0.24 | 0.14 | 0.20 | 0.22 |

Asumiendo que las clases son equiprobables, calcular:

- a) Las probabilidades a posteriory $P(y \mid x), y \in \{SETO, VERS, VIRG\}$, para una flor cuyo tamaño de pétalos es $x = 7 \, \mathrm{cm}^2$
- b) La decisión óptima de clasificación de esta flor y la probabilidad de que dicha decisión sea errónea
- c) La mejor decisión y la correspondiente probab. de error para tamaños de pétalos $1, 2, \ldots, 10$ cm²
- d) La mínima probabilidad de error de decisión esperada para cualquier flor Iris; es decir, $P_{\star}(\text{error})$
- e) Repetir los calculos anteriores, asumiendo que las probabilidades a priori son: $P(\mathsf{SETO}) = 0.3, \ P(\mathsf{VERS}) = 0.5, \ P(\mathsf{VIRG}) = 0.2$

Algunas soluciones: a) 0.0, 0.33, 0.67; b) VIRG, 0.33; d) 0.05 (5%) e.a) 0.0, 0.55, 0.44; e.b) VERS, 0.44; e.d) 0.04 (4%)

Septiembre, 2022 DSIC – UPV

- 1 Teoría de la decisión estadística ⊳ 2
- 2 Estimación empírica de la probabiliad de error > 7
 - 3 Aprendizaje estadístico ⊳ 12
 - 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
 - 5 La amenaza de la dimensionalidad ▷ 24
 - 6 Notación ⊳ 26

Estimación de la probabilidad de error

Sea $P_*(\mathrm{error})$ la verdadera probabilidad de error asociada a la función de decisión de Bayes,

Sea $P_f(\text{error}) \stackrel{\text{def}}{=} p$ la verdadera probabilidad de error de un sistema basado en f.

Una estimación empírica (\hat{p}) de p puede obtenerse contabilizando el número de errores de decisión, N_e , que se producen en una *muestra* de test con N datos:

$$\hat{p} = \frac{N_e}{N}$$

Si N >>, podemos asumir que \hat{p} se distribuye normalmente como:

$$\hat{p} \sim \mathcal{N}\left(p, \frac{p(1-p)}{N}\right)$$

Intervalo de confianza al 95%:

$$P(\hat{p} - \epsilon \le p \le \hat{p} + \epsilon) = 0.95; \qquad \epsilon = 1.96 \sqrt{\frac{\hat{p}(1-\hat{p})}{N}}$$

Métodos de partición de datos

Para evaluar un sistema de *Aprendizaje Automático*, se necesitan datos etiquetados, no solo para estimar el error, sino para aprender los modelos de decisión. Dado un conjunto de datos, este se puede dividir de diversas formas en subconjuntos de *entrenamiento* y de *test*:

- Resustitución (Resubstitution): Todos los datos disponibles se utilizan tanto para para entrenamiento como para test. Inconveniente: es (muy) optimista.
- Partición (Hold Out): Los datos se dividen en un subconjunto para entrenamiento y otro para test. Inconveniente: desaprovechamiento de datos.
- Validación Cruzada en B bloques (B-fold Cross Validation): Los datos se dividen aleatoriamente en B bloques. Cada bloque se utiliza como test para un sistema entrenado con el resto de bloques. Inconvenientes: Reduce el número de datos de entrenamiento (sobre todo cuando B es pequeño) y el coste computacional se incrementa con B.
- Exclusión individual (Leaving One Out): Cada dato individual se utiliza como dato único de test de un sistema entrenado con los N-1 datos restantes. Equivale a Validación Cruzada en N bloques. Inconveniente: máximo coste computacional.

Resustitución y partición

Conjunto de N muestras

Datos

Conjunto de entrenamiento y test N,N_e

Resustitución

Subconjunto
de
entrenamiento
N-N'

N', N' Subconjunto
e de test

Partición

ullet Resustitución. Error: $\frac{N_e}{N}$. Talla de entrenamiento: N.

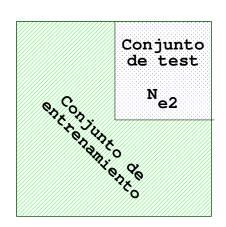
• Partición: Error: $\frac{N_e'}{N'}$. Talla de entrenamiento: N-N'.

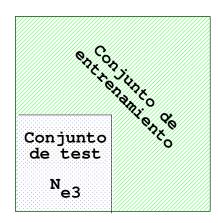
Validación cruzada

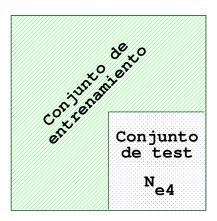
B=4

| N/4 | N/4 |
|-----|-----|
| N/4 | N/4 |









- Error: $\frac{N_{e1}+N_{e2}+N_{e3}+N_{e4}}{N}$.
- Talla de entrenamiento efectiva: $\frac{3N}{4}$.

- 1 Teoría de la decisión estadística > 2
- 2 Estimación empírica de la probabiliad de error > 7
- 3 Aprendizaje estadístico > 12
 - 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
 - 5 La amenaza de la dimensionalidad ▷ 24
 - 6 Notación ⊳ 26

Marco estadístico de Aprendizaje Automático

Aprendizaje:

Estimación de $P(y \mid x)$ mediante algún criterio adecuado.

Generalmente el aprendizaje se basa en estimar P(x,y), ya que $P(y\mid x)=P(x,y)/P(x)$.

• Decisión o Inferencia (clasificación o regresión):

Para cada dato de *test*, $x \in \mathcal{X}$, calcular $f^{\star}(x)$; es decir, obtener una y tal que $P(y \mid x)$ sea máxima:

$$f^{\star}(x) = \operatorname*{arg\,max}_{y \in \mathcal{Y}} P(y \mid x)$$

La función $f^*(\cdot)$ es siempre la misma para cualquier problema; lo que cambia es la distribución $P(y \mid x)$.

Aprendizaje estadístico: Máxima Verosimilitud

Criterio de máxima verosimilitud (MV) para estimación de $P(y \mid x)$:

Se asume que la función de probabilidad conjunta P(x,y) depende de un *vector* de parámetros¹, θ ; es decir, $P(x,y) \equiv P(x,y;\theta), \theta \in \mathbb{R}^D$.

Dado un conjunto de entrenamiento $S \subset \mathcal{X} \times \mathcal{Y}$, la probabilidad (o "verosimilitud") de que $P(x, y; \theta)$ genere S, y su logaritmo, son:

$$P(S; \boldsymbol{\theta}) = \prod_{(x,y)\in S} P(x,y; \boldsymbol{\theta}), \qquad L_S(\boldsymbol{\theta}) = \sum_{(x,y)\in S} \log P(x,y; \boldsymbol{\theta})$$

Estimación de máxima verosimilitud de θ :

$$\hat{\boldsymbol{\theta}} = \operatorname*{arg\,max}_{\boldsymbol{\theta}} L_S(\boldsymbol{\theta})$$

- Si $P(x, y; \theta^*)$ es la verdadera distribución de la que se ha extraido S, $P(x, y; \hat{\theta}) \to P(x, y; \theta^*)$ cuando $|S| \to \infty \Rightarrow$
- MV es consistente con la minimización de la esperanza del error de decisión

^{1.} Ej: (μ, σ) de una Gausiana, o probs. de transición y emisión en modelos ocultos de Markov discretos.

Aprendizaje por MV: regla de Bayes

Frecuentemente puede simplificarse el aprendizaje por MV descomponiendo la probabilidad conjunta como:

$$P(y \mid x) = \frac{P(y) P(x \mid y)}{P(x)}$$

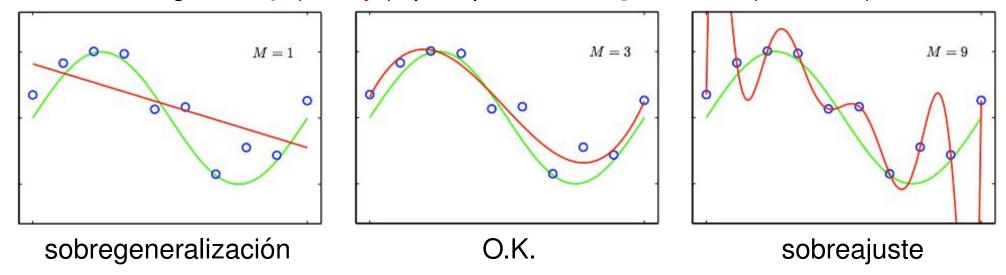
donde P(y) es la probabilidad a priori de y y $P(x \mid y)$ es la probabilidad condicional, o verosimilitud de x dada y.

Ejercicio: Aplicar el criterio de máxima verosimilitud en este caso, asumiendo los correspondientes modelos que $P(y) \approx P(y; \theta)$ y $P(x \mid y) \approx P(x \mid y; \theta)$

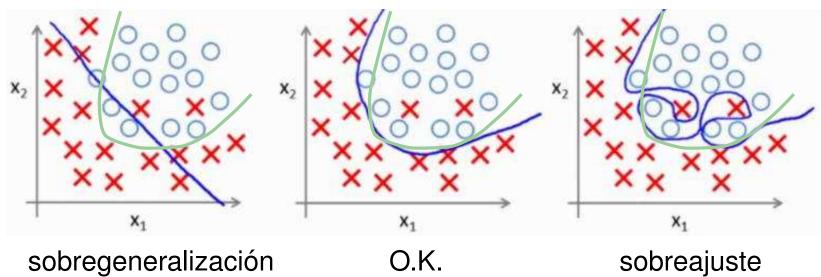
- 1 Teoría de la decisión estadística ⊳ 2
- 2 Estimación empírica de la probabiliad de error > 7
- 3 Aprendizaje estadístico ⊳ 12
- 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
 - 5 La amenaza de la dimensionalidad ▷ 24
 - 6 Notación ⊳ 26

Sobregeneralización y sobreajuste: ejemplos

Modelos de regresión f (en rojo) que aproximan a $g: \mathbb{R} \to \mathbb{R}$ (en verde)



Front. de decisión (azul) que aproximan a las de un clasificador $g: \mathbb{R}^2 \to \{\times, \circ\}$ (verde)



- El compromiso entre sobreajuste y sobregeneralización está estrechamente relacionado con el compromiso entre el sesgo y la varianza.
- Se asume que $\mathcal{X} \equiv \mathbb{R}^{d_x}$, $\mathcal{Y} \equiv \mathbb{R}$ (sin pérdida de generalidad).
- Se dispone de un conjunto de entrenamiento $S \subset \mathcal{X} \times \mathcal{Y}$ de tamaño |S| = N.
- La función "verdadera" a aprender $g: \mathcal{X} \to \mathcal{Y}$ es observada mediante sensores imprecisos como $y = g(\boldsymbol{x}) + \epsilon$, con $(\boldsymbol{x}, y) \in \mathcal{X} \times \mathcal{Y}$, y una imprecisión o "ruido" ϵ que verifica: $\mathbb{E}[\epsilon] = 0$, $\mathbb{V}[\epsilon] = \tau^2$.
- El problema consiste en encontrar un "buen" modelo f, aprendido a partir del conjunto de entrenamiento S. El criterio de éxito es conseguir que la esperanza de error de generalización para cualquier $x \in \mathcal{X}$ sea pequeña, teniendo en cuenta que g es desconocida.

La esperaza de error de generalización se puede expresar como:

$$R_g(f, \boldsymbol{x}, y) \stackrel{\mathsf{def}}{=} \mathbb{E}_{S, \epsilon} \left[\mathcal{E}(f_S(\boldsymbol{x}), y) \right]$$

donde $\mathcal{E}(\cdot)$ es una función de error que mide la disimilitud entre la predicción de nuestro modelo aprendido $f_S(x)$ y lo que observamos y.

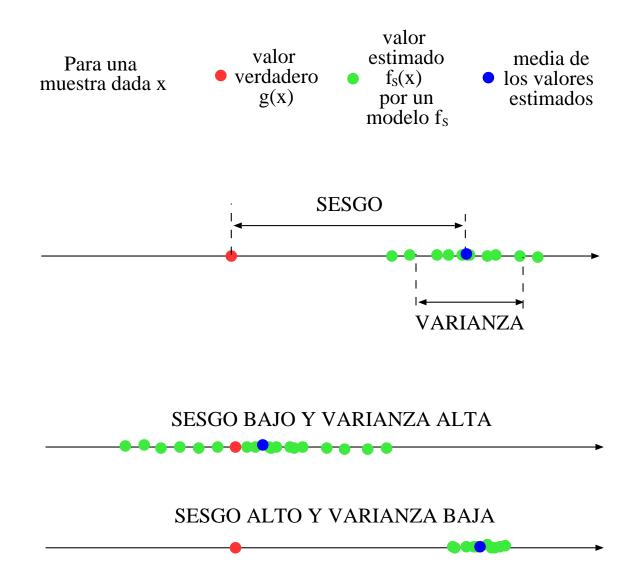
- Sesgo (o Bias): $B_S(g,f,\boldsymbol{x}) = \mathbb{E}_S\left[f_S(\boldsymbol{x})\right] g(\boldsymbol{x})$
- Varianza: $V_S(f, \boldsymbol{x}) = \mathbb{E}_S \left[\left(\mathbb{E}_S \left[f_S(\boldsymbol{x}) \right] f_S(\boldsymbol{x}) \right)^2 \right]$
- Propiedad: Si la función de error $\mathcal{E}(\cdot)$ es el *error cuadrático*, se verifica:

$$R_g(f, \boldsymbol{x}, y) \equiv \mathbb{E}_{S,\epsilon} \left[\mathcal{E}(f_S(\boldsymbol{x}), y) \right] = N(g, \boldsymbol{x}, y) + \left(B_S(g, f, \boldsymbol{x}) \right)^2 + V_S(f, \boldsymbol{x})$$

donde $N(g, \boldsymbol{x}, y)$ es el error irreducible causado por el ruido ϵ :

$$N(g, \boldsymbol{x}, y) = \mathbb{E}_{\epsilon} \left[(y - g(\boldsymbol{x}))^2 \right] = \mathbb{E}_{\epsilon} \left[\epsilon^2 \right] \stackrel{\text{def}}{=} \tau^2$$

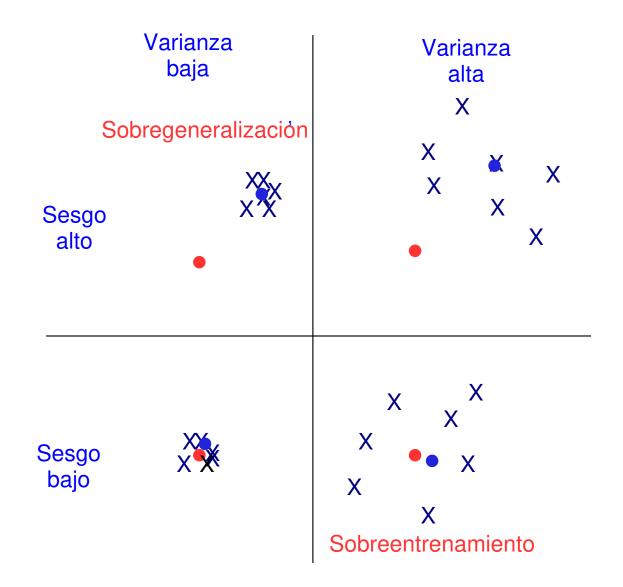
• Estimación del sesgo y la varianza: por valización cruzada, asumiendo que el ruido es nulo ($\tau=0$).



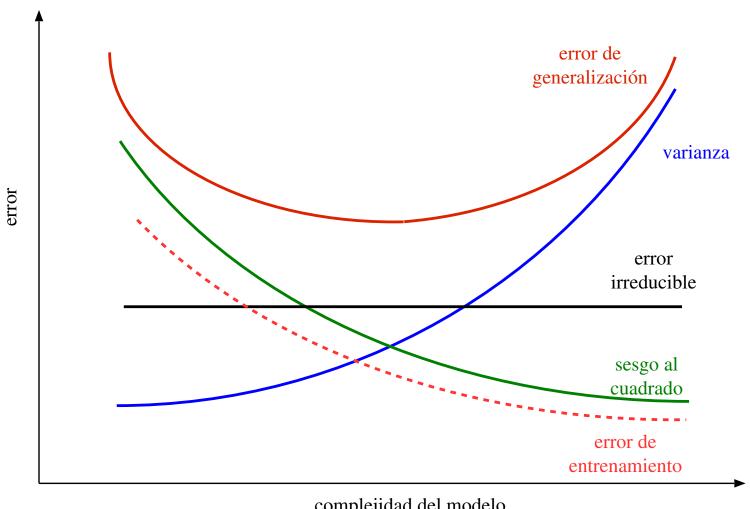
Los puntos verdes son las predicciones de f_S al variar los datos de entrenamiento, S.

Septiembre, 2022 DSIC – UPV

[Singh. Understanding the Bias-Variance Tradeoff. 2018]



[Papachristoudis. The Bias-Variance Tradeoff. 2019]



complejidad del modelo

[Avati. Bias-Variance Analysis:Theory and Practice, 2020]

- Varianza alta. Síntoma: si el error de entrenamiento es bajo pero el error de validación cruzada es alto, seguramente el modelo tendrá una gran varianza:
 - Probable sobreajuste.
 - Es inútil cambiar a modelo más grande.
 - Soluciones para reducir la varianza: aumentar la regularización, obtener un conjunto de datos más grande, disminuir el número de características, usar un modelo más pequeño, etc.
- Sesgo alto. Síntoma: si el modelo no se ajusta bien a los datos de entrenamiento, seguramente el sesgo será alto.
 - Probable sobregeneralización.
 - Es inútil gastar tiempo y recursos en obtener más datos.
 - Soluciones para reducir el sesgo: disminuir la regularización, usar más características, usar un modelo más grande, etc.

- 1 Teoría de la decisión estadística ▷ 2
- 2 Estimación empírica de la probabiliad de error > 7
- 3 Aprendizaje estadístico ⊳ 12
- 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
- 5 La amenaza de la dimensionalidad > 24
 - 6 Notación ⊳ 26

La amenaza de la dimensionalidad

- Si $\mathcal{X} \equiv \mathbb{R}^d$, cuando d es muy grande, aparecen diversos fenómenos adversos que se conocen comúnmente como la "amenaza de la dimensionalidad".
- La causa común de estos problemas es que, cuando aumenta d, el volumen del espacio (por ej., de un hipercubo) aumenta exponencialmente y los datos aparecen muy dispersos.
- Ej.: bastan $10^2=100$ puntos para muestrear un intervalo unidad (un hipercubo en \mathbb{R}^1) para que los puntos no disten más de $10^{-2}=0.01$ entre sí. Pero en \mathbb{R}^{10} harían falta 10^{20} puntos.
- Curiosidad relacionada con lo anterior:
 si d>>>, ¡los puntos de un hipercubo tienden a concentrarse "cerca de sus vértices"!.
 Si d>>>, el volumen de un hipercubo de lado 2r es (2r)^d, mientras que el de una hiperesfera de radio r (contenida en él) es mucho menor: 2r^dπ^{d/2}/d Γ(d/2).

Al aumentar d, el volumen de la hiperesfera resulta insignificante con respecto al del hipercubo:

$$d \to \infty \Rightarrow \frac{2r^d \pi^{d/2}}{d\Gamma(d/2)} \frac{1}{(2r)^d} \to 0$$

- Con frecuencia, estos fenómenos causan problemas de sobregeneralización y sobreajuste.
- Soluciones: determinación de la "dimensionalidad intrínseca", técnicas de reducción de la dimensionalidad, etc.

- 1 Teoría de la decisión estadística ⊳ 2
- 2 Estimación empírica de la probabiliad de error > 7
- 3 Aprendizaje estadístico ⊳ 12
- 4 Sesgo-varianza y sobregeneralización-sobreajuste ⊳ 16
- 5 La amenaza de la dimensionalidad ▷ 24
- 6 Notación > 26

Notación

- C: número de clases en un problema de clasificación
- S: muestra finita de aprendizaje $(S \subset \mathcal{X} \times g(\mathcal{X}))$
- N = |S|: (número de muestras)
- \mathcal{N} : distribución o densidad de probabilidad gaussiana o normal.
- log: logaritmo (de base arbritaria)
- $P(x; \theta)$: probabilidad de x según un modelo cuyos parámetros están dados por el vector θ
- $\max_x(\cdot)$ $(\min_x(\cdot))$ y $\arg\max_x(\cdot)$ $(\arg\min_x(\cdot))$: operadores que devuelven el máximo (mínimo) variando x y el argumento x que maximiza (minimiza) una función, respectivamente
- • ∏ y ∑: operadores productorio y sumatorio, respectivamente
- $L_S(.)$: logaritmo de la verosimilitud de un conjunto S
- \mathbb{R}^d : espacio vectorial real de d dimensiones
- $\mathbb{E}[\cdot]$: Valor esperado o esparanza estadística
- ullet : ruido de medición de la salida y de la función g
- $\mathcal{E}(\cdot,\cdot)$: función de error. Mide la discrepachia entre sus argumentos.
- au^2 : varianza de ϵ
- Γ : función gamma; si el argumento es natural, $\Gamma(n) = (n-1)!$