APRENDIZAJE SUPERVISADO CON SCIKIT-LEARN

Abraham Jain Jiménez

Contents

1	Aprendizaje Supervisado (SL)		2
2	Sintaxis general de scikit-learn para SL		
3	3 Selección del modelo 3.1 Algoritmo Simple Cross-Validatio	n	3
	3.2 Algoritmo K-Fold Cross-Validatio		4
4	4 División del conjunto de datos en	scikit-learn	5
	4.1 Argumentos de la función train_	cest_split	5
	4.2 Desbalance de clases en un proble	ma de clasificación	5
5	5 K-Fold Cross-Validation en scikit	-learn	6
	5.1 Estructura de KFold()		6
6	6 Optimización de hiperparámetros	en scikit-learn	6
	6.1 Algoritmo Grid Search Cross-Vali	dation	7
	6.2 Algoritmo Randomized Search Cr	oss-Validation	8
7	Grid Search CV en scikit-learn		8
8	Randomized Search CV en scikit-learn		9
9	9 Estadística, complejidad, y curva d	Estadística, complejidad, y curva de aprendizaje de los modelos	
	9.1 Estadística del estimador		10
	9.2 Complejidad de los modelos, su va	lidación y la curva de aprendizaje	11
	9.3 Curva de aprendizaje por K-Fold		12
	9.4 Overfitting		14
	9.5 Underfitting		15
10	10 Pipelines en scikit-learn	1	15
	10.1 Fuga de datos		15
	10.2 Sintaxis de las pipelines en sciki	t-learn	16

1 Aprendizaje Supervisado (SL)

Una learning machine es un objeto Θ que puede ser conceptualizado como una función que mapea una base de datos D_f a un estimador \hat{f} del valor original (que arrojaría un modelo ideal f, el cual se desconoce en la práctica):

$$\Theta: D_f \to \hat{f}$$

El estimador \hat{f} corresponde al modelo de Machine Learning implementado para el problema.

En aprendizaje supervisado se entrena el modelo a partir de un conjunto de pares de datos $D_{\text{train}} = \{\vec{x}_i, f(\vec{x}_i) = y_i\}_{i=1}^N$, en donde el conjunto de $\vec{x}_i \in \mathbb{R}^d$ son los vectores de características (comúnmente abordados como vectores columna), y y_i es la etiqueta asociada al problema de regresión o clasificación.

En el caso de clasificación, el espectro de y_i es discreto, mientras que en el caso de regresión toma valores continuos.

2 Sintaxis general de scikit-learn para SL

Sintaxis para implementación de un modelo:

```
from sklearn.module import Model
model = Model()
model.fit(X, y)
predictions = model.predict(X_new)
print(predictions)
```

En donde X representa a la matriz de diseño asociada a los datos (la que concatena los vectores columna $\vec{x_i}$):

$$X := [\vec{x}_1, \dots, \vec{x}_N] \in \mathbb{R}^{d \times N}$$

Así mismo, y representa al vector de etiquetas:

$$\vec{y} = \begin{pmatrix} y_1 \\ \vdots \\ y_N \end{pmatrix}$$

(De ahí la notación X, y, con mayúscula y minúscula respectivamente).

Módulos de aprendizaje supervisado en scikit-learn:

Módulo	Modelos	Ejemplo de clase
sklearn.linear_model	Modelos lineales (regresión, clasificación)	LogisticRegression
sklearn.neighbors	K-NN	${\tt KNeighborsClassifier}$
sklearn.tree	Árboles de decisión	DecisionTreeClassifier
sklearn.ensemble	Ensambles	RandomForestClassifier
sklearn.svm	SVM	SVC
sklearn.model_selection	Validación cruzada, splits	train_test_split
sklearn.metrics	Métricas de evaluación	confusion_matrix

3 Selección del modelo

La meta de un modelo de ML es lograr un error de generalización tan bajo como sea posible. Esto se hace mediante un proceso llamado *cross-validation* (validación cruzada).

La idea de la validación cruzada es dividir el conjunto de datos original en:

- Training Set: El conjunto de entrenamiento. En donde ajustas el modelo de ML a los datos del problema.
- Development Set: El conjunto donde evalúas el rendimiento del modelo. En donde se toman las decisiones de la selección del modelo y se ajustan los hiperparámetros.

Para este proceso se tienen dos algoritmos populares de partición: Simple Cross-Validation y K-Fold Cross-Validation.

3.1 Algoritmo Simple Cross-Validation

Sean $M = \{M_1, \dots, M_d\}$ un conjunto finito de modelos, S el dataset original, $S_{train} = \{\vec{x}, f(\vec{x}) = y\}$ el training set, y $S_{dev} = \{\vec{x}^*, y^*\}$ el dev set. El algoritmo de validación cruzada simple es:

- 1. Dividir S aleatoriamente en S_{train} y S_{dev} (una partición común es 70% vs 30% respectivamente).
- 2. Entrenar cada modelo M_i únicamente sobre S_{train} para encontrar el estimador \hat{f}_i .
- 3. Seleccionar el \hat{f}_i con el menor error de generalización $(Err(\hat{f}))$ en el S_{dev} .

3.2 Algoritmo K-Fold Cross-Validation

Retomando los conjuntos definidos en el algoritmo anterior, en donde S_{train} es el conjunto de entrenamiento con m muestras, el algoritmo de validación cruzada por k-pliegues es:

- 1. Dividir S_{train} aleatoriamente en k subconjuntos de m/k pares de muestras de entrenamiento $(\vec{x}, f(\vec{x}))$, los cuales serán denotados por S_1, \ldots, S_k .
- 2. Cada $M_i \in M$ se evalúa como sigue:

Para
$$j = 1, \dots, K$$

- Entrenar el modelo M_i en $S_1 \cup \cdots \cup S_{j-1} \cup S_{j+1} \cup \cdots \cup S_K$ (es decir, entrenarlo en todas las particiones menos en S_j) para obtener un estimador \hat{f}_{ij} .
- Evaluar \hat{f}_{ij} en S_j para obtener un estimador del error $\widehat{Err}_{S_j}(\hat{f}_{ij})$.
- El error de generalización estimado de M_i es calculado como el promedio de los $\{\widehat{Err}_{S_i}(\hat{f}_{ij})\}$ sobre j:

Error Promedio =
$$\frac{1}{K} \sum_{i=1}^{K} \widehat{Err}_i$$

3. Se toma el modelo M_i con el menor error de generalización estimado y se retiene en S_{train} . El estimador \hat{f} es la respuesta final.

El estimador del error de generalización es una métrica asociada al rendimiento del modelo. Por ejemplo, en regresión multilineal podría ser R^2 , en tal caso el error promedio es $R^2_{\text{promedio}} = \frac{1}{K} \sum_{i=1}^K R_i^2$.

4 División del conjunto de datos en scikit-learn

Sintaxis:

```
from sklearn.model_selection import train_test_split

X_train, X_test, y_train, y_test = train_test_split(X,

y,

test_size,
 random_state,
 stratify)

model = Model()

model.fit(X_train, y_train)

print(model.score(X_test, y_test))
```

4.1 Argumentos de la función train_test_split

- test_size: Proporción del conjunto de test. Por ejemplo, test_size = 0.2 implica un 20% del dataset para test. También puede ser un entero (número de muestras). Si no se incluye este argumento o se asigna None, el valor por defecto es 0.25.
- random_state: Fija la semilla generadora de valores aleatorios para que el proceso de división sea reproducible.
- stratify: Se usa en problemas de clasificación. Este argumento garantiza que la proporción de clases en los conjuntos de entrenamiento y prueba sea similar a la del conjunto original. Típicamente se utiliza stratify = y. Es decir, este argumento mantiene la proporción de clases en el conjunto de entrenamiento y prueba, es muy útil en desbalance de clases.

4.2 Desbalance de clases en un problema de clasificación

El argumento stratify = y genera lo que se conoce como muestras estratificadas (*stratified samples*). Una muestra estratificada es una muestra que se selecciona de manera que las proporciones de ciertos grupos, en este caso las divisiones del conjunto original, se mantengan igual que en la población original.

Por ejemplo, si en un conjunto de datos el 70% de las observaciones pertenece a la clase A y el 30% a la clase B, una muestra estratificada mantendrá esa misma proporción.

Evaluando si hay desbalance de clases antes de dividir el conjunto:

```
#Balance de clases del dataframe original
print(y["columna etiqueta"].value_counts())

#Balance de clases del conjunto train
print(y_train["columna etiqueta"].value_counts())

#Balance de clases del conjunto test
print(y_test["columna etiqueta"].value_counts())
```

5 K-Fold Cross-Validation en scikit-learn

Sintaxis para K-folds:

```
from sklearn.model_selection import cross_val_score, KFold
kf = KFold(n_splits, shuffle, random_state)
model = Model()
cv_results = cross_val_score(model, X, y, cv=kf)
```

5.1 Estructura de KFold()

- n_splits define el número de particiones (folds) de la validación.
- shuffle indica si se mezclan los datos o no (True, False).
- random_state define la semilla para reproducibilidad.

Función cross_val_score()

Devuelve un arreglo NumPy con la puntuación de cada fold. Usa por defecto la métrica default del modelo, score().

6 Optimización de hiperparámetros en scikit-learn

En un modelo de ML, los hiperparámetros son configuraciones del modelo que se definen para el proceso de entrenamiento. Dado que estos precisamente afectan cómo se entrena el modelo, deben de optimizarse para que el rendimiento sea el mejor posible de acuerdo a las necesidades de cada proyecto.

Por ejemplo, en los modelos K-NN y K-means (aunque este último es no supervisado), K es un hiperparámetro. En regresión polinomial, el orden M del polinomio (número de parámetros entrenables) es un hiperparámetro. En árboles de decisión, max_depth lo es. Etc.

Algunas de las técnicas de optimización de hiperparámetros, es decir, técnicas para encontrar los mejores hiperparámetros de un modelo de ML son *Grid Search Cross-Validation* y *Randomized Search Cross-Validation*

6.1 Algoritmo Grid Search Cross-Validation

Siendo que los valores de un hiperparámetro pueden tener un espectro continuo o discreto, el algoritmo Grid Search CV es el siguiente:

1. Se define un espacio de búsqueda:

Se toma un conjunto de hiperparámetros y un conjunto de valores posibles para cada uno de ellos.

Sea $H = \{H_i\}_{i=1}^N$ el conjunto de hiperparámetros a ajustar y $V_i = \{a_j^i\}_{j=1}^n$ el conjunto de valores que puede tomar el hiperparámetro H_i (si el espectro de este conjunto es continuo, estamos hablando de valores dentro de un rango).

```
param_grid = {
    "H_1": [lista (o rango continuo) de valores de H_1],
    "H_N": [lista (o rango continuo) de valores de H_N]
}
```

2. Se construye la malla:

Se forma una lista de todas las combinaciones posibles de esos hiperparámetros y sus valores, un conjunto de pares (Hiperparámetro, Valor):

$$Malla = \{(H_i, a_j^i)\}$$

3. Se evalúa cada combinación por K-Fold Cross-Validation:

Se implementa un proceso K-Fold CV en cada par (H_i, a_j^i) para encontrar la mejor combinación de hiperparámetros que optimiza (maximiza o minimiza según el caso) una métrica de rendimiento del modelo.

6.2 Algoritmo Randomized Search Cross-Validation

La desventaja con Grid search es que es costoso computacionalmente, el consumo de tiempo y recursos suele ser alto, por lo que random search es una alternativa menos costosa.

Este algoritmo selecciona hiperparámetros aleatoriamente, crea un conjunto y entrena el modelo con él. Puede que no encontre el mejor conjunto, pero hay mayores probabilidades de encontrar uno cercano al mejor, lo que ahorra mucho costo computacional.

Retomando los términos vistos en Grid Search CV, el algoritmo Randomized Search CV es el siguiente:

1. Se define un espacio de búsqueda:

A diferencia de Grid Search CV, Randomized Search CV no necesita recibir una lista exacta de valores para los hiperparámetros, se pueden dar distribuciones.

2. Se toman N combinaciones de hiperparámetros:

El algoritmo elige aleatoriamente N combinaciones de hiperparámetros y sus valores, y es el usuario el que define cuántas serán.

3. Se evalúa cada combinación por K-Fold Cross-Validation:

Con esto se calcula el promedio del score, o sea la métrica de rendimiento.

4. Elección de la mejor combinación de hiperparámetros:

Se elige la mejor combinación según el score promedio en el proceso K-Fold CV.

7 Grid Search CV en scikit-learn

```
from sklearn.model_selection import GridSearchCV
from sklearn.module import Model
```

```
#Datos
    X, y = DataSet
    # Definimos el modelo
    model = Model()
    # Definimos el grid de hiperparámetros
10
    param_grid = {
11
         'Hiperparámetro i-ésimo': [conjunto de valores para el hiperparámetro]
12
13
14
    # Se implementa Grid Search CV. scoring recibe la métrica del problema
15
    grid_search = GridSearchCV(estimator=model,
16
                                 param_grid=param_grid,
                                 cv, scoring)
18
    # Entrenamiento
    grid_search.fit(X, y)
    # Resultados
23
    print("Mejores parámetros:", grid_search.best_params_)
    print("Mejor score promedio:", grid_search.best_score_)
```

8 Randomized Search CV en scikit-learn

```
from sklearn.model_selection import RandomizedSearchCV
from sklearn.module import Model
from scipy.stats import randint

# Datos
X, y = DataSet

# Modelo
model = Modelo()

# Espacio de búsqueda (distribuciones)
param_distributions = {
    'Hiperparámetro': randint(x_inicial, x_final)
```

```
}
14
15
     # Búsqueda aleatoria
16
     random_search = RandomizedSearchCV(
17
         estimator=model,
18
         param_distributions=param_distributions,
19
                             # Número entero de combinaciones a tomar
         n_iter,
20
                              # Número de folds
         cv,
21
         scoring,
                           # Métrica
22
         random_state
23
24
25
     # Se efectúa el algoritmo Randomized Search
26
     random_search.fit(X, y)
27
28
     # Resultados
29
     print("Mejores hiperparámetros:", random_search.best_params_)
30
     print("Mejor score promedio:", random_search.best_score_)
31
```

9 Estadística, complejidad, y curva de aprendizaje de los modelos

En el primer capítulo vimos que una *learning machine* es un objeto conceptualizado como una función que mapea una base de datos a un estimador del valor o función original.

De lo anterior, un buen modelo de Machine Learning es aquel que produce un estimador \hat{f} que arroja resultados muy parecidos a los valores reales f.

9.1 Estadística del estimador

El estimador (o modelo) es una función que depende de los datos de entrenamiento $D_{train} = \{\vec{x}_i, y_i\}_{i=1}^N$, y el qué tan bueno es puede ser descrito mediante las siguientes medidas:

• Bias (sesgo): Mide la diferencia entre la predicción promedio del modelo y el valor original.

$$Bias(\hat{f}) = \mathbb{E}(\hat{f}) - f$$

• Varianza: Mide la dispersión alrededor del promedio del estimador.

$$Var(\hat{f}) = \mathbb{E}[(\hat{f} - \mathbb{E}(\hat{f}))^2]$$

En la práctica, el sesgo y la varianza conducen a dos conceptos importantes sobre el rendimiento del modelo: overfitting y underfitting.

9.2 Complejidad de los modelos, su validación y la curva de aprendizaje

- La complejidad de un modelo de Machine Learning se estima mediante el número de parámetros a entrenar. Se cuantifica mediante la curva de aprendizaje que grafica la relación Métrica de Error vs Complejidad del Modelo (M).
- La curva de aprendizaje es una gráfica que muestra como varía el rendimiento de un modelo mientras aumenta el tamaño del conjunto de entrenamiento, através de una curva de entrenamiento y una de validación. Esto nos muestra cómo aprende el modelo y es útil para detectar sobreajuste.
- La validación de los datos mediante algún algoritmo de Cross-Validation es fundamental, pues se divide el conjunto de datos en entrenamiento y prueba para evaluar el modelo con información fuera de la de entrenamiento. De esta manera se verifica que el modelo efectivamente aprende y no solo memoriza.
- La curva de aprendizaje nos ayuda a ver en qué región de las curvas de entrenamiento y aprendizaje, de la métrica de error en función de M, radica el aprendizaje.
- En la gráfica veremos 2 líneas, la de entrenamiento que muestra el desempeño del modelo en los datos de entrenamiento y la de validación (o prueba) que muestra el desempeño del modelo en los datos que nunca ha visto. En el eje x se muestra el tamaño del conjunto de entrenamiento, y en el eje y una métrica de error (puede ser Precision, Recall, F1-score, etc).



Figure 1: Ejemplo de curva de aprendizaje

9.3 Curva de aprendizaje por K-Fold CV en scikit-learn

```
from sklearn.module import Model
    from sklearn.model_selection import train_test_split
    from sklearn.model_selection import learning_curve
    X, y = Dataset
    X_train, X_test, y_train, y_test = train_test_split(X,
                                                           test_size,
8
                                                           random_state)
10
    model = Model()
11
     #Paso 1: Generar la curva de aprendizaje para observar posible overfitting
13
     train_sizes, train_scores, val_scores = learning_curve(
                                                               model/pipeline,
15
                                                               X_train,
                                                               y_train,
17
                                                               cv,
                                                               train_sizes,
19
20
                                                               scoring
                                                               )
21
     #Paso 2: Calcular las medias y desviaciones estándar de los scores
23
     train_mean = np.mean(train_scores, axis=1)
     train_std = np.std(train_scores, axis=1)
25
    test_mean = np.mean(test_scores, axis=1)
     test_std = np.std(test_scores, axis=1)
27
     #Paso 3: Graficar la curva de aprendizaje (el siguiente formato es común)
29
30
     #Curva de entrenamiento
31
    plt.figure(figsize=(10, 6))
32
    plt.plot(train_sizes, train_mean, label="Puntuación de entrenamiento",
33
                 color="blue", marker="o")
34
    plt.fill_between(train_sizes, train_mean - train_std,
35
                         train_mean + train_std, color="blue", alpha=0.1)
36
37
     \newpage #Esta línea corresponde al código latex, no es de Python
38
39
```

```
#Curva de validación
40
     plt.plot(train_sizes, test_mean, label="Puntuación de validación",
41
                 color="green", marker="o")
42
     plt.fill_between(train_sizes, test_mean - test_std,
43
                         test_mean + test_std, color="green", alpha=0.1)
44
45
     plt.title("Curva de Aprendizaje para el modelo")
46
    plt.xlabel("Tamaño del Conjunto de Entrenamiento")
47
    plt.ylabel("Métrica")
48
    plt.grid(True)
49
    plt.legend(loc="best")
50
    plt.show()
```

Observaciones:

• El argumento train_sizes de la función learning_curve corresponde a los porcentajes del conjunto de entrenamiento a usar.

Por ejemplo, puede usarse train_sizes=np.linspace(0.1, 1.0, 10), en donde los parámetros son np.linespace(start, stop, num), esto quiere decir que se va a empezar con el 10% de los datos del conjunto de entrenamiento, gráficamente esto se verá en el primer punto de la curva de aprendizaje.

El valor de 1.0 en stop indica que el último punto será utilizando el 100% del conjunto de entrenamiento total. Además, num=10 indica que se van a generar 10 puntos iguales, con un espacio de 10%, por lo que la función entrenará y evaluará el modelo 10 veces.

• La línea plt.plot(train_sizes, train_mean, label="Puntuación de entrenamiento", color="blue", marker="o") realiza una gráfica donde se muestra cómo aumentan los tamaños del conjunto de entrenamiento (train_sizes).

A su vez, train_mean es una lista que contiene la métrica media del modelo en el conjunto de entrenamiento según van avanzando los tamaños del conjunto de prueba.

• La función plt.fill_between() dibuja un área sombreada alrededor de la curva línea de arriba, que indica la desviación estandar de las puntuaciones de entrenamiento para ver la dispersión de las puntuaciones que se obtuvieron a lo largo de la validación cruzada.

Esta función recibe el tamaño de conjunto de entrenamiento y un límite inferior y superior para el área sombreada dadas las ecuaciones train_mean - train_std, train_mean + train_std.

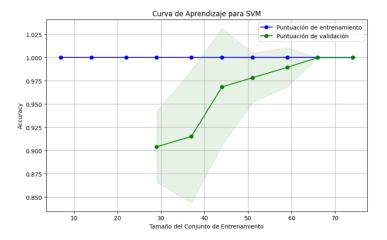
9.4 Overfitting

El sobreajuste está relacionado con un modelo de varianza alta, es decir, con alto rendimiento durante el entrenamiento, pero deficiente en testing.

En la curva de aprendizaje, si la gráfica muestra que la curva de entrenamiento tiene un gran rendimiento mientras que la de validación tiene un menor rendimiento o no mejora mucho a lo largo del camino, se indica un sobreajuste.

El overfitting se combate, por ejemplo, incrementando la regularización, disminuyendo el número de características o afinanfo hiperparámetros.

Por ejemplo, consideremos la siguiente curva de aprendizaje de un modelo SVM:



Para el rendimiento del entrenamiento (línea azul) podemos ver que se tiene una Accuracy perfecta para todos los tamaños en el conjunto de entrenamiento, además que no tiene una sombra azul alrededor, lo que indica que también hay mucha consistencia en el entrenamiento a lo largo de la validación cruzada.

Para el rendimiento en la validación (línea verde) podemos ver que se empezó relativamente bajo, y mientras se aumenta el tamaño del conjunto de entrenamiento, la Accuracy mejora aún más. Primero aumentó un poco y después tuvo un aumento casi lineal, y al final, tiene una Accuracy del 100%.

La banda sombreada alrededor de la línea indica que hubo mucha variabilidad en el rendimiento, pero que fue bajando al agregar más datos.

Podríamos decir que el modelo presenta overfitting, pues al ver la curva, podemos ver que el modelo está memorizando los datos de entrenamiento en lugar de aprender patrones que se apliquen a datos nunca antes vistos, ya que al inicio había una gran diferencia entre las curvas, y comenzó a disminuir de manera drástica.

Lo que habría qué hacer en este caso del modelo SVM, es encontrar un mejor parámetro C o probar distintos tipos de kernel.

9.5 Underfitting

El infraajuste está relacionado con un modelo de bias alto.

Si ambas curvas tienen un bajo rendimiento y no mejora el modelo a lo largo de los datos, el modelo es demasiado simple para los datos y hay que mejorarlo.

El underfitting se combate, por ejemplo, aumentando las características o reduciendo la regularización.

10 Pipelines en scikit-learn

Una pipeline, comunmente traducido como canalización, es un objeto que sirve para ejecutar una serie de transformaciones y construir un modelo en un único flujo de trabajo.

Las pipelines son útiles para organizar el código (por ejemplo, en el caso en el que todo un equipo trabaja sobre un mismo notebook), para evitar fuga de datos (data leakage) y facilitar tareas como cross-validation y la búsqueda de hiperparámetros con GridSearchCV o RandomizedSearchCV.

10.1 Fuga de datos

La fuga de datos ocurre cuando se utiliza información del conjunto de prueba en procesos en los que únicamente debe usarse el conjunto de entrenamiento, ya sea durante el propio entrenamiento del modelo o durante las etapas de preprocesamiento que afectan al entrenamiento. Esto genera un modelo que no generaliza bien, un modelo poco robusto.

Por las razones anteriores es que se suele dividir el conjunto de datos en training y test, por ejemplo, antes de la imputación de valores faltantes.

10.2 Sintaxis de las pipelines en scikit-learn

```
from sklearn.pipeline import Pipeline

pipe = Pipeline(steps)
```

En donde steps es una secuencia de N pasos donde cada paso desde el primero hasta el N-1 debe ser un transformador, es decir, de la clase transformers de scikit-learn. El último paso, N, es un estimador, un modelo de ML.

```
steps = [("transformación 1", Transformador1()),

("transformación N-1", TransformadorN-1()),
("modelo", Model())]
```

10.3 Ejemplo: Escalando datos para aplicar un modelo K-NN mediante una pipeline

Mediante una pipeline, se van a escalar los datos mediante la transformación StandardScaler() como parte del preprocesamiento de datos para un modelo K-NN.