

# APPRENDIMENTO AUTOMATICO

Alessandro Zappatore

Università degli studi di Torino  
Anno accademico 2025/2026, 1° semestre

## 1 Introduzione

### 1.1 Definizione di Machine Learning (ML)

Thomas Mitchell; 1996; Machine Learning

*A computer program is said to learn from experience with respect to some class of tasks and performance measure, if its performance at tasks in, as measured by, improves with experience.*

È la combinazione di tre oggetti l'**esperienza E** sotto forma di esempi del problema risolto al computer, un **task T** da risolvere (classificazione degli esempi in un certo numero di categorie, assegnazione di un numero associato agli esempi, riconoscimento di un'immagine), sotto una **misura di performance P** un valore per misurare quanto sta andando bene.

Il programma del computer fa apprendimento automatico basandosi sugli esempi se le sue performance migliorano man mano che vede gli esempi.

**Esempio del melone** Assumendo di avere dei dati sulla maturazione dei meloni vogliamo sapere se il frutto è maturo o no.

ID	Color	Root	Sound	Ripe
1	green	curly	muffled	true
2	dark	curly	muffled	true
3	green	straight	crisp	false
4	dark	slightly curly	dull	false

Ora troviamo un melone con le seguenti caratteristiche e vogliamo sapere se è maturo:

Color	Root	Sound
green	curly	dull

In questo caso abbiamo un **task**, sapere se è maturo, delle **performance**, quanto è accurata la nostra predizione e dell'**esperienza** i meloni comprati in precedenza.

Questo tipo di lavoro è chiamato **apprendimento supervisionato**, dove un essere umano andrà a segnare qual è la risposta giusta. Nell'**apprendimento non supervisionato** la colonna delle risposte non è presente, ma si andrà a raggruppare risposte simili.

## 1.2 Terminologia

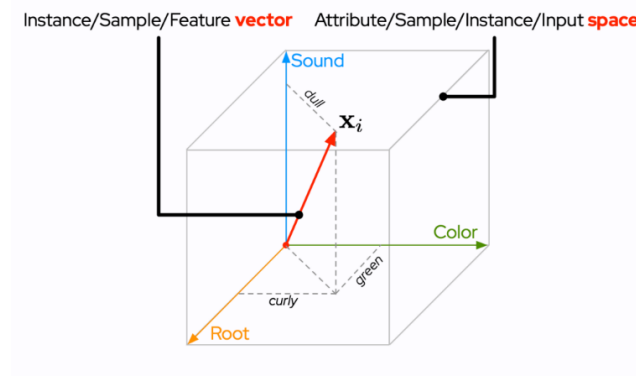
Attributes/Features				Label/Class $y$	
	ID	Color	Root	Sound	Ripe
Training set	1	green	curly	muffled	true
	2	dark	curly	muffled	true
	3	green	straight	crisp	false
	4	dark	slightly curly	dull	false
Test set	1	green	curly	dull	?
	Sample/Instance $\mathbf{x}_i$				
Attribute value/Feature value $x_{i1}$					

Le colonne della tabella sono chiamate **attributi** o **features** dell'esempio, l'elemento che ci dice come risolvere il task è chiamato **etichetta** o **classe** dell'esempio, tipicamente la classe viene denotata con una  $y_i$  minuscola.

Una riga della tabella, senza considerare la colonna della classe, è chiamato **sample** o **istanza** dell'esempio, in genere denotata con una  $X_i$  per dire che è l'iesimo esempio. [Tutte le volte che parleremo di vettori saranno rappresentati da lettere maiuscole, invece i valori scalari saranno rappresentati in corsivo]

Il singolo valore di una colonna è chiamato **attribute value** o **feature value** ed è rappresentato da un valore in corsivo  $x_{i1}$  in questo caso la prima feature dell'iesimo esempio.

L'insieme degli esempi che usiamo per indurre la regola che poi utilizzeremo per classificare è chiamato **set di training** e spesso al fianco si trova un altro insieme di esempio, chiamato **test set**, che serve per riuscire a capire quanto bene stiamo performando.



Quanto gli esempi vengono immaginati in uno spazio euclideo di qualche tipo, in questo caso a tre dimensioni, spesso ci si riferisce all'esempio come **instance vector** oppure **sample vector**, **feature vector**, l'intero insieme di tutti i possibili esempi è chiamato anche **attribute space**, **sample space**, **instance space**, **input space**.

## 1.3 Notazione

Symbol	Meaning
$\mathcal{X}$	instance space, in many cases $\mathcal{X} = \mathbb{R}^d$
$\mathcal{Y}$	label space, e.g., $\mathcal{Y} = \{0, 1\}$ for binary classification
$\mathbf{x}_i \in \mathcal{X}$	$i$ -th instance/sample, $\mathbf{x}_i = [x_{i1}, x_{i2}, \dots, x_{id}]^T$
$d$	dimensionality of the instance space
$y_i \in \mathcal{Y}$	label of the $i$ -th instance, e.g., $y_i = 1$ if the watermelon is ripe, $y_i = 0$ otherwise
$D$	Dataset, $D = \{(\mathbf{x}_1, y_1), (\mathbf{x}_2, y_2), \dots, (\mathbf{x}_n, y_n)\}$
$n$	number of instances in the dataset
$h$	model/hypothesis, a function $h: \mathcal{X} \rightarrow \mathcal{Y}$ that maps instances to labels
$\mathcal{L}$	Learning algorithm $\mathcal{L}: \mathcal{P}(\mathcal{X} \times \mathcal{Y}) \rightarrow \mathcal{H}$ , where $\mathcal{P}$ is the power set and $\mathcal{H}$ is the hypothesis space
$\mathbb{I}$	Indicator function, $\mathbb{I}(P)$ (sometimes denoted as $\mathbb{I}[P]$ ) is 1 if $P$ is true, 0 otherwise

## 1.4 Altra terminologia

Il **training** è un processo utilizzato da algoritmo di machine learning per costruire un modello dai dati. I dati utilizzati durante questo processo sono chiamati **training data**, dove ogni esempio è chiamato **training example** e l'insieme di tutti gli esempi è chiamato **training set**.

### Obiettivo del Machine Learning

L'obiettivo dell'apprendimento automatico è trovare un **ipotesi** che è capace di approssimare la **ground-truth** su dati che non ha mai visto.

## 1.5 Tasks

I più importanti tasks che si possono fare con l'apprendimento automatico sono:

- **Predittivi**: predire un numero o una caratteristica, solitamente sono supervisionati
  - **Classificazione**, abbiamo un certo numero di etichette negli esempi, se le etichette sono solo due si parla di classificazione **binaria** invece se sono di più si parla di classificazione **multiclasse**.
  - **Regressione**, è un caso di predizione dove l'insieme delle etichette corrisponde con un intervallo continuo, cerchiamo di predire dei numeri.
- **Descrittivi**: descrivere qualcosa su come è strutturato il data set, solitamente non supervisionati
  - **Clustering**
  - **Regole di associazione**

**Learning supervisionato** l'etichetta è fornita dall'utente

**Learning non supervisionato** l'etichetta non esiste

## 1.6 Assunzione i.i.d

Nella maggioranza dei casi, in particolare in tutti gli algoritmi che vedremo nel corso, si assume che i dati siano **Indipendenti** e **Identicamente Distribuiti**.

Nel momento in cui ho estratto un istanza con la sua etichetta il prossimo lo estraggo dalla stessa distribuzione di probabilità, perché se cambia la distribuzione non ho speranza di apprendere nulla.

**Indipendenti** perché fissata la distribuzione, se io pesco due esempi, l'aver estratto un esempio non ha implicazione sull'estrazione di un altro esempio. [Ex. estraggo una pallina dall'urna, poi la rimetto dentro e riestraggo. La probabilità del primo e del secondo caso sarà la medesima]

- **Indipendenza**:  $P((X_i, y_i) | (X_1, y_1), \dots, (X_{i-1}, y_{i-1})) = P((X_i, y_i)) \quad \forall i$
- **Identicamente distribuiti**: Tutte le istanze provengono dalla stessa distribuzione sottostante. Ciò significa anche che i dati di training e i dati di test devono provenire dalla stessa distribuzione.

### Esempio

Immaginando di gestire una fabbrica di di cupcake. Ogni cupcake è fatto:

- usando la **stessa ricetta** (identicamente distribuita)
- e **e cotti in uno stampo separato** senza influenzare gli altri (indipendenti)

Quindi, se assaggi 10 cupcake a caso e hanno tutti un sapore dolce, puoi presumere che anche i cupcake futuri saranno dolci, perché il tuo campione è i.i.d.

## Esempio - What if

Cosa succede se:

- All'improvviso usi **due ricette diverse** → non distribuite in modo identico.
- Cuoci i cupcake nello **stesso stampo e l'impasto si mescola** → non indipendente.

## 1.7 Spazio delle ipotesi

### 1.7.1 Deduzione Vs Induzione

**Deduzione** vuol dire che parto da degli assiomi, ho delle regole per combinare gli assiomi e ottengo una deduzione. La deduzione è un processo **corretto**, se assumo che gli assiomi siano corretti allora qualsiasi cosa io deduca da questi assiomi deve essere vera per forza.

**L'Induzione** è il processo inverso, si parte da oggetti specifici, gli esempi, e cerco di dedurre una regola generale.

Il processo di Apprendimento Automatico si basa interamente sul principio dell'induzione.

## Esempio

**Esempio di deduzione:**

- Tutti gli umani sono mortali
- Socrate è un uomo
- Quindi, Socrate è mortale

**Esempio di induzione:**

- Dopo aver osservato che ogni essere umano conosciuto prima o poi muore, potremmo dedurre che tutti gli esseri umani sono mortali.

### 1.7.2 Symbolic concept learning

Con i metodi induttivi vogliamo provare a costruire delle regole logiche, e in questo caso ci troviamo nel campo del **symbolic concept learning** e una sua forma più estesa è chiamata **Inductive Logic Programming**, dei linguaggi che ci permettono di lavorare con la logica per costruire queste regole in modo induttivo.

La forma base del concept learning è chiamato **boolean concept learning** dove l'obiettivo è costruire una funzione  $h : \chi \mapsto \{0, 1\}$ .

## Esempio

Supponendo di voler predire se un melone è maturo e la formula è:

$$ripe \iff (color = ?) \wedge (root = ?) \wedge (sound = ?)$$

Al posto dei punti interrogativi possiamo mettere un valore oppure un **asterisco \*** per dire che **non interessa il valore specifico**.

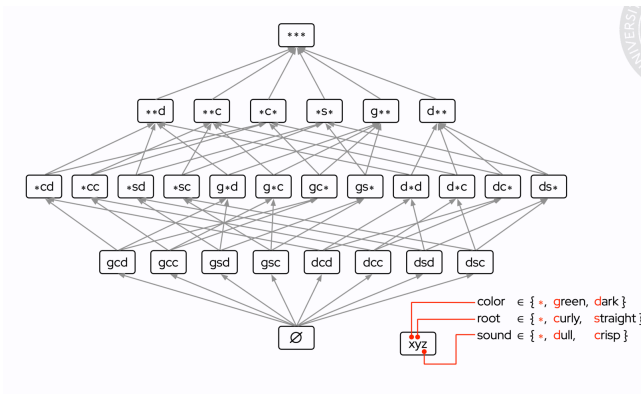
In questo caso il melone sarà maturo se il suono è dull il resto non mi interessa.

$$ripe \iff (color = *) \wedge (root = *) \wedge (sound = dull)$$

### 1.7.3 Spazio delle ipotesi

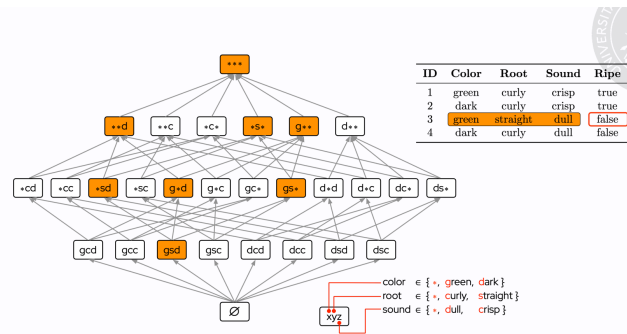
Lo **Spazio delle ipotesi** è l'insieme di tutte le ipotesi (tutti i possibili modelli) che posso apprendere utilizzando uno specifico algoritmo di apprendimento. [Nell'esempio sopra citato è l'insieme di tutte le formule booleane che posso ottenere].

Possiamo pensare all'apprendimento automatico come un **processo di ricerca all'interno dello spazio delle ipotesi**, e devo trovare l'ipotesi migliore in base ai dati che ho.

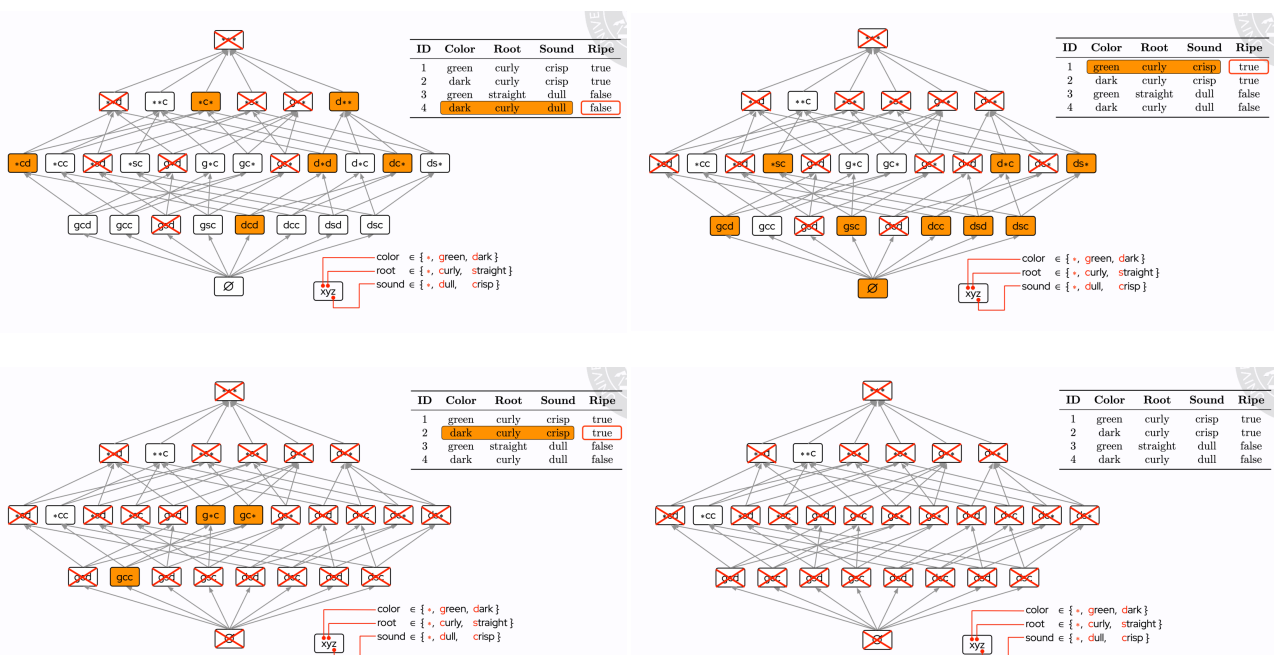


### 1.7.4 Spazio delle versioni

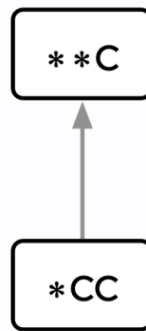
Lo **spazio delle versioni** è un **sottoinsieme dello spazio delle ipotesi** che è consistente con tutti gli **esempi di training**. Sostanzialmente prendo solo gli esempi che danno una risposta giusta [nel caso dei meloni se trovo un esempio con suono *dull* ma non maturo lo andrò a scartare].



L'ipotesi in arancione non è consistente con l'esempio, perché questo avrebbe detto a qualsiasi cosa mature. *\*d* dice che dovrebbe dare maturo e anche questo non va bene. Tutte le caselle evidenziate in arancione non sono consistenti con l'esempio in questione, quindi decido di eliminarle.



Vado a controllare tutti gli esempi e alla fine andrò a vedere che lo spazio delle versioni finale sarà:



Nell'esempio lo spazio delle versioni consiste in due ipotesi:

- $ripe \iff (color = *) \wedge (root = *) \wedge (sound = crisp)$
- $ripe \iff (color = *) \wedge (root = curly) \wedge (sound = crisp)$

Dato quello che sappiamo del dataset le due sono equivalenti e non c'è una giusta.

### 1.7.5 Bias induttivo

Nel caso dovesse arrivare un nuovo esempio del tipo  $Color = green, Root = straight, Sound = crisp$ , avremmo una regola che dice maturo e una che dice non maturo.

Senza altre informazioni non possiamo decidere quale delle due ipotesi è corretta, però un algoritmo non può restituire un insieme di ipotesi.

Tutti gli algoritmi di apprendimento hanno un **bias induttivo**, non basato sui dati.

Si può scegliere di preferire delle regole più generali o all'opposto potrebbe preferire una regola più specifica.

Ogni algoritmo di apprendimento DEVE avere un bias induttivo, altrimenti non potrebbe concludere l'apprendimento. Potrei anche scegliere una risposta a caso ma non sarebbe una soluzione furba da prendere.

**Occam's Razor** è un principio che a parità di ipotesi consistenti devo scegliere quella più semplice come bias induttivo.

Semplice può avere molti significati diversi, in genere la più utilizzata è quella che fa meno assunzioni sui dati.

**No Free Lunch Theorem** in modo informale dice che nessun algoritmo di apprendimento universalmente migliore di altri quando le sue performance sono misurate su tutti i possibili mondi.

### 1.7.6 No Free Lunch Theorem

Denotiamo con:

- $P(h \mid X, \mathcal{L}_a)$ : **probabilità** che l'algoritmo  $\mathcal{L}_a$  restituisca l'ipotesi  $h$  dati i dati  $X$ 
  - $h$  è l'ipotesi, quello che stiamo imparando
  - $X$  è il training set
  - $\mathcal{L}_a$  è l'algoritmo di apprendimento
- $f$  è la **ground truth** il modello vero sottostante che vogliamo apprendere
- l'errore **out-of-sample** dell'ipotesi  $h$ , denotato con  $E_{ote}$ , è la media dell'errore su tutti gli elementi che non sono presenti nel training set, che sono commessi dai modelli appresi tramite  $\mathcal{L}_a$  sul training set  $X$ .

$$E_{ote}(\mathcal{L}_a \mid X, f) = \sum_h \sum_{x \in \chi - X} P(X) \mathbb{I}(h(X) \neq f(X)) P(h \mid X, \mathcal{L}_a)$$

Faccio la somma su tutte le possibili ipotesi, dopo di che sommo su tutti gli esempi che non sono nel training set ottenuto da  $\mathcal{X}$  (spazio di tutti i possibili esempi) togliendo gli elementi del training set.  $P(X)$  è la probabilità di estrarre uno specifico esempio per la funzione indicatrice  $\mathbb{I}(h(X) \neq f(X))$  (restituisce 1 se l'espressione è vera e il modello sta sbagliando a predire l'etichetta di  $X$  e 0 altrimenti) tutto per la probabilità di  $h$  su tutti i modelli.

### Dimostrazione

Vogliamo dimostrare che l'errore non dipende da  $\mathcal{L}_a$ , quindi un algoritmo vale l'altro in media.

$$\begin{aligned} \sum_f E_{ote}(\mathcal{L}_a | X, f) &= \sum_f \sum_h \sum_{\mathbf{x} \in \mathcal{X}-X} P(\mathbf{x}) \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) P(h | X, \mathcal{L}_a) \\ &= \sum_{\mathbf{x} \in \mathcal{X}-X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \sum_f \mathbb{I}(h(\mathbf{x}) \neq f(\mathbf{x})) \\ &= \sum_{\mathbf{x} \in \mathcal{X}-X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \frac{1}{2} 2^{|\mathcal{X}|} \\ &= \frac{1}{2} 2^{|\mathcal{X}|} \sum_{\mathbf{x} \in \mathcal{X}-X} P(\mathbf{x}) \sum_h P(h | X, \mathcal{L}_a) \\ &= \frac{1}{2} 2^{|\mathcal{X}|} \sum_{\mathbf{x} \in \mathcal{X}-X} P(\mathbf{x}) \cdot 1 \end{aligned}$$

Nella diapositiva precedente, il termine  $\frac{1}{2} 2^{|\mathcal{X}|}$  è il risultato della somma degli errori di tutte le possibili ipotesi binarie. Dato uno spazio campionario  $\mathcal{X}$ , esistono  $2^{|\mathcal{X}|}$  modi per etichettare gli esempi e, quindi,  $2^{|\mathcal{X}|}$  possibili ipotesi distinte. Se fissiamo un esempio  $X$  e un'ipotesi  $h$ , metà di queste ipotesi sarà in disaccordo con  $h$  su  $X$ , mentre l'altra metà sarà in accordo.

### Esempio

Consideriamo  $\mathcal{X} = \{X_1, X_2, X_3\}$ , ci concentriamo su un esempio randomico (facciamo  $X_2$ ), e assumiamo  $h(X_2) = 0$ , le funzioni in disaccordo con  $h$  su  $X_2$  sono:

Function	$f(\mathbf{x}_1)$	$f(\mathbf{x}_2)$	$f(\mathbf{x}_3)$
$f_1$	0	0	0
$f_2$	0	0	1
$f_3$	0	1	0
$f_4$	0	1	1
$f_5$	1	0	0
$f_6$	1	0	1
$f_7$	1	1	0
$f_8$	1	1	1

In generale, per qualsiasi  $X$  ed etichetta di  $h$ , metà delle  $2^{|\mathcal{X}|}$  funzioni sono in disaccordo con  $h$ .

Quindi abbiamo dimostrato che:

$$\sum_f E_{ote}(\mathcal{L}_a | X, f) = \frac{1}{2} 2^{|\mathcal{X}|} \sum_{X \in \mathcal{X}-X} P(X)$$

**Osservazione** Il teorema assume che si possa mediare su tutte le possibili  $f$  ma nel mondo non tutte le ipotesi sono ugualmente importanti. Questo è un risultato interessante, perché dimostra che **l'errore medio fuori campione** di un algoritmo di apprendimento è **indipendente dall'algoritmo stesso**. Ciò significa che **nessun algoritmo di apprendimento è migliore di un altro** quando si calcola la media su tutti i possibili problemi.

## 2 Selezione e valutazione di modelli

### 2.1 Accuracy e Error rate

Il modo più semplice per misurare la bontà di un modello è quella di contare il numero di predizioni sbagliate che esso compie.

$$E = \frac{a}{m}$$

Dove  $a$  solo il numero di predizioni sbagliate ed  $m$  le predizioni totali  $E$  sarà il suo **error rate**.

L'**accuratezza** è calcolata:

$$accuracy = 1 - E = \frac{m - a}{m}$$

L'errore quando viene valutato sul training set è chiamato **empirical error** o **training error**. Quando calcolo l'errore su un data set indipendente si chiamerà **generalization error** o **test error**.

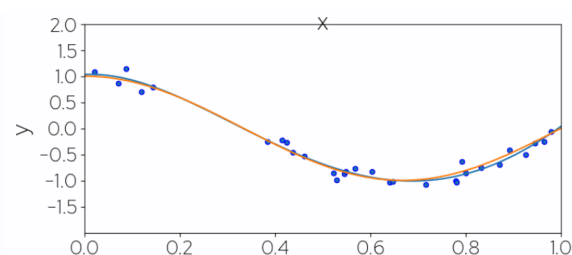
#### Nota

L'obiettivo principale di un algoritmo di apprendimento è quello di **minimizzare l'errore di generalizzazione**.

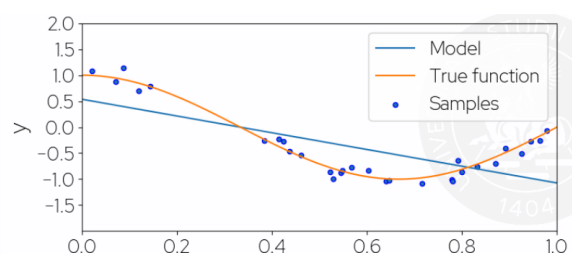
Durante l'addestramento non possiamo calcolare direttamente il **generalization error**, perché non abbiamo accesso ai nuovi esempi, quindi lo approssimiamo minimizzando il **training error**.

### 2.2 Overfitting

Quando un **modello si adatta troppo bene ai dati di training**, è probabile che alcune peculiarità degli esempi di training vengano assunte come proprietà generali dei dati. Questo porta a un modello che funziona bene sul set di training ma male sui nuovi campioni. Questo fenomeno è chiamato **overfitting**.



Il **fenomeno opposto**, in cui il modello è troppo semplice per catturare i modelli sottostanti nei dati, è chiamato **underfitting**.



L'**underfitting** è solitamente facilmente risolvibile utilizzando un modello più complesso. L'**overfitting** è più difficile da risolvere, poiché richiede un attento equilibrio tra complessità del modello e capacità di generalizzazione. Ciò nonostante, la maggior parte degli algoritmi di apprendimento dispone di meccanismi per prevenire l'overfitting, come **regularization techniques** o **early stopping**.

In genere si preferisce fare un leggero overfitting per avere una capacità espressiva sufficiente.

### 2.3 Metodi di valutazione

Possiamo valutare le prestazioni di un modello misurandone l'**errore di generalizzazione** su nuovi campioni. Tuttavia, non abbiamo accesso a nuovi campioni durante l'addestramento.

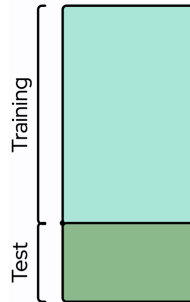


Utilizziamo invece diverse tecniche per stimare l'errore di generalizzazione sulla base dei dati di addestramento.

### 2.3.1 Validazione Hold-out

Divido l'insieme dei dati in due parti:

- **Training set:** dati che darò in pasto all'algoritmo per l'apprendimento.
- **Test set:** dati che utilizzerò per valutare.

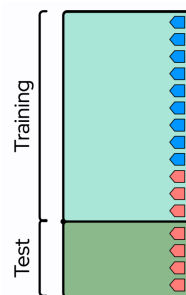


```
1 from sklearn.model_selection import train_test_split
2 ...
3
4 #Assume X,y contains the dataset
5
6 X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3,
7                                                    random_state=42)
```

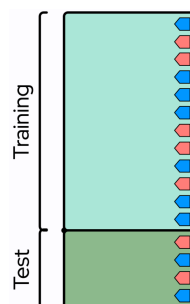
Come effettuare lo split:

- **Simple split**

I primi  $n$  dati gli prendo come training e i restanti come test. Ma se ho dei dati non casuali rischio di avere un test set non veritiero.



- **Stratified split** Si mescolano i dati prima di estrarli poi procedo a prendere i primi  $n$  come training e il restante come test.

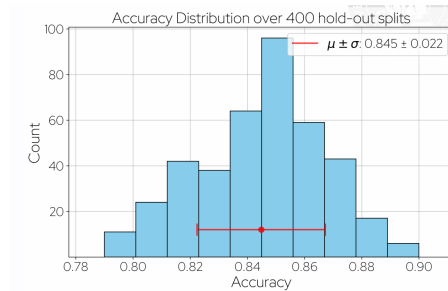


```

1 from model_selection import train_test_split
2 ...
3
4 #Assume X,y contains the dataset
5
6 X_train, X_test, y_train, y_test = train_test_split(X, y, test_size
7     =0.3, shuffle=True, #(default) sufficient for large datasets
8     stratify=y, #useful for small and/or imbalanced datasets
9     random_state=42)

```

Se ripetiamo l'esperimento con il metodo di valutazione hold-out molte volte otterremo tanti risultati diversi, perché training e test set cambiano.



Per ottenere una stima dell'errore di generalizzazione più affidabile possiamo ripetere la validazione hold-out molteplici volte e facciamo la media dei risultati.

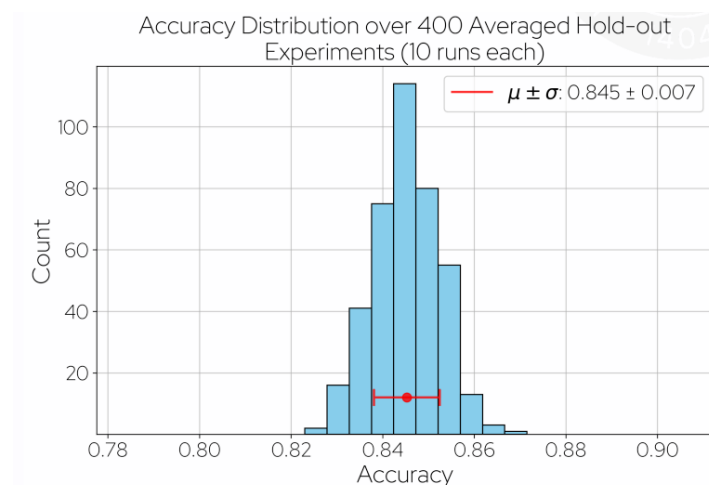
La media di  $n$  r.v. **indipendenti**, ognuno con media  $\mu$  e varianza  $\sigma^2$  è una nuova r.v. con:

**Media**

$$\frac{1}{n} \sum_{i=1}^n E_i = \frac{1}{n} \sum_{i=1}^n \mu = \mu$$

**Varianza**

$$\frac{1}{n^2} \sum_{i=1}^n \sigma^2 = \frac{\sigma^2}{n}$$

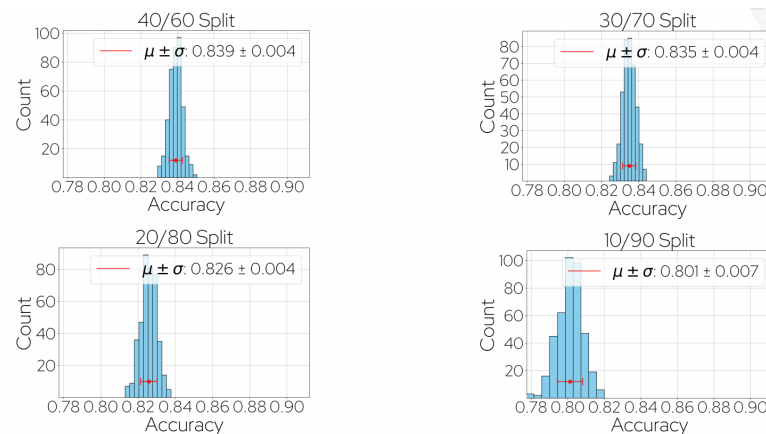


**Modifica del rapporto di divisione** Una cosa che influisce sull'ampiezza della campana è come stiamo separando il training set dal test set.



Nel momento in cui mettiamo più esempi nel training set otterremo un classificatore che dovrebbe essere più bravo a predire.

All'aumentare della percentuale di esempi nel test set avremo un'accuratezza minore ma la varianza diminuisce.

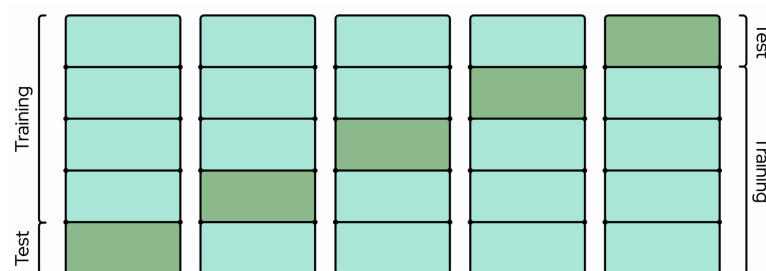


Continuando ad aumentare la percentuale di esempi per il test set la media andrà sempre peggiorando ma la varianza non migliorerà all'infinito anzi ricomincerà ad aumentare.

Se il dataset è grande abbastanza, la **validazione hold-out** è un **semplice ed efficace** metodo per stimare l'errore di generalizzazione.

Ma, se il **dataset** è **piccolo**, per tenere da parte una quantità sostanziale di dati per il testing potrebbe portare ad una stima non precisa dell'errore di generalizzazione. In questi casi si può usare la **cross-validation**.

### 2.3.2 Cross validation



Dividiamo il dataset in  $k$  parti, **ripetiamo il processo di hold-out**  $k$  volte. La prima volta utilizziamo i primi  $k - 1$  **fold** come training set e l'ultimo come test set, la volta successiva utilizziamo il penultimo come test set e tutti gli altri come training set e così via. Alla fine facciamo una **media** e otteniamo una **stima dell'errore di generalizzazione**.

Questa tecnica ha il vantaggio che l'algoritmo di apprendimento ha avuto l'opportunità di vedere, almeno una volta, tutti gli esempi.

### Metodo più flessibile

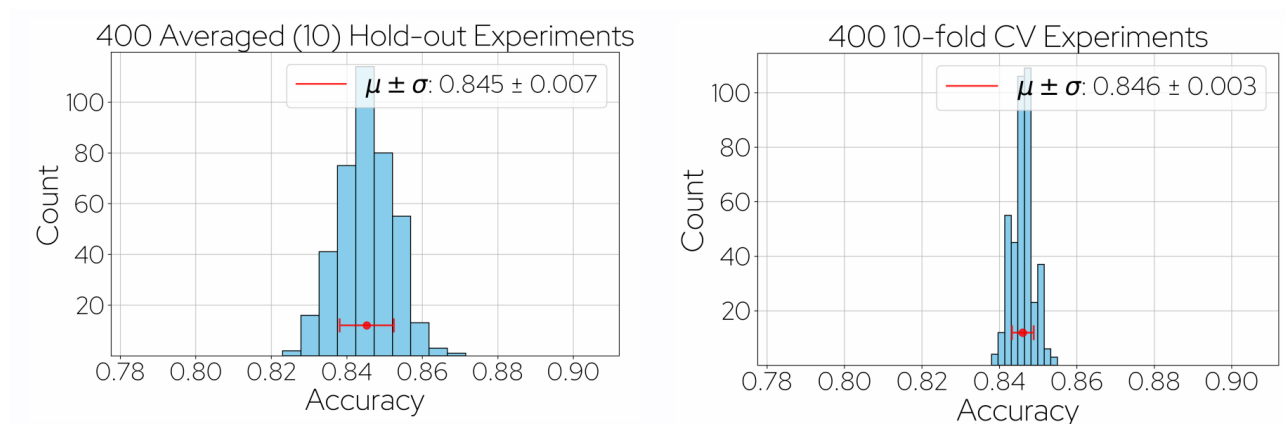
```
1 from sklearn.model_selection import KFold
2 from sklearn.linear_model import LogisticRegression
3 from sklearn.metrics import accuracy_score
4 import numpy as np
5
6 # Assume X,y contains the dataset
7
8 clf = LogisticRegression()
9
10 kf = KFold(n_splits=5, shuffle=True, random_state=42)
11 accuracies = []
12 for train_index, test_index in kf.split(X):
13     X_train, X_test = X[train_index], X[test_index]
14     y_train, y_test = y[train_index], y[test_index]
15
16     clf.fit(X_train, y_train)
17     score = accuracy_score(y_test, clf.predict(X_test))
18     accuracies.append(score)
19
20 print(f"x-val accuracy: {np.array(accuracies).mean()}")
```

Per sapere in modo veloce l'errore di generalizzazione.

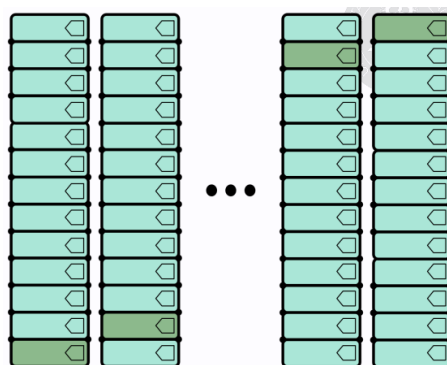
```
1 from sklearn.model_selection import cross_val_score
2 from sklearn.linear_model import LogisticRegression
3
4 # Assume X,y contains the dataset
5
6 clf = LogisticRegression()
7 scores = cross_val_score(clf, X, y, cv=5)
8 print(f"x-val accuracy: {scores.mean()}")
```

**Differenza tra hold-out e cross-validation:** Nella **cross validation**, ogni campione viene utilizzato per il test **una sola volta**, mentre se **ripetiamo hold-out**, alcuni campioni possono essere utilizzati **più volte per il test** e altri potrebbero **non essere mai utilizzati per il test**. Ciò si traduce in una stima più affidabile dell'errore di generalizzazione (**varianza minore**).

Se il **dataset è sufficientemente grande**, la differenza è trascurabile



### 2.3.3 Leave-One-Out



**Leave-One-Out** è un caso estremo di cross-validation dove **ogni campione viene utilizzato per il test una sola volta**, mentre tutti gli altri campioni vengono utilizzati per l'addestramento. Di conseguenza, l'**errore di generalizzazione** viene stimato con una **varianza molto bassa**. Tuttavia, il **costo computazionale** è molto elevato, poiché è necessario addestrare il modello  $m$  volte, dove  $m$  è il numero di campioni nel set di dati.

### 2.3.4 Bootstrapping

Dato un set di dati  $D$  con campioni  $m$ , il nostro obiettivo è stimare l'**errore di generalizzazione** di un modello addestrato sull'**intero set di dati**. Tuttavia, la validazione hold-out e la cross-validation richiedono di addestrare il modello su un sottoinsieme di dati, il che può portare a una stima distorta dell'errore di generalizzazione. Per superare questo problema, possiamo utilizzare il **bootstrapping**. L'idea è quella di **creare più campioni bootstrap** dal set di dati originale  $D$ , ciascuno contenente  $m$  campioni, campionando con restituzione.

#### Definizione

Un **campione bootstrap** è un campione ottenuto campionando con sostituzione dal set di dati originale un numero di esempi pari alla dimensione del set di dati originale.

#### Nota

I **campioni bootstrap non sono disgiunti**. Infatti, ogni campione è ottenuto campionando con sostituzione dal dataset originale, quindi **alcuni campioni potrebbero essere ripetuti** nello stesso campione bootstrap e **altri potrebbero non comparire in esso**.

In realtà è facile calcolare la probabilità che un campione non venga selezionato in un campione bootstrap:

$$P(\text{sample not selected}) = \left(1 - \frac{1}{m}\right)^m$$

Per valori grandi di  $m$ , questa probabilità è approssimativamente  $e^{-1} \approx 0.3679$ , il che significa che in media, circa il **37% dei campioni non viene selezionato** in un campione bootstrap.

Sia  $D'$  un campione bootstrap ottenuto da  $D$ . Possiamo **addestrare un modello** su  $D'$  e **valutarne le prestazioni** sui campioni in  $D - D'$  che non sono stati selezionati nel campione bootstrap. In questo modo, possiamo ottenere una stima dell'errore di generalizzazione del modello addestrato su un campione che ha la stessa dimensione del dataset originale.

#### Nota

Il bootstrapping è **particolarmente utile** quando il **set di dati è piccolo** o quando non esiste un modo efficace per suddividerlo in set di training e test. Quando il set di dati è più grande, il bootstrapping di solito non è necessario e vengono utilizzate la validazione hold-out o la validazione incrociata.

## 2.4 Tuning dei parametri

Uno dei motivi per cui si utilizzano i metodi di valutazione sopra descritti è la **selezione del modello migliore** tra un insieme di modelli candidati. Questo può significare selezionare il **miglior algoritmo di apprendimento** o selezionare i **migliori iperparametri** per un dato algoritmo di apprendimento.

### Definizione

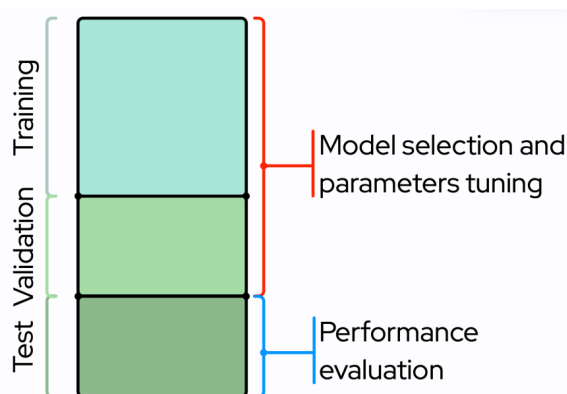
I **parametri** sono gli "oggetti" che l'algoritmo di apprendimento manipola per adattare il modello ai dati, come i pesi in una rete neurale o i coefficienti in un modello di regressione lineare. Gli **iperparametri** sono parametri dell'algoritmo di apprendimento stesso, come l'altezza di un albero decisionale o il parametro di regolarizzazione in un modello di regressione lineare.

La stima dell'errore di generalizzazione utilizzando le tecniche descritte può essere utilizzata per due scopi:

- **Selezione del modello o ottimizzazione dei parametri:** ovvero, selezionare il modello migliore tra un insieme di modelli candidati o selezionare i migliori iperparametri per un dato algoritmo di apprendimento.
- **Stima delle prestazioni:** ovvero stimare le prestazioni del modello finale sulla base di dati non visibili.

Per capire quale è l'algoritmo migliore facciamo un esperimento, prendiamo il dataset, facciamo l'addestramento prima con un set di iperparametri poi con un altro set, valutiamo l'errore di generalizzazione in entrambi i casi e scegliamo quello con l'errore più basso.

Così facendo stiamo valutando basandoci sul test set per fare una scelta quindi bisogna fare **attenzione a non sovraadattare il modello** al set di test. Ciò significa che non dovremmo utilizzare il **set di test per ottimizzare gli iperparametri** del modello, poiché ciò porterebbe a una stima distorta dell'errore di generalizzazione del modello finale.



Per non utilizzare il test set per decidere quali iperparametri utilizzare si divide il dataset in **3 parti**:

- **Training set**
- **Validation set:** una parte di esempi messa da parte per fare la stima degli **iperparametri**
- **Test set:** utilizzato alla fine di tutto quando il modello è stato già scelto per sapere quanto vale l'**errore di generalizzazione** del modello

### Esempio

Supponiamo di voler selezionare i migliori iperparametri per un algoritmo di apprendimento automatico. Si dispone di un set di 1000 iperparametri tra cui scegliere e si desidera misurare l'errore utilizzando il set di test. Poiché abbiamo visto che questo potrebbe rappresentare un problema, teniamo da parte anche un set aggiuntivo di esempi, il set di validazione, per misurare l'errore sul classificatore scelto.

## Esempio

Poiché sia i set di validazione che quelli di test sono **campioni finiti**, la misurazione dell'errore su di essi introdurrà un po' di rumore nella stima dell'errore di generalizzazione, ovvero:

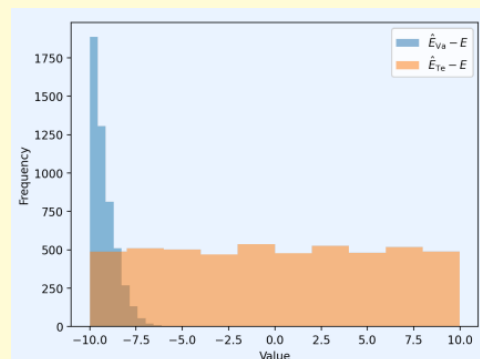
$$\hat{E}_{Tc} = E + \epsilon_{Te}, \quad \hat{E}_{Val} = E + \epsilon_{Val}$$

Si scelgono quindi gli iperparametri che riducono al minimo l'errore sul set di convalida.

**Domanda:** alla fine del processo, i due errori  $\hat{E}_{Te}$  e  $\hat{E}_{Val}$  saranno ancora stimatori senza bias dell'errore di generalizzazione? In altri termini,  $\mathbb{E}[\hat{E}_{Te}] = \mathbb{E}[\hat{E}_{Val}] = E$ ?

La media dello stimatore basata sul Validation set avrà un bias, invece quella basata sul Test set sarà senza bias.

```
1 # 1000 hyper-parameters to set, each yielding an error in (0, 100)
2 means = np.random.uniform(0, 100, 1000)
3
4 valid_error_dist = []
5 test_error_dist = []
6
7 N = 5000
8 for i in range(N):
9     samples = np.array(
10         [
11             [
12                 m,                                     #E
13                 m + np.random.uniform(-10, 10)        #E_val
14                 m + np.random.uniform(-10, 10)        #E_test
15             ]
16             for m in means
17         ]
18     )
19
20 #selects the best hp according to R_val
21 amin = np.argmin(samples[:, 1])
22
23 valid_error_dist.append(samples[amin, 1] - samples[amin, 0])
24 test_error_dist.append(samples[amin, 2] - samples[amin, 0])
```



## 2.5 Misurazione delle performance

**Diversi indicatori di performance** riflettono le diverse esigenze dei compiti e producono risultati di valutazione diversi. La scelta dell'indicatore di performance corretto è fondamentale per una corretta valutazione del modello.

### 2.5.1 Mean Square Error (MSE)

L'errore quadratico medio è una misura di prestazione comune per le attività di regressione. In generale, se si conosce la **distribuzione dei dati**  $\mathcal{D}$ , l'errore quadratico medio di una funzione è definito come:

$$E(f; \mathcal{D}) = \mathbb{E}_{(X,y) \sim \mathcal{D}}[(f(X) - y)^2] = \int_{(X,y) \sim \mathcal{D}} (f(X) - y)^2 p(X, y) dX dy$$

Nella maggior parte dei casi, non conosciamo la distribuzione dei dati  $\mathcal{D}$ , ma disponiamo di un set di dati  $D = \{(X_i, y_i)\}_{i=1}^m$  di  $m$  campioni estratti da  $\mathcal{D}$ . In questo caso, possiamo stimare l'errore quadratico medio come:

$$E(f; D) = \frac{1}{m} \sum_{i=1}^m (f(X_i) - y_i)^2$$

### 2.5.2 Error rate

Analogamente all'errore quadratico medio, possiamo definire il **tasso di errore** e l'**accuratezza** per le attività di classificazione. La forma generale, supponendo di conoscere la distribuzione dei dati, è:

$$E(f; \mathcal{D}) = \mathbb{E}_{(X,y) \sim \mathcal{D}}[\mathbb{I}(f(X) \neq y)] = \int_{(X,y) \sim \mathcal{D}} \mathbb{I}(f(X) \neq y) p(X, y) dX dy$$

Dove  $\mathbb{I}$  è la **funzione indicatrice** che restituisce 1 se la condizione è vera e 0 altrimenti.

Se disponiamo di un set di dati  $D = \{(X_i, y_i)\}_{i=1}^m$  di  $m$  campioni estratti da  $\mathcal{D}$ , possiamo stimare il tasso di errore come:

$$E(f; D) = \frac{1}{m} \sum_{i=1}^m \mathbb{I}(f(X_i) \neq y_i)$$

### 2.5.3 Accuracy

L'accuratezza è il **complementare dell'error rate**:

$$acc(f; \mathcal{D}) = 1 - E(f; \mathcal{D}) = 1 - \mathbb{E}_{(X,y) \sim \mathcal{D}}[\mathbb{I}(f(X) \neq y)]$$

o, considerando un dataset  $D = \{(X_i, y_i)\}_{i=1}^m$  di  $m$  campioni estratti da  $\mathcal{D}$ :

$$acc(f; D) = 1 - E(f; D) = 1 - \frac{1}{m} \sum_{i=1}^m \mathbb{I}(f(X_i) \neq y_i)$$

### 2.5.4 Matrice di confusione

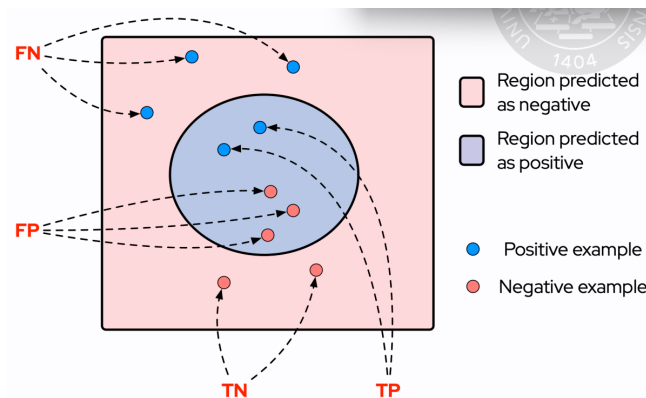
È possibile definire molte altre misure di performance, a seconda del compito e dei requisiti specifici. Per le attività di classificazione, molte di queste misure possono essere derivate dalla **matrice di confusione**.

	Predicted Positive	Predicted Negative
Actual Positive	<b>TP</b>	<b>FN</b>
Actual Negative	<b>FP</b>	<b>TN</b>

con:

- **TP: True Positive** (numero degli esempi che sono stati predetti positivi ed erano veramente positivi)
- **FP: False Positive** (predetti positivi ma in realtà negativi)
- **TN: True Negative** (predetti negativi e veramente negativi)
- **FN: False Negative** (predetti negativi ma in realtà positivi)





### 2.5.5 Precision, Recall

A volte, gli **errori** non sono **ugualmente importanti**. Ad esempio, in un'attività di diagnosi di cancro, un falso negativo (mancanza di una malattia) può essere più critico di un falso positivo (diagnosi errata di una malattia).

In questo esempio, potremmo voler dare **priorità al richiamo** (recall) (la capacità di identificare tutti i casi di cancro) rispetto alla **precisione** (la capacità di evitare false diagnosi di cancro).

In un'attività di rilevamento dello spam, d'altra parte, potremmo voler dare **priorità alla precisione** (per evitare di etichettare erroneamente email legittime come spam) rispetto al **richiamo** (recall) (per identificare tutti i messaggi di spam).

Più formalmente, la **precisione** è definita come:

$$precision = \frac{TP}{TP + FP} = \frac{TP}{\#predicted\ positives}$$

e il **richiamo** (recall) è definito come:

$$recall = \frac{TP}{TP + FN} = \frac{TP}{\#actual\ positives}$$

**Precision** e **recall** vengono spesso utilizzati insieme, poiché forniscono informazioni complementari sulle prestazioni del modello. **Di solito sono contraddittorie**, il che significa che l'aumento di una spesso porta a una diminuzione dell'altra.

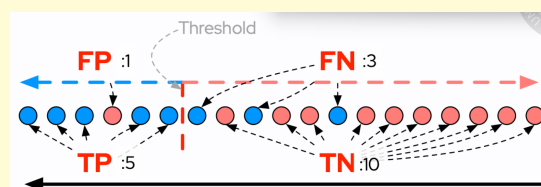
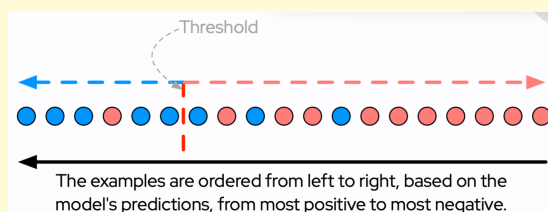
Ad esempio, se iniziamo a classificare **più campioni come positivi**, aumenteremo il numero di veri positivi, ma anche il numero di falsi positivi, **diminuendo** così la **precisione**, ma **aumentando** il **recall**.

D'altra parte, se iniziamo a classificare **meno campioni come positivi**, diminuiranno il numero di falsi positivi, **aumentando** così la **precisione**, ma anche il numero di falsi negativi, **diminuendo** così il **recall**.

### 2.5.6 P-R Plots

Supponiamo di avere un classificatore che fornisca un **punteggio di confidenza** per ciascun campione, indicando quanto è sicuro che il campione appartenga alla classe positiva. È quindi possibile variare una **soglia** su questo punteggio per ottenere diversi valori di precision e recall.

#### Esempio

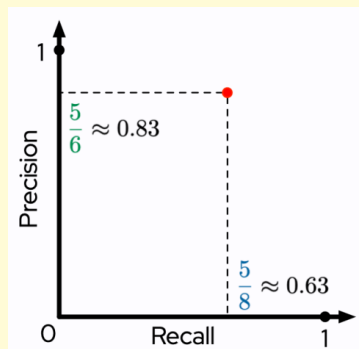


## Esempio

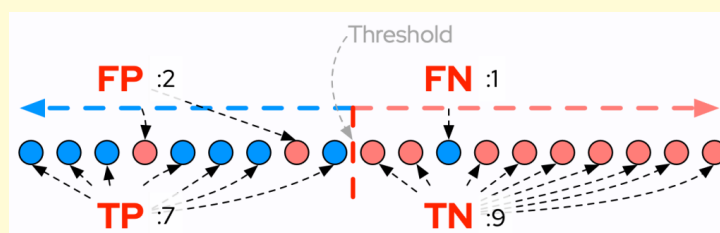
In questo esempio ho  $FP = 1$ ,  $FN = 3$ ,  $TP = 5$ ,  $TN = 10$

$$precision = \frac{TN}{TP + FP} = \frac{5}{6}$$

$$recall = \frac{TP}{TP + FN} = \frac{5}{8}$$

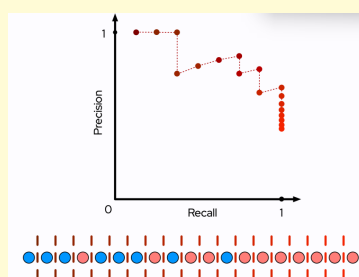
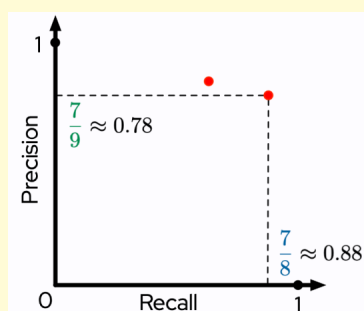


Cambiando la posizione della soglia otterrò:



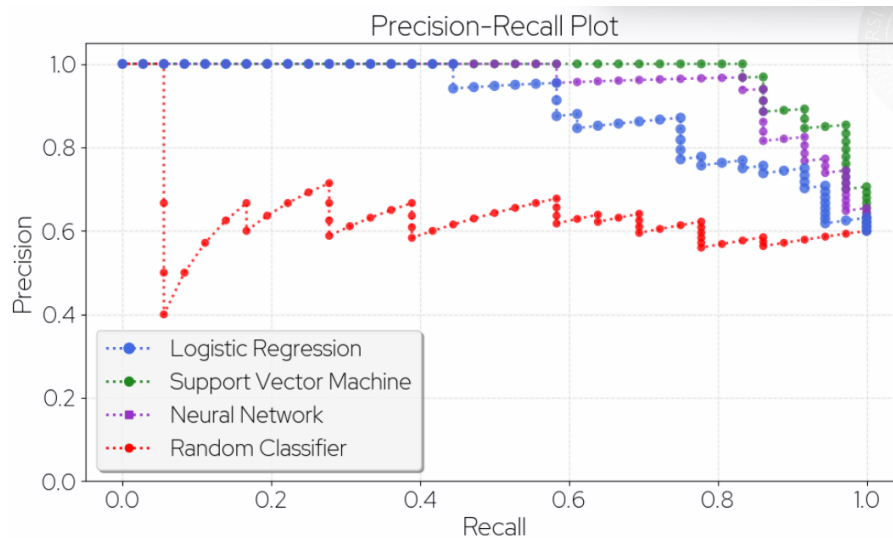
$$precision = \frac{TN}{TP + FP} = \frac{7}{9}$$

$$recall = \frac{TP}{TP + FN} = \frac{7}{8}$$



Dovendo confrontare più classificatori che restituiscono una soglia di confidenza ottengo un grafico

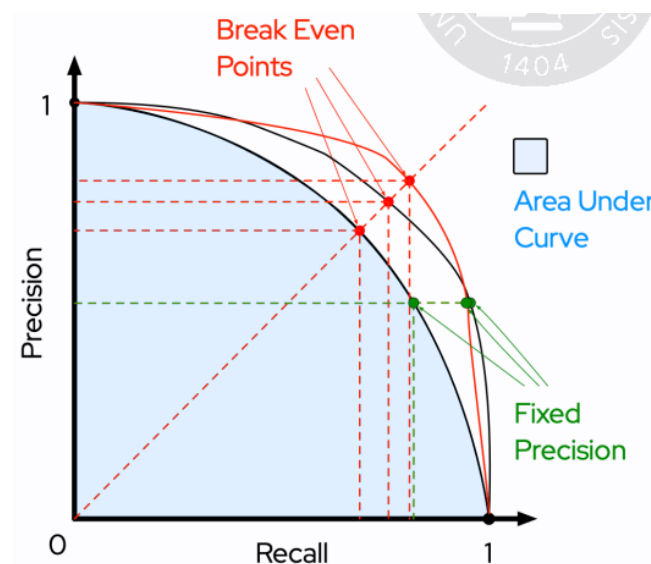
del tipo:



In particolare si può vedere che le **Support Vector Machine** (in verde) dominano tutti gli altri classificatori, se dovessi scegliere un classificatore sceglierei questo perché a parità di threshold vince su tutti gli altri.

Come selezioniamo gli studenti migliori date alcune curve precisione-richiamo?

- **Fissare un dato punto di precision** o recall e selezionare il modello che raggiunge il miglior richiamo o precisione in quel punto.
- Selezionare la curva con l'**area sotto la curva (AUC) più alta** (n.b. difficile da calcolare).
- Selezionare il **miglior punto di break-even**, ovvero il punto in cui precision e recall sono uguali.



**F1-score** Una misura importante che combina precision e recall è il **punteggio F1**, definito come la **media armonica** di precision e recall:

$$F1 = \frac{2}{\frac{1}{precision} + \frac{1}{recall}} = \frac{2 \times precision \times recall}{precision + recall} = \frac{2 \times TP}{TOT + FP - FN}$$

o in forma più generale ( $F_\beta$ -score):

$$F_\beta = \frac{1 + \beta^2}{\frac{1}{precision} + \frac{\beta^2}{recall}} = \frac{(1 + \beta^2) \times precision \times recall}{\beta^2 \times precision + recall}$$

## Media armonica ponderata

La media armonica ponderata di due valori  $a$  e  $b$  è definita come:

$$\frac{(w_a + w_b)}{\frac{w_a}{a} + \frac{w_b}{b}}$$

## Nota

La F-misura definita da  $F_\beta$  misura quanto sono bravo a recuperare gli esempi rispetto ad un utente che pensa che la recall sia  $\beta$  volte più importante della precision.

Supponiamo di voler **calcolare la media** dei contributi di **diverse matrici di confusione** (ad esempio, perché ci troviamo in un problema multi-classe, o vogliamo combinare i risultati di diversi round di convalida incrociata). Indichiamo con  $P$  e  $R$  le statistiche di **precision** e **recall**.

Questo può essere fatto in due modi:

1. **Macro-averaging**: calcolo la Precision e la Recall per ogni matrice di confusione, denotate come  $(P_1, R_1), (P_2, R_2), \dots, (P_n, R_n)$ . Prendendo la loro media abbiamo la precision, recall e  $F_1$  macro-averaged:

$$macro-P = \frac{1}{n} \sum_{i=1}^n P_i$$

$$macro-R = \frac{1}{n} \sum_{i=1}^n R_i$$

$$macro-F_1 = \frac{2 \times macro-P \times macro-R}{macro-P + macro-R}$$

2. **Micro-averaging**: calcolare le medie elemento per elemento nelle matrici di confusione, per ottenere  $\overline{TP}, \overline{FP}, \overline{TN}, \overline{FN}$ , e quindi calcola la micro precision, recall e  $F_1$  come:

$$micro-P = \frac{\overline{TP}}{\overline{TP} + \overline{FP}}$$

$$micro-R = \frac{\overline{TP}}{\overline{TP} + \overline{FN}}$$

$$micro-F_1 = \frac{2 \times micro-P \times micro-R}{micro-P + micro-R}$$

- **Macro-averaging** tratta tutte le matrici di confusione allo stesso modo, indipendentemente dalle loro dimensioni. Questo significa che matrici di confusione di piccole dimensioni possono avere un impatto significativo sul risultato finale.
- **Micro-averaging** attribuisce maggiore peso alle matrici di confusione più grandi, poiché contribuiscono maggiormente al conteggio complessivo di TP, FP, TN e FN. Ciò significa che il risultato finale è più rappresentativo della performance complessiva di tutte le matrici di confusione.

Ciò è importante, ad esempio, nei problemi di classificazione multiclasse in cui le classi possono essere sbilanciate.

### Esempio $Macro-F_1$

Assumendo di avere tre matrici di confusione:

$$CM_1 = \begin{bmatrix} 10 & 2 \\ 1 & 7 \end{bmatrix} \quad CM_2 = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \quad CM_3 = \begin{bmatrix} 9 & 1 \\ 1 & 8 \end{bmatrix}$$

CM	precision	recall	F1-score
CM <sub>1</sub>	0.9091	0.8333	0.8695
CM <sub>2</sub>	0.8000	0.7273	0.7619
CM <sub>3</sub>	0.9000	0.9000	0.9000
Avg	0.8697	0.8202	0.8438

$$macro-F_1 = \frac{2 \times macro-P \times macro-R}{macro-P + macro-R} = \frac{2 \times 0.8697 \times 0.8202}{0.8697 + 0.8202} \approx 0.8442$$

### Esempio $Micro-F_1$

Con le stesse matrici di confusione di prima:

$$CM_1 = \begin{bmatrix} 10 & 2 \\ 1 & 7 \end{bmatrix} \quad CM_2 = \begin{bmatrix} 8 & 3 \\ 2 & 6 \end{bmatrix} \quad CM_3 = \begin{bmatrix} 9 & 1 \\ 1 & 8 \end{bmatrix} \Rightarrow \overline{CM} = \begin{bmatrix} 9 & 2 \\ 1.3333 & 7 \end{bmatrix}$$

La precision e recall micro-averaged sono:

$$micro-P = \frac{9}{9 + 1.3333} = 0.8710 \quad micro-R = \frac{9}{9 + 2} = 0.8182$$

La  $F_1$  micro-averaged è:

$$micro-F_1 = \frac{2 \times micro-P \times micro-R}{micro-P + micro-R} = \frac{2 \times 0.8710 \times 0.8182}{0.8710 + 0.8182} = 0.8438$$

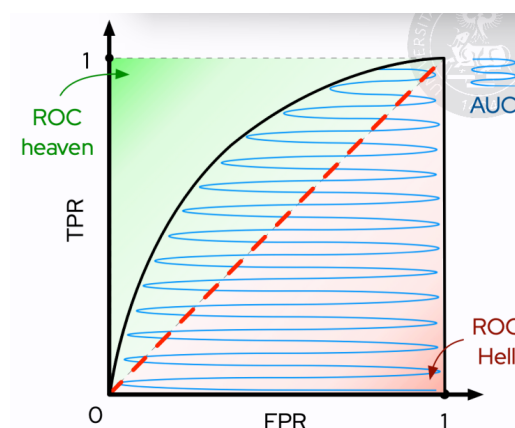
## 2.5.7 ROC e AUC

Se, invece di utilizzare precision e recall, tracciamo il **false positive rate (FPR)** rispetto al **true positive rate (TPR)**, otteniamo un grafico **ROC** (Receiver Operating Characteristic curve).

$$FPR = \frac{FP}{FP + TN} = \frac{FP}{\#actual\ negative}$$
$$TPR = \frac{TP}{TP + FN} = \frac{TP}{\#actual\ positives}$$

Come nei grafici P-R, diciamo che un learner  $A$  è migliore di un learner  $B$  se la curva ROC di  $A$  racchiude interamente la curva ROC di  $B$ . Tuttavia, quando esistono intersezioni, nessun learner è generalmente migliore dell'altro.

Un modo per confrontare le curve ROC intersecate è calcolare le **aree sotto le curve ROC**.



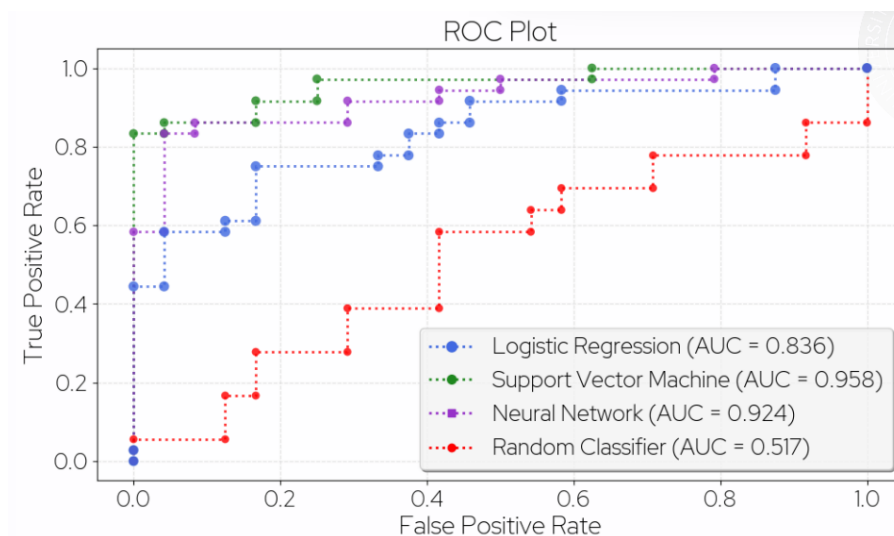
In alto a sinistra (**ROC heaven**) troviamo classificatori che **non sbagliano mai**, in basso a destra (**ROC Hell**) troviamo classificatori che **sbagliano sempre** e al centro sono presenti i peggiori classificatori perché rispondono sempre a caso. Noi **vogliamo stare il più lontano possibile dalla diagonale**.

**Area Under the Curve (AUC)** Nel caso delle curve ROC, l'area sotto la curva (AUC) è facile da calcolare (anche per le curve teoriche, poiché è sempre non decrescente).

Si può anche dimostrare che è correlata all'errore di ranking del classificatore.

$$1 - AUC = \ell_{rank} \triangleq \frac{1}{m^+ m^-} \sum_{X^+ \in D^+} \sum_{X^- \in D^-} \mathbb{I}[f(X^+) < f(X^-)] + \frac{1}{2} \mathbb{I}[f(X^+) = f(X^-)]$$

Somma su tutti gli esempi positivi, somma su tutti gli esempi negativi calcoliamo un punto di errore se il ranking dell'esempio positivo è minore del ranking dell'esempio negativo, abbiamo anche un altro termine perché possiamo avere dei casi in cui c'è un pareggio in questo caso assegnano mezzo punto di errore. Facciamo la somma di tutto e per normalizzarlo dividiamo tutto per il numero di esempi positivi moltiplicata per il numero di esempi negativi.



```

1 # ...
2 # Assume X_train, X_test, y_train, y_test are defined
3
4 clf = LogisticRegression()
5 clf.fit(X_train, y_train)
6
7 y_scores = clf.predict_proba(X_test)[: , 1]
8
9 # Compute ROC curve and AUC
10 fpr, tpr, _ = roc_curve(y_test, y_scores)
11 roc_auc = auc(fpr, tpr)
12
13 # You can easily plot the ROC curve using matplotlib
14 plt.plot(fpr, tpr)
15
16 # Alternatively, you can directly use roc_auc_score
17 roc_auc2 = roc_auc_score(y_test, y_scores)
18
19 # For Precision-Recall, we don't usually compute
20 # AUC, but we can compute the average precision score
21 avg_precision = average_precision_score(y_test, y_scores)

```