Introduzione all'apprendimento automatico

Algoritmi per l'intelligenza artificiale

Vincenzo Bonnici
Corso di Laurea Magistrale in Scienze Informatiche
Dipartimento di Scienze Matematiche, Fisiche e Informatiche
Universitá degli Studi di Parma

2025-2026

Apprendimento automatico

Nel campo dell'apprendimento automatico classico, esistono tre tipi principali di attività: **supervisionate** (supervised), **semi-supervisionate** (semi-supervised) e **non supervisionate** (unsupervised).
Di "recente" si é anche affermato il ramo dell'**apprendimento per rinforzo** (reinforcement learning).

La differenza principale tra questi tipi di attività del "machine learning" è il livello di disponibilità dei "dati di verità di base" (**ground truth**, termine usato in vari campi per riferirsi alle informazioni fornite dall'osservazione diretta – cioè prove empiriche – in contrapposizione alle informazioni fornite dall'inferenza), che è una conoscenza preliminare di ciò che il risultato del modello dovrebbe essere (l'output) per un determinato input.

Apprendimento automatico

L'apprendimento automatico **supervisionato** mira ad apprendere una funzione che, dato un campione di dati e output desiderati, si avvicina a una funzione che mappa gli input agli output.

L'apprendimento automatico **semi-supervisionato** ha lo scopo di etichettare i punti dati senza etichetta utilizzando le conoscenze apprese da un piccolo numero di dati etichettati;

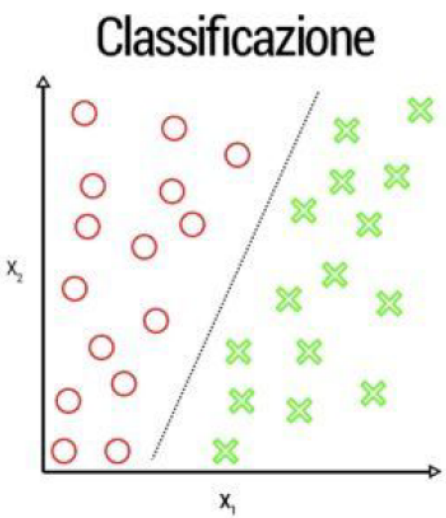
L'apprendimento automatico **senza supervisione** non ha output etichettati, quindi il suo obiettivo è dedurre la struttura naturale presente all'interno di un insieme di dati.

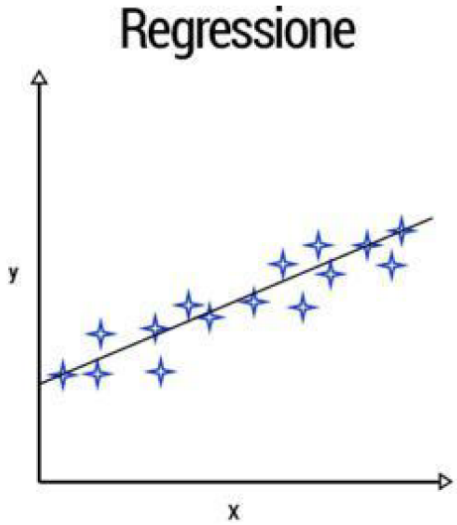
L'apprendimento **con rinforzo** punta a realizzare agenti autonomi in grado di scegliere azioni da compiere per il conseguimento di determinati obiettivi tramite interazione con l'ambiente in cui sono immersi, in modo da massimizzare la nozione di premio cumulativo.

Apprendimento supervisionato

L'apprendimento **supervisionato** viene in genere svolto nel contesto della

- **classificazione**, quando vogliamo mappare l'input alle etichette di output
- **regressione**, quando vogliamo mappare l'input a un output continuo.





Algoritmi comuni nell'apprendimento supervisionato includono regressione logistica, classificatore bayesiano naif (generalmente per la categorizzazione di testi), macchine a vettori di supporto (modelli associati ad algoritmi di apprendimento per la regressione e la classificazione), reti neurali artificiali e le cosiddette foreste casuali (classificatori d'insieme composti da molti alberi di decisione).

Apprendimento supervisionato

Sia nella regressione che nella classificazione, l'obiettivo è trovare **relazioni** o **strutture specifiche** nei dati di input che ci consentano di produrre in modo efficace dati di output corretti.

Si noti che l'output "corretto" è determinato interamente dai **dati di addestramento**, quindi mentre abbiamo una "verità di base" che il nostro modello riterrà vera, non si può dire che le etichette dei dati siano sempre corrette nelle situazioni del **mondo reale**. Le etichette dei dati "rumorose" o "errate" ridurranno chiaramente l'efficacia del modello.

Apprendimento supervisionato: overfitting

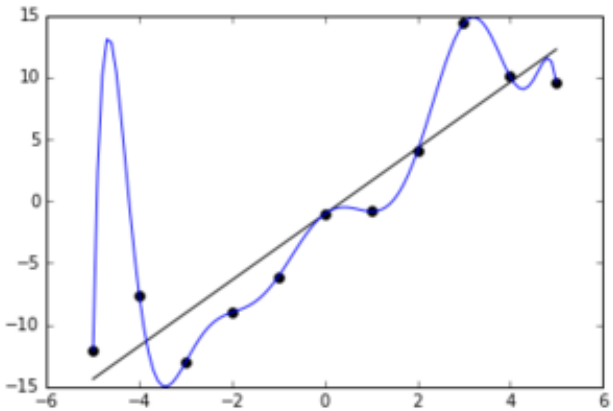
La **complessità** del modello si riferisce alla complessità della funzione che si sta tentando di apprendere, simile al grado di un polinomio. Il corretto livello di complessità del modello è generalmente determinato dalla natura dei dati di allenamento.

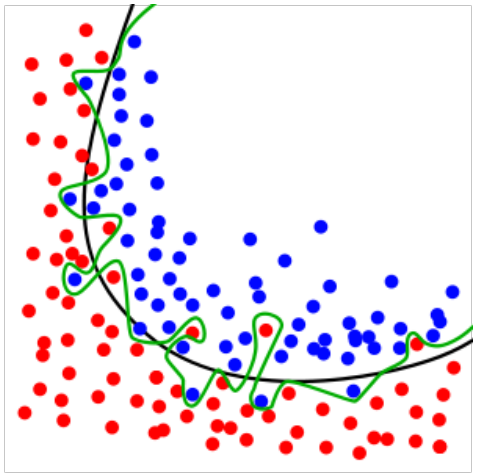
Se hai una **piccola quantità** di dati o se i tuoi **dati non sono distribuiti uniformemente** in diversi scenari possibili, dovresti optare per un modello a **bassa complessità**. Ciò è dovuto al fatto che un modello ad alta complessità verrà "sovradattato" (**overfitting**, un modello statistico molto complesso si adatta ai dati osservati – **il campione** – perché ha un numero eccessivo di parametri rispetto al numero di osservazioni) se utilizzato su un numero ridotto di punti dati.

L'overfitting si riferisce all'apprendimento di una funzione che si adatta molto bene ai dati di training, ma **non generalizza** ad altri punti dati: si sta imparando rigorosamente a produrre i dati di training senza apprendere la tendenza o la struttura effettiva nei dati che guida a questo output.

Apprendimento supervisionato: overfitting

Immaginate di cercare di adattare una curva tra 2 punti. In teoria, è possibile utilizzare una funzione di qualsiasi grado, ma in pratica, si potrebbe parsimoniosamente aggiungere complessità, e procedere con una funzione lineare.





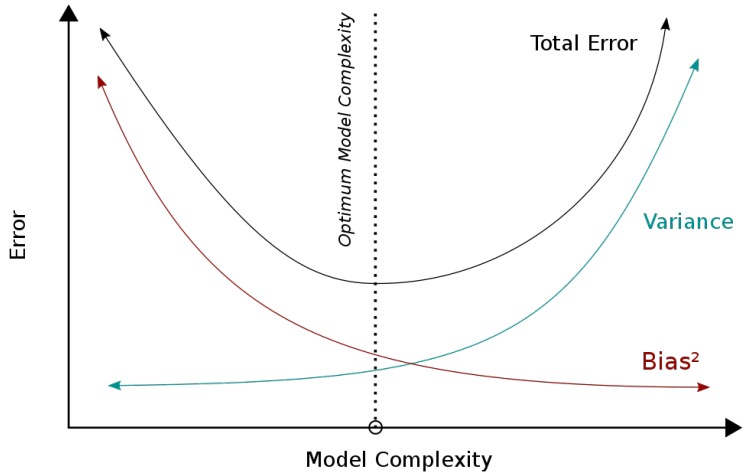
Apprendimento supervisionato: compromesso bias-varianza

Il compromesso bias-varianza si riferisce anche alla generalizzazione del modello. In qualsiasi modello, c'è un equilibrio tra

- **distorsione** (bias), che è il termine di errore costante,
- e la **varianza**, che è la quantità in base alla quale l'errore può variare tra diversi set di dati.

Il problema é quindi quello di creare un modello che da un lato cattura accuratamente le regolairtá dei dati di addestramento, ma dall'altro lato é in grado di generalizzare bene su dati non di addestramento.

Apprendimento supervisionato: compromesso bias-varianza

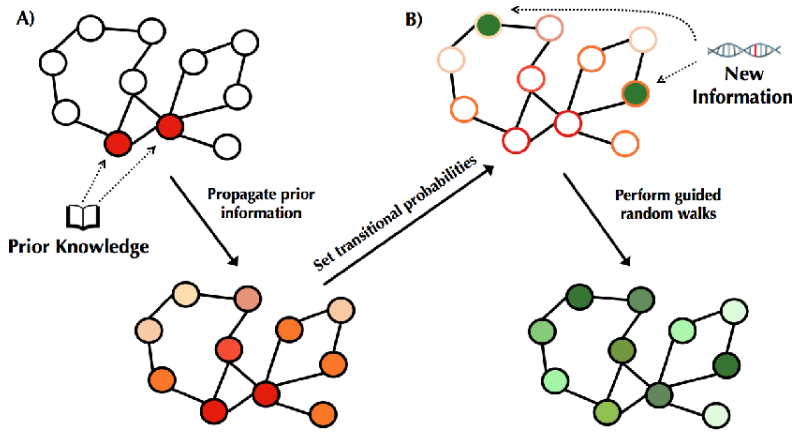


In generale, l'aumento della distorsione (e la riduzione della varianza) si traduce in modelli con livelli di prestazione relativamente garantiti, che possono essere fondamentali in determinate attività. Inoltre, per produrre modelli che si generalizzano bene, la varianza del modello deve essere ridimensionata in base alle dimensioni e alla complessità dei dati di allenamento. I set di dati semplici e di piccole dimensioni devono in genere essere appresi con modelli a bassa varianza e set di dati complessi e di grandi dimensioni spesso richiedono modelli con varianza più elevata per apprendere appieno la struttura dei dati.

Apprendimento semi-supervisionato

Se stessimo cercando di rilevare messaggi inappropriati in un social network, non ci sarebbe modo di ottenere informazioni etichettate a mano su ogni messaggio, poiché ce ne sono semplicemente troppe e sarebbe troppo costoso. Invece, possiamo etichettare a mano un sottoinsieme di essi e sfruttare le tecniche semi-supervisionate per utilizzare questo piccolo set di dati etichettati per aiutarci a comprendere il resto del contenuto dei messaggi appena arrivano.

Alcuni metodi semi-supervisionati comuni sono le macchine vettoriali di supporto trasversali e i metodi basati su grafi, ad esempio la propagazione delle etichette.



Apprendimento semi-supervisionato: presuppposti

I metodi semi-supervisionati devono fare alcune ipotesi (presupposti) sui dati al fine di giustificare l'utilizzo di una piccola serie di dati etichettati per trarre conclusioni sui punti dati non etichettati.

- **continuità**: si presume che i punti dati "vicini" tra loro abbiano maggiori probabilità di avere un'etichetta comune.
- **ipotesi del cluster**: si presume che i dati formino naturalmente cluster discreti e che i punti nello stesso cluster abbiano maggiori probabilità di condividere un'etichetta.
- **presupposto molteplice**: si presume che i dati si trovino approssimativamente in uno spazio di dimensioni inferiori (o collettore) rispetto allo spazio di input. Questo scenario è rilevante quando un sistema non osservabile o difficile da osservare con un numero ridotto di parametri produce output osservabile ad alta dimensione.

Apprendimento non supervisionato

I metodi **senza supervisione** trovano **modelli intrinseci** nei dati.

Le attività più comuni nell'apprendimento senza supervisione sono il **clustering** (raggruppamento), l'apprendimento della **rappresentazione** e la **stima della densità**.
In tutti questi casi, desideriamo conoscere la struttura intrinseca dei nostri dati **senza utilizzare etichette** fornite in modo esplicito. Alcuni algoritmi comuni includono il clustering, l'analisi dei componenti principali e gli autocodificatori (autoencoders).

Poiché non vengono fornite etichette, non esiste un modo specifico per confrontare le **prestazioni** del modello nella maggior parte dei metodi di apprendimento senza supervisione.

Apprendimento non supervisionato

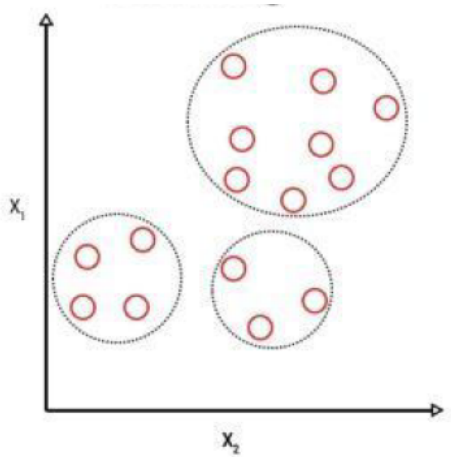
Abbiamo due tecniche che ci vengono in aiuto nell'affrontare problemi di apprendimento non supervisionato:

- il **clustering**
- la **riduzione della dimensionalità dei dati**

Clustering

Il Clustering è una tecnica esplorativa che consente di aggregare all'interno di gruppi (detti cluster) dei dati i quali non abbiamo precedente conoscenza di appartenenza a gruppi.

Avremo quindi dei grossi data set dove i dati al loro interno hanno degli elementi simili tra di loro. All'interno di ogni singolo gruppo (o cluster) troveremo quindi quei dati che hanno molte caratteristiche simili tra loro.

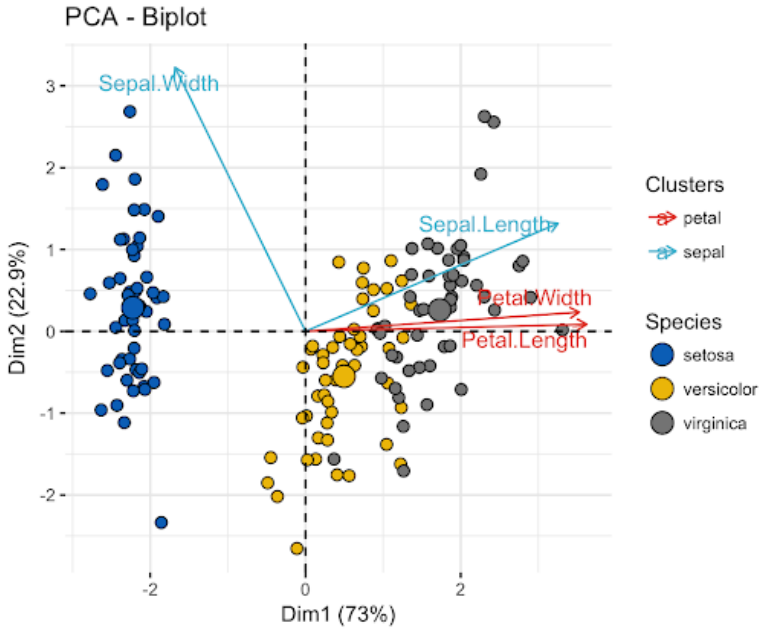


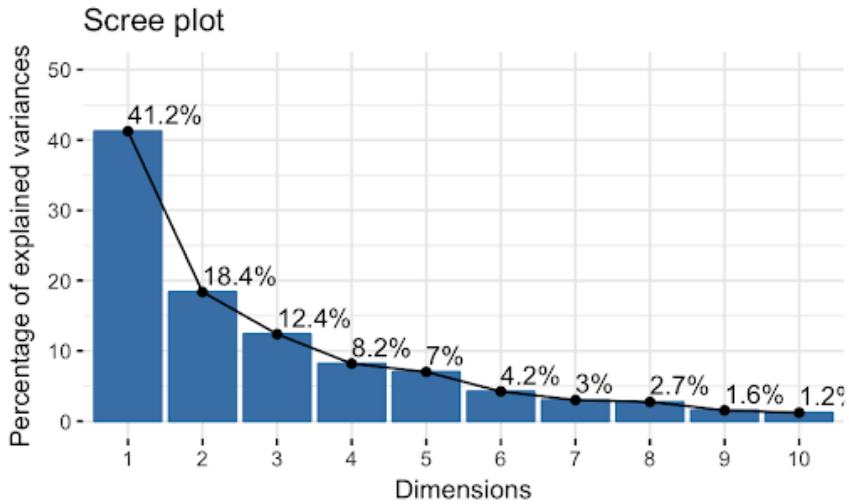
Il clustering è un'ottima tecnica che ci permette quindi di scovare relazioni tra i dati.

Riduzione della dimensionalità

La riduzione della dimensionalità senza supervisione è un approccio molto utilizzato nella pre-elaborazione delle features (caratteristiche), con l'obiettivo di eliminare il "rumore" dai dati.

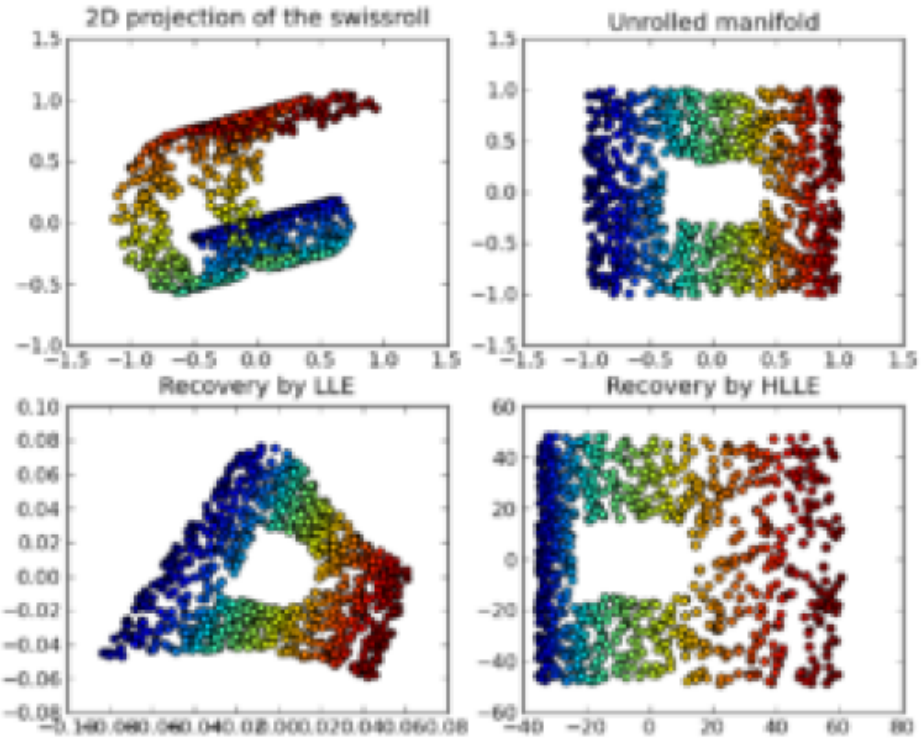
Questa riduzione può anche causare una minore prestazione predittiva, ma può anche rendere lo spazio dimensionale più compatto al fine di mantenere le informazioni più rilevanti.





Riduzione della dimensionalità

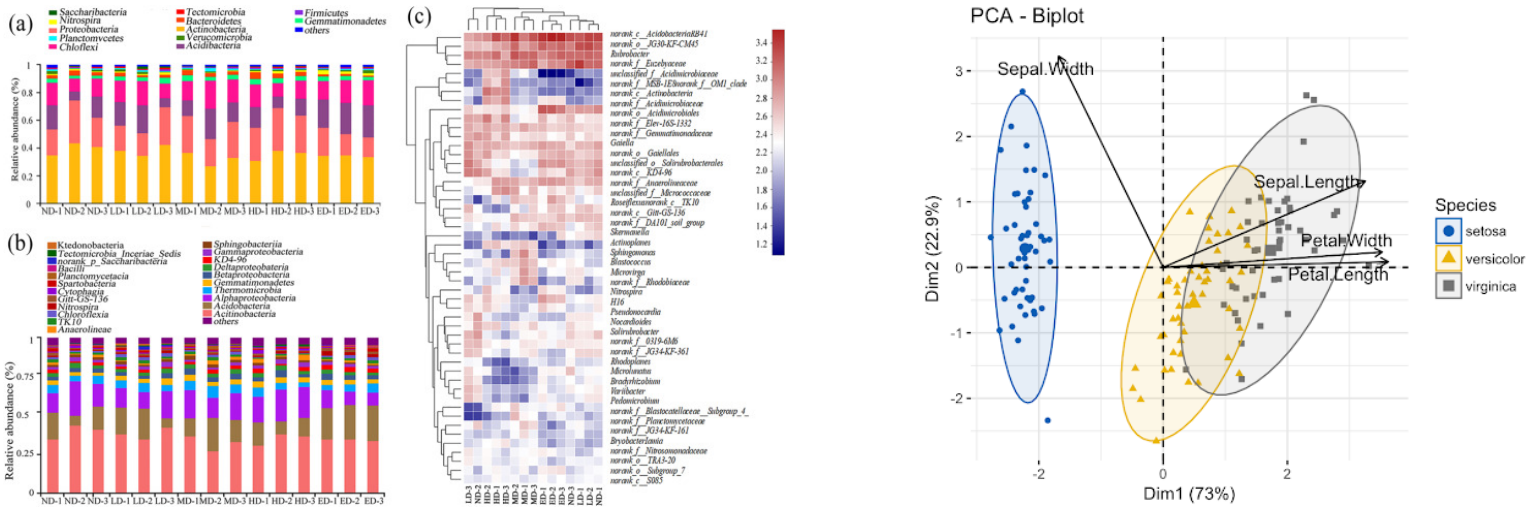
La riduzione della dimensionalità può essere utile anche per la rappresentazione dei dati, come ad esempio all'interno di un feature space (spazio delle caratteristiche) a elevata dimensionalità, che possono essere così proiettati su uno spazio 1D, 2D e 3D



Apprendimento non supervisionato: analisi esplorativa

L'apprendimento senza supervisione è molto utile nell'**analisi esplorativa** (exploratory data analysis) perché può identificare automaticamente la struttura nei dati.

Ad esempio, se un analista tentasse di segmentare i consumatori, i metodi di clustering senza supervisione sarebbero un ottimo punto di partenza per la loro analisi.



In situazioni in cui è impossibile o impraticabile per un essere umano proporre tendenze nei dati, l'apprendimento non supervisionato può fornire informazioni iniziali che possono poi essere utilizzate per testare/verificare singole ipotesi.