UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Laurea triennale in Informatica

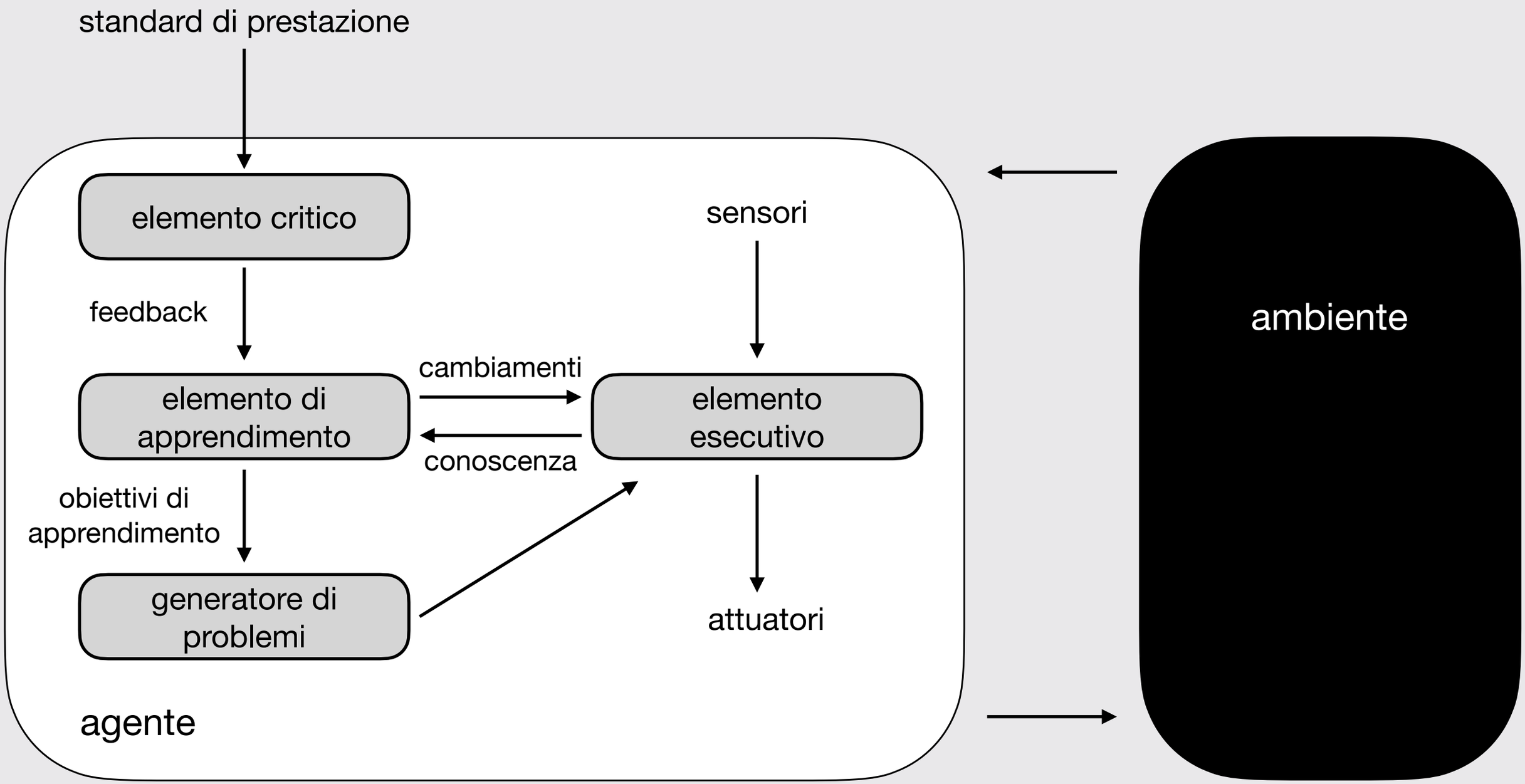
Fondamenti di Intelligenza Artificiale

Lezione 13 - Teoria dell'Apprendimento

Teoria dell'Apprendimento

Agenti capaci di apprendere

L'apprendimento presenta il vantaggio di permettere agli agenti di operare in ambienti inizialmente sconosciuti diventando col tempo più competenti.



Teoria dell'Apprendimento

Agenti capaci di apprendere

L'apprendimento presenta il vantaggio di permettere agli agenti di operare in ambienti inizialmente sconosciuti diventando col tempo più competenti.

Un agente di questo tipo ha quattro componenti principali:

—> **Elemento di apprendimento.** L'elemento responsabile del miglioramento interno.

—> **Elemento esecutivo.** L'elemento responsabile della selezione delle azioni esterne. Questo è l'elemento che abbiamo considerato finora come agente.

—> **Elemento critico.** L'elemento responsabile di fornire feedback sulle prestazioni correnti dell'agente, così che l'elemento di apprendimento possa determinare se e come modificare l'elemento esecutivo affinché si comporti meglio in futuro.

—> **Generatore di problemi.** L'elemento responsabile di suggerire azioni che portino ad esperienze nuove e significative che, chiaramente, portino l'agente ad apprendere nuove conoscenze da sfruttare poi per migliorare le sue azioni.

Teoria dell'Apprendimento

Agenti capaci di apprendere

L'apprendimento presenta il vantaggio di permettere agli agenti di operare in ambienti inizialmente sconosciuti diventando col tempo più competenti.

Cosa significa apprendere

L'apprendimento consiste in qualunque processo tramite il quale un sistema migliora le sue prestazioni sulla base dell'esperienza

Nella nostra accezione, l'apprendimento ha a che fare con degli agenti intelligenti che migliorano automaticamente operando in un ambiente.

Cosa significa apprendere, più tecnicamente

Apprendimento = **Migliorare** con **l'esperienza** nell'esecuzione di un **task**;

- Migliorare nell'esecuzione del task T;
- Rispetto alla misura di prestazione P;
- Sulla base dell'esperienza E.

L'esempio della classificazione delle e-mail spam

- T = Identificare le e-mail che un utente non vuole ricevere;
- P = % di e-mail spam filtrate (in)correttamente
- E = Database di e-mail etichettate come spam/no-spam da uno o più utenti.

Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

> **Machine learning.** Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Gli algoritmi che considereremo in questa parte del corso consentono di andare oltre la programmazione classica, nel senso che non si limiteranno ad eseguire dei comandi espliciti, ma saranno in grado di prendere **decisioni data-driven**.

Nell'ultimo decennio, il machine learning è diventato estremamente popolare, ma ha una storia ben più lunga! Ad esempio, il termine "regressione" fu introdotto nel 1889 ed il primo algoritmo di regressione lineare fu realizzato all'inizio del 1800 da Gauss.

Sono due le caratteristiche che hanno portato alla popolarità del machine learning: la disponibilità dei **dati** e la disponibilità di **strumenti computazionali adeguati**.

Oggi come oggi, il machine learning è all'apice del suo successo e rappresenta la branca dell'informatica che cresce maggiormente in termini di ricerca e utilizzo.

Questo è però un corso di **fondamenti**: introdurremo perciò le basi che consentono di costruire agenti intelligenti capaci di apprendere —> non parleremo dettagliatamente di deep learning né tantomeno di quantum machine learning.

L'obiettivo è quello di essere capaci di estrarre adeguatamente i dati, oltre che progettare ed implementare algoritmi di *shallow* machine learning.

Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Apprendimento supervisionato

L'apprendimento supervisionato è quello in cui un agente apprende usando dei dati *etichettati*.

Le etichette determinano la *variabile dipendente*, ovvero quello che l'agente dovrà apprendere.

Quindi, per ogni osservazione, oltre ai dati di input è noto anche il valore della variabile dipendente.

L'apprendimento si dice *supervisionato* proprio perché il progettista deve fornire all'agente delle etichette che abiliteranno l'apprendimento.

Apprendimento non supervisionato

L'apprendimento non supervisionato è quello in cui un agente apprende usando dati *non* etichettati.

L'agente sarà quindi in grado di imparare senza conoscere il valore reale della variabile dipendente.

Generalmente, agenti non supervisionati vengono usati per problemi più complessi di quelli supervisionati.

L'apprendimento si dice non supervisionato perché il progettista lascerà all'agente il compito di apprendere sulla base dei dati a disposizione.

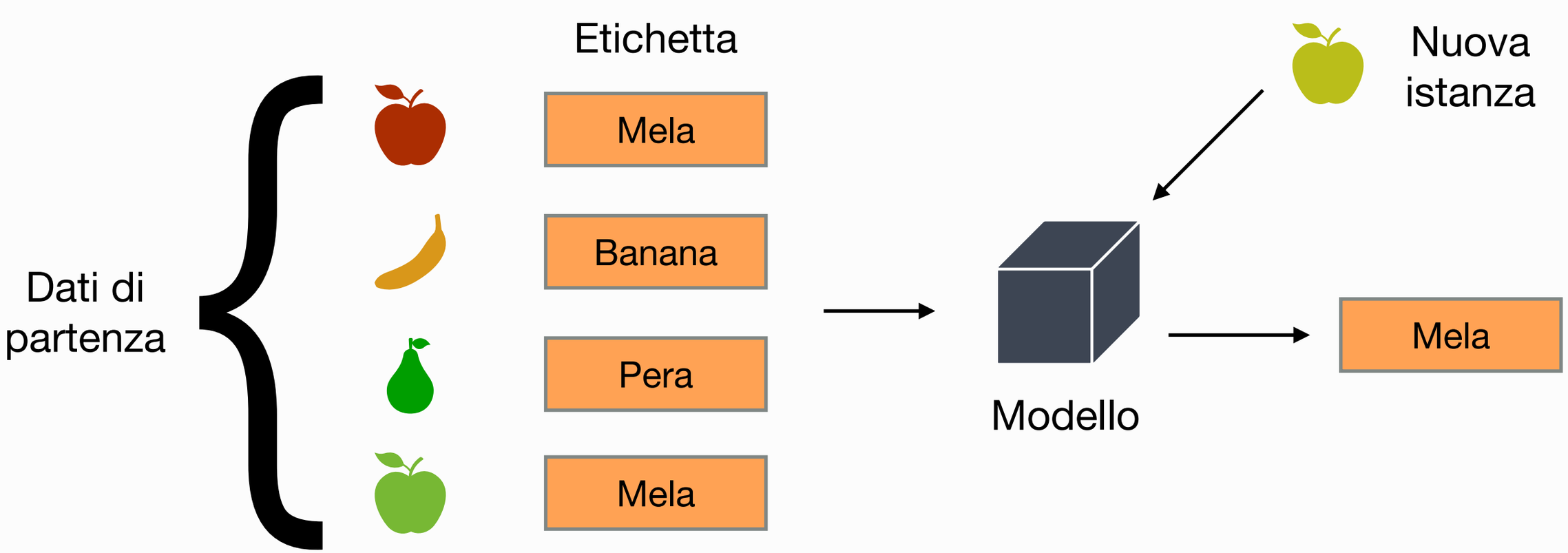
Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Apprendimento supervisionato

Apprendimento non supervisionato



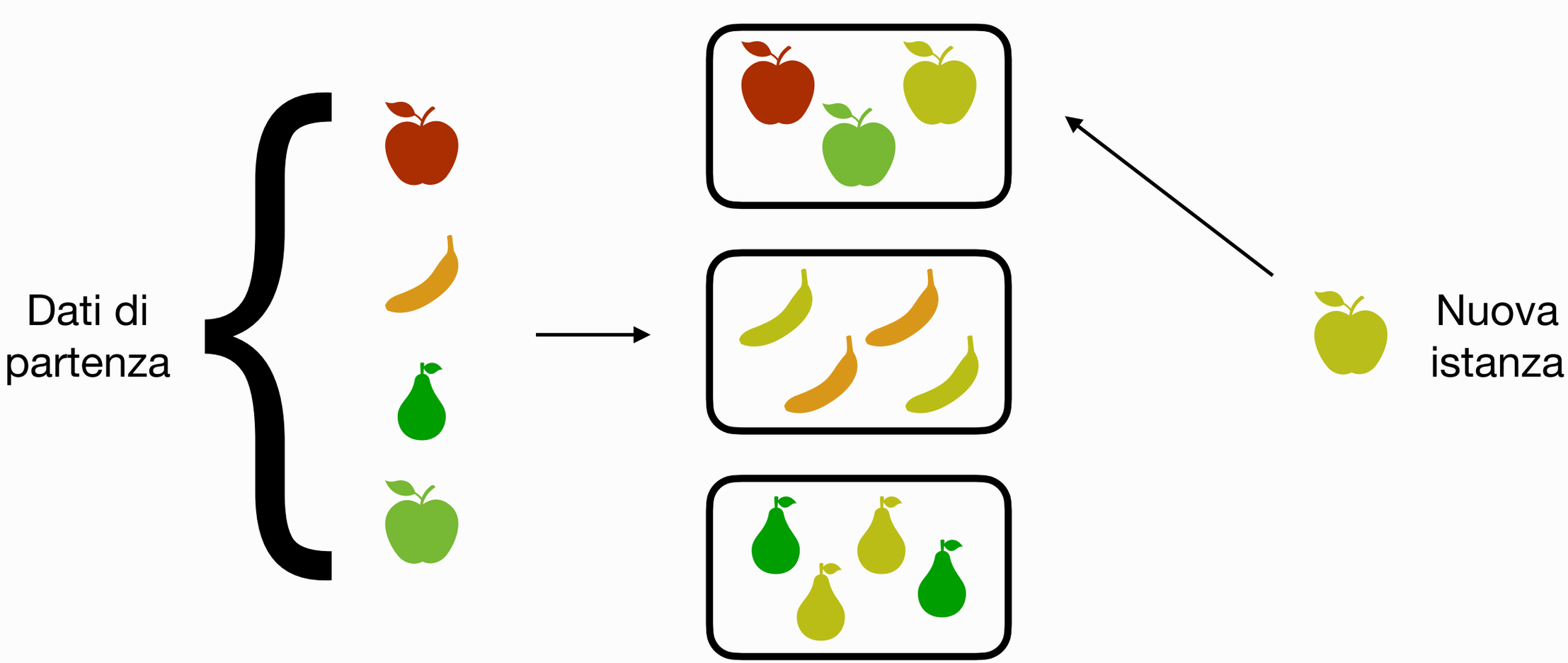
Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Apprendimento supervisionato

Apprendimento non supervisionato



Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Apprendimento supervisionato

Apprendimento non supervisionato

Oltre alla classica distinzione tra apprendimento supervisionato e non supervisionato, esistono altre tipologie di machine learning, come l'apprendimento semi-supervisionato e per rinforzo.

Nell'apprendimento semi-supervisionato alcuni dei dati sono etichettati, altri no. L'agente intelligente sarà tenuto ad apprendere quali sono le etichette mancanti.

Nell'apprendimento per rinforzo, l'agente compierà azioni in maniera sequenziale e, al termine di ogni sequenza, gli verrà assegnata una "ricompensa" che ha lo scopo di incoraggiare comportamenti corretti.

Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Oltre alla classificazione degli algoritmi, un altro modo di suddividere i problemi di machine learning si basa sull'output che si intende ottenere. In particolare:

Regressione | Classificazione | Clustering

Per output si intende il range di valori che la variabile dipendente potrà assumere. Se questo è continuo, allora si parla di **regressione**.

—> Esempio: Stimare lo stipendio di una persona in base al titolo di studio;

Se questo è discreto, allora si parla di **classificazione**.

—> Esempio: Valutare se una e-mail è spam in base al suo oggetto;

Se questo è la suddivisione dei dati in gruppi, allora si parla di **clustering**.

—> Esempio: Identificare se esistono gruppi di utenti sul web con comportamento simile.

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Oltre alla classificazione degli algoritmi, un altro modo di suddividere i problemi di machine learning si basa sull'output che si intende ottenere. In particolare:

ring

Riduzione della dimensionalità

Mining di associazioni

umere. Se

dio;

Esistono altre centinaia di problemi. Ad esempio, la riduzione della dimensionalità viene usata per ridurre le caratteristiche significative ed eliminare le caratteristiche ridondanti in un vasto insieme di dati.

Il mining delle associazioni serve ad identificare dei pattern comuni in un insieme di transazioni. Se avete mai sentito parlare di *market basket analysis*, allora sapete di cosa stiamo parlando.

Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

Machine learning. Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Qual è l'algoritmo migliore? La risposta è, ovviamente: dipende!

Esistono centinaia di algoritmi di machine learning. A prescindere dallo specifico algoritmo da utilizzare, è importante innanzitutto caratterizzare il problema da trattare - quindi, valutare se questo è, ad esempio, un problema supervisionato di classificazione.

	Non supervisionato	Supervisionato
Continua	Clustering & Dimensionality Reduction - SVD - PCA - K-means	Regressione - Lineare - Polinomiale Alberi di decisione, Random Forest
Discreta	Association analysis - Apriori - FP-Growth Hidden Markov Model	Classificazione - KNN - Alberi di decisione - Logistic Regression - Naive-Bayes - SVM

Teoria dell'Apprendimento

Agenti capaci di apprendere, ma come?

> **Machine learning.** Il machine learning esplora lo studio e la costruzione di algoritmi che possano *imparare dai dati* e sulla base di questi fare previsioni.

Qual è l'algoritmo migliore? La risposta è, ovviamente: dipende!

Esistono centinaia di algoritmi di machine learning. A prescindere dallo specifico algoritmo da utilizzare, è importante innanzitutto caratterizzare il problema da trattare - quindi, valutare se questo è, ad esempio, un problema supervisionato di classificazione.

Dato che per ogni problema ci sono vari algoritmi, come facciamo a scegliere quale usare?

Facile, ci si affida al **metodo empirico**. Se la teoria ci aiuta a fare una prima selezione del problema e degli algoritmi che possono essere utilizzati, la pratica ci fa scegliere la soluzione migliore.

Procediamo dunque alla **misura dell'errore**: si costruiscono diversi modelli, si calcola l'errore per ciascuno di essi e si sceglie poi quello con i migliori risultati.

In altri termini, la misura dell'errore ci fornisce una base di confronto tra più modelli. Per capire meglio quello di cui stiamo parlando, consideriamo l'esempio di un problema di apprendimento supervisionato di regressione: la costruzione di un modello di stima dell'altezza di una persona in base al peso, genere ed età.

Errore, Bias e Varianza

Errore. L'errore, o residuo, di un modello di machine learning è la differenza tra il valore stimato della variabile da predire e il suo valore attuale.

Nell'esempio che tratteremo, l'errore è la differenza tra l'altezza stimata e quella reale.

Possiamo rappresentare i dati di input per ciascuna persona del nostro dataset con un vettore del tipo:

$$\overrightarrow{x} \equiv (x_1, x_2, \ldots x_p)_i$$

Nel nostro caso p=3 poiché abbiamo tre parametri sulla base dei quali fare predizione e, quindi, la terna $(x_1, x_2, x_3)_i$ rappresenta genere, peso ed età dell'i-esima persona.

La nostra variabile dipendente, di tipo continuo, sarà data dall'altezza stimata e verrà chiamata y_i.

Costruire un modello di machine learning significa trovare quella funzione *f* per cui:

$$y_i = f(\overrightarrow{x_i})$$

Due esempi:

f(u, 70kg, 35) = 170cm;
f(d, 60kg, 35) = 163cm.

Se l'altezza di queste due persone fosse proprio quella riportata dalla funzione, allora il nostro errore sarebbe pari a zero.

Errore, Bias e Varianza

Errore. L'errore, o residuo, di un modello di machine learning è la differenza tra il valore stimato della variabile da predire e il suo valore attuale.

Tuttavia, sappiamo che persone dello stesso peso, genere ed età possono avere altezze diverse. Ad esempio, nel nostro dataset potremmo avere:

$$\overrightarrow{x_3} = (u,70,35); y_3 = 170;$$
$$\overrightarrow{x_4} = (u,70,35); y_4 = 180;$$
$$\overrightarrow{x_5} = (u,70,35); y_5 = 175;$$

La nostra funzione *f*, a parità di input, restituisce sempre lo stesso output. Questo implica che il fenomeno ha una *variabile intrinseca* che rende impossibile la creazione di un modello perfetto.

Per questa ragione, si introduce il concetto di *errore irriducibile*, ovvero una misura di variabilità intrinseca del fenomeno in esame —> in altri termini, quell'errore che avremo sempre e comunque.

$$y_i = f(\overrightarrow{x_i}) + \epsilon_{irr}$$

Ma l'errore irriducibile non è l'unico errore da considerare… abbiamo anche l'errore dovuto al modello di machine learning.

Teoria dell'Apprendimento

Errore, Bias e Varianza

Errore. L'errore, o residuo, di un modello di machine learning è la differenza tra il valore stimato della variabile da predire e il suo valore attuale.

Se l'errore irriducibile *dipende esclusivamente dai dati* che abbiamo a disposizione, dobbiamo considerare che i modelli di machine learning *non sono infallibili* e potrebbero produrre predizioni errate.

Se indicassimo con $\tilde{y}_i$ l'altezza stimata dal modello, allora possiamo dire che:

$$y_i = \tilde{y}_i + \epsilon_{irr} + \epsilon$$

Tutti gli sforzi relativi alla ricerca del miglior modello di machine learning puntano a minimizzare l'errore riducibile. Questo errore dipende da due fattori principali.

Bias. Il modello ha un certo bias se, quando viene addestrato su diversi dataset, l'output che restituisce è sistematicamente *sbagliato*.

Il bias indica l'insieme di assunzioni usate dal modello per predire un valore di output dati degli input che non ha ancora incontrato (anche detto underfitting).

Varianza. Il modello ha una certa varianza se, quando viene addestrato su diversi dataset, l'output che restituisce è sistematicamente *diverso*.

Un'alta varianza è anche detta overfitting (approfondiremo più avanti).

Teoria dell'Apprendimento

Errore, Bias e Varianza

Errore. L'errore, o residuo, di un modello di machine learning è la differenza tra il valore stimato della variabile da predire e il suo valore attuale.

Se l'errore irriducibile *dipende esclusivamente dai dati* che abbiamo a disposizione, dobbiamo considerare che i modelli di machine learning *non sono infallibili* e potrebbero produrre predizioni errate.

Se indicassimo con $\tilde{y}_i$ l'altezza stimata dal modello, allora possiamo dire che:

$$y_i = \tilde{y}_i + \epsilon_{irr} + \epsilon$$

Tutti gli sforzi relativi alla ricerca del miglior modello di machine learning puntano a minimizzare l'errore riducibile. Questo errore dipende da due fattori principali.

$$\epsilon = bias + varianza$$

Quindi, l'obiettivo è quello di rendere nulli bias e varianza!

Sfortunatamente, bias e varianza sono inversamente correlati —> tanto diminuisce il bias tanto aumenta la varianza e viceversa.

Quindi, è necessario trovare un *compromesso bias-varianza*, ovvero un compromesso tra la "flessibilità" del modello ed il comportamento su dati che non ha mai visto.

Che implicazioni ha tale compromesso sulle prestazioni dei modelli di machine learning?

Underfitting e overfitting

Approfondiamo i problemi di underfitting e overfitting.

Underfitting

Un modello con bias elevato è più semplice di quanto dovrebbe essere e quindi tende a sotto-dimensionare i dati. In altre parole, è uno *studente superficiale*: il modello non riesce ad apprendere e acquisire gli schemi intricati del set di dati.

Chiaramente, un modello di questo tipo non si adatta correttamente all'insieme di dati di input e quindi avrà una **bassa precisione** quando dovrà predire nuovi dati, ovvero sbaglierà molto frequentemente.

Altrettanto chiaramente, un modello di questo tipo **non potrà risolvere problemi complessi**, ovvero problemi per i quali l'insieme di dati di input è particolarmente intricato (come, ad esempio, il problema visto in precedenza, in cui più persone con le stesse caratteristiche hanno altezze diverse).

Teoria dell'Apprendimento

Underfitting e overfitting

Approfondiamo i problemi di underfitting e overfitting.

Overfitting

Un modello con varianza elevata è più complesso di quanto dovrebbe essere e quindi tende a sovra-dimensionare i dati. In altre parole, è uno *studente che studia a memoria e/o tende a complicare troppo le cose.*

Un modello di questo tipo ha due possibili conseguenze: non riesce ad apprendere dati anche solo leggermente diversi da quelli che già conosce oppure si comporta in maniera eccessivamente complessa, peggiorando le prestazioni.

Fatte queste premesse, un modello di questo tipo tenderà a risolvere **problemi semplici utilizzando soluzioni complesse**, non essendo capace di generalizzare le competenze acquisite sull'insieme di dati di input.

Underfitting e overfitting, l'importanza della progettazione e della valutazione empirica

Per diagnosticare problemi di underfitting e overfitting, è necessario valutare il modello generato su un insieme di dati quanto più ampio possibile —> più dati abbiamo, più è facile per un algoritmo di machine learning apprendere correttamente.

In alcuni casi, è possibile risolvere o almeno mitigare i rischi di underfitting e overfitting lavorando sulla configurazione degli algoritmi di machine learning.

Alcune operazioni tipicamente utilizzate riguardano:

- La selezione delle caratteristiche rilevanti, tramite la quale un algoritmo di machine learning riesce ad apprendere "meglio", focalizzando l'attenzione sui soli dati che rappresentano la variabile dipendente;

- La convalida incrociata, tramite la quale vengono generate una serie di insiemi di dati di test, così da consentire all'algoritmo di machine learning di perfezionare l'apprendimento sui vari insiemi di test;

- La configurazione dei parametri, quando possibile (o meglio, per gli algoritmi parametrici di machine learning). Questa consente all'algoritmo di poter studiare meglio i dati di input e, quindi, ridurre il rischio di underfitting o overfitting;

- L'aumento della dimensione dei dati di input, ovvero fornire all'algoritmo di machine learning la possibilità di avere a disposizione un insieme più ampio di osservazioni dalle quali apprendere.

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Laurea triennale in Informatica

Fondamenti di Intelligenza Artificiale

Lezione 13 - Teoria dell'Apprendimento

Classificazione, Regressione, Clustering

Consideriamo i seguenti problemi e proviamo a capire quale metodologia di apprendimento sarebbe meglio applicare.

Caso 1. Supponiamo di voler costruire un modello di machine learning capace di valutare se un utente di un sito web sarà interessato o meno all'acquisto di un certo prodotto.

Caso 1.

Regressione | Classificazione | Clustering

Teoria dell'Apprendimento

Classificazione, Regressione, Clustering

Consideriamo i seguenti problemi e proviamo a capire quale metodologia di apprendimento sarebbe meglio applicare.

Caso 2. Supponiamo di voler costruire un modello di machine learning capace di identificare automaticamente i numeri scritti a mano su un foglio.

Caso 2.

Caso 1.

Regressione | Classificazione | Clustering

Classificazione, Regressione, Clustering

Consideriamo i seguenti problemi e proviamo a capire quale metodologia di apprendimento sarebbe meglio applicare.

Caso 3. Supponiamo di voler costruire un modello di machine learning capace di identificare degli insiemi di utenti che si comportano in maniera simile su un sito di e-commerce.

Caso 2.

Caso 1.

Caso 3.

Regressione

Classificazione

Clustering

Teoria dell'Apprendimento

Classificazione, Regressione, Clustering

Consideriamo i seguenti problemi e proviamo a capire quale metodologia di apprendimento sarebbe meglio applicare.

Caso 4. Supponiamo di voler costruire un modello di machine learning capace di stimare il valore di mercato di un'azione in base all'andamento dei tre giorni precedenti.

Caso 4.

Regressione

Caso 2.

Caso 1.

Classificazione

Caso 3.

Clustering