DIPARTIMENTO DI INGEGNERIA INFORMATICA, MODELLISTICA,
ELETTRONICA E SISTEMISTICA

Corso di Laurea Triennale in Ingegneria Informatica

Tesi di Laurea

Crittografia quantistica e cyber security

Relatore:

Prof.
Floriano De Rango

Candidato:

Giovanni Lorenzo
Murfuni
Mat. 230599

ANNO ACCADEMICO 23/24

Dedica e Ringraziamenti...

Indice

Capitolo 1

Introduzione

1.1 Storia

L'IA nasce con Turing nel 1950, mentre, il termine "Artificial Intelligence" viene coniato da John Mccarthy.
Il Libro consigliato è S.Russel, P.Norvig, Artificial Intelligence: A modern approach, Prentice Hall Ed.
Esame:

- Prova orale.
- Progettino.
- (Forse) Prova Scritta.
- Durante il corso si svolgerà una gara progettuale che da 1 punto bonus partecipazione e 3 punti bonus vittoria.

È possibile trovare esercizi e codici su myLab con codice INUWRTQL inserendolo in combinazione al codice del libro acquistato.

Cos'è l'intelligenza artificiale?

L'intelligenza artificiale è nelle nostre vite da moltissimo tempo, tuttavia pochi individui ne conoscevano gli sviluppi. Alcuni esempi possono essere, robot "faccendieri", droni o macchine a guida autonoma.

Cos'è la razionalità computazionale?

Definizione 1. *È la capacità di raggiungere gli obiettivi prefissati in modo da massimizzarne l'utilità.*

No-Monotonic-Reasoning

Che cosa vuol dire "No-Monotonic-Reasoning"? È un termine che si tramanda dalla nascita del pensiero filosofico. La logica classica è una logica monotona, ovvero, aggiungere nuove conoscenze implica una crescita del numero di conclusioni.
Tuttavia, una nuova conoscenza otrebbe invalidare le vecchie conoscienze, implicando quella che chiamiamo "eccezione", così i ricercatori nel campo dell'IA lavorano sul **Common-Sense Reasoning** raggiungendo lo sviluppo di pensiero non monotòno.
Quali sono le conseguenze dello sviluppo di un pensiero non monotòno?
La conseguenza principale è quella dell'aumento della complessità computazionale degli algoritmi decisionali, arrivando anche a raggiungere classi di co mplessità agli apici della piramide dell'hardness. Il vantaggio stà nel fatto che, questi linguaggi, sono estremamente espressivi.
Che intendiamo con "espressivo"?

Definizione 2. *In questo caso, definiziamo l'espressività come la capacità di un linguaggio di riuscire ad esprimere tutti i problemi della stessa classe di complessità alla quale appartiene la computazione, legata alla risoluzione dei problemi intrinseci nel linguaggio in analisi.*

Intercorriamo in atri due concetti di cruciale importanza:

- Complessità. *Quanto è potente questa logica? Che complessità di problemi possiamo affrontare con questa logica?*
- Espressività. *Quanti problemi posso esprimere con questa logica?*

La teoria dell'aspressività ci consente di comprendere quali sono i problemi risolvibili con la logica (nello specifico contesto corrente) in analisi.

Lo studio dell'Intelligenza Artificiale, fra l'altro, coinvolge lo studio della risoluzione di problemi complessi a livello prettamente algoritmico. Durante il corso, verranno esplorate vari temi cruciali come:

- Complessità strutturale.
- Ipergrafi.
- Teoria dei giochi (esempio della cooperazione dei detenuti, concetto strettamente connesso al "problema di Nash").
- Fair Division And Fair Allocation Problem

Approcci alla modellazione

Common-Sense-Reasoning (Dal modello all'inferenza)

Controllare dalle slide "Lezione 1"

- Model
- Inference
- New Data

Data → Model

- Machine Learning
- Correlation
- Causality: Qual'è la causa dell'evento in questione? La corrispondenza ad un modello statistico non implica necessariamente un contesto di casualità diretta.

Neural Networks

Le reti neurali sono composte da neuroni artificiali che calcolano una funzione restituendo un output in base all'input processato (parametri calcolati nella rete). Ogni neurone della rete potrebbe anche avere funzioni diverse (solitamente tutti i neuroni hanno la stessa funzione). Nelle reti neurali, abbiamo due gradi di libertà:

1. Struttura della rete:
    - Topologia della rete.
    - Tipo di funzioni.
2. I parametri delle funzioni utilizzate.

Per ogni input da processare è possibile associarvi un peso. Modificando tali pesi è possibile cambiare il significato della funzione.
Il "Machine Learning" consiste nell'estrazione di un modello a partire da un dataset specifico. Il problema è di questa tipologia: In molti casi non si possiede alcuna garanzia sulla bontà dell'output, impedendo al modello addestrato di effettuare una generalizzazione del modello reale.[1] In genere il modello addestrato, viene allenato su un "training set" (o insieme di allenamento).

fig.1 sul quad 27/02

Tornando alla Fig[1.0], perché il modello è considerato una "black box"? Tale denominazione è dovuta all'incapacità di interpretare i parametri (incapacità dell'essere umano).
Il problema dell'interpretazione implica, inequivocabilmente, un problema di spiegabilità. Tale problematica è cruciale per ambienti delicati come: medicina, biologia, economia ecc.
È possibile trovare tali problemi anche in: SVM, Decision Trees, ecc. Altri problemi che possiamo incontrare sul modello addestrato sono:

- Overfitting: modello troppo specifico al training set.
- Underfittin: modello troppo generalizzato rispetto al training set.

Cercare le definizioni corrette

[1] Il modello addestato è imprevedibile quando si ha a che fare con input mai visti prima.

Agenti

Gli agenti sono strumenti molto utilizzati in questo ambito, si distinguono in varie tipologie:

- Reflex: Sono agenti ai quali viene detto cosa fare in base al contesto in cui si trovano.
- Planning: Sono agenti che hanno un obiettivo specifico, devono essere in grado di inventare dei piani (plan o stategia) per raggiungere il loro obiettivo (goal).
- Utilitiy-Based: Sono agenti che hanno un obiettivo specifico e dei requisiti, devono essere in grado di creare un plan per raggiungere il goal soddisfando i requisiti specificati.

Alcuni sistemi si compongono di più agenti, è il caso dei multiple-agents. Gli agenti PEAS (Performance, Envitoment, Actuators, Sensors), servono a valtuare: l'abilità, la capacità di conoscere l'ambiente, la capacità di agire nell'ambiente e la misurazione dell'ambiente. Tali ambienti sono i più completi perché possono agire concretamente sull'ambiente. L'osservazione dell'ambiente può essere di due tipi:

- Completa.
- Parziale.

L'azione nell'ambiente, invece, può essere stocastica (o probabilistica), casi in cui non si hanno tutte le informazioni necessarie per essere sicuri dell'effetto causato. L'ambiente in sé può essere: statico o dinamico. In altre parole, tali caratteristiche rappresentano la capacità dell'ambiente di cambiare o rimanere invariato. Un ambiente statico o sicuro può diventare insicuro se ci sono "Multiple Agents", implica la combinazione delle attività così come quella delle incertezze.

Problema della curva di regressione, prendere fig.2 su quad 27/02

recuperare gli appunti da ciccio DeM

1.2 Algoritmo Free Search

Dato il nodo corrente, valutiamo le possibili azioni. Aggiungo d, p, e alla "fringe" (o frangia) F (opportuna struttura dati). Estraggo un nodo da F, suppress d. Aggiungo b, c, e ad F. A questo punto i nodi che abbiamo visitato sono s e d, ovvero tutti quei nodi di cui conosciamo i successivi. Se solo uno di questi nodi fosse il Goal a quest'ora avremmo finito.
Quello che avviene nella fringe è fondamentale per raggiungere il goal giusto.
Possiamo implementare la frangia come una pila (stack) o come una coda (queue), il che ci conduce a due tipi di visite per il grafo, in profondità (stack) e quella per livelli (queue).
La stratrgia vista in precedenza (a pila) è corretta, ma non completa. Utilizziamo adesso una strategia a queue (o coda).
Dovendo tenere conto anche dei pesi del camnmino la cosa migliore sarebbe una priority queue.

fig.1 28/02

fig.2 28/02

slide 13 lez 1

slide 15 esempio

fig.3 28/02

fig.4 28/02

Appunti lezione 3 Cartella Altro/File/ciccio De M

fig.1 030325 lezione 4

1.2.1 Informed Search

Capitolo 2

Capitolo

Capitolo 3

Capitolo

Capitolo 4

Capitolo

Capitolo 5

Capitolo

Capitolo 6

Capitolo