PROF. FABRIZIO MONTANARO – PROF.SSA STELLA BECCARIA

A.S. 2020/2021 - MATERIA INFORMATICA

CLASSE 5° A LSSA

ALGORITMI DI CALCOLO NUMERICO

- Introduzione al calcolo numerico (problema, algoritmo, esecutore, programma)
- Problemi decidibili, non decidibili e intrattabili
- Metodi di calcolo numerico: generalità e concetto di errore
- Esempi di algoritmi di calcolo numerico:
  - calcolo della radice quadrata
  - calcolo approssimato di Pigreco (Archimede, Tsu Chung-Chi, Cusano, Montecarlo)
  - ricerca degli zeri di una funzione (bisezione, metodi delle tangenti, corde e secanti, iterazione di punto fisso)
  - integrazione numerica (metodi dei rettangoli, trapezi e parabole, Montecarlo)
  - derivazione numerica
- Rappresentazione di numeri interi e reali:
  - floating-point IEEE 754
  - approssimazioni e precisione della macchina (epsilon)
- Generazione di numeri casuali: generalità e tipologia di generatori (fisici e algoritmici)
- Esempi di algoritmi di generazione pseudo-casuale:
  - middle-square, linear congruential generator e algoritmo MersenneTwister
- I frattali di Newton

LA SICUREZZA DEI SISTEMI INFORMATICI

- Le minacce alla sicurezza (naturali e umane)
- Gli obiettivi fondamentali della sicurezza (riservatezza, integrità e disponibilità)
- Ulteriori obiettivi (autenticazione, autorizzazione, tracciabilità e non ripudio)
- La valutazione dei rischi informatici
- Principali tipologie di attacchi informatici e possibili contromisure

LA CRITTOGRAFIA

- Concetti introduttivi (terminologia, chiave, principi di Kerckhoff e di Shannon)
- Metodi crittografici (criteri a sostituzione e a trasposizione)
- Cifrari a blocchi (S-box, P-box e reti SP)
- Algoritmi a chiave simmetrica (DES, 3-DES, AES)
- Algoritmi a chiave asimmetrica (chiave pubblica e privata, cenni di aritmetica modulare)
- Funzionamento dell'algoritmo RSA
- Gli algoritmi di hashing (MD5, SHA) e la firma digitale
- Distribuzione delle chiavi pubbliche e certificati digitali

LA SICUREZZA DEI DATI INFORMATICI

- Crimini informatici
- Misure per prevenire accessi non autorizzati ai dati
- Tecniche per generare delle password sicure
- Cenni sulla sicurezza delle reti e delle applicazioni (social network, email)
- Il backup dei dati

IL LINGUAGGIO SQL

- Classificazione delle istruzioni SQL (DDL, DML, DCL, TCL)
- Data Manipulation Language (INSERT, UPDATE, DELETE)
- Il comando SELECT:
  - interrogazioni di base su una singola tabella
  - interrogazioni su più tabelle (JOIN)
  - ordinamento dei dati (ORDER BY)
  - eliminazione dei duplicati (DISTINCT)
  - operatori aggregati (COUNT, SUM, MAX, MIN, AVG)
  - raggruppamenti (GROUP BY, HAVING)

COMPLESSITÀ COMPUTAZIONALE

- Complessità computazionale ed efficienza degli algoritmi
- Calcolo della complessità in numero di passi base
- Complessità nei casi: migliore, medio e peggiore
- Complessità asintotica

CALCOLABILITÀ

- Classificazione dei problemi in base al costo computazionale
- Algoritmi deterministici e non deterministici
- Classi di complessità: problemi N e NP – Il problema "N versus NP"
- Esempio: la crittografia e il problema della fattorizzazione

SISTEMI E AUTOMI

- Definizione di sistema e sottosistema e classificazione dei sistemi
- Lo stato interno di un sistema
- Descrizione del comportamento di un sistema: funzione di transisizione dello stato, funzione di trasformazione delle uscite, definizione formale di sistema
- Rappresentazione dei sistemi: i modelli
- Definizione di modello e classificazione dei modelli
- Gli automi a stati finiti: definizione e rappresentazione (diagramma degli stati e tabella di transizione)

- Gli automi esecutori: potenza di calcolo
- La macchina di Turing e la tesi di Church-Turing
- Esistenza dei problemi indecidibili: il problema dell'arresto

INTELLIGENZA ARTIFICIALE

- Generalità e concetti introduttivi: definizione di intelligenza artificiale
- Nascita dell'intelligenza artificiale: la proposta di Dartmouth
- I diversi approcci all'intelligenza artificiale:
  - "Agire come gli umani": il test di Turing
  - "Pensare come gli umani": le scienze cognitive
  - "Pensare in modo razionale": le leggi del pensiero e la logica
  - "Agire in modo razionale": gli agenti razionali
- Intelligenza artificiale forte e debole
- Paradigmi utilizzati:
  - simbolico (le scienze cognitive)
  - sub-simbolico (il connessionismo e le neuroscienze)
- I sistemi esperti
- Le reti neurali
- Riflessioni sull'intelligenza artificiale

<u>Laboratorio</u>

- Implementazione di algoritmi di calcolo numerico utilizzando Python
- Esercizi sul linguaggio SQL utilizzando Python e MySQL
- Esercizi sugli automi

Lecco, 05/06/2021

Prof. Fabrizio Montanaro

Prof.ssa Stella Beccaria