UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Teoria dell'Informazione e Codici Correttori di Errori

2627-1-F4002Q033

Obiettivi

Coerentemente con gli obiettivi formativi del Corso di Studio, l'insegnamento si propone di fornire allo studente le *conoscenze* riguardanti l'acquisizione degli strumenti per la trasmissione di informazione su canali con rumore, al fine di analizzare procedure di scambio ottimali nella rilevazione e correzione di errori. Tempo permettendo verranno impartiti alcuni rudimenti su linguaggi di programmazione simbolica come Magma e Gap. Tali strumenti servono ad enfatizzare gli aspetti sperimentali della scoperta matematica. Verranno altresì fornite le *competenze* necessarie a comprendere e analizzare le principali tecniche e metodi dimostrativi connessi all teoria, e le *abilità* utili ad applicarle per risolvere esercizi e affrontare problemi.

1. Conoscenza e capacità di comprensione (Knowledge and understanding)
   Gli studenti acquisiranno una conoscenza di base dei principi fondamentali della teoria dei codici correttori, inclusi concetti quali codifica, decodifica, distanza di Hamming, codici lineari, codici ciclici e proprietà di correzione d'errore. Tali conoscenze si baseranno su manuali di testo e materiali didattici aggiornati e saranno il fondamento per studi più approfonditi.

2. Conoscenza e capacità di comprensione applicate (Applying knowledge and understanding)
   Gli studenti saranno in grado di applicare i concetti appresi per analizzare e progettare semplici sistemi di codifica e decodifica in contesti reali o simulati, riconoscendo le caratteristiche dei codici correttori e la loro applicabilità in ambito delle comunicazioni digitali e informatiche.

3. Autonomia di giudizio (Making judgements)
   Il corso promuoverà lo sviluppo della capacità di valutare in modo critico l'efficacia e l'efficienza dei diversi codici correttori, di selezionare metodi opportuni per specifici problemi, e di interpretare i risultati ottenuti attraverso metodi teorici e computazionali.

4. Abilità comunicative (Communication skills)
   Gli studenti impareranno a comunicare in modo chiaro e preciso i concetti della teoria dei codici, utilizzando la terminologia tecnica appropriata, sia in forma scritta che orale, anche in contesti collaborativi e interdisciplinari.

5. Capacità di apprendimento (Learning skills)
   Il corso stimolerà l’autonomia nello studio, fornendo gli strumenti per approfondire in modo autonomo argomenti correlati, affrontare esercizi complessi e prepararsi ad esami o corsi successivi nel campo della matematica applicata o dell’informatica teorica.

Contenuti sintetici

Teoria dell’Informazione, trasmissione messaggi, probabilita' di errore, entropia, Teorema di Shannon, canale simmetrico, codici correttori di errore, alfabeti, campi finiti, codici lineari, codici di Hamming, ciclici, di Reed-Solomon e Muller, polinomio enumeratore, Teoremi di MacWilliams. Teoria invarianti gruppi finiti.

Programma esteso

Trasmissioni con rumore, alfabeto, parole di lunghezza fissata, codici a blocchi; canale simmetrico m-ario con probabilità p, codici di ripetizione, codice binario di Hamming (7,4,3); distanza di Hamming, lunghezza, dimensione e distanza minima di un codice, sphere packing bound, Gilbert-Varshamov bound, codici perfetti, cenni ai codici di Golay e di Hamming; Codici lineari, peso minimo, estensione di codici; Matrice generatrice di un codice, forma sistematica e standard, codici duali, matrici di controllo, distanza minima di un codice lineare; Cenni all'aritmetica dei campi finiti; Esistenza di codici autoduali, spazi simplettici e ortogonali; Decodifica di codici lineari, coset leaders, sindromi; Spazi proiettivi, decomposizione in spazi affini, codici di Hamming, codici 1-perfetti, unicità monomiale, traslati di codici lineari; Duali di codici di Hamming, codici a peso costante, teorema di Bonisoli; Gruppo degli automorfismi dei codici di Hamming; Struttura campi finiti, elementi primitivi; Polinomi ciclotomici su campi finiti; Fattorizzazione di x^n-1, polinomi minimi, struttura automorfismi campo finito, cenni teoria di Galois; classi ciclotomiche, gradi fattori irriducibili x^n-1, formula d’inversione di Moebius; Definizione di codici ciclici, Teorema di Prange; Duale codice ciclico, polinomi generatori; Generazione di codici ciclici, codici di Golay come codici ciclici, BCH bound; Teorema di MacWilliams sull’estensione di mappe lineari preservanti pesi a trasformazioni globali monomiali; Polinomi enumeratori, teorema di MacWilliams, esempi C=0, C=Rep e loro duali, caratteri di un gruppo; Esempi di anelli con caratteri non degeneri, leggi di ortogonalita'; Teorema di Lloyd sui codici perfetti; Introduzione alla teoria degli invarianti dei gruppi finiti, Teoremi di Noether e di Molien, serie di Hilbert-Poincaré, gruppi generati da pseudo-riflessioni, anelli di Cohen-Macaulay, Teorema di Chevalley-Shephard-Todd.

Prerequisiti

Algebra Lineare, Teoria dei Gruppi, Teoria dei Campi Finiti, Nozioni elementari di Termodinamica e Probabilità.

Modalità didattica

L'insegnamento prevede lezioni frontali per 56 ore (8 CFU), articolate in: lezioni teoriche in modalità di didattica erogativa (DE), in cui si fornisce la conoscenza di definizioni, risultati e teoremi rilevanti e altre in modalità di didattica interattiva (DI), in cui si intende fornire competenze e abilità necessarie per utilizzare tali nozioni nella risoluzione di esercizi e nell'analisi di problemi

Le attuali disposizioni rettorali prevedono che la lezione sia fruibile sia in presenza che da remoto. Le lezioni verranno videoregistrate e saranno rese disponibili agli studenti sulla piattaforma e-learning del corso.

Materiale didattico

Testo di Riferimento:

- Hall, Notes on Coding Theory, 2005
- Appunti videoscritti delle singole lezioni reperibili su questa piattaforma.
- Appunti scritti in LaTeX in formato pdf reperibili su questa piattaforma.

Altri Testi:

- Huffman and Pless, Fundamentals of error-correcting codes, 2010
- MacWilliams and Sloane, The Theory of Error-Correcting Codes, 1977
- Smith, Polynomial invariants of finite groups, 1995

Periodo di erogazione dell'insegnamento

Secondo semestre

Modalità di verifica del profitto e valutazione

L'esame consiste in un'interrogazione orale in cui vengono accertate sia l'acquisizione dei contenuti teorici impartiti nel corso sia le capacita' di analisi e risoluzione di problemi.

Le attuali disposizioni rettorali richiedono che la prova orale dell’esame si svolga in presenza a meno che lo studente non rientri in particolari e categorie riportate nel decreto rettorale. In tal caso la prova orale potrà essere sostenuta da remoto mediante piattaforma WebEx con accesso reso disponibile sulla pagina e-learning dell’insegnamento.

Orario di ricevimento

Su appuntamento.

Sustainable Development Goals

ISTRUZIONE DI QUALITÁ