



UNIVERSITÀ  
DEGLI STUDI DI MILANO-BICOCCA

## SYLLABUS DEL CORSO

### Combinatorica Algebrica

2021-1-F4001Q090

---

#### 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 alla teoria, e le *abilità* utili ad applicarle per risolvere esercizi e affrontare problemi.

#### Contenuti sintetici

Teoria dell'Informazione, trasmissione messaggi, probabilità 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 fissa, 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 ortogonalità; 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 cui si fornisce la conoscenza di definizioni, risultati e teoremi rilevanti e altre in cui si intende fornire competenze e abilità necessarie per utilizzare tali nozioni nella risoluzione di esercizi e nell'analisi di problemi

A seguito della corrente emergenza sanitaria legata a Covid-19, al momento (A/A 2020/21) si prevede che le lezioni del presente insegnamento verranno comunque videoregistrate, sia nel caso siano in presenza sia nel caso siano tenute da remoto, e saranno rese disponibili agli studenti sulla piattaforma e-learning.

## 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 inizia con la discussione della risoluzione con l'ausilio del programma di manipolazione simbolica Magma di un problema precedentemente concordato.

Al termine di tale discussione verrà effettuata un'interrogazione orale in cui vengono accertate sia l'acquisizione dei contenuti teorici impartiti nel corso sia le capacità di analisi e risoluzione di problemi.

Entrambe gli aspetti contribuiscono allo stesso modo per la decisione del voto d'esame.

Nel caso di esito finale negativo verrà comunicato al candidato se è necessario risolvere un nuovo esercizio o se, quello già risolto, possa essere considerato valido per una nuova prova orale.

Fino all'esaurimento della corrente emergenza sanitaria, la prova orale dell'esame si svolgerà da remoto mediante piattaforma WebEx o analoga, con accesso reso disponibile sulla pagina e-learning dell'insegnamento.

## **Orario di ricevimento**

Su appuntamento. A causa dell'emergenza sanitaria, il ricevimento si svolgerà in modalità telematica mediante piattaforma WebEx o analoga.

---