CODICI LINEARI
a.a. 2016-2017

Insegnamento: *Codici Lineari*		
Docente: Francesco Mazzocca		
Settore Scientifico - Disciplinare: MAT/03	**CFU** **8=8L**	**ORE** **64**
Obiettivi formativi: Acquisizione dei risultati fondamentali e dei metodi dell'algebra e della geometria su campi finiti per la costruzione e l'utilizzazione dei codici correttori di errori.		
Propedeuticità: Algebra 1, Geometria 1		
Modalità di svolgimento: lezioni in aula.		
Modalità di accertamento del profitto: superamento di una prova orale.		

Legenda: L= Lezioni, E= Esercitazioni, La= Attività di Laboratorio.

PROGRAMMA

SISTEMI DI COMUNICAZIONE. Il problema della trasmissione dell'informazione. I contributi di C.E.Shannon e R.W.Hamming.
Alfabeti, parole su un alfabeto, codici su un alfabeto: prime definizioni ed esempi. Il *codice fiscale italiano*. Il codice *ISBN*. Il codice *MORSE*. Il codice *ASCII*. Il codice a barre *EAN*. Alcuni codici di Hamming. Schema di Shannon di un sistema di comunicazione.
Sorgenti di informazione senza memoria: definizione, distribuzione di probabilità, entropia, esempi. Compressione di dati: algoritmo di Huffman e algoritmo di Shannon-Fano. Codici istantanei e disuguaglianza di Kraft. Codifica di sorgente e relativo teorema di Shannon.
Canali di trasmissione senza memoria: definizione, matrice di transizione, rumore, entropia, flusso medio di informazione e capacità. Canali simmetrici. Sistemi di comunicazione discreti. Codifica di canale e relativo teorema di Shannon.
Schemi di decodifica. Affidabilità di un sistema di comunicazione.

GENERALITA' SUI CODICI. (n,M)-Codici q-ari. Distanza di Hamming. Distanza minima. Sfere di Hamming. Codici sistematici. Disuguaglianza di Singleton e codici MDS.
Decodifica di minima distanza: rilevazione e correzione di errori. Codici e-correttori. Disuguaglianza di Hamming e codici perfetti. I codici perfetti banali e il codice di Hamming Ham(3,2).
Il problema fondamentale della teoria dei codici e la funzione Aq(n,d). Codici di ripetizione. Disuguaglianza di Gilbert-Varshamov. Algoritmi di decodifica di minima distanza. Decodifica con tabelle standard. Equivalenza di codici. Il problema di Eulero dei 36 ufficiali e quadrati latini. Quadrati latini ortogonali e enunciato del teorema di R.C.Bose - E.T.Parker – S.S.Shikhande. Massimo numero di quadrati latini mutuamente ortogonali. Calcolo di Aq(4,3).

CODICI LINEARI. Prime definizioni, proprietà ed esempi. Peso minimo. Matrici generatrici. Il codice binario di Golay. Equivalenza di codici lineari. Prodotto scalare standard e ortogonalità in V(n,q). Codice duale. Matrici di controllo. Codice esteso. Il codice binario di Golay esteso. Codifica e decodifica con tabelle standard. Sindromi e decodifica a sindromi. Codici binari autoduali e studio dei codici binari di Golay.
Teoremi relativi alla relazione fondamentale tra la distanza minima e le matrici di controllo di un codice lineare. Il codice ternario di Golay. (n,d-1)-insiemi e (n,d-1)-insiemi ottimi negli spazi vettoriali su campi di Galois. Packing problem negli spazi vettoriali su campi di Galois, problema fondamentale della teoria dei codici lineari e equivalenza dei due problemi. La funzione $\max_{d-1}(m,q)$. Codici lineari MDS. Determinanti di Vandermonde. Curve razionali normali in V(m,q), iperovali regolari in V(3,q) e codici MDS associati. Costruzione e proprietà dei codici di Hamming. Decodifica veloce dei codici di Hamming binari. Le funzioni $\max_3(m,2)$ e $\max_3(3,q)$.
Richiami sui campi finiti. Richiami su: l'anello F[x] dei polinomi su un campo, ideali di F[x], quozienti di F[x], l'anello quoziente $Fq[x]/(x^n-1)$. Codici ciclici: definizione, esempi, caratterizzazione, polinomio generatore, polinomio di controllo. Numero dei codici ciclici. Ciclicità dei codici binari di Hamming.

Codici BCH binari 2-correttori. Introduzione alla crittografia asimmetrica e algoritmo RSA. Il criptosistema di McEliece.

CODICI LINEARI E PIANI FINITI. Piani proiettivi: definizione e prime proprietà. Piani proiettivi su campi. Piani proiettivi finiti. Matrice d'incidenza di un piano proiettivo finito e sue proprietà. Codice lineare (binario) associato ad un piano proiettivo finito d'ordine n e sue prime proprietà. Proprietà del codice lineare associato ad un piano proiettivo finito d'ordine n=2(mod 4). Polinomio enumeratore dei pesi di un codice lineare e relazione di MacWilliams. Non esistenza del piano proiettivo d'ordine 10.