DIARIO DELLE LEZIONI DI MATEMATICA DISCRETA
A.A. 2018-19

Mercoledì 27 Febbraio

Presentazione del Corso. Introduzione alla Teoria dei grafi: grafo (semplice), vertici, archi (o lati), vertici adiacenti, estremi di un arco, archi adiacenti (o consecutivi). Ordine di un grafo. Grafi banali e completi. Rappresentazione di un grafo. I multigrafi: relazione coi grafi. Grafi diretti ed orientazione di un grafo. Isomorfismo tra grafi (cenni sulle classi di complessità P e NP e sulla non probabile NP-completezza del problema). Unione, intersezione e prodotto di grafi. Grafo complementare e grafo linea. Esempi. Sottografi di un grafo (e di un multigrafo): sottografi indotti. Intorno e grado (o valenza) di un vertice. Massimo e minimo grado di un grafo. Grafi regolari: K^n, C^n, i solidi platonici.

Giovedì 28 Febbraio

Pseudografi e cappi. Grado medio di un grafo. La relazione fondamentale (valida anche per multigrafi) $|E(G)| = \frac{1}{2}\sum_{v\in V} d_G(v)$. Il numero dei vertici di grado dispari di un grafo è pari. Ogni grafo con almeno un arco contiene un sottografo H tale che $\delta(H) > \epsilon(H) \geq \epsilon(G)$. La definizione di cammino: estremi e vertici interni. Lunghezza di un cammino. Cammini semplici. Circuiti e cicli. Calibro e circonferenza di un grafo. Un grafo G tale che $\delta(G) \geq 2$ contiene un cammino semplice di lunghezza almeno $\delta(G)$ ed un ciclo di lunghezza almeno $\delta(G) + 1$. Passeggiata. Se in un grafo vi è una passeggiata da x in y vi è un cammino semplice da x in y. Distanza tra due vertici di un grafo e diametro del grafo. Vertice centrale e raggio di un grafo. Disuguaglianze tra gli invarianti: $g(G) \leq 2\mathrm{diam}(G) + 1$ e $\mathrm{rad}(G) \leq \mathrm{diam}(G) \leq 2\mathrm{rad}(G)$. Limite superiore per $|V(G)|$ in funzione di $\Delta(G)$ e $\mathrm{rad}(G)$. Definizione di (multi)grafo e sottoinsieme di un grafo connesso.

Mercoledì 6 Marzo

Se G è connesso, allora $|E(G)| \geq |V(G)| - 1$. Definizione di componente connessa di un (multi)grafo. Foreste, alberi e foglie: definizioni ed osservazioni. Alberi filogenetici: costruzione. Teoremi di caratterizzazione per gli alberi. Numero di componenti connesse di una foresta. Sottografo

ricoprente di un grafo. Ogni grafo connesso ammette almeno un sottoalbero che lo ricopre: dimostrazione non costruttiva.

Giovedì 7 Marzo

Osservazioni sugli alberi ricoprenti. Costruzione di un albero ricoprente di costo minimo. Efficienza dell'algoritmo. Il Problema dei Ponti di Konigsberg: modellizzazione mediante un multigrafo ed un grafo. Cammini, circuiti e multigrafi euleriani. Teorema di Eulero di caratterizzazione dei (multi)grafi euleriani. Osservazione sui grafi k-regolari che sono euleriani. Cammini, cicli e grafi hamiltoniani. Condizioni necessarie (semplici) per l'hamiltonianità di un grafo. Teorema di Ore (senza dimostrazione). Teorema di Dirac. Osservazioni sul bound su $\delta(G)$ nel Teorema di Dirac. Esempi ed osservazioni sulla connessione nei grafi.

Mercoledì 13 Marzo

Dimostrazione del Teorema di Ore. Definizione di grafo k-connesso e grado di connessione $\mathcal{K}(G)$ di un grafo G. Condizioni necessarie e sufficienti affinchè $\mathcal{K}(G) = 1$. $\mathcal{K}(C^n)$ e $\mathcal{K}(K^n)$. Cammini semplici indipendenti. Teorema di caratterizzazione dei grafi 2-connessi. Se un grafo G è hamiltoniano, allora è 2-connesso. Costruzione dei grafi 2-connessi. Versione globale del Teorema di Menger (senza dimostrazione). Origini storiche dello studio dei grafi hamiltoniani: il problema del viaggiatore sul dodecaedro. Evoluzione del problema: il problema del commesso viaggiatore. Non efficienza dell'algoritmo banale: osservazioni. Impossibilità dell'uso dell'algoritmo ingordo.

Giovedì 14 Marzo

Alcuni risultati computazionali (storici e recenti) sul problema del commesso viaggiatore. Definizione di sequenza dei gradi di un grafo e di sequenza hamiltoniana di interi. Teorema di Chvatal di caratterizzazione delle sequenze hamiltoniane. Definizione di grafo r-partito e r-partito completo. Il caso $r = 2$: grafi bipartiti. Esempi. C^n è bipartito se, e solo se, n è pari. Teorema di caratterizzazione dei grafi bipartiti (con almeno due vertici). I grafi bipartiti ed i problemi di assegnazione.

Mercoledì 20 Marzo

Definizione di accoppiamento ed accoppiamento massimo di un grafo ed accoppiamento ottimale di un grafo bipartito. Copertura di un grafo ed indice di copertura. Osservazioni ed esempi. Cammini alternanti e cammini aumentanti. Il Teorema di Konig sulla cardinalità di un accoppiamento massimo di un grafo bipartito con almeno due vertici. Algoritmo (ungherese) per la costruzione di un accoppiamento massimo in grafi bipartiti tramite i cammini aumentanti. Il Teorema (dei matrimoni) di P. Hall. Corollario: grafi bipartiti k-regolari hanno un accoppiamento ottimale.

Giovedì 21 Marzo

Applicazioni del Teorema di Hall: condizioni necessarie e sufficienti per l'esistenza di un sistema di rappresentanti per una famiglia di sottoinsiemi non-vuoti di un insieme; matrici di permutazione. Introduzione al problema della colorazione dei vertici di un grafo. Definizione. Grafi d-colorabili e numero cromatico $\chi(G)$ di un grafo G. Esempi. Grafi 1- e 2-colorabili. Il problema dei 4 colori: notizie storiche. Un algoritmo per colorare i vertici di un grafo: osservazioni sul fatto che in generale non è ottimale e soluzioni migliori per l'ordinamento dei vertici. La limitazione data dall'algoritmo: $\chi(G) \leq \Delta(G)+1$. Il limite è raggiunto per grafi completi e cicli di lunghezza dispari. Il Teorema di Brooks: se G è connesso e non è un ciclo di lunghezza dispari o un grafo completo, allora $\chi(G) \leq \Delta(G)$ (enunciato). Colorazione dei lati di un grafo: un approccio concreto al problema. Grafi d-colorabili nei lati. Indice cromatico $\chi'(G)$ di un grafo G. Una limitazione immediata: $\chi'(G) \geq \Delta(G)$. Indice cromatico di cicli. Sul numero di giornate di un torneo a girone unico con n squadre.

Mercoledì 27 Marzo

Dimostrazione del Teorema di Brooks. Indice cromatico di un grafo completo.

Giovedì 28 Marzo

Il Teorema di Konig: se G è bipartito, $\chi'(G) = \Delta(G)$. Il Teorema di Vizing: per ogni grafo G, $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$. Introduzione alla Teoria di Ramsey. Enunciato del Teorema di Ramsey: per ogni intero r esiste

un intero n tale che ogni grafo con almeno n vertici, o il suo complementare, ha un sottografo isomorfo a K^r. Numeri di Ramsey $R(n)$. Definizione di colorazione debole dei lati di un grafo. Enunciato del Teorema di Ramsey in termini di colorazioni deboli.

Mercoledì 3 Aprile

Dimostrazione del Teorema di Ramsey e limite superiore per $R(n)$. Il Teorema di Erdos: per ogni $n \geq 3$, $R(n) > 2^{\frac{n}{2}}$. I numeri $R(n, m)$: alcune osservazioni e proprietà. Esistenza dei numeri $R(n, m)$ (e nuova dimostrazione del Teorema di Ramsey). Teorema di Ramsey generalizzato: colorazioni con $c > 2$ colori (solo enunciato). Teoria di Ramsey per insiemi: c-colorazioni di $[V]^k$, dove V è un insieme qualsiasi non-vuoto. Sottoinsiemi $[k]$-monocromatici di V.

Giovedì 4 Aprile

Il Teorema di Ramsey generalizzato nel caso infinito: se $k, c \geq 1$ e V è un insieme con infiniti elementi, per ogni c-colorazione di $[V]^k$ esiste $X \subseteq V$ infinito $[k]$-monocromatico. Lemma di Konig. Il Teorema di Ramsey generalizzato nel caso finito: se $k, c, n \geq 1$ esiste un intero r tale che, dato un insieme finito V con $|V| \geq r$ ed una qualsiasi c-colorazione di $[V]^k$, esiste $X \subseteq V$ di cardinalità n che è $[k]$-monocromatico. Semplici applicazioni della Teoria di Ramsey: colorazione dei 3-sottoinsiemi di un insieme di punti del piano; ogni successione reale ha una sottosuccessione strettamente monotona o costante.

Mercoledì 10 Aprile

Teorema di Schur sulle r-partizioni e sue applicazioni ad equazioni in $\mathbb{Z}_p$. Introduzione alla Teoria dei codici correttori di errori: canale di trasmissione, codifica e decodifica. Semplici esempi: raddoppio della parola, controllo di parità, triplicazione della parola. Definizioni di base: alfabeto, parole, lunghezza delle parole. Codice e lunghezza del codice. Distanza tra le parole. Decodifica di massima probabilità. Minima distanza e capacità di correzione di errori di un codice.

Giovedì 11 Aprile

Ancora sulla capacità di correzione di errori. Codici lineari. Peso di una parola e relazione tra pesi delle parole e distanze tra le parole in un codice lineare. Minimo peso. Distribuzione dei pesi di un codice. Posizioni di informazione e posizioni di ridondanza. Codici equivalenti. Matrice dei generatori di un codice e metodo di codifica. Matrice dei generatori in forma scalare ridotta. Prodotto interno tra i vettori di un codice lineare. Il codice ortogonale di un codice dato. Matrice di controllo di parità. Condizione necessaria e sufficiente affinchè una parola appartenga ad un codice lineare. Forma di una matrice di controllo di parità nota la matrice dei generatori in forma scalare ridotta. Utilizzo per la codifica.

Mercoledì 17 Aprile

Codici estesi e punturati: osservazioni. Codici autortogonali ed autoduali. Esempi. Condizioni necessarie e sufficienti affinchè un codice lineare binario sia autortogonale. Coset leaders e tabella standard di un codice lineare: decodifica mediante essa. Sindrome di un vettore. Esistenza di una biezione tra le sindromi di V_n ed i laterali di un (n, k)-codice lineare. Applicazioni del risultato nella decodifica: vantaggi. Packing radius e covering radius di un (n, k, d)-codice lineare. Codici perfetti e quasi perfetti.

Mercoledì 8 Maggio

Esempi di codici perfetti. I codici perfetti banali. Caratterizzazioni del packing radius e del covering radius. Peso di un vettore e lineare dipendenza tra le colonne di una matrice di controllo di parità di un codice lineare. Caratterizzazione del peso minimo di un codice lineare in funzione del numero di colonne linearmente indipendenti di una sua matrice di controllo di parità. Singleton bound. Numero minimo di posizioni contenenti un insieme di informazione. Lo Sphere Packing Bound. Codici perfetti: il $(23, 12, 7)$-codice binario di Golay e l'$(11, 6, 5)$-codice ternario di Golay (senza costruzione).

Giovedì 9 Maggio

Costruzione dei $(\frac{q^r-1}{q-1} =: n, n-r, 3)$-codici generali di Hamming (che sono perfetti) su $GF(q)$. Teorema di caratterizzazione dei codici perfetti

(senza dimostrazione). Codici ciclici. Lo shift register ed i suoi componenti: lo storage element ed il binary adder. Esempio di shift register (relativo al $(7, 4, 3)$-codice binario di Hamming). Definizione di shift ciclico e codice ciclico. Codici ciclici ed anello quoziente $R_n := GF(q)[x]/I$, dove I è l'ideale generato da $x^n - 1$ in $GF(q)[x]$. Caratterizzazione dei codici ciclici come ideali di R_n.

Mercoledì 15 Maggio

Il polinomio generatore di un codice ciclico. Generatori di un codice ciclico e fattorizzazione del polinomio $x^n - 1$. Dimensione di un codice e matrice dei generatori di un codice ciclico con polinomio generatore $g(x)$. Esempi. Reciproco di un polinomio. Matrice di controllo di parità di un codice ciclico: l'ortogonale di un codice ciclico è ciclico.

Giovedì 16 Maggio

Lo shift register per il $(7, 4, 3)$-codice binario di Hamming. Inclusione tra codici ciclici. Il codice ciclico binario dei vettori di peso pari. Codici ciclici autortogonali: condizioni necessarie e sufficienti. Generatori idempotenti di codici ciclici: prime proprietà. Laterali ciclotomici di n rispetto a p. Relazioni colla fattorizzazione del polinomio $x^n - x$. Polinomi minimi e radici.

Mercoledì 22 Maggio

Caratterizzazioni dei polinomi binari idempotenti (di R_n). Un codice ciclico binario di lunghezza dispari ammette un generatore idempotente. Numeri di codici ciclici binari di lunghezza dispari. Idempotenti ed ideali minimali. Gli ideali/codici $C_1 + C_2$ e $C_1 \cap C_2$ di R_n: polinomi generatori e generatori idempotenti in funzione dei polinomi generatori e generatori idempotenti degli ideali/codici C_1 e C_2 di R_n. Relazione tra il polinomio generatore ed il generatore idempotente di un codice ciclico binario di lunghezza dispari. Il gruppo di un codice lineare: definizione ed osservazioni. Codici ciclici, $G(V_n)$ e $G(\langle h \rangle)$.

Giovedì 23 Maggio

Le permutazioni σ e τ: la loro coniugazione. Il sottogruppo generato da σ e τ ed il suo ordine in $G(C)$ dove C è un codice ciclico binario di lunghezza dispari. La permutazione μ_a in un codice ciclico binario C di lunghezza dispari coprima con a manda C in un codice ciclico C' ed il suo generatore idempotente nel generatore idempotente di C'. Introduzione alla classe dei codici a residui quadratici (QR codici). Residui quadratici o quadrati nel gruppo moltiplicativo di un campo finito. Prodotto di quadrati e non-quadrati. Condizioni necessarie e sufficienti affinchè 2 sia un quadrato in $GF(p)$ (senza dimostrazione). Un codice ciclico binario di lunghezza $p \equiv_8 \pm 1$ è a residui quadratici se è mandato in sè stesso dalle permutazioni μ_a per ogni quadrato a di $GF(p)$. I generatori idempotenti dei QR codici.

Martedì 28 Maggio

I codici $Q_1 := \langle e_1(x) \rangle$, $Q_2 := \langle e_2(x) \rangle$, $Q_1' := \langle 1 + e_2(x) \rangle$ e $Q_2' := \langle 1 + e_1(x) \rangle$: relazione tra di essi, somma, intersezione e dimensioni (se -1 è un non-quadrato in $GF(p)$). Polinomi generatori di tali codici. Autortogonalità. Studio del gruppo dei codici estesi $\bar{Q}_i$ di Q_i: retta proiettiva e punti della retta proiettiva. Richiami sull'azione di gruppo su di un insieme.

Mercoledì 29 Maggio

Azione di $GL(q)$ e $SL(q)$. Gruppo lineare proiettivo e lineare proiettivo speciale $PSL(2, q)$. Generatori di $PSL(2, q)$. Teorema di Gleason-Prange: $PSL(2, p) \leq G(\bar{Q}_i)$ (dimostrazione nel caso $p = 7$ e cenno della dimostrazione se $p \equiv_8 -1$). Transitività di $G(\bar{Q}_i)$. Equivalenza e parametri dei codici $\bar{Q}_1$ e $\bar{Q}_2$. Se $p \equiv_8 -1$, $\bar{Q}_1$ e $\bar{Q}_2$ sono doppiamente pari. Se $p \equiv_8 1$, $\bar{Q}_1$ e $\bar{Q}_2$ contengono solo vettori di peso pari.

Giovedì 30 Maggio

Codici punturati equivalenti. Il minimo peso di un QR codice è dispari. Inoltre, se $p \equiv_8 -1$, $A_i = 0$ se $i \not\equiv_4 0, 3$. Teorema di Assmus-Mattson: un QR codice di lunghezza p ha minimo peso d tale che $d^2 \geq p$. Inoltre, se $p \equiv_8 -1$, $d^2 - d + 1 \geq p$. Tabella dei minimi pesi per QR codici di lunghezza piccola.