

DIDATTICA EROGATA 2025/2026

Scienze Computazionali (LM-40 R)

Dipartimento: MATEMATICA E FISICA

Codice CdS: 104653

INSEGNAMENTI

Primo semestre

20410882 - AC310 - ANALISI COMPLESSA (- MAT/03,MAT/05 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CHIERCHIA LUIGI	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CHIERCHIA LUIGI	72	
Mutuato da: 20410882 AC310 - ANALISI COMPLESSA in Matematica L-35 R CHIERCHIA LUIGI	72	

20410408 - AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE (- MAT/02 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	
Mutuato da: 20410408 AL310 - ISTITUZIONI DI ALGEBRA SUPERIORE in Matematica L-35 R BARROERO FABRIZIO	72	

20410445 - AL410 - ALGEBRA COMMUTATIVA (- MAT/02 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410445 AL410 - ALGEBRA COMMUTATIVA in Matematica LM-40 R TURCHET AMOS	72	
Mutuato da: 20410445 AL410 - ALGEBRA COMMUTATIVA in Matematica LM-40 R TURCHET AMOS	72	
Mutuato da: 20410445 AL410 - ALGEBRA COMMUTATIVA in Matematica LM-40 R TURCHET AMOS	72	

20410609 - AM300 - ANALISI MATEMATICA 5 (- MAT/05 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410609 AM300 - ANALISI MATEMATICA 5 in Matematica L-35 R HAUS EMANUELE	72	
Mutuato da: 20410609 AM300 - ANALISI MATEMATICA 5 in Matematica L-35 R HAUS EMANUELE	72	
Mutuato da: 20410609 AM300 - ANALISI MATEMATICA 5 in Matematica L-35 R HAUS EMANUELE	72	

20410876 - AM400-ISTITUZIONI DI ANALISI SUPERIORE (- MAT/05 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410876 AM400-ISTITUZIONI DI ANALISI SUPERIORE in Matematica LM-40 R FEOLA ROBERTO	72	
Mutuato da: 20410876 AM400-ISTITUZIONI DI ANALISI SUPERIORE in Matematica LM-40 R FEOLA ROBERTO	72	

Dettaglio	Ore	Canale
Mutuato da: 20410876 AM400-ISTITUZIONI DI ANALISI SUPERIORE in Matematica LM-40 R FEOLA ROBERTO	72	

20410756 - AM420 - EQUAZIONI ALLE DERIVATE PARZIALI (- MAT/05 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410756 AM420 - EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BESSI UGO	60	
Mutuato da: 20410756 AM420 - EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BESSI UGO	60	
Mutuato da: 20410756 AM420 - EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R BESSI UGO	60	

20410413 - AN410 - ANALISI NUMERICA 1 (- MAT/08 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	
Mutuato da: 20410413 AN410 - ANALISI NUMERICA 1 in Matematica L-35 R FERRETTI ROBERTO	72	

20410447 - CP410 - TEORIA DELLA PROBABILITÀ (- MAT/06 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	
Fruito da: 20410414 CP410 - TEORIA DELLA PROBABILITÀ in Matematica L-35 R CANDELLERO ELISABETTA	72	

20410457 - CP430 - CALCOLO STOCASTICO (- MAT/06 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410457 CP430 - CALCOLO STOCASTICO in Matematica LM-40 R CANDELLERO ELISABETTA	60	
Mutuato da: 20410457 CP430 - CALCOLO STOCASTICO in Matematica LM-40 R CANDELLERO ELISABETTA	60	
Mutuato da: 20410457 CP430 - CALCOLO STOCASTICO in Matematica LM-40 R CANDELLERO ELISABETTA	60	

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A (- MAT/02 - 6 CFU - 60 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MEROLA FRANCESCA	60	Carico didattico	

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B (- MAT/02 - 3 CFU - 12 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MEROLA FRANCESCA	12	Carico didattico	

20410436 - FS420 - MECCANICA QUANTISTICA (- FIS/02 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R LUBICZ VITTORIO	60	
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R TARANTINO CECILIA	60	
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R LUBICZ VITTORIO	60	
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R TARANTINO CECILIA	60	
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R LUBICZ VITTORIO	60	
Frutto da: 20410015 MECCANICA QUANTISTICA in Fisica L-30 R TARANTINO CECILIA	60	

20410437 - FS430- TEORIA DELLA RELATIVITÀ (- FIS/02 - 6 CFU - 48 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20402258 TEORIA DELLA RELATIVITA' in Fisica LM-17 R FRANCIA DARIO	48	
Frutto da: 20402258 TEORIA DELLA RELATIVITA' in Fisica LM-17 R FRANCIA DARIO	48	
Frutto da: 20402258 TEORIA DELLA RELATIVITA' in Fisica LM-17 R FRANCIA DARIO	48	

20411003 - FS520 – RETI COMPLESSE (- FIS/03,INF/01 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
GUARINO STEFANO	60	Affidamento in convenzione	

20410560 - MODULO A - PROGRAMMAZIONE IN PYTHON (- INF/01 - 3 CFU - 30 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
RAVONI ALESSANDRO	30	Contratto	

20410435 - FS440 - ACQUISIZIONE DATI E CONTROLLO DI ESPERIMENTI (- FIS/04 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20401070 ACQUISIZIONE DATI E CONTROLLO DI ESPERIMENTI in Fisica LM-17 R N0 Branchini Paolo	60	
Frutto da: 20401070 ACQUISIZIONE DATI E CONTROLLO DI ESPERIMENTI in Fisica LM-17 R N0 Branchini Paolo	60	
Frutto da: 20401070 ACQUISIZIONE DATI E CONTROLLO DI ESPERIMENTI in Fisica LM-17 R N0 Branchini Paolo	60	

20410449 - GE410 - GEOMETRIA ALGEBRICA 1 (- MAT/03 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R CAPORASO LUCIA	66	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R BRUNO ANDREA	6	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R CAPORASO LUCIA	66	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R BRUNO ANDREA	6	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R CAPORASO LUCIA	66	
Mutuato da: 20410449 GE410 - GEOMETRIA ALGEBRICA 1 in Matematica LM-40 R BRUNO ANDREA	6	

20410560 - MODULO B - PROGRAMMAZIONE IN MATLAB (- INF/01 - 3 CFU - 30 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PAPA FEDERICO	30	Esperto di alta qualificazione retribuito	

20410427 - IN490 - LINGUAGGI DI PROGRAMMAZIONE (- INF/01 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LOMBARDI FLAVIO	72	Esperto di alta qualificazione retribuito	

20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ (- MAT/01 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	72	Affidamento a titolo gratuito	
PEDICINI MARCO	48	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410417 IN410-CALCOLABILITÀ E COMPLESSITÀ in Scienze Computazionali LM-40 R PEDICINI MARCO	72	

20411002 - IN510 – QUANTUM COMPUTING MODULO A (- ING-INF/05 - 3 CFU - 27 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20810323 QUANTUM COMPUTING in Ingegneria informatica LM-32 DI BATTISTA GIUSEPPE	27	
Fruito da: 20810323 QUANTUM COMPUTING in Ingegneria informatica LM-32 DI BATTISTA GIUSEPPE	27	
Fruito da: 20810323 QUANTUM COMPUTING in Ingegneria informatica LM-32 DI BATTISTA GIUSEPPE	27	

20411002 - IN510 – QUANTUM COMPUTING MODULO B (- INF/01 - 3 CFU - 30 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	30	Affidamento a titolo gratuito	

20410432 - IN550 – MACHINE LEARNING (- INF/01 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BONIFACI VINCENZO	60	Carico didattico	

20410451 - LM410 -TEOREMI SULLA LOGICA 1 - MODULO A (- MAT/01 - 6 CFU - 48 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410451-1 LM410 -TEOREMI SULLA LOGICA 1 - MODULO A in Matematica LM-40 R MAIELI ROBERTO	48	

20410451 - LM410 -TEOREMI SULLA LOGICA 1 - MODULO B (- MAT/01 - 3 CFU - 24 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410451-2 LM410 -TEOREMI SULLA LOGICA 1 - MODULO B in Matematica LM-40 R TORTORA DE FALCO LORENZO	24	

20410613 - LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA (- MAT/01 - 6 CFU - 60 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410613 LM430 - LOGICA E FONDAMENTI DELLA MATEMATICA in Matematica LM-40 R TORTORA DE FALCO LORENZO	60	

20410555 - ST410-STATISTICA (- MAT/06 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
MARTINELLI FABIO	60	Carico didattico	

Secondo semestre

20410520 - AL420 - TEORIA ALGEBRICA DEI NUMERI (- MAT/02 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410520 AL420 - TEORIA ALGEBRICA DEI NUMERI in Matematica LM-40 R BARROERO FABRIZIO	60	
Mutuato da: 20410520 AL420 - TEORIA ALGEBRICA DEI NUMERI in Matematica LM-40 R BARROERO FABRIZIO	60	
Mutuato da: 20410520 AL420 - TEORIA ALGEBRICA DEI NUMERI in Matematica LM-40 R BARROERO FABRIZIO	60	

20410757 - AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI (- MAT/05 - 3 CFU - 30 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410757_2 AM410 - MODULO B - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R ESPOSITO PIERPAOLO	30	

20410757 - AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI (- MAT/05 - 3 CFU - 30 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410757_1 AM410- MODULO A - INTRODUZIONE ALLE EQUAZIONI ALLE DERIVATE PARZIALI in Matematica LM-40 R ESPOSITO PIERPAOLO	30	

20410637 - AM450 - ANALISI FUNZIONALE (- MAT/05 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410637 AM450 - ANALISI FUNZIONALE in Matematica LM-40 R BESSI UGO	72	
Mutuato da: 20410637 AM450 - ANALISI FUNZIONALE in Matematica LM-40 R BESSI UGO	72	
Mutuato da: 20410637 AM450 - ANALISI FUNZIONALE in Matematica LM-40 R BESSI UGO	72	

20410420 - AN420 - ANALISI NUMERICA 2 (- MAT/08 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
FERRETTI ROBERTO	48	Carico didattico	
GIULIANI ALESSANDRO	12	Carico didattico	

20410556 - CP450 - METODI PROBABILISTICI E ALGORITMI ALEATORI (- MAT/06 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
QUATTROPANI MATTEO	60	Carico didattico	

20410428 - CR510 – CRITTO SISTEMI ELLITTICI (- MAT/02 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
CAPUANO LAURA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410428 CR510 – CRITTO SISTEMI ELLITTICI in Scienze Computazionali LM-40 R CAPUANO LAURA	60	

20410410 - FM310 - ISTITUZIONI DI FISICA MATEMATICA (- MAT/07 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	42	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R MARCELLI GIOVANNA	30	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	42	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R MARCELLI GIOVANNA	30	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R GIULIANI ALESSANDRO	42	
Mutuato da: 20410410 FM310 - ISTITUZIONI DI FISICA MATEMATICA in Matematica L-35 R MARCELLI GIOVANNA	30	

20410416 - FM410-COMPLEMENTI DI MECCANICA ANALITICA - Modulo A (- MAT/07 - 3 CFU - 30 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20410084 COMPLEMENTI DI MECCANICA ANALITICA - MOD A in Fisica L-30 R REUVERS Robin Johannes Petrus	30	

20410416 - FM410-COMPLEMENTI DI MECCANICA ANALITICA - Modulo B (- MAT/07 - 3 CFU - 30 ore - ITA)

Curricula: Crittografia e sicurezza informatica

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20410085 COMPLEMENTI DI MECCANICA ANALITICA - MOD. B in Fisica L-30 R MARCELLI GIOVANNA	30	

20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING (- MAT/07 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	14	Bando	
REUVERS ROBIN JOHANNES PETRUS	34	Carico didattico	
TERESI LUCIANO	24	Affidamento a titolo gratuito	
Da assegnare	14	Bando	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410875 FM530 - METODI MATEMATICI PER IL MACHINE LEARNING in Scienze Computazionali LM-40 R REUVERS Robin Johannes Petrus	34	
Mutuato da: 20410875 FM530 - METODI MATEMATICI PER IL MACHINE LEARNING in Scienze Computazionali LM-40 R TERESI LUCIANO	24	
Mutuato da: 20410875 FM530 - METODI MATEMATICI PER IL MACHINE LEARNING in Scienze Computazionali LM-40 R		

20430001 - FM540 - METODI COMPUTAZIONALI PER MODELLI STOCASTICI (- MAT/07 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

20410434 - FS450 - ELEMENTI DI MECCANICA STATISTICA (- FIS/02 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20401806 ELEMENTI DI MECCANICA STATISTICA in Fisica L-30 R NO RAIMONDI ROBERTO	60	
Frutto da: 20401806 ELEMENTI DI MECCANICA STATISTICA in Fisica L-30 R NO RAIMONDI ROBERTO	60	
Frutto da: 20401806 ELEMENTI DI MECCANICA STATISTICA in Fisica L-30 R NO RAIMONDI ROBERTO	60	

20410444 - GE430 - GEOMETRIA RIEMANNIANA (- MAT/03 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410444 GE430 - GEOMETRIA RIEMANNIANA in Matematica LM-40 R PONTECORVO MASSIMILIANO	60	
Mutuato da: 20410444 GE430 - GEOMETRIA RIEMANNIANA in Matematica LM-40 R PONTECORVO MASSIMILIANO	60	
Mutuato da: 20410444 GE430 - GEOMETRIA RIEMANNIANA in Matematica LM-40 R PONTECORVO MASSIMILIANO	60	

20410566 - FS470 - PRINCIPI DI ASTROFISICA (- FIS/05 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R LA FRANCA FABIO	60	
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R MATT GIORGIO	60	

Dettaglio	Ore	Canale
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R LA FRANCA FABIO	60	
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R MATT GIORGIO	60	
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R LA FRANCA FABIO	60	
Frutto da: 20410499 Principi di Astrofisica in Fisica L-30 R MATT GIORGIO	60	

20410429 - FS510 - METODO MONTECARLO (- FIS/01 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R FRANCESCHINI ROBERTO	40	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R BUSSINO SEVERINO ANGELO MARIA	20	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R FRANCESCHINI ROBERTO	40	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R BUSSINO SEVERINO ANGELO MARIA	20	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R FRANCESCHINI ROBERTO	40	
Mutuato da: 20410429 FS510 - METODO MONTECARLO in Fisica LM-17 R BUSSINO SEVERINO ANGELO MARIA	20	

20410425 - GE460 - TEORIA DEI GRAFI (- MAT/03 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
SCHAFFLER LUCA	60	Carico didattico	

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410425 GE460 - TEORIA DEI GRAFI in Scienze Computazionali LM-40 R SCHAFFLER LUCA	60	

20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA (- INF/01 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
PEDICINI MARCO	60	Carico didattico	

20410411 - GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE (- MAT/03 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R SUPINO PAOLA	12	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R SUPINO PAOLA	12	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R MASCARENHAS MELO ANA MARGARIDA	60	
Mutuato da: 20410411 GE310 - ISTITUZIONI DI GEOMETRIA SUPERIORE in Matematica L-35 R SUPINO PAOLA	12	

20410567 - GE470-SUPERFICI DI RIEMANN (- MAT/03 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R LELLI CHIESA MARGHERITA	48	
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R VERRA ALESSANDRO	12	
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R LELLI CHIESA MARGHERITA	48	
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R VERRA ALESSANDRO	12	
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R LELLI CHIESA MARGHERITA	48	
Mutuato da: 20410567 GE470-SUPERFICI DI RIEMANN in Matematica LM-40 R VERRA ALESSANDRO	12	

20410426 - IN480 - CALCOLO PARALLELO E DISTRIBUITO (- INF/01 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
LOMBARDI FLAVIO	72	Affidamento in convenzione	

20411014 - IN580- ETHICAL HACKING (- ING-INF/03 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	60	
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	60	
Fruito da: 20810554 ETHICAL HACKING in Ingegneria delle Telecomunicazioni LM-27 CARLI MARCO	60	

20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA (- MAT/09 - 9 CFU - 72 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
BONIFACI VINCENZO	72	Affidamento a titolo gratuito	
BONIFACI VINCENZO	48	Carico didattico	

20430002 - IN590 - NATURAL LANGUAGE PROCESSING (- INF/01 - 6 CFU - 60 ore - ITA)

Curricula: Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche

Docenti:

Nominativo	Ore	Tipo incarico	Canale
Da assegnare	60	Bando	
Da assegnare	60	Bando	
Da assegnare	60	Bando	

20410455 - LM420 - TEOREMI SULLA LOGICA 2 (- MAT/01 - 6 CFU - 36 ore - ITA)

Curricula: Analisi dei dati e statistica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20710122 TEOREMI SULLA LOGICA, 2 in Scienze filosofiche LM-78 R TORTORA DE FALCO LORENZO	36	
Fruito da: 20710122 TEOREMI SULLA LOGICA, 2 in Scienze filosofiche LM-78 R TORTORA DE FALCO LORENZO	36	

20410529 - LM510 - TEORIE LOGICHE 1 (- MAT/01 - 6 CFU - 36 ore - ITA)

Curricula: Analisi dei dati e statistica - Modellistica fisica e simulazioni numeriche

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 20710091 TEORIE LOGICHE 1 - LM in Scienze filosofiche LM-78 R MAIELI ROBERTO	36	

Dettaglio	Ore	Canale
Fruito da: 20710091 TEORIE LOGICHE 1 - LM in Scienze filosofiche LM-78 R MAIELI ROBERTO	36	

20410438 - MF410 - FINANZA COMPUTAZIONALE (- SECS-S/06 - 9 CFU - 60 ore - ITA)

Curricula: *Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche*

Mutuazioni:

Dettaglio	Ore	Canale
Fruito da: 21201730 FINANZA COMPUTAZIONALE in Finanza e impresa LM-16 R CESARONE FRANCESCO	60	
Fruito da: 21201730 FINANZA COMPUTAZIONALE in Finanza e impresa LM-16 R CESARONE FRANCESCO	60	
Fruito da: 21201730 FINANZA COMPUTAZIONALE in Finanza e impresa LM-16 R CESARONE FRANCESCO	60	

20410627 - TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI (- MAT/02 - 6 CFU - 60 ore - ITA)

Curricula: *Analisi dei dati e statistica - Crittografia e sicurezza informatica - Modellistica fisica e simulazioni numeriche*

Mutuazioni:

Dettaglio	Ore	Canale
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	30	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	30	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R PAPPALARDI FRANCESCO	30	
Mutuato da: 20410627 TN410 - INTRODUZIONE ALLA TEORIA DEI NUMERI in Matematica LM-40 R		

INCARICHI DIDATTICI DEL CORSO DI LAUREA

Nominativo	Tot.Ore	Tipo incarico	Ore	Attività didattica
BONIFACI VINCENZO	132	Carico didattico	48	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Affidamento a titolo gratuito	72	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Carico didattico	48	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Affidamento a titolo gratuito	72	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Carico didattico	48	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Affidamento a titolo gratuito	72	20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA
		Carico didattico	60	20410432 - IN550 – MACHINE LEARNING
CAPUANO LAURA	60	Carico didattico	60	20410428 - CR510 – CRITTOSISTEMI ELLITTICI
FERRETTI ROBERTO	60	Carico didattico	48	20410420 - AN420 - ANALISI NUMERICA 2
		Carico didattico	48	20410420 - AN420 - ANALISI NUMERICA 2
GIULIANI ALESSANDRO	12	Carico didattico	12	20410420 - AN420 - ANALISI NUMERICA 2
GUARINO STEFANO	60	Affidamento in convenzione	60	20411003 - FS520 – RETI COMPLESSE
LOMBARDI FLAVIO	144	Affidamento in convenzione	72	20410426 - IN480 - CALCOLO PARALLELO E DISTRIBUITO
		Esperto di alta qualificazione retribuito	72	20410427 - IN490 - LINGUAGGI DI PROGRAMMAZIONE
MARTINELLI FABIO	60	Carico didattico	60	20410555 - ST410-STATISTICA
MEROLA FRANCESCA	72	Carico didattico	60	20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA
		Carico didattico	12	20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA
PAPA FEDERICO	30	Esperto di alta qualificazione retribuito	30	20410560 - IN400 - PROGRAMMAZIONE IN PYTHON E MATLAB
PEDICINI MARCO	162	Affidamento a titolo gratuito	72	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Carico didattico	48	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Affidamento a titolo gratuito	72	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Carico didattico	48	20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ
		Carico didattico	60	20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA
		Affidamento a titolo gratuito	30	20411002 - IN510 – QUANTUM COMPUTING
QUATTROPANI MATTEO	60	Carico didattico	60	20410556 - CP450 - METODI PROBABILISTICI E ALGORITMI ALEATORI
RAVONI ALESSANDRO	30	Contratto	30	20410560 - IN400 - PROGRAMMAZIONE IN PYTHON E MATLAB
REUVERS ROBIN JOHANNES PETRUS	34	Carico didattico	34	20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING
SCHAFFLER LUCA	60	Carico didattico	60	20410425 - GE460 - TEORIA DEI GRAFI
TERESI LUCIANO	24	Affidamento a titolo gratuito	24	20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING
DOCENTE NON DEFINITO	324	Bando	14	20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING
		Bando	14	20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING
		Bando	60	20430002 - IN590 - NATURAL LANGUAGE PROCESSING
		Bando	60	20430002 - IN590 - NATURAL LANGUAGE PROCESSING
		Bando	60	20430002 - IN590 - NATURAL LANGUAGE PROCESSING
Totale ore	1324			

CONTENUTI DIDATTICI

20410445 - AL410 - ALGEBRA COMMUTATIVA

Docente: TURCHET AMOS

Italiano

Prerequisiti

Conoscenze e risultati studiati nei corsi AL110 e AL210

Programma

Anelli e ideali, ideali massimali e ideali primi, nilradicale e radicale di Jacobson, spettro di un anello. Moduli, moduli finitamente generati e Lemma di Nakayama, successioni esatte, prodotto tensoriale, restrizione ed estensione degli scalari. Anelli e moduli di frazioni, localizzazione. Serie di composizione e lunghezza di un modulo. Condizioni sulle catene. Anelli Noetheriani, Teorema della Base di Hilbert. Estensioni intere, teoremi di Lying Over, Going-up. Teorema di Normalizzazione di Noether e Teorema degli zeri di Hilbert. Dimensione di Krull e Teorema dell'ideale principale di Krull. Grado di trascendenza. Dimensione di anelli Noetheriani locali. Anelli regolari.

Testi

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021

Bibliografia di riferimento

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021 D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag, 1995.

Modalità erogazione

Testi da definire

Modalità di valutazione

Esoneri o prova scritta su esercizi e prova orale consistente di un seminario più una parte standard su teoremi e dimostrazioni.

English

Prerequisites

Knowledge and results from the courses AL110 and AL210

Programme

Rings and ideals, maximal ideals and prime ideals, nilradical and Jacobson radical, spectrum of a ring. Modules, finitely generated modules and Nakayama's Lemma, exact sequences, tensor product, restriction and extension of scalars. Rings and modules of fractions, localization. Composition series and length of a module. Chain conditions. Noetherian rings, Hilbert's Basis Theorem. Integral extensions, Lying Over and Going-up theorems. Noether normalization theorem and Hilbert's Nullstellensatz. Krull dimension and Krull's principal ideal theorem. Transcendence degree. Dimension of local Noetherian rings. Regular rings.

Reference books

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021

Reference bibliography

M. F. Atiyah, I. G. Macdonald, Introduction to Commutative Algebra. Addison-Wesley, 1996. A. Gathmann, Commutative Algebra, Lecture notes. A. Chambert-Loir, (Mostly) Commutative Algebra, Springer Cham, 2021 D. Eisenbud, Commutative Algebra with a view toward Algebraic Geometry, Springer-Verlag, 1995.

Study modes

-

Exam modes

-

20410876 - AM400-ISTITUZIONI DI ANALISI SUPERIORE

Docente: FEOLA ROBERTO

Italiano

Prerequisiti

Calcolo in una e più variabili, Teoria della misura di Lebesgue

Programma

Teoria della misura, misure esterne, costruzione di misure di Borel sui reali. Teoria dell'integrazione, teoremi di passaggio al limite, convergenza in media e in misura, integrazione sugli spazi prodotto. Misure di Radon, regolarità, funzionali lineari positivi sulle funzioni continue, Teorema di rappresentazione di Riesz. Misure con segno, teoremi di decomposizione, differenziazione di misure, funzioni a

variazione limitata, Teorema fondamentale del calcolo. Spazi L_p , proprietà di base, spazi duali, teoremi di densità. Cenni di teoria geometrica della misura.

Testi

G. Folland - "Real Analysis" - Wiley

Bibliografia di riferimento

G. Folland - "Real Analysis" - Wiley

Modalità erogazione

Testi da definire

Modalità di valutazione

Esercizi assegnati a casa (tre assegnazioni in totale) e prova orale sul programma del corso.

English

Prerequisites

Calculus in one and more variables, Lebesgue measure theory

Programme

Measure theory, outer measures, construction of Borel measures. Integration theory, limit theorems, convergence in mean and in measure, integration on product spaces. Radon measures, regularity, positive linear functionals, Riesz representation theorem. Signed measures, decomposition theorems, differentiation, BV functions, fundamental theorem of calculus. L_p spaces, basic properties, dual spaces, density theorems. Introduction to geometric measure theory

Reference books

G. Folland - "Real Analysis" - Wiley

Reference bibliography

G. Folland - "Real Analysis" - Wiley

Study modes

-

Exam modes

-

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA

(CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO B)

Docente: MEROLA FRANCESCA

Italiano

Prerequisiti

Conoscenze di base di algebra.

Programma

Argomenti avanzati di crittografia. Fra le possibilità: Protocolli, firme, crittografia PostQuantum.

Testi

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Bibliografia di riferimento

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Modalità erogazione

lezioni in presenza: ci sarà anche probabilmente la possibilità di seguire online

Modalità di valutazione

prova scritta: di norma 4 esercizi teorico/pratici, durata di norma 2 ore e 30. prova orale: facoltativa per una votazione ≤ 26

English

Prerequisites

Basic knowledge of algebra.

Programme

Advanced topics in cryptography. Amongst the possibilities: Protocols, Digital signatures, PostQuantum Cryptography

Reference books

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Reference bibliography

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Study modes

-

Exam modes

-

20410625 - CR410-CRITTOGRAFIA A CHIAVE PUBBLICA

(CR410-CRITTOGRAFIA A CHIAVE PUBBLICA - MODULO A)

Docente: MEROLA FRANCESCA

Italiano

Prerequisiti

Conoscenze di base di algebra.

Programma

Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici. Introduzione alla crittoanalisi. Introduzione alla crittografia a chiave pubblica. Il crittosistema RSA. Test di primalità. Algoritmi di fattorizzazione. Alcuni attacchi all'RSA. Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal. il crittosistema di Massey-Omura. Firma digitale. Cenni su alcuni protocolli crittografici.

Testi

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Bibliografia di riferimento

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Modalità erogazione

lezioni in presenza: ci sarà anche probabilmente la possibilità di seguire online

Modalità di valutazione

prova scritta: di norma 4 esercizi teorico/pratici, durata di norma 2 ore e 30. prova orale: facoltativa per una votazione ≤ 26

English

Prerequisites

Basic knowledge of algebra.

Programme

Introduction to cryptography. Classic ciphers. Introduction to cryptanalysis. Introduction to public-key cryptography. The RSA cryptosystem. Primality tests. Factorization algorithms. Some attacks on the RSA. The discrete logarithm problem. Diffie-Hellman key exchange. Elgamal cryptosystem. Massey-Omura cryptosystem. Digital signatures. Overview of some cryptographic protocols.

Reference books

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Reference bibliography

Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici D. Stinson: Cryptography - theory and practice

Study modes

-

Exam modes

-

20410416 - FM410-COMPLEMENTI DI MECCANICA ANALITICA

(FM410-COMPLEMENTI DI MECCANICA ANALITICA - Modulo A)

Docente: REUVERS ROBIN JOHANNES PETRUS

Italiano

Prerequisiti

Programma

Testi da definire

Testi

Testi da definire

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Testi da definire

Modalità di valutazione

Testi da definire

English

Prerequisites

Programme

-

Reference books

-

Reference bibliography

-

Study modes

-

Exam modes

-

20410875 - FM530 - METODI MATEMATICI PER IL MACHINE LEARNING

Docente: REUVERS ROBIN JOHANNES PETRUS

Italiano

Prerequisiti

Programma

Testi da definire

Testi

Testi da definire

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Testi da definire

Modalità di valutazione

Testi da definire

English

Prerequisites

Programme

-

Reference books

-

Reference bibliography

-

Study modes

-

Exam modes

-

20410417 - IN410-CALCOLABILITÀ E COMPLESSITÀ

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Non ci sono prerequisiti.

Programma

1) Computabilità, complessità e rappresentabilità: - Introduzione ai problemi di decisione, procedure algoritmiche e non algoritmiche, computazioni deterministiche, procedure discrete, nozione di alfabeto, di parola. Decidibilità e semidecidibilità di un insieme. Computazioni deterministiche, finitarie e discrete. Algoritmi formali: definizione formale di algoritmo, configurazioni di input, di output, funzione di transizione. Esempio di formalizzazione di un algoritmo. Decidibilità per automa finito. Rappresentazione degli automi mediante matrici. Monoide libero delle parole. Semianelli formali. Automi Finiti Non-deterministici. Linguaggi Regolari. Equivalenza tra automi deterministici e quelli non-deterministici. - Macchine di Turing: definizione, decidibilità per macchina di Turing, tempo di arresto, spazio di arresto. Costo della computazione. Complessità: caso peggiore e caso medio. Indipendenza del tempo di decisione da un numero finito di configurazioni di input. Funzioni di complessità, classi di complessità DTIME e DSPACE (deterministic time and space). Inclusione $DTIME(T(n)) \# DSPACE(T(n)) \# DTIME(2^{\lceil cT(n) \rceil})$. Pumping Lemma per gli insiemi decidibili in tempo lineare. Simulazione di algoritmi, simulazione della macchina di Turing a seminastro, simulazione di una macchina multinastro. Macchine di Turing speciali. Teorema di Speedup lineare per macchine di Turing con alfabeto esteso. Valutazione del coefficiente di accelerazione in relazione agli alfabeti. Decidibilità di insiemi di numeri naturali. Indipendenza dalla rappresentazione. Considerazioni sulla complessità. - Turing calcolabilità: definizione di funzione Turing calcolabile, funzioni caratteristiche di insiemi Turing decidibili, la classe delle funzioni Turing calcolabili è chiusa per composizione, coppia, ricorsione primitiva e minimizzazione. Esempi di funzioni Turing calcolabili. Funzioni Ricorsive: equivalenza tra Turing computabilità e funzioni ricorsive. Funzione di Ackermann ([1] capp. 1,2,3,4,5 e [4] cap. 1). - Funzioni costruibili in tempo. Nozione di T-orologio. Esempi di alcune funzioni costruibili in tempo. Chiusura per composizione. - Macchine di Turing non-deterministiche: caratterizzazione mediante la decidibilità di insiemi proiezione. Definizione della classe delle funzioni non-deterministiche polinomiali. Problemi NP-completi. 2) Lambda calcolo e programmazione funzionale: - Programmazione dichiarativa: cenni storici sul lambda calcolo, definizioni di base, i termini del lambda calcolo, la sostituzione semplice. Relazioni sui lambda termini. Congruenze, passaggio al contesto. #-equivalenza. L#-equivalenza passa al contesto. Chiusura transitiva di una relazione, proprietà di Church-Rosser. Quozientamento dei lambda-termini rispetto all'alpha equivalenza. - Definizione di beta-redesso e di beta-riduzione. Teorema di Church-Rosser per la beta-riduzione. Forme normali per beta-riduzione. Strategie di beta-riduzione. Strategia normalizzante: riduzione di sinistra (left most-outer most). Riduzione di testa. Termini Risolubili. Forme Normali di Testa. Teorema di caratterizzazione della risolubilità. - Rappresentazione delle funzioni ricorsive: teorema di lambda definibilità. Esistenza del punto fisso per il lambda termini. Punto Fisso di Church ed punto fisso di Curry. - Rappresentazione di altri tipi di dato nel lambda-calcolo: coppie, liste, alberi, soluzione di equazioni ricorsive su lambda-termini ([2] capp. 1, 2, 5).

Testi

[1] DEHORNOY, P., COMPLEXITÉ ET DECIDABILITÉ. SPRINGER-VERLAG, (1993). [2] KRIVINE, J.-L., LAMBDA CALCULUS: TYPES AND MODELS. #ELLIS HORWOOD, (1993). [3] SIPSER, M., INTRODUCTION TO THE THEORY OF COMPUTATION. THOMSON COURSE TECHNOLOGY, (2006).

Bibliografia di riferimento

G. Lolli, Hilbert e la logica, Le Matematiche, [S.I.], v. 55, n. 3, p. 93-126, mar. 2005. ISSN 2037-5298. Dexter C. Kozen, Theory of Computation, Springer-Verlag (2006). G. Ausiello, G. Gambosi, F. d'Amore Linguaggi, Modelli, Complessità Aho, Hopcroft, Ullman, Design and Analysis of Computer Programming. A. Bernasconi, B. Codenotti, Introduzione alla complessità computazionale, Springer-Verlag. H. Hermes, Enumerability, Decidability, Computability, Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, n. 127, Springer-Verlag. F. Cardone and J. R. Hindley, History of Lambda-calculus and Combinatory Logic, from Swansea University Mathematics Department Research Report No. MRRS-05-06.

Modalità erogazione

Lezione frontale in aula.

Modalità di valutazione

L'esame consiste di due parti: un esame scritto, sostituibile con due prove in itinere (il voto finale viene calcolato pesando la prima prova al 35% e la seconda al 65%) e una prova orale opzionale, prevista per supplire alle insufficienze lievi (a partire dal 15, compreso) o per migliorare il voto ottenuto allo scritto.

English

Prerequisites

There is no required background.

Programme

1) Computability, complexity and representability: - Introduction to decision problems, algorithmic and non-algorithmic procedures, deterministic computations, discrete procedures, the notion of alphabet, of speech. Decidability and semi-decidability of a set. Deterministic, finitary and discrete computations. Formal algorithms: formal definition of algorithm, configurations of input, output, transition function. Example of formalization of an algorithm. Decidability for finished automata. Representation of the automata by matrices. Free Monoid of words. Formal semi-rings. Non-deterministic finite automata. Regular Languages. Equivalence between deterministic and non-deterministic automata. - Turing machines: definition, decidability for Turing machine, stopping time, stopping space. Cost of computation. Complexity: worst-case and average case. Independence of decision time from a finite number of input configurations. Complexity functions, complexity classes DTIME and DSPACE (deterministic time and space). Inclusion $DTIME(T(n)) \# DSPACE(T(n)) \# DTIME(2^{\lceil cT(n) \rceil})$. Pumping Lemma. Simulation of algorithms, simulation of the half tape Turing machine, simulation of a multi-tape machine. Special Turing machines. Linear Speedup theorem for Turing machines with an extended alphabet. Evaluation of acceleration coefficient in relation to alphabets. Decisions of natural number sets. Independence from representation. Considerations concerning complexity. - Turing computability: definition of Turing computable function, characteristic functions of Turing decidable sets, the class of Turing computable functions is closed by composition, concatenation, primitive recursion and minimization. Examples of Turing computable functions. Recursive Functions: equivalence between Turing computability and recursive functions. Ackermann function ([1] chapter 1,2,3,4,5 and [4] chapter 1). - Time-constructible functions. The notion of T-clock. Examples of some time constructible function. Closure by composition. - Non-deterministic Turing machines: characterization through the decidability of

projection sets. Definition of the class of polynomial non-deterministic functions. NP-complete problems. 2) Lambda calculus and functional programming: - Declarative programming: a historical outline on the lambda calculus, basic definitions, the terms of the lambda calculus, the simple substitution. Relations on the lambda terms. Congruences, transition to the context. #-equivalence. alpha-equivalence passes to the context. The transitive closure of a relationship, owned by Church-Rosser. Listing of lambda-terms concerning alpha-equivalence. - Definition of beta-reduction and beta-equivalence. Church-Rosser's theorem for beta-reduction. Normal forms for beta-reduction. Beta-reduction strategies. Normalizing strategy: left reduction (left most-outer most). Head reduction. Soluble Terms. Head Normal Forms. Solvability characterization theorem. - Representation of the recursive functions: lambda definability theorem. Existence of the fixed point for the lambda terms. Church Fixed Point and Curry fixed point. - Representation of other data types in the lambda-calculus: pairs, lists, trees, the solution of recursive equations on lambda-terms ([2] chapters 1, 2, 5).

Reference books

[1] DEHORNOY, P., COMPLEXITÉ ET DECIDABILITÉ. SPRINGER-VERLAG, (1993). [2] KRIVINE, J.-L., LAMBDA CALCULUS: TYPES AND MODELS. #ELLIS HORWOOD, (1993). [3] SIPSER, M., INTRODUCTION TO THE THEORY OF COMPUTATION. THOMSON COURSE TECHNOLOGY, (2006).

Reference bibliography

G. Lolli, Hilbert e la logica, Le Matematiche, [S.I.], v. 55, n. 3, p. 93-126, mar. 2005. ISSN 2037-5298. Dexter C. Kozen, Theory of Computation, Springer-Verlag (2006). G. Ausiello, G. Gambosi, F. d'Amore Linguaggi, Modelli, Complessità Aho, Hopcroft, Ullman, Design and Analysis of Computer Programming. A. Bernasconi, B. Codenotti, Introduzione alla complessità computazionale, Springer-Verlag. H. Hermes, Enumerability, Decidability, Computability, Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, n. 127, Springer-Verlag. F. Cardone and J. R. Hindley, History of Lambda-calculus and Combinatory Logic, from Swansea University Mathematics Department Research Report No. MRRS-05-06.

Study modes

-

Exam modes

-

20410626 - IN440 - OTTIMIZZAZIONE COMBINATORIA

Docente: BONIFACI VINCENZO

Italiano

Prerequisiti

Conoscenza di un linguaggio di programmazione e di strutture dati elementari: liste, code, pile. [IN110 Algoritmi e strutture dati] La conoscenza del linguaggio di programmazione Python è fortemente consigliata. [IN400a Programmazione in Python]

Programma

1. Problemi di ottimizzazione e di ottimizzazione combinatoria. Enumerazione delle soluzioni. 2. Fondamenti di analisi degli algoritmi. Trattabilità computazionale. Ordine asintotico di crescita. 3. Grafi. Connettività ed attraversamento. Bipartizioni. Connettività in grafi diretti. Grafi diretti aciclici ed ordinamento topologico. 4. Algoritmi avidi. Schedulazione di intervalli. Caching ottimo. Cammini minimi in un grafo. Albero ricoprente a costo minimo. 5. Divide et impera. Il mergesort. Conteggio di inversioni. Coppia di punti più vicina. 6. Programmazione dinamica. Schedulazione di intervalli pesati. Principi della programmazione dinamica. Somme di sottoinsiemi e problema della bisaccia. Cammini minimi tra tutte le coppie. Cammini minimi e protocollo basato su vettori delle distanze. 7. Flussi di rete. Flusso massimo e algoritmo di Ford-Fulkerson. Flussi massimi e tagli minimi in una rete. Cammini aumentanti. Abbinamenti bipartiti. Cammini disgiunti in grafi diretti e non diretti. 8. Intrattabilità computazionale. Riduzioni tempo-polinomiali. Riduzioni attraverso "gadget". Certificazione efficiente e definizione di NP. Problemi NP-completi. Problemi di copertura, impaccamento, partizionamento, sequenziamento, numerici. Altri esempi.

Testi

Jon Kleinberg, Eva Tardos. Algorithm Design. Pearson Education, 2013.

Bibliografia di riferimento

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. Introduzione agli algoritmi e strutture dati. McGraw-Hill, 3a edizione, 2010. Sanjoy Dasgupta, Christos Papadimitriou, Umesh Vazirani. Algorithms. McGraw-Hill, 2016. Bernhard Korte, Jens Vygen. Ottimizzazione combinatoria. Springer, 2011. Michael R. Garey, David S. Johnson. Computers and Intractability. Freeman, 1979.

Modalità erogazione

Testi da definire

Modalità di valutazione

La prova orale consiste in un colloquio approfondito alla lavagna.

English

Prerequisites

Knowledge of a programming language and of elementary data structures: lists, queues, and stacks. [IN110 Algoritmi e strutture dati] Knowledge of the Python programming language is highly suggested. [IN400a Programmazione in Python]

Programme

1. Optimization and combinatorial optimization problems. Enumeration of solutions. 2. Basics of algorithm analysis. Computational tractability. Asymptotic order of growth. 3. Graphs. Graph connectivity and graph traversal. Graph bipartiteness. Connectivity in directed

graphs. Directed acyclic graphs and topological ordering. 4. Greedy algorithms. Interval scheduling. Optimal caching. Shortest paths in a graph. Minimum spanning trees. 5. Divide and conquer. Mergesort. Counting inversions. Closest pair of points. 6. Dynamic programming. Weighted interval scheduling. Principles of dynamic programming. Subset sums and knapsacks. All-pairs shortest paths. Shortest paths and distance vector protocols. 7. Network flow. Maximum flow and the Ford-Fulkerson algorithm. Maximum flows and minimum cuts in a network. Augmenting paths. Bipartite matching. Disjoint paths in directed and undirected graphs. 8. Computational intractability. Polynomial-time reductions. Reductions via "gadgets". Efficient certification and the definition of NP. NP-complete problems. Covering, packing, partitioning, sequencing, and numerical problems. Other examples.

Reference books

Jon Kleinberg, Eva Tardos. Algorithm Design. Pearson Education, 2013.

Reference bibliography

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. Introduction to Algorithms. McGraw-Hill, 3rd edition, 2009. Sanjoy Dasgupta, Christos Papadimitriou, Umesh Vazirani. Algorithms. McGraw-Hill, 2016. Bernhard Korte, Jens Vygen. Combinatorial Optimization. Springer, 4th edition, 2008. Michael R. Garey, David S. Johnson. Computers and Intractability. Freeman, 1979.

Study modes

-

Exam modes

-

20410424 - IN450- ALGORITMI PER LA CRITTOGRAFIA

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Nozioni elementari di teoria dei numeri, probabilità discreta ed algebra lineare, programmazione di base.

Programma

1. Crittografia Classica - Crittosistemi di base: cifratura per sostituzione, per traslazione, per permutazione, affine, di Vigenère, di Hill. Cifratura a flusso (sincrona e asincrona), Linear feedback shift registers (LFSR) su campi finiti, Cifrario autokey. Cifrari prodotto. Crittoanalisi di base: classificazione degli attacchi; crittoanalisi per i cifrari affini, per la cifratura a sostituzione (analisi delle frequenze), per la cifratura di Vigenere: Kasiski test, indice di coincidenza; crittoanalisi del cifrario di Hill e degli LFSR: attacchi algebrici, cube attack. 2. Applicazione della Teoria di Shannon alla crittografia - Sicurezza dei cifrari: sicurezza computazionale, sicurezza dimostrabile, sicurezza incondizionata. Richiami di calcolo delle probabilità: variabili aleatorie discrete, probabilità congiunta, probabilità condizionata, variabili aleatorie indipendenti, Teorema di Bayes. Variabili aleatorie associate a crittosistemi. Sistemi di cifratura a sicurezza perfetta. Crittosistema di Vernam. Entropia. Codici di Huffman. Spurious Keys e Unicity distance. 3. Cifrari a blocchi - Schemi di cifratura iterativi; Reti di Sostituzione-Permutazione (SPN); Crittoanalisi lineare per SPN: Piling-Up Lemma, approssimazione lineare di S-boxes, attacchi lineari a S-boxes; Crittoanalisi differenziale per SPN; Cifrari di tipo Feistel; DES: descrizione e analisi; AES: descrizione; Cenni sui campi finiti: operazioni su campi finiti, algoritmo di Euclide generalizzato per il calcolo del mcd e degli inversi; Modi operativi per i cifrari a blocchi. 4. Funzioni Hash e Codici per l'autenticazione di messaggi - Funzioni di hash e integrità dei dati. Funzioni di hash sicure: resistenza alla controimmagine, resistenza alla seconda controimmagine, resistenza alla collisione. Il modello dell'oracolo random: funzioni di hash ideali, proprietà di indipendenza. Algoritmi randomizzati, collisione sul problema della seconda controimmagine, collisione sul problema della controimmagine. Funzioni di hash iterate; la costruzione di Merkle-Damgard. Algoritmo di Hash Sicuro (SHA-1). Codici di Autenticazione (MAC): codici di autenticazione nidificati (HMAC).

Testi

[1] Antoine Joux, Algorithmic Cryptanalysis, (2010) CRC Press. [2] Douglas Stinson, Cryptography: Theory and Practice, 3rd edition, (2006) Chapman and Hall/CRC. [3] Delfs H., Knebl H., Introduction to Cryptography, (2007) Springer Verlag.

Bibliografia di riferimento

[-] Serge Vaudenay, A Classical Introduction to Cryptography, Applications for Communications Security (2006) Springer-Verlag. [-] Th. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay A Classical Introduction to Cryptography Exercise Book Springer Verlag (2006). [-] S. Mangano, Mathematica Cookbook ISBN: 9789863470106 Publisher: O'Reilly (2014). [-] Schneier, Applied Cryptography (2006) Chapman and Hall/CRC. [-] Katz, Lindell, Introduction to Modern Cryptography (2006) Chapman and Hall/CRC. [-] Rudolf Lidl, Harald Niederreiter, Finite Fields, 2nd edition, In Encyclopedia of Mathematics and its Applications, (2007) Cambridge University Press.

Modalità erogazione

Lezioni in aula e sessioni di programmazione al laboratorio informatico.

Modalità di valutazione

Esame scritto e valutazione del progetto di programmazione.

English

Prerequisites

Basic number theory, basic discrete probability theory, basic linear algebra, basic computer programming.

Programme

1. Classic Cryptography - Basic cryptosystems: encryption by substitution, by translation, by permutation, affine cryptosystem, by Vigenère, by Hill. Stream encryption (synchronous and asynchronous), Linear feedback shift registers (LFSR) on finite fields, Autokey cypher. Product cyphers. Basic cryptanalysis: classification of attacks; cryptoanalysis for affine cyphers, for substitution cypher

(frequency analysis), for Vigenere cypher: Kasiski test, coincidence index; cryptanalysis of Hill's cypher and LFSR: algebraic attacks, cube attack. 2. Application of Shannon theory to cryptography - Security of cyphers: computational security, provable security, unconditional security. Basics of probability: discrete random variables, joint probability, conditional probability, independent random variables, Bayes' theorem. Random variables associated with cryptosystems. Perfect secrecy for encryption systems. Vernam cryptosystem. Entropy. Huffman codes. Spurious Keys and Unicity distance. 3. Block cyphers - iterative encryption schemes; Substitution-Permutation Networks (SPN); Linear cryptanalysis for SPN: Piling-Up Lemma, linear approximation of S-boxes, linear attacks on S-boxes; Differential cryptanalysis for SPN; Feistel cyphers; DES: description and analysis; AES: description; Notes on finite fields: operations on finite fields, Euclid's generalized algorithm for the computation of the GCD and inverse; Operating modes for block cyphers. 4. Hash functions and codes for message authentication - Hash functions and data integrity. Safe hash functions: resistance to the pre-image, resistance to the second pre-image, collision resistance. The random oracle model: ideal hash functions, properties of independence. Randomized algorithms, collision on the problem of the second pre-image, collision on the problem of the pre-image. Iterated hash functions; the construction of Merkle-Damgard. Safe Hash Algorithm (SHA-1). Authentication Codes (MAC): nested authentication codes (HMAC).

Reference books

[1] Antoine Joux, Algorithmic Cryptanalysis, (2010) CRC Press. [2] Douglas Stinson, Cryptography: Theory and Practice, 3rd edition, (2006) Chapman and Hall/CRC. [3] Delfs H., Knebl H., Introduction to Cryptography, (2007) Springer Verlag.

Reference bibliography

[-] Serge Vaudenay, A Classical Introduction to Cryptography, Applications for Communications Security (2006) Springer-Verlag. [-] Th. Baigneres, P. Junod, Y. Lu, J. Monnerat, S. Vaudenay A Classical Introduction to Cryptography Exercise Book Springer Verlag (2006). [-] S. Mangano, Mathematica Cookbook ISBN: 9789863470106 Publisher: O'Reilly (2014). [-] Schneier, Applied Cryptography (2006) Chapman and Hall/CRC. [-] Katz, Lindell, Introduction to Modern Cryptography (2006) Chapman and Hall/CRC. [-] Rudolf Lidl, Harald Niederreiter, Finite Fields, 2nd edition, In Encyclopedia of Mathematics and its Applications, (2007) Cambridge University Press.

Study modes

-

Exam modes

-

20411002 - IN510 – QUANTUM COMPUTING

(IN510 – QUANTUM COMPUTING MODULO A)

Docente: DI BATTISTA GIUSEPPE

Italiano

Prerequisiti

Non ci sono particolari prerequisiti.

Programma

Qubit, coppie di qubit, registri, porte logiche con uno o piu' qubit, no cloning theorem, l'operatore di Hadamard, teletrasporto, computazioni reversibili, l'algoritmo di Bernstein Vazirani, l'algoritmo di Shor, amplitudine amplification e l'algoritmo di Groover, teoria della complessità e quantum computing

Testi

Slides del docente.

Bibliografia di riferimento

I testi consigliati (per sola consultazione) sono: E. G. Rieffel, W. H. Polak Quantum Computing: a Gentle Introduction MIT Press N. S. Yanofsky, M. A. Mannucci Quantum Computing for Computer Scientists Cambridge

Modalità erogazione

Lezioni in aula.

Modalità di valutazione

Scritto di circa un'ora.

English

Prerequisites

None.

Programme

Qubit, pairs of qubits, registries, logic functions, no cloning theorem, Hadamard operator, teleportation, reversible computations, Bernstein Vazirani algorithm, Shor algorithm, amplitude amplification and the Groover algorithm, complexity theory and quantum computing

Reference books

Slides by the teacher.

Reference bibliography

The recommended texts (for consultation only) are: E. G. Rieffel, W. H. Polak Quantum Computing: a Gentle Introduction MIT Press N. S. Yanofsky, M. A. Mannucci Quantum Computing for Computer Scientists Cambridge

Study modes

-

Exam modes

-

20411002 - IN510 – QUANTUM COMPUTING

(IN510 – QUANTUM COMPUTING MODULO B)

Docente: PEDICINI MARCO

Italiano

Prerequisiti

Algebra Lineare. Calcolabilità e Complessità.

Programma

Elementi di Algebra Lineare: Spazi di Hilbert, Prodotti e prodotti tensore, matrici, spazi complessi e prodotto scalare, grafi, somma dei cammini nel grafo. Funzioni booleane, quantum bits e fattibilità computazionale. Matrici speciali: Hadamard Matrices, Fourier Matrices, Computazioni reversibili e matrici di permutazione, matrici diagonali, riflessioni. Vettori di inizializzazione, controllo e copia di stati di base. Algoritmi: Phil Algorithm, Deutsch's Algorithm, Superdense Coding and Teleportation. The Deutsch-Jozsa Algorithm. Simon's Algorithm. Shor's Algorithm, Quantum Part of the Algorithm, Analysis of the Quantum Part, Continued Fractions. FactoringIntegers: Basic Number Theory, Periods Give the Order, Factoring. Grover's Algorithm: The binary case, the general case, with k Unknowns, Grover Approximate Counting.

Testi

Richard J. Lipton, Kenneth W. Regan Introduction to Quantum Algorithms via Linear Algebra, Second Edition, ISBN 9780262045254, (2021), MIT Press

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Corso di Letture.

Modalità di valutazione

L'esame consiste nella presentazione di un seminario su un tema da concordare con il docente.

English

Prerequisites

Linear Algebra. Computability and Complexity

Programme

Basic Linear Algebra: Hilbert Spaces, Products and Tensor Products, Matrices, Complex Spaces and Inner Products, Matrices, Graphs, and Sums Over Paths. Boolean Functions, Quantum Bits, and Feasibility: Feasible Boolean Functions, Quantum Representation of Boolean Arguments Quantum Feasibility. Special Matrices: Hadamard Matrices, Fourier Matrices, Reversible Computation and Permutation Matrices, Feasible Diagonal Matrices, Reflections. Tricks: Start Vectors, Controlling and Copying Base States, The Copy-Uncompute Trick, Superposition Tricks, Flipping a Switch, Measurement Tricks, Partial Transforms. Algorithms: Phil's Algorithm: Phil Measures Up, Quantum Mazes versus Circuits versus Matrices. Deutsch's Algorithm: Superdense Coding and Teleportation. The Deutsch-Jozsa Algorithm. Simon's Algorithm. Shor's Algorithm, Quantum Part of the Algorithm, Analysis of the Quantum Part, Continued Fractions. FactoringIntegers: Basic Number Theory, Periods Give the Order, Factoring. Grover's Algorithm: The binary case, the general case, with k Unknowns, Grover Approximate Counting.

Reference books

Richard J. Lipton, Kenneth W. Regan Introduction to Quantum Algorithms via Linear Algebra, Second Edition, ISBN 9780262045254, (2021), MIT Press

Reference bibliography

-

Study modes

-

Exam modes

-

20410432 - IN550 – MACHINE LEARNING

Docente: BONIFACI VINCENZO

Italiano

Prerequisiti

Conoscenza del linguaggio di programmazione Python. [IN400a Programmazione in Python] Elementi di probabilità discreta, algebra lineare ed analisi matematica.

Programma

1. Apprendimento automatico. Tipi di apprendimento. Funzioni di costo. Minimizzazione del rischio empirico. Generalizzazione ed overfitting. 2. Ottimizzazione di modelli. Funzioni convesse. Discesa del gradiente. Discesa stocastica del gradiente. 3. Regressione. Regressione lineare. Basi di funzioni. Selezione dei predittori. Regolarizzazione. 4. Classificazione. Modelli generativi. Nearest neighbor. Regressione logistica. Support vector machines. Reti neurali. 5. Combinazione di modelli. Alberi di decisione. Boosting. Bagging. 6. Apprendimento non supervisionato. Clustering K-means. Clustering gerarchico. Analisi delle componenti principali. 7. Applicazione dei metodi nel linguaggio di programmazione Python. Esempi d'uso delle librerie NumPy, Pandas, SciKit-Learn, e PyTorch.

Testi

J. Watt, R. Borhani, A. Katsaggelos. Machine Learning Refined. Cambridge University Press, 2nd edition, 2020.

Bibliografia di riferimento

A. Géron. Hands-On Machine Learning with SciKit-Learn, Keras, and Tensorflow. O'Reilly, 3rd edition, 2022.
 M. Mohri, A. Rostamizadeh, A. Talwalkar. Foundations of Machine Learning. MIT Press, 2nd edition, 2018.
 S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning. Cambridge University Press, 2014.
 G. James, D. Witten, T. Hastie, R. Tibshirani. Introduzione all'apprendimento statistico. Piccin, 2020.
 K.P. Murphy. Probabilistic Machine Learning. MIT Press, 2022.
 T. Hastie, R. Tibshirani, J. Friedman. Gli elementi dell'apprendimento statistico. Piccin, 2025.
 C.M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.

Modalità erogazione

Lezioni teoriche frontali ed esercitazioni di laboratorio nel linguaggio di programmazione Python. Per il diario delle lezioni si consulti il sito del docente: <http://ricerca.mat.uniroma3.it/users/vbonifaci/in550.html> Le lezioni saranno in presenza e verranno anche trasmesse e registrate.

Modalità di valutazione

L'esame si compone di due parti: un progetto software ed un esame orale. Nella parte di progetto software, gli studenti identificheranno ed analizzeranno un dataset utilizzando le metodologie presentate durante le lezioni, preparando un quaderno Python interattivo (Jupyter) ed una presentazione. L'esame orale consisterà, oltre che nella discussione del progetto, in domande su tutto il programma del corso.

English

Prerequisites

Knowledge of the Python programming language. [IN400a Programmazione in Python] Elements of discrete probability, linear algebra and real analysis.

Programme

1. Machine learning. Types of learning. Loss functions. Empirical risk minimization. Generalization and overfitting. 2. Model optimization. Convex functions. Gradient descent. Stochastic gradient descent. 3. Regression. Linear regression. Basis functions. Feature selection. Regularization. 4. Classification. Generative models. Nearest neighbor. Logistic regression. Support vector machines. Neural networks. 5. Ensemble methods. Decision trees. Boosting. Bagging. 6. Unsupervised learning. K-means clustering. Hierarchical clustering. Principal component analysis. 7. Application of the methods using the Python language. Examples using the NumPy, Pandas, SciKit-Learn, and PyTorch libraries.

Reference books

J. Watt, R. Borhani, A. Katsaggelos. Machine Learning Refined. Cambridge University Press, 2nd edition, 2020.

Reference bibliography

A. Géron. Hands-On Machine Learning with SciKit-Learn, Keras, and Tensorflow. O'Reilly, 3rd edition, 2022.
 M. Mohri, A. Rostamizadeh, A. Talwalkar. Foundations of Machine Learning. MIT Press, 2nd edition, 2018.
 S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning. Cambridge University Press, 2014.
 G. James, D. Witten, T. Hastie, R. Tibshirani. An Introduction to Statistical Learning. Springer, 2nd edition, 2013.
 K.P. Murphy. Probabilistic Machine Learning. MIT Press, 2022.
 T. Hastie, R. Tibshirani, J. Friedman. The Elements of Statistical Learning. Springer, 2nd edition, 2008.
 C.M. Bishop. Pattern Recognition and Machine Learning. Springer, 2006.

Study modes

-

Exam modes

-

20410451 - LM410 -TEOREMI SULLA LOGICA 1

(LM410 -TEOREMI SULLA LOGICA 1 - MODULO A)

Docente: MAIELI ROBERTO

Italiano

Prerequisiti

nessun requisito specifico

Programma

Parte 1: Alcune nozioni preliminari. Relazioni d'ordine e alberi, definizioni induttive, dimostrazioni per induzione, assioma di scelta e lemma di König. Parte 2: Dimostrabilità e soddisfacibilità. Linguaggio formale del primo ordine: alfabeto, termini, formule, sequenti. Strutture per un linguaggio del primo ordine: strutture, termini e formule a parametri in una struttura, valutazione di termini, formule e sequenti. Calcolo dei sequenti per la logica del primo ordine: il calcolo dei sequenti LK di Gentzen. Sequenti derivabili e derivazioni. Correttezza delle regole di LK. Analisi canonica e teorema fondamentale: costruzione dell'analisi canonica (con e senza tagli) e dimostrazione del teorema fondamentale dell'analisi canonica. Conseguenze del teorema fondamentale dell'analisi canonica: teoremi di completezza, eliminabilità del taglio, compattezza, Löwenheim-Skolem. Parte 3: Verso la teoria della dimostrazione: il teorema di eliminazione del taglio. La procedura di eliminazione del taglio. Definizione dei passi elementari di eliminazione del taglio. Prima strategia dimostrativa (riduzione a grandi passi). Seconda strategia dimostrativa (rovesciamento delle derivazioni). Cenni sulla complessità della procedura di eliminazione del taglio. Qualche conseguenza immediata del teorema di eliminazione del taglio.

Testi

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
<https://sites.google.com/view/lm410/home>

Bibliografia di riferimento

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
<https://sites.google.com/view/lm410/home>

Modalità erogazione

Il corso prevede Didattica frontale; Discussioni con gli studenti e dibattiti sugli argomenti trattati; Esercitazioni; La frequenza non è obbligatoria ma è vivamente raccomandata. Nel caso di un prolungamento dell'emergenza sanitaria da COVID-19 verranno valutate le modalità di svolgimento delle attività didattiche. Si cercherà di limitare l'inevitabile danno agli studenti dovuto ad un'eventuale necessità di tenere il corso a distanza preservando, per quanto possibile, l'interattività durante le lezioni. È previsto lo streaming sincrono delle lezioni senza registrazione delle lezioni svolte in aula.

Modalità di valutazione

Esame scritto e/o orale, di durata variabile, in media tra 45 e 60 minuti. Nel caso di misure restrittive dovute alla emergenza sanitaria da COVID-19 verranno valutate le modalità di svolgimento degli esami. Si cercherà di limitare l'inevitabile danno agli studenti dovuto ad un'eventuale necessità di tenere gli esami a distanza.

English

Prerequisites

No specific prerequisite

Programme

Part 1: Some preliminary notions. Order relations and trees, inductive definitions, proofs by induction, axiom of choice and König's lemma. Part 2: Provability and satisfiability. First order formal language: alphabet, terms, formulas, sequents. Structures for first order languages: structures, terms and formulas with parameters in a structure, value of terms, formulas and sequents. The calculus of sequents for first order logic: Gentzen's LK. Derivable sequents and derivations. Correctness of the rules of LK. Canonical analysis and fundamental theorem: construction of the canonical analysis (with and without cuts) and proof of the fundamental theorem of the canonical analysis. Consequences of the fundamental theorem: completeness theorem, compactness theorem, eliminability of cuts, Löwenheim-Skolem's theorem. Part 3: Towards proof-theory: the cut-elimination theorem. The cut-elimination procedure. Definition of the elementary steps of cut-elimination. First proof strategy (big reduction steps). Second proof strategy (reversion of derivations). The complexity of the cut-elimination procedure (sketch). Some immediate consequences of the cut-elimination theorem.

Reference books

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
<https://sites.google.com/view/lm410/home>

Reference bibliography

V. Michele Abrusci e Lorenzo Tortora de Falco, Logica. Vol. 1 Dimostrazioni e modelli al primo ordine, Springer, 2014
<https://sites.google.com/view/lm410/home>

Study modes

-

Exam modes

-

20410555 - ST410-STATISTICA

Docente: MARTINELLI FABIO

Italiano

Prerequisiti

Avere seguito un corso base di teoria della probabilità e di analisi matematica in più variabili

Programma

Variabili casuali e la loro distribuzione, funzione generatrice dei momenti, media varianza e covarianza. Modello di campionamento casuale e modello statistico. Statistica: concetto, esempi, statistica sufficiente e minimale. Stimatori puntuali: definizione e proprietà desiderata, momenti, massima verosimiglianza e Bayes. Metodi computazionali: Newton-Raphson, algoritmo EM Migliorare uno stimatore: Rao-Blackwell, stimatore UMVU, statistica completa, Lehman-Scheffé e Cramer-Rao Intervalli di confidenza: intuitivo,

quantit' a pivotale, IC per Bayes e IC asintotico. Verifica d'ipotesi: rapporto di verosimiglianza, test via quantit' a pivotale (test Z e T), dualit' a con IC, test UMP, Neyman-Pearson e Karlin-Rubin. Metodi non parametrici: goodness-of-fit, tabella di contingenza, Kolmogorov-Smirnov e test tramite graduatoria. Analisi della varianza (ANOVA) e test F. Regressione: lineare, lineare multipla, lineare generalizzata e Logistica/Poisson

Testi

Introduzione alla Statistica, S.M. Ross, Apogeo - Maggioli Editore. testo aggiuntivo: Luca Leuzzi, Enzo Marinari, Giorgio Parisi
CALCOLO DELLE PROBABILITÀ: un trattatello per principianti volenterosi

Bibliografia di riferimento

Testi da definire

Modalità erogazione

Le lezioni si terranno in aula con scrittura sulla lavagna o su tablet

Modalità di valutazione

La valutazione in itinere consiste nel risolvere in circa 10 giorni e per tre volte durante il corso una serie di quesiti di carattere pratico (esercizi) e teorico. Ciascuno foglio riceve un voto da 0 a 10. L'esame finale consiste di 4 esercizi, ciascuno articolato in 2 o 3 quesiti a carattere teorico e pratico. Il voto finale e' il massimo tra il voto dell'esame finale e $2/3 \times (\text{voto esame finale}) + \text{media dei voti dei fogli di esercizi}$

English

Prerequisites

A basic course in probability theory and in multivariable calculus

Programme

Random variables and their distribution, moment generating function, mean variance and covariance. Random sampling model and statistical model. Statistics: concept, examples, sufficient statistics. Point estimators: definition and desired properties, moments, maximum likelihood and Bayes. Computational methods: Newton-Raphson, EM algorithm Improving an estimator: Rao-Blackwell, UMVU estimator, full statistic, Lehman-Scheff #e II and Cramer-Rao Confidence intervals: intuitive, pivotal quantity, IC for Bayes and asymptotic IC. Hypothesis testing: likelihood ratio, pivotal quantity test (Z and T test), duality with IC, UMP, Neyman-Pearson and Karlin-Rubin tests. Non-parametric methods: goodness-of-fit, contingency table, Kolmogorov-Smirnov and ranking tests. Analysis of variance (ANOVA) and F. Regression: linear, multiple linear, generalized linear and Logistic / Poisson

Reference books

Statistical Inference, Casella e Berger, 2nd Edition, Duxbury Advanced Series. Additional reference: Luca Leuzzi, Enzo Marinari, Giorgio Parisi CALCOLO DELLE PROBABILITÀ: un trattatello per principianti volenterosi

Reference bibliography

-

Study modes

-

Exam modes

-