

# Sommario

<b>Gli autori</b> .....	<b>XV</b>
<b>Prefazione - Piccoli dati crescono</b> .....	<b>XVII</b>
<i>di Milena Sinigaglia</i>	
<b>Introduzione</b> .....	<b>XXI</b>
<i>di Antonio Teti</i>	

## **PARTE PRIMA - SVILUPPO E UTILIZZO DI METODI STATISTICI, PROBABILISTICI E MATEMATICI APPLICATI AI SISTEMI COMPLESSI**

<b>Capitolo 1 - Fondamenti di matematica</b> .....	<b>3</b>
<i>di Marta Biancardi</i>	
1.1 Insiemi	3
1.1.1 Relazione di inclusione e operazioni tra insiemi	4
1.2 Elementi di Logica	5
1.2.1 Predicati e quantificatori	7
1.3 Relazioni	8
1.3.1 Relazione di equivalenza	8
1.3.2 Relazione d'ordine	8
1.4 Le strutture algebriche	9
1.4.1 Leggi di composizione	9
1.4.2 Strutture algebriche	10
1.5. Insiemi numerici	12
1.5.1 Insieme dei numeri naturali	12
1.5.2 Insieme dei numeri interi relativi	12
1.5.3 Insieme dei numeri razionali	14
1.5.4 Comune multiplo e comune divisore	15
1.5.5 Proporzioni	16
1.5.6 Insieme dei numeri reali	17
1.5.7 Valore assoluto e distanza euclidea	18

1.5.8 Intervalli in $\mathbb{R}$	19
1.5.9 Insiemi limitati	19
1.5.10 Radicali, potenze, logaritmi	20
1.5.11 Insieme dei numeri complessi	22
1.6 Calcolo combinatorio	24
1.7 Funzioni	26
1.8 Limiti di funzioni	29
1.9 Funzioni continue	31
1.10 Derivazione	32
1.10.1 Derivate delle funzioni elementari	33
1.10.2 Regole di derivazione	33
1.10.3 Differenziale	34
1.10.4 Applicazioni del calcolo differenziale	35
1.10.5 Grafici delle funzioni	37
1.11 Integrali	37
1.11.1 Integrali indefiniti immediati	38
1.11.2 Metodi di integrazione	39
1.11.3 Integrale definito	40
1.12 Serie numeriche	40
1.12.1 Serie notevoli	41
1.13 Funzioni reali di due o più variabili reali	43
1.13.1 Derivate parziali	44
1.13.2 Massimi e minimi liberi	45
1.13.3 Massimi e minimi vincolati	47
1.14 Matrici	48
1.14.1 Operazioni tra matrici	49
1.14.2 Determinante	50
1.14.3 Rango di una matrice	51
1.15 Sistemi lineari	52
1.15.1 Sistemi di $n$ equazioni in $n$ incognite	52
1.15.2 Sistemi di $m$ equazioni in $n$ incognite	53
1.15.3 Metodo di Jacobi	53
1.16 Spazi vettoriali	54
1.16.1 Sottospazi vettoriali e base di uno spazio vettoriale	56
1.16.2 Prodotto scalare in $\mathbb{R}^n$ e basi ortonormali	58
1.16.3 Algoritmo di Gram-Schmidt	59
1.17 Autovalori e autovettori	61
1.17.1 Metodi iterativi per il calcolo di autovalori	63
1.17.2 Metodo delle potenze	63
1.17.3 Metodo delle potenze inverse	64
1.17.4 Metodo di Jacobi per matrici simmetriche	64
1.18 Matematica Finanziaria	66
1.19 Teoria dei sistemi	69
1.19.1 Caratteristiche di un sistema	69
1.19.2 Sistemi	70
1.19.3 Caratteristiche della risposta di un sistema	71
1.19.4 Classificazione dei sistemi	72

1.20	Modelli computazionali	73
1.21	Problemi e algoritmi	74
1.22	L'algoritmo	77
1.23	Teoria delle decisioni	78
1.23.1	Decisioni in condizioni di certezza	80
1.23.2	Decisioni in condizioni di rischio	80
1.23.3	Decisioni in condizioni di incertezza	81
1.24.	Teoria dei giochi	82
1.25	Test di verifica	85
<b>Capitolo 2 - Fondamenti di Calcolo delle probabilità.....</b>		<b>89</b>
<i>di Barbara Cafarelli, Alessio Pollice</i>		
	Premessa	89
2.1	Eventi e probabilità	89
2.1.1	Eventi e loro rappresentazione matematica	89
2.1.2	Algebra degli insiemi e logica degli eventi	91
2.1.3	Diverse interpretazioni della probabilità	95
2.1.4	Assiomi e rudimenti della probabilità	97
2.1.5	Prime proprietà e teoremi della probabilità	99
2.2	Eventi numerici e variabili aleatorie	108
2.2.1	Probabilità di eventi numerici	108
2.2.2	Variabili aleatorie discrete	109
2.2.3	Variabili aleatorie continue	111
2.2.4	Funzione di ripartizione	112
2.2.5	Vettori aleatori	115
2.2.6	Distribuzioni marginali e condizionate	119
2.2.7	Indipendenza tra variabili aleatorie	121
2.2.8	Trasformazioni di variabili aleatorie	122
2.3	Valori caratteristici di distribuzioni	126
2.3.1	Valori attesi di variabili e vettori aleatori	126
2.3.2	Momenti di variabili aleatorie	131
2.4	Distribuzioni di uso comune	141
2.4.1	Alcuni cenni sui processi stocastici	141
2.4.2	Il processo bernoulliano	142
2.4.3	La distribuzione di Poisson	145
2.4.4	La funzione di densità gaussiana	150
2.5	Successioni di variabili aleatorie	156
2.5.1	Convergenza in distribuzione e teorema centrale di convergenza	156
2.5.2	Convergenza in probabilità e legge debole dei grandi numeri	157
2.5.3	Convergenza quasi certa e legge forte dei grandi numeri	159
<b>Capitolo 3 - Metodi statistici .....</b>		<b>161</b>
<i>di Antonio Bevilacqua</i>		
3.1	Cenni storici e definizione della statistica	161
	Battute benevole e spiritose (ma non troppo)	163
	La Statistica (Trilussa)	163
3.2	I termini della statistica	163

3.3	Gli indici statistici descrittivi	164
3.4	Medie analitiche	165
3.4.1	Media aritmetica	165
3.4.2	Media armonica e media geometrica	168
3.5	Medie di posizione	169
3.5.1	Moda	169
3.5.2	Mediana	169
3.5.3	Quartili e percentili	170
3.6	Indici di dispersione	171
3.7	Indici descrittivi e forma di una distribuzione statistica	173
3.8	Regressione	174
3.8.1	Grafico dei residui	176
3.8.2	Coefficiente di determinazione	176
3.9	Rappresentazioni grafiche	177
3.9.1	Diagramma a barre e istogramma	178
3.9.2	Ortogramma	179
3.9.3	Diagramma a settori circolari	179
3.9.4	Box-plot	180
3.10	Statistica inferenziale	181
3.10.1	Il concetto di stimatore e il teorema del limite centrale	181
3.10.2	Proprietà degli stimatori e stime puntuali	182
3.10.3	Gli intervalli di confidenza	182
3.11	Verifica delle ipotesi	184
3.11.1	Definizione del test delle ipotesi	184
3.11.2	Ipotesi sulla media	185
3.11.3	Ipotesi sulla differenza tra medie	186
3.11.4	Confronto di medie per campioni appaiati (campioni dipendenti)	187
3.12	Analisi della varianza	187

**Capitolo 4 - Complessità ed economia:  
economia dei sistemi complessi ..... 193**

*di Giuseppe Festa, Antonio Festa*

4.1	Fondamenti della complessità	193
4.2	Verso una possibile economia della complessità	197
4.3	Alcune metodologie artificial intelligence based nell'analisi dell'economia della complessità	199
4.3.1	Social network analysis	199
4.3.2	Algoritmo genetico	200
4.3.3	Modellizzazione basata su agenti e multiagenti	200
4.4	Computazione digitale classica vs. computazione neurale	202
4.5	Dalla gestione della complessità alla gestione del caos	203
4.6	Conclusione	204
	Bibliografia	206

**Capitolo 5 - Fondamenti di Teoria dell'informazione.....209**

*di Franco Chiaraluce*

5.1	Introduzione	209
5.2	Alfabeti discreti	210

5.3	Informazione ed entropia	211
5.4	Entropia condizionata e informazione mutua	213
5.5	Teorema della codifica di sorgente	215
5.6	Rate-distortion theory	217
5.7	Capacità di un canale discreto	219
5.8	Segnali continui	220
5.9	Campionamento e quantizzazione	221
5.10	Capacità di un canale continuo	224
5.11	Esempi pratici di codifica di sorgente	224
5.12	Codice di Huffman	225
5.13	Codice di Shannon-Fano	226
5.14	Codice di Lempel-Ziv	227
5.15	Tecniche di compressione	229
5.16	Compressione di segnali audio	229
5.17	Compressione di immagini e segnali video	230
5.18	Compressione di archivi digitali	231
	Bibliografia	232

## **PARTE SECONDA - MODELLI, LINGUAGGI E TECNOLOGIE PER LA GESTIONE DEI DATI**

### **Capitolo 6 - Ambiti applicativi, tipologie e gestione dei dati.....235** *di Claudia Diamantini*

### **Capitolo 7 - Dati strutturati e gestione di dati transazionali .....239** *di Claudia Diamantini*

7.1	Il concetto di Database Management System	239
7.2	Il Modello relazionale	242
7.2.1	Definizione di base di dati relazionale	243
7.2.2	Vincoli di integrità	247
7.2.3	Normalizzazione in basi di dati relazionali	248
7.3	Linguaggio SQL	252
7.3.1	SQL-DDL	252
7.3.2	SQL-DML	256
7.4	Gestione delle transazioni	264
7.4.1	Modello di Transazione	265
7.4.2	Gestione della concorrenza	267
7.4.3	Gestione dell'affidabilità	273

### **Capitolo 8 - Database NOSQL.....277** *di Claudia Diamantini*

8.1	Motivazioni e caratteristiche	277
8.2	Proprietà BASE	281
8.3	Modelli di dati NOSQL	287
8.3.1	Modello Key-Value	290
8.3.2	Modello a Documento	290

8.3.3 Modello Column Family	291
8.3.4 Modello a grafo	294
Bibliografia	297
<b>Capitolo 9 - Gestione di dati multimediali.....</b>	<b>299</b>
<i>di Primo Zingaretti</i>	
9.1 Rappresentazione di dati multimediali	300
9.1.1 Digitalizzazione	300
9.1.2 Tecniche di compressione	304
9.1.3 Archiviazione	305
9.2 Introduzione alla progettazione di sistemi multimediali	308
9.3 Multimedia su Internet	314
Bibliografia	318
<b>PARTE TERZA - DATA ANALYTICS E DATA MINING</b>	
<b>Capitolo 10 - Data Warehouse e Business Analytics .....</b>	<b>321</b>
<i>di Domenico Potena</i>	
10.1 Caratteristiche dei sistemi direzionali e di supporto alle decisioni	321
10.2 Modello multidimensionale	323
10.3 Architettura di un Data Warehouse	325
10.4 On-line Analytical Processing	330
<b>Capitolo 11 - Data Mining .....</b>	<b>333</b>
<i>di Domenico Potena</i>	
11.1 Il processo di Knowledge Discovery in Databases	333
11.2 Task di Data Mining	338
11.3 Tecniche di Data Mining	339
11.3.1 Alberi decisionali	340
11.3.2 Approcci per il clustering	341
11.3.3 Association Rule Learning	342
11.3.4 Reti Neurali	342
11.4 Data Mining per applicazioni Big Data	347
<b>Capitolo 12 - Strumenti per il Data Analytics .....</b>	<b>349</b>
<i>di Domenico Potena</i>	
12.1 Le suite di Business Analytics	349
12.2 Le suite per il Data Mining	351
<b>Capitolo 13 - Evoluzioni e trend.....</b>	<b>355</b>
<i>di Domenico Potena</i>	
13.1 Self-service, exploratory intelligence	355
13.2 Deep Learning	358
13.3 Process Mining	360
Bibliografia	363

## **PARTE QUARTA - ORGANIZZAZIONE E DISTRIBUZIONE DELLE INFORMAZIONI IN AMBITO AZIENDALE**

### **Capitolo 14 - Dati e Sistemi informativi aziendali .....369**

*di Emanuele Frontoni*

14.1 Informazione e organizzazioni: il sistema informativo	369
14.2 Sistemi e modelli	372
14.3 Il sistema impresa, tra dati e informazioni	374
14.4 I sistemi informativi	377

### **Capitolo 15 - I processi aziendali e i dati.....381**

*di Emanuele Frontoni*

15.1 Processi fondamentali	383
15.2 Il sistema azienda: visione per funzioni o visione per processi	384
15.3 Azienda e sistema informativo: dati e architettura d'insieme	386

### **Capitolo 16 - Soluzioni informatiche per l'impresa .....389**

*di Emanuele Frontoni*

16.1 Sistema informatico e applicazioni	389
16.2 Le relazioni fra i livelli di applicazioni	391
16.3 I sistemi integrati di gestione	393
16.4 La business intelligence	396
16.5 I dati multimediali	398
16.6 Il rapporto azienda-clienti sulla rete	399
16.7 ICT e business: situazione corrente e possibili evoluzioni future	401

### **Capitolo 17 - Il sistema informatico .....403**

*di Emanuele Frontoni*

17.1 La struttura di un'applicazione software	406
17.2 L'evoluzione tecnologica: dai sistemi monolitici ai sistemi distribuiti	407
17.3 Panoramica sulle tecnologie correnti per lo sviluppo di applicazioni	408
17.4 Le soluzioni di integrazione dati: Service Oriented Architecture	410
17.5 Virtual computing e macchine virtuali	412
17.6 Cloud computing	415
Bibliografia	419

### **Capitolo 18 - Il sistema aziendale .....421**

*di Augusta Consorti e Michelina Venditti*

18.1 L'azienda e il suo fine	421
18.2 L'azienda e i suoi subsistemi	422
18.2.1 Il subsistema organizzativo	423
18.2.2 Il subsistema gestionale	425
18.2.3 Il subsistema informativo o del controllo	426
18.3 Le decisioni nelle aziende	428
18.4 Alcuni indicatori del successo aziendale	429
Bibliografia	432

<b>Capitolo 19 - Ergonomia cognitiva per il data analyst .....</b>	<b>433</b>
<i>di Davide Pietroni e Sibylla Verdi Hughes</i>	
19.1 Cablati per credere	433
19.2 Improbabili elaboratori di probabilità	435
19.3 Causalità o casualità	438
19.4 Il museo degli errori	440
19.5 Storie e algoritmi	442
<b>Capitolo 20 - La ricerca informativa e l'intelligence .....</b>	<b>447</b>
<i>di Antonio Teti</i>	
20.1 L'informazione come base per la conoscenza	447
20.1 La comunicazione in rete: concetti generali	448
20.3 Il processo di ricerca delle informazioni	449
20.4 Il concetto di intelligence	450
20.5 Il ciclo di intelligence	452
<b>Capitolo 21 - Open Source Intelligence (OSINT) .....</b>	<b>455</b>
<i>di Antonio Teti</i>	
21.1 Il concetto di Open Source Intelligence (OSINT)	455
21.2 OSINT: tipologie di informazioni	456
21.3 Le fonti dell'OSINT	456
21.4 OSINT e Cyberspazio	458
21.5 Il processo di ricerca delle informazioni	459
21.6 Fruttori di informazioni e metodologie di analisi	460
21.7 L'approccio mentale dell'analista	463
21.8 Metodologie per l'intelligence analysis: Analytic Tradecraft	464
<b>Capitolo 22 - Proprietà intellettuale .....</b>	<b>467</b>
<i>di Giuseppe Vero</i>	
22.1 Definizione e concetti	467
22.2 Il diritto d'autore	468
22.3 Strumenti normativi di tutela	468
22.4 Il brevetto	470
22.5 Il marchio	470
22.6 Il segreto industriale/commerciale	471
22.7 La "due diligence"	472
22.8 Diritti di proprietà intellettuale	472
<b>Capitolo 23 - Trattamento dei dati personali .....</b>	<b>475</b>
<i>di Giuseppe Vero</i>	
23.1 La direttiva europea	475
23.2 Le finalità della direttiva europea	476
23.3 I diritti	476
23.4 Il trasferimento dei dati	477
23.5 Il gruppo di lavoro "Articolo 29"	478
23.6 Le sanzioni	479
23.7 Il responsabile della protezione di dati	479



23.8	Trattamento dei dati personali	481
23.9	Il diritto all'oblio	482
23.10	Il trasferimento nell'UE ed extra UE	483
23.11	Modelli organizzativi	483
23.12	Il consenso	486
23.13	Il Titolare del trattamento dei dati	487
23.14	Il Responsabile del trattamento in outsoucer	487
23.15	L'Internal Audit	488

## PARTE QUINTA - GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

### Capitolo 24 - Fondamenti di crittografia .....497

*di Franco Chiaraluce*

24.1	Basi di crittografia	497
24.2	Cenni storici di crittografia	498
24.3	Principi di Kerckhoffs	508
24.4	Modelli di attacco	509
24.5	Crittografia simmetrica e asimmetrica	511

### Capitolo 25 - Crittografia simmetrica .....515

*di Franco Chiaraluce*

25.1	Sistema DES	515
25.2	Sistema AES	521
25.3	Modalità operative	528
	Bibliografia	533

### Capitolo 26 - Crittografia asimmetrica.....535

*di Marco Baldi*

26.1	Introduzione alla crittografia asimmetrica	535
26.2	Scambio di chiavi di Diffie-Hellman	538
26.3	Sistema RSA	539
26.3.1	Generazione delle chiavi	539
26.3.2	Cifratura	540
26.3.3	Decifratura	540
26.3.4	Sicurezza del sistema RSA	540
26.4	Sistema ElGamal	541
26.4.1	Generazione delle chiavi	541
26.4.2	Cifratura	541
26.4.3	Decifratura	541
26.4.4	Osservazioni	542
26.5	Sistemi asimmetrici post-quantici	542
26.5.1	Sistemi basati su reticoli	542
26.5.2	Sistemi basati su codici	543
26.5.3	Sistemi basati su polinomi a variabili multiple	543
26.5.4	Altre tecniche	543
	Bibliografia	544

<b>Capitolo 27 - Funzioni hash.....</b>	<b>545</b>
<i>di Marco Baldi</i>	
27.1 Principi delle funzioni hash	545
27.2 Secure Hash Algorithm	547
27.3 Message integrity code e message authentication code	548
27.4 Attacchi alle funzioni hash	550
Bibliografia	552
<b>Capitolo 28 - Firme digitali.....</b>	<b>553</b>
<i>di Marco Baldi</i>	
28.1 Principi degli schemi di firma digitale	553
28.2 Firma RSA e firma cieca	555
28.2.1 Generazione delle chiavi	555
28.2.2 Procedura di firma	555
28.2.3 Procedura di verifica	555
28.2.4 Hash e firma	555
28.2.5 Firma cieca	557
28.3 Firma ElGamal	557
28.3.1 Generazione delle chiavi	557
28.3.2 Procedura di firma	557
28.3.3 Procedura di verifica	558
28.4 Schema DSA	558
28.4.1 Generazione delle chiavi	558
28.4.2 Procedura di firma	558
28.4.3 Procedura di verifica	558
28.5 Attacchi agli schemi di firma digitale	559
Bibliografia	560
<b>Capitolo 29 - Standard e protocolli di sicurezza delle reti.....</b>	<b>561</b>
<i>di Marco Baldi</i>	
29.1 Protocolli di autenticazione	561
29.2 Distribuzione delle chiavi	563
29.2.1 Distribuzione di chiavi per cifrari simmetrici	563
29.2.2 Distribuzione di chiavi per cifrari asimmetrici	565
29.3 Certificati X.509	567
29.4 Protocolli SSL/TLS e HTTPS	569
29.5 Protocollo IPsec e reti private virtuali	572
29.6 Protocollo IEEE 802.1x	573
Bibliografia	575
<b>Capitolo 30 - Infrastrutture per memorizzare e trasferire informazioni digitali. Sistemi di protezione .....</b>	<b>577</b>
<i>di Giovanni Cancellieri</i>	
30.1 Supporti per la memorizzazione dei dati	577
30.2 Rete di trasporto	581

30.3 Rete di accesso	584
Bibliografia	591
<b>Capitolo 31 - Information warfare e cyberwarfare .....</b>	<b>593</b>
<i>di Antonio Teti</i>	
31.1 Il concetto di information warfare	593
31.2 Tipologie di information warfare	593
31.2 Il concetto di Cyberwarfare	596
<b>Capitolo 32 - Geopolitica del Cyberspazio .....</b>	<b>601</b>
<i>di Antonio Teti</i>	
32.1 Il concetto di geopolitica	601
32.2 Strumenti di comunicazione di massa nella geopolitica	603
32.3 Geopolitica e cyberspazio	604