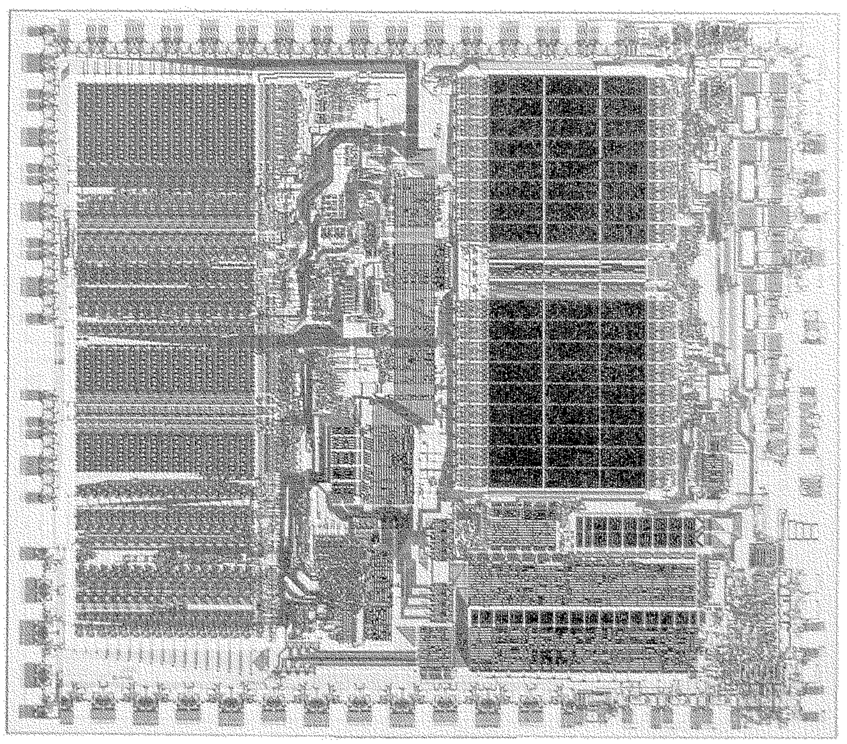
Mario Vascon

ANALISI e SINTESI DEI SISTEMI LOGICI COMBINATORI e SEQUENZIALI



Sistemi di numerazione

CLEUP EDITRICE - PADOVA

Mario Vascon

Dipartimento di Fisica G. Galilei
Università di Padova

ANALISI E SINTESI dei SISTEMI LOGICI COMBINATORI e SEQUENZIALI

In copertina:
Microprocessore a 16 bit

Dipartimento di Fisica "Galileo Galilei", Padova.

Stampato nel mese di Febbraio del 1997 presso la
C.L.E.U.P. "Cooperativa Libraria Editrice Universitaria di Padova"
Via G. Prati 19 - Padova.

Ad Aldo e a Luca

The object of science, properly so called, is the knowledge of laws and relations. To be able to distinguisch what is essential to this end, from what is only accidentally associated with it, is one of the most important conditions of the scientific progress.

George Boole

Indice

Prefazione

La teoria dei sistemi logici ha assunto, negli ultimi anni, con la sua applicazione alla Elettronica digitale, una importanza fondamentale per le implicazioni tecnologiche tra le più importanti della nostra epoca.

Tale teoria, nata con l'applicazione, da parte di Shannon, dell'Algebra di Boole ai circuiti di commutazione, e via via sviluppatasi col contributo di studiosi come Karnaugh, Quine, McKluskey, Huffman, Mealy, Moore, Gill, Ginzburg e moltissimi altri, è relativamente giovane.

Un gran numero di articoli di rivista è stato scritto, così pure un certo numero di volumi sulla teoria matematica di base e un ragguardevole numero di volumi a carattere didattico.

Ma se qualcuno volesse, di questa branca della teoria dei sistemi, soprattutto per la sua parte riguardante la logica sequenziale, tentare di eseguire una sintesi, ad un giusto equilibrio tra teoria ed applicazione, durerebbe una certa fatica.

Questo è dovuto sicuramente alla giovinezza di questa materia della quale molti autori analizzano settori ancora inesplorati dalla ricerca, come è logico, piuttosto che codificare e standardizzare tutto ciò che sinora è stato fatto.

Molto di questa codificazione e standardizzazione è stato fatto, ma non si è raggiunto ancora il livello al quale si è pervenuti per scienze più anziane.

Per cui chi intendesse cominciare ad occuparsi dei sistemi logici combinatori e sequenziali, troverebbe una certa iniziale difficoltà nei testi di base, dovuta talvolta ad una certa discordanza di definizioni fra i testi, talvolta ad un certo squilibrio tra le basi matematiche della teoria e le sue applicazioni.

Per tali motivi lo studente, o chiunque altro inizi questo studio e che scopra dei punti in sospeso o dei punti aldilà dei quali intuisce l'esistenza di ulteriori basi da approfondire, deve ricorrere alle fonti primarie, argomento per argomento.

Questo lavoro vuole collocarsi come un tentativo di esposizione della materia ricostruendola passo passo, così come si è sviluppata, mostrando al contempo il contributo delle altre materie e degli uomini che ad essa hanno dedicato il loro interesse e il loro lavoro.

Si è cercato di mettere in risalto il più possibile il contributo delle materie affini e dei ricercatori, perchè questo dona sicuramente alla materia più vita, più calore e più smalto.

Lo schema della esposizione è generalmente di tipo induttivo-deduttivo, e fa uso di formalismi soltanto quando questi rappresentano la sintesi di un concetto induttivamente acquisito e quindi una economia di pensiero.

Per rendere il volume autoconsistente è stata riportata in Appendice tutta la parte (non molta invero) di Algebra essenziale alla trattazione.

È stato dato risalto particolarmente ai metodi di sintesi, introducendo il più possibile metodologie generali unificate e computerizzabili.

Si giunge, nella sintesi, fino allo stadio dello schema a blocchi. Ciò perchè, a questo stadio, le metodologie sono ancora del tutto generali nel senso che lo schema a blocchi di sintesi è comune a tutte le successive realizzazioni eseguite con dispositivi di qualsivoglia natura: elettronica, fluidodinamica, magnetica, ottica, ecc...

Lo stadio successivo comporterebbe la scelta della natura dei dispositivi, del tipo dei componenti e della loro interconnessione fisica. Questo stadio non è stato preso in esame, vuoi per la particolare dovizia di descrizioni di cui è stato fatto oggetto, soprattutto nel campo della Elettronica, vuoi perchè, in tempi di rapidi mutamenti della tecnologia, come sono quelli d'oggigiorno, ogni descrizione di componenti rischia di essere obsoleta ancor prima di essere stampata.

Man mano si procede nel tentativo di scrivere un testo didattico, ci si rende conto sempre di più di quale difficoltà questo comporti e risulta sempre più chiaro quanto sia più facile scrivere qualcosa che sia rivolto a conoscitori della materia. L'insidia della esposizione professionistica è sempre presente, ma non è sempre facile accorgersi di questa sua presenza.

È proprio per questo continuo sospetto di presenza che il testo forse pecca per una sua esposizione eccessivamente didascalica, ma se questo è vero, ciò non mi preoccupa, perchè il suo scopo è didattico, essendo diretto ai non addetti ai lavori, sia che essi abbiano solide basi matematiche, sia che non. La semplificazione nella esposizione porta talvolta ad un lieve scostamento da alcuni classici, talvolta porta a qualche definizione non codificata, ma spero, mai, alla distorsione dell'essenza dei concetti. Ogni definizione o nuovo concetto, o applicazione, sono integrati da una quantità di esempi che possono sembrare o eccessivi nel numero, o banali, ad un lettore che già sia a conoscenza della materia, ma che possono essere utili ad un lettore che a conoscenza non ne sia.

Desidero ringraziare tutti coloro che mi hanno aiutato:

- I ragazzi del corso 1981/82 (un corso veramente "di annata") che con il loro interesse per l'argomento hanno agito come stimolo alla prima stesura di queste note, e come filtro agli immancabili errori.
- Il collega Tullio A. Minelli per la revisione dei Complementi di Algebra
- I colleghi Emilio Borchi e Gabriele Torelli per i loro consigli e il loro incoraggiamento.
- Il signor Angelo Rampazzo per la grafica accurata.

Mario Vascon

0

Introduzione

Possiamo definire:

DEF. P0_C0.0.1 Sistema una scatola nera dotata di *Ingresso* e di *Uscita* attraverso i quali accetta e fornisce *Informazioni.*

Possiamo intendere come *Informazione* (o *"segnale"* , termine preso a prestito dalla Elettronica) di ingresso o di uscita di un sistema, come ogni comunicazione che possa essere scambiata tra il mondo esterno e il sistema, in un linguaggio a loro comune.

La definizione di Sistema, che a rigore dovrebbe essere desunta dalla Cibernetica, è molto generale ed applicabile a tutti i campi di cui si occupa la Cibernetica stessa, dalla Psicologia alla Teoria della Informazione, dalla Meccanica alla Fisica.

Ogniqualvolta ad esempio, si esegue una misura, si preleva una informazione da un fenomeno fisico, che può essere considerato come un Sistema.

Questa informazione (o *"segnale"*) si dice **analogica** quando è di natura continua, cioè è una funzione del tempo, priva di discontinuità.

L'informazione si dice invece **digitale** (dall'Inglese digit cioè numero) o **numerica** o **logica**, quando è di natura discontinua.

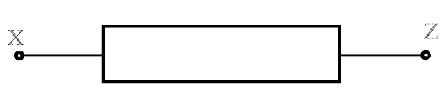
Possiamo allora definire:

DEF. P0_C0.0.2 Sistema Analogico una scatola nera che accetta al suo ingresso, eventualmente elabora al suo interno, e fornisce alla sua uscita, informazioni di natura analogica.

DEF. P0_C0.0.3 Sistema Logico una scatola nera che accetta al suo ingresso, eventualmente elabora al suo interno, e fornisce alla sua uscita informazioni di natura logica.

Nei sistemi logici di cui ci occuperemo, le informazioni che questi scambiano col mondo esterno, devono essere espresse in un opportuno linguaggio o **codice** (vedi P1_C1.7) comune allo stesso tempo e al sistema e al suo mondo esterno.

Un sistema logico semplice, ad esempio ad un ingresso ed a una uscita, può essere schematizzato in una scatola nera con un terminale d'ingresso (x) ed un terminale d'uscita (z) come in figura.



La grandezza presente al terminale x può assumere per ipotesi solo valori discreti, e così pure quella al terminale z. Ora la domanda che spontaneamente nasce è: quanti valori discreti, tra loro distinti può assumere questa grandezza?

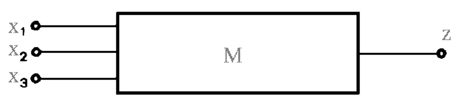
Il numero di tali valori è una scelta legata al tipo di codice col quale il sistema funziona e colloquia col mondo esterno.

Se ad esempio l'ingresso x può assumere due valori distinti soltanto, ciò vuol dire che le informazioni che si possono fornire al sistema, tra loro distinte, sono due e ciò ancora vuol dire che, supponendo lo stesso il codice d'ingresso e di uscita, le informazioni che si possono trarre dal sistema sono due.

Ad ogni una delle due informazioni che noi introdurremo nel sistema, questo risponderà all'uscita, con una delle due informazioni che potrà fornire. Possiamo anche supporre, per semplicità, di associare le due informazioni distinte ai due numeri 0 ed 1. La legge con la quale il sistema risponde, associando ad uno dei due numeri all'ingresso uno dei due numeri (0,1) all'uscita, dipende dalla struttura interna del sistema stesso.

Un codice basato su due elementi distinti si chiama **codice binario.**

Supponiamo ora che il nostro sistema logico, basato sul codice binario possegga tre terminali d'ingresso x_1 x_2 x_3 ed un solo terminale d'uscita.



Altra domanda che spontaneamente nasce è: quante informazioni tra loro distinte (**configurazioni di ingresso** vedi App.B.16) possono essere fornite al sistema?; tante quante sono le disposizioni con ripetizioni di classe 3 che si possono ottenere con gli elementi dell'insieme binario $(0, 1) : 2^3$ (cfr. App.A.4). Esse sono: (000), (001), (010), (011), (100), (111), mentre sempre soltanto due sono quelle che il sistema può dare all'uscita.

Se in un sistema logico del tipo della seconda figura, l'uscita è univocamente determinata dalla configurazione d'ingresso (x_1 x_2 x_3), il sistema si chiama **sistema logico combinatorio.** Mediante il codice binario, si può costruire un **sistema di numerazione binario** (o **in base 2)** , associando, ad ogni configurazione ad una variabile (x_1) un numero da 0 ad 1, ad ogni configurazione a due variabili (x_1 x_2) un numero da 0 a 3, ad ogni configurazione a 3 variabili (x_1 x_2 x_3) un numero da 0 ad 8, e così via (vedi prima parte 1.A.3).

Le informazioni dunque scambiate tra il sistema ed il mondo esterno possono essere anche rappresentate come numeri espressi nel sistema di numerazione binario.

Al sistema di numerazione in base 2 può essere poi associata un' **Algebra binaria** (vedi P1_C1.10) che permette di poter rappresentare analiticamente **funzioni binarie a più variabili** (vedi P1_C2) mediante un numero ristretto di **operatori binari fondamentali** che servono ad eseguire tutte le operazioni dell'Algebra binaria.

Se si conosce il comportamento del sistema binario combinatorio, cioè, se si sa esattamente come il sistema reagisce all'uscita in funzione di tutte le possibili configurazioni d'ingresso, questo, con opportune tecniche (P1_C4.7, P1_C5.4), può essere rappresentato con una o più funzioni logiche binarie che ne simulano il comportamento.

Una funzione binaria è rappresentata analiticamente mediante operatori binari. Se questi operatori possono essere materializzati cioè essere realizzati in qualche modo fisicamente (P1_C1.9), mediante essi possono essere realizzate fisicamente tutte le possibili funzioni binarie e quindi tutti i sistemi logici binari (**Sintesi dei sistemi** P1_C4, P1_C5).

Può accadere che l'uscita di un sistema logico non sia univocamente determinata dall'ingresso (nel senso che può darsi il caso che allo stesso ingresso corrispondano più uscite) in quanto l'uscita non è soltanto funzione dell'ingresso, ma anche della successione temporale degli ingressi. Nel senso che tutto va come se l'associazione funzionale ingresso-uscita dipendesse dalla sequenza temporale in cui si presentano gli ingressi, oltre che dai valori assunti dagli ingressi stessi. In tal caso il sistema si dice **Sistema logico sequenziale** (P2_C1).

Anche in questo caso, mediante l'algebra binaria, si può associare (introducendo accanto agli operatori binari fondamentali altri operatori chiamati **elementi di memoria**) ad ogni sistema sequenziale una o più **macchine sequenziali a stati finiti.** Esse sono l'analogo delle funzioni binarie del caso dei sistemi combinatori (P2_C1).

Essendo poi una macchina sequenziale a stati finiti rappresentabile analiticamente mediante operatori binari ed elementi di memoria, se questi in qualche modo possono essere fisicamente realizzati, possono esserlo anche le macchine sequenziali, ed i sistemi sequenziali associati (vedi P2_C2, P2_C3, P2_C4).

Parte 1

SISTEMI E CIRCUITI COMBINATORI

Parte 1

Capitolo 1

Parte A. Sistemi di numerazione.

P1_C1.1 Introduzione

Lo scopo di questo capitolo è quello di introdurre alcuni concetti fondamentali che sono alla base della logica combinatoria e sequenziale.

Questi concetti riguardano i sistemi di numerazione e i fondamenti dell'algebra di Boole.

I due argomenti sono trattati rispettivamente nella parte A e nella parte B di questo capitolo.

Nella parte A si è cercato di schematizzare e di semplificare quanto possibile le nozioni irrinunciabili per la comprensione dei sistemi di numerazione, e di accennare all'idea di codice, inserendola nel contesto di tali sistemi.

La semplificazione nella esposizione di tale materia forse porta ad un lieve scostamento dalle esposizioni classiche, ma si pensa che questo non vada a scapito della comprensione dell'essenza delle cose.

Al lettore che volesse approfondire la materia, si consiglia la bibliografia a fine capitolo, dalla quale altra più vasta bibliografia si può dedurre.

Nella parte B vengono introdotte le basi dell'algebra di Boole deducendola, anche qui in modo schematico e semplificato, dalle strutture algebriche erigibili su un insieme costituito da due soli elementi.

Anche in questo caso al lettore che non volesse fermarsi ai soli concetti essenziali per la comprensione della logica combinatoria e sequenziale, si consiglia la bibliografia a fine capitolo, dalla quale più vasta bibliografia sulla materia può essere desunta.

P1_C1.2 Generalità. Sistema di numerazione a base 10

Contare o *numerare* significa associare, ad ogni quantità di oggetti, uno ed un solo *numero,* il quale descrive quantitativamente, in modo oggettivo ed univoco, quella "quantità" di oggetti.

È antica e quasi generale abitudine dell'uomo contare in un particolare sistema di numerazione che è chiamato *sistema di numerazione decimale.*

Ciò significa scegliere un insieme di dieci elementi distinti, detti *simboli* : $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, tra i quali l'elemento nullo (0) e quello unità (1), a ciascuno dei quali, nell'ordine, è associata una quantità gradualmente crescente di una unità.

Mediante l'insieme di questi elementi ed alcune regole da definire una volta per tutte, si possono anche costruire tutti i numeri superiori al nove, associabili ad una qualsiasi quantità di oggetti, purchè essa sia finita.

Abbiamo visto, di questo sistema *decimale*, qual'è l'*insieme* di simboli su cui esso si basa; vediamo ora quali sono le *regole* per rappresentare un numero superiore al nove.

Per rappresentare un numero superiore al nove, si dispongono più elementi dell'insieme, l'uno in seguito all'altro, in tal modo:

- Il primo simbolo da destra rappresenta le unità,
- Il secondo simbolo da destra rappresenta le decine,
- Il terzo simbolo da destra rappresenta le centinaia,
- ... e così via.

Ogni "posto" o *cifra* (da destra a sinistra), ha dunque un suo "peso"; il primo posto ha peso 1, il secondo ha peso 10, il terzo ha peso 100, ... ecc. ..., nel senso che, se si vuole leggere un numero a più cifre, ad esempio, bisogna moltiplicare ogni simbolo della $i-esima$ cifra per il peso associato a quella cifra e sommare tutti i prodotti ottenuti.

Esempio P1_C1.2.1 Ad esempio, il numero:

$$\begin{aligned} 1\ 4\ 7\ 8\ 5 &= 1 \cdot 10^4 + 4 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 5 \cdot 10^0 \\ &| \\ &= 10000 + 4000 + 700 + 80 + 5 \\ &| \\ &= 14785 \end{aligned}$$

Il numero invece:

$$\begin{aligned} 1\ 4\ 7,\ 8\ 5 &= 1 \cdot 10^2 + 4 \cdot 10^1 + 7 \cdot 10^0 + 8 \cdot 10^{-1} + 5 \cdot 10^{-2} \\ &| \\ &= 100 + 40 + 7 + 0.8 + 0.05 \\ &| \\ &= 147.85 \end{aligned}$$

Ricapitolando, associare ad una certa "quantità" un numero, in modo oggettivo ed univoco, significa eseguire una *numerazione* .

Scegliere poi un insieme costituito da un numero finito, detto *base,* di elementi detti *simboli* e stabilire un insieme di regole dette *regole di codificazione,* per poter scrivere e leggere una quantità qualunque in modo oggettivo ed univoco, significa definire un *sistema di numerazione.*

P1_C1.3 Sistemi di numerazione a base B

Il sistema di numerazione a base 10 che noi comunemente siamo soliti usare, è uno degli infiniti sistemi di numerazione possibili.

Come si può desumere da paragrafo precedente, per definire un sistema di numerazione, basta fissare una *base* e le *regole di codificazione.*

Per ogni base B infatti, otteniamo un diverso sistema di numerazione variando le regole di codificazione.

Fissando alcune regole di codificazione, per contro, e variando la base B otteniamo un diverso sistema di numerazione.

Notiamo che, come elementi di un insieme di un sistema a base B si conviene di scegliere i primi B simboli del sistema a base 10 se $B \leq 10$, i primi 10 simboli del sistema a base 10 più altri k simboli se $B = (10 + k)$.

Esempio P1_C1.3.1 In un sistema a base B=2 (binario) gli elementi dell'insieme sono:

$$(0, 1)$$

In un sistema di numerazione a base B=3 (ternario), gli elementi dell'insieme sono:

$$(0, 1, 2)$$

In un sistema di numerazione a base B=8 (ottale), gli elementi dell'insieme sono:

$$(0, 1, 2, 3, 4, 5, 6, 7)$$

In un sistema di numerazione a base B=16 (esadecimale) gli elementi scelti per l'insieme sono:

$$(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F)$$

Supponiamo ora di fissare come regola di codificazione, analoga per tutti i sistemi, una **regola ponderale,** cioè supponiamo di associare ad ogni *n-sima* cifra (contata da destra a sinistra) di un numero A espresso nel sistema di numerazione a base B, $(A)_B$, un peso pari a B^n.

In analogia a quanto visto per il sistema decimale, allora, un numero $(A)_B$ ad n cifre scritto nel sistema di numerazione a base B sarà espresso mediante la:

$$(A)_B = a_n \ldots a_3 a_2 a_1 a_0,$$

dove $a_i (i = 0, \ldots, n)$ è uno dei simboli dell'insieme degli elementi del sistema di numerazione a base B, collocato nella posizione, o cifra, $i - esima$.

Il numero A sopra scritto, sarà allora interpretato, nel sistema decimale, come:

$$(A)_{10} = a_n B^n + \ldots + a_3 B^3 + a_2 B^2 + a_1 B^1 + a_0 B^0$$

Esempio P1_C1.3.2 **Scriviamo i primi 17 numeri nei sistemi: decimale, ottale, esadecimale, separando i simboli dei tre insiemi (o numeri ad una cifra costituenti la BASE) dai numeri a più cifre**

$\underline{B=10}$

0123456789 $\searrow$

$(10)_{10}(11)_{10}(12)_{10}(13)_{10}(14)_{10}(15)_{10}(16)_{10}$

$\underline{B=8}$

01234567 $\searrow$

$(10)_8(11)_8(12)_8(13)_8(14)_8(15)_8(16)_8(17)_8(20)_8$

$\underline{B=16}$

$0123456789ABCDEF$ $\searrow$

$(10)_{16}$

Esempio P1_C1.3.3 **Trasformare in decimale il numero in base 3:** $(21021)_3$

$$(21021)_3 = (2 \cdot 3^4 + 1 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0)10 = (196)_{10}$$

Esempio P1_C1.3.4 **Trasformare in decimale il numero in base 5:** $(31402)_5$

$$(3 \cdot 5^4 + 1 \cdot 5^3 + 4 \cdot 5^2 + 0 \cdot 5^1 + 2 \cdot 5^0)_{10} = (2102)_{10}$$

Esempio P1_C1.3.5 **Trasformare in decimale il numero in base 8:** $(14705)_8$

$$(14705)_8 = (1 \cdot 8^4 + 4 \cdot 8^3 + 7 \cdot 8^2 + 0 \cdot 8^1 + 5 \cdot 8^0)_{10} = (6597)_{10}$$

Esempio P1_C1.3.6 **Trasformare in decimale il numero in base 16:** $(14705)_{16}$

$$(14705)_{16} = (1 \cdot 16^4 + 4 \cdot 16^3 + 7 \cdot 16^2 + 0 \cdot 16^1 + 5 \cdot 16^0)_{10} = (83717)_{10}$$

Abbiamo visto il modo di rappresentare, nel sistema a base 10, un numero qualunque scritto in un sistema a base B qualunque.

Vediamo ora come si può, dato un numero qualunque espresso in un sistema a base 10, rappresentare questo numero in un sistema a base B qualunque.

Ricordiamo a tale scopo che un numero $(A)_B$

$$(A)_B = a_n \dots a_3 a_2 a_1 a_0 \qquad \text{(P1\_C1.3.1)}$$

si esprime, nel sistema decimale, come:

$$(A)_{10} = a_n B^n + \dots a_3 B^3 + a_2 B^2 + a_1 B^1 + a_0 B^0.$$

Dividiamo ora l'espressione P1_C1.3.1 per B: otterremo un quoziente Q_1 ed un resto a_0. Dividiamo Q_1 per B: otterremo un quoziente Q_2 ed un resto $a_1 \dots$ e così via finchè il quoziente non è divisibile per B.

$$(A)_1 0 = B \underbrace{(a_n B^{n-1} + \dots + a_3 B^2 + a_2 B^1 + a_1 B^0)}_{Q_1} + a_0$$

$$Q_1 = B(a_n B^{n-2} + \dots + a_3 B^1 + a_2 B^0) + a_1$$

$$Q_{n-1} = B(a_n B^0) + a_{n-1}$$

$$Q_n = a_n$$

Come si vede, i resti $a_0, \dots, a_n$, altro non sono che i simboli (dell'insieme a base B) che compongono il numero $(A)_B$.

Quanto visto sopra fornisce il metodo per esprimere un numero decimale qualunque $(A)_{10}$ in un qualunque sistema di numerazione a base B.

Basta dividere il numero decimale per B ed annotare il resto a_0; poi dividere per B il quoziente Q_1 ed annotare il resto a_1; poi dividere il nuovo quoziente Q_2 ed annotare il resto $a_2 \dots$ e così via, finchè l'ultimo quoziente non sia minore di B.

A questo punto i resti successivi, l'uno accanto all'altro, ordinati da destra a sinistra, rappresentano il numero A espresso nel sistema a base B.

Esempio P1_C1.3.7 **Trasformare nel sistema a base 3 (ternario) il numero** $(196)_{10}$

$$\begin{aligned} 196 &= 3 \cdot 65 + 1 \\ 65 &= 3 \cdot 21 + 2 \\ 21 &= 3 \cdot 7 + 0 \\ 7 &= 3 \cdot 2 \\ 2 &= 2 \end{aligned} \qquad (196)_{10} = (21021)_3$$

Esempio P1_C1.3.8 **Trasformare nel sistema a base 5 (quinario) il numero** $(2102)_{10}$

$$\begin{aligned} 2102 &= 5 \cdot 420 + 2 \\ 420 &= 5 \cdot 84 + 0 \\ 84 &= 5 \cdot 16 + 4 \\ 16 &= 5 \cdot 3 + 1 \\ 3 &= 3 \end{aligned} \qquad (2102)_{10} = (31402)_5$$

Esempio P1_C1.3.9 **Trasformare nel sistema a base 8 (ottale) il numero** $(6597)_{10}$

$$\begin{aligned} 6597 &= 8 \cdot 824 + 5 \\ 824 &= 8 \cdot 103 + 0 \\ 103 &= 8 \cdot 12 + 7 \\ 12 &= 8 \cdot 1 + 4 \\ 1 &= 1 \end{aligned} \qquad (6597)_{10} = (14705)_8$$

Esempio P1_C1.3.10 **Trasformare nel sistema a base 16 (esadecimale) il numero** $(83717)_{10}$

$$\begin{aligned} 83717 &= 16 \cdot 5232 + 5 \\ 5232 &= 16 \cdot 327 + 0 \\ 327 &= 16 \cdot 20 + 7 \\ 20 &= 16 \cdot 1 + 4 \\ 1 &= 1 \end{aligned} \qquad (83717)_{10} = (14705)_{16}$$

Esercizio P1_C1.3.1 **Trasformare nei sistemi a base 2,3,4,5,6,7,8,9 i due numeri** $(123)_{10}, 512_{10}$

$$\begin{aligned} (123)_{10} &= (1111011)_2 \\ &= (11120)_3 \\ &= (1323)_4 \\ &= (443)_5 \\ &= (323)_6 \\ &= (234)_7 \\ &= (173)_8 \\ &= (146)_9 \end{aligned} \qquad \begin{aligned} (512)_{10} &= (1000000000)_2 \\ &= (200222)_3 \\ &= (20000)_4 \\ &= (4022)_5 \\ &= (2212)_6 \\ &= (1331)_7 \\ &= (1000)_8 \\ &= (628)_9 \end{aligned}$$

Vediamo ora quante cifre n occorrono, in un sistema a base b, per scrivere il numero più grande esprimibile con N cifre in un sistema a base B. A tale scopo notiamo che con N cifre in base B possiamo costruire B^N "disposizioni con ripetizioni di classe N su B elementi distinti" (vedi App. A.4) e perciò scrivere B^N numeri da 0 a $B^N - 1$.

Nel sistema in base b invece, con n cifre possiamo costruire b^n "disposizioni con ripetizioni di classe n su b elementi distinti" e perciò possiamo scrivere b^n numeri.

La relazione dunque che lega n ad N e che andavamo cercando è la:

$$B^N = b^n$$

$$N = n \log_B(b)$$

$$n = \frac{N}{\log_B(b)}$$

Esempio P1_C1.3.11 **Vediamo quante cifre n occorrono, nel sistema di numerazione a base due, per scrivere** $(99)_{10}, (999)_{10}, (9999)_{10}$

$$(99)_{10} \Longrightarrow \begin{array}{l} N = 2 \\ B = 10 \\ b = 2 \end{array} \qquad n = \frac{2}{log_{10}(2)} \simeq \frac{2}{.301029995} \simeq 6.64 \simeq 7$$

Infatti: $(99)10 = (1100011)_2$

$$(9999)_{10} \Longrightarrow \begin{array}{l} N = 4 \\ B = 10 \\ b = 2 \end{array} \qquad n = \frac{4}{log_{10}(2)} = \frac{4}{.3} = 13.29 \simeq 14$$

Infatti: $(9999)_{10} = (10011100001111)_2$

$$(999)_{10} \Longrightarrow \begin{array}{l} N = 3 \\ B = 10 \\ b = 2 \end{array} \qquad n = \frac{3}{log_{10}(2)} = \frac{3}{.3} = 9.97 \simeq 10$$

Infatti: $(999)_{10} = (11110011)_2$

P1_C1.4 Esempi di programmi di conversione

Le formule di conversione dal sistema decimale ad un sistema in base B qualunque e da un sistema in base B qualunque al sistema decimale, sono facilmente traducibili in semplici programmi per calcolatore.

Ne mostreremo due possibili esempi, comprensibili a chiunque abbia un minimo di dimestichezza con la programmazione.

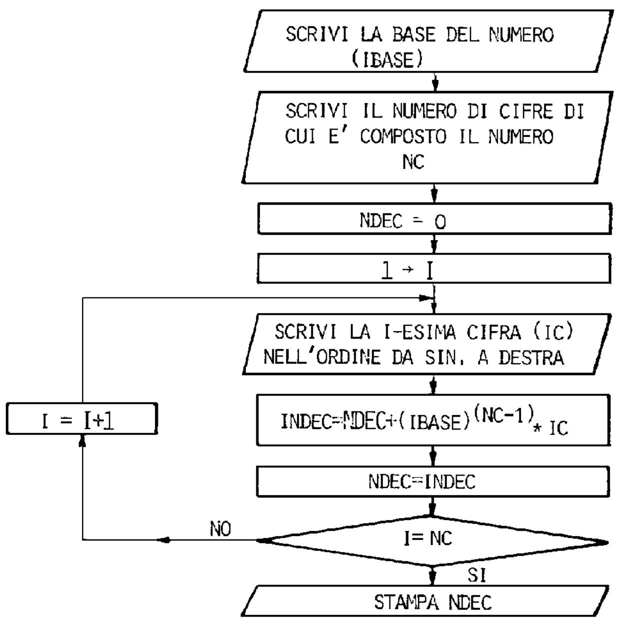
P1_C1.4.1 Conversione base qualunque → base 10

I parametri d'ingresso del programma sono:

1. La base del sistema (variabile $IBASE$) in cui è scritto il numero in esame.
2. Il numero di cifre NC che compongono il numero.
3. Le cifre IC da introdursi ad una ad una, cominciando dalla prima a sinistra.

In figura viene riportato il flow-chart dell'algoritmo. Dopo aver introdotto gli ingressi $IBASE$ ed NC, mediante il ciclo con I che varia da 1 ad NC, richedendo ogni singolo IC, vengono eseguiti ad uno ad uno i prodotti delle cifre per i loro rispettivi pesi: $IBASE^{NC-1} \cdot IC$, e tali prodotti vengono sommati a tutti i precedenti: $INDEC = NDEC + IBASE^{NC-1}$, $NEC = INDEC$.

Alla fine, esaurito il ciclo quando $I = NC$, la variabile $NDEC$ contenente la somma dei prodotti di tutte le cifre per i loro rispettivi pesi, fornisce il numero in base 10.



P1_C1.4.2 Conversione base 10 → base qualunque

I parametri d'ingresso sono:

1. Il numero in base 10 in esame (NDEC).
2. La base del sistema (IBASE) nel quale il numero deve essere convertito.

Ci serviamo di due vettori IA e IB di dimensioni pari a 20 supponendo che le cifre che compongono il numero in esame non siano in numero superiore a 20.

Dopo aver azzerato i vettori ed aver richiesto i parametri d'ingresso, il programma controlla se il numero decimale è minore della base; se si, il programma entra nella fase di scrittura senza manipolare il dato, dopo aver posto IB(1)=NDEC. Se no, viene calcolata la parte intera del quoziente NDEC/IBASE,

$$INDB = PARTEINTERA\,(NDEC/IBASE)$$

quindi il resto Q_1 che viene depositato nella prima casella del vettore IB:

$$IB(1) = NDEC - IBASE \cdot INDB$$

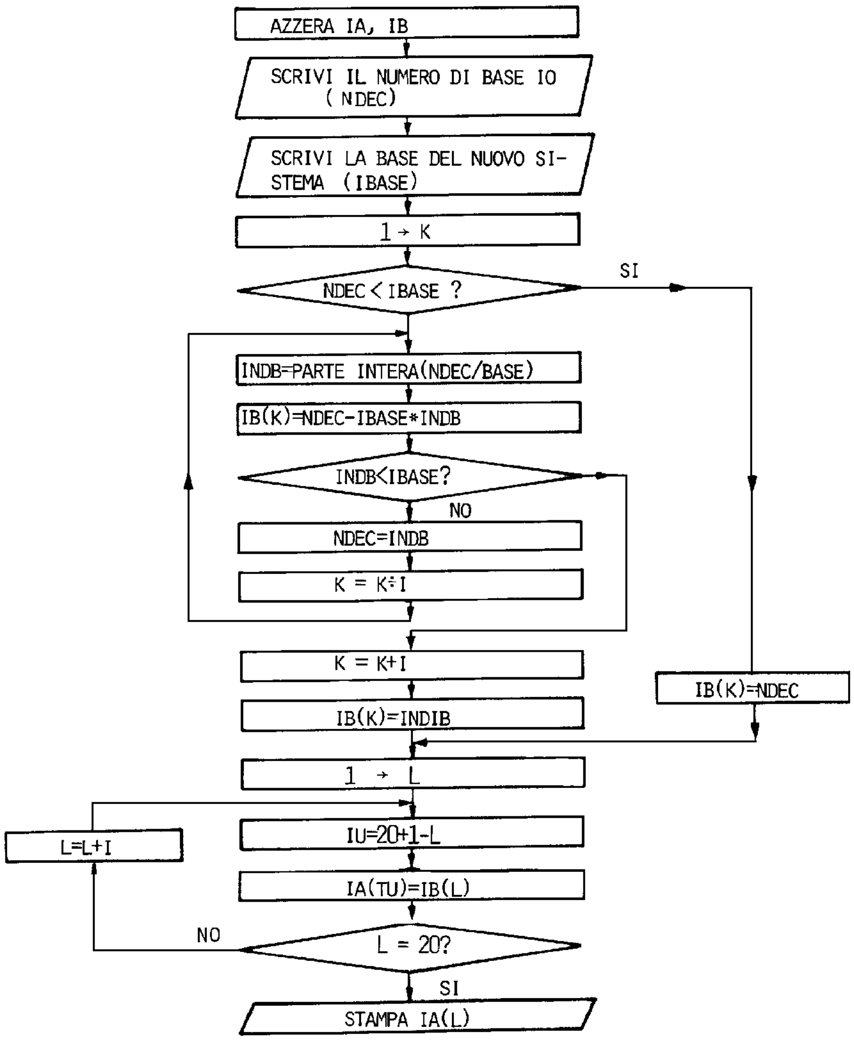
Se INDB è minore di IBASE, viene incrementato il contatore K, e viene posto IB(2)=INDB, quindi si passa alla fase di scrittura. Se no, NDEC viene posto eguale a INDB, viene incrementato il contatore K ($K = 2$) e si ritorna ad eseguire il ciclo che valuta il nuovo quoziente, il nuovo resto ... e così via.

Alla fine del ciclo, il vettore IB contiene tutti i successivi resti calcolati, nell'ordine, dal meno significativo al più significativo.

Nell'ultimo ciclo (in L), si caricano in IA i resti, nell'ordine, dal più significativo al meno significativo (facilitazione questa per una più agevole scrittura in Fortran, fase inutile ad esempio nel caso di un linguaggio come il Basic). Si passa poi alla stampa del vettore IA.

Volendo scrivere un numero espresso in un sistema a base B, in un sistema a base B', si possono combinare i due programmi visti; con il programma 1) si converte il numero scritto nel sistema a base B nel sistema a base 10, col programma 2) si converte il numero scritto nel sistema a base 10, nel sistema a base B'.

Nelle pagine in fine paragrafo vengono dati un esempio di scrittura Fortran di tale algoritmo ed alcuni esempi di calcolo desunti dall'esercizio P1_C1.3.1.


AZZERA IA, IB
SCRIVI IL NUMERO DI BASE IO (NDEC)
SCRIVI LA BASE DEL NUOVO SI-STEMA (IBASE)
1 → K
NDEC < IBASE ?
SI
INDB=PARTE INTERA(NDEC/BASE)
IB(K)=NDEC-IBASE*INDB
INDB<IBASE?
NO
NDEC=INDB
K = K÷I
K = K+I
IB(K)=INDIB
IB(K)=NDEC
1 → L
L=L+I
IU=20+1-L
IA(TU)=IB(L)
NO
L = 20?
SI
STAMPA IA(L)

```
:LI,S,1,FCONV

FTN4,L
      PROGRAM CONV
10    WRITE(1,100)
100   FORMAT(3/,"BASE DEL SISTEMA ?")
      READ(1,*) IBASE
      WRITE(1,200)
200   FORMAT("NUMERO DI CIFRE ?")
      READ(1,*) NC
      WRITE(1,300)
300   FORMAT("SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA
      NDEC=0
      DO 500 I=1,NC
      READ(1,*) IC
      INDEC=NDEC+(IBASE**(NC-I))*IC
      NDEC=INDEC
500   CONTINUE
      WRITE(1,600) NDEC
600   FORMAT(/,"E@UIV. DECIM. =",I5,/)
      CALL COD1(NDEC)
      GOTO 10
      END
      END$
**** LIST END ****
@
:LI,S,1,FCOD1

FTN4,L
      SUBROUTINE COD1(NDEC)
      DIMENSION IA(20),IB(20)
      WRITE(1,100)
100   FORMAT("BASE NUOVO SISTEMA?")
      READ(1,*) IBASE
      DO 105 L=1,20
      IA(L)=0
      IB(L)=0
105   CONTINUE
      K=1
      IF(NDEC-IBASE) 225,210,210
210   INDB=NDEC/IBASE
      IB(K)=NDEC-IBASE*INDB
      IF(INDB-IBASE) 220,215,215
215   NDEC=INDB
      K=K+1
      GOTO 210
220   K=K+1
      IB(K)=INDB
      GOTO227
225   IB(K)=NDEC
227   DO 230 L=1,K
      IU=20+1-L
      IA(IU)=IB(L)
230   CONTINUE
      WRITE(1,300) IBASE,(IA(L),L=20-K+1,20)
300   FORMAT(/,"NUMERO NEL SISTEMA BASE",F5.2,/,20I5,/)
      RETURN
      END
      END$
**** LIST END ****
```

```
:RU,CONV


BASE DEL SISTEMA ?
9
NUMERO DI CIFRE ?
3
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
1
4
6

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
2

NUMERO NEL SISTEMA BASE 2.00
    1    1    1    1    0    1    1


BASE DEL SISTEMA ?
8
NUMERO DI CIFRE ?
3
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
1
7
3

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
7

NUMERO NEL SISTEMA BASE 7.00
    2    3    4


BASE DEL SISTEMA ?
7
NUMERO DI CIFRE ?
3
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
2
3
4

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
6

NUMERO NEL SISTEMA BASE 6.00
    3    2    3
```

```
BASE DEL SISTEMA ?
6
NUMERO DI CIFRE ?
3
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
3
2
3

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
5

NUMERO NEL SISTEMA BASE 5.00
    4    4    3


BASE DEL SISTEMA ?
5
NUMERO DI CIFRE ?
3
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
4
4
3

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
4

NUMERO NEL SISTEMA BASE 4.00
    1    3    2    3


BASE DEL SISTEMA ?
4
NUMERO DI CIFRE ?
4
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
1
3
2
3

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
3

NUMERO NEL SISTEMA BASE 3.00
    1    1    1    2    0
```

```
BASE DEL SISTEMA ?
3
NUMERO DI CIFRE ?
5
SCRIVI LE CIFRE DA SIN.,CIASCUNA SEGUITA DA C.L.
1
1
1
2
0

EQUIV. DECIM. =  123

BASE NUOVO SISTEMA?
2

NUMERO NEL SISTEMA BASE 2.00
    1    1    1    1    0    1    1
```

P1_C1.5 Sistema di numerazione binario naturale

DEF. P1_C1.5.1 Un sistema di numerazione con base B =2 e con regola di codificazione ponderale, si definisce **sistema di numerazione binario naturale.**

Il sistema di numerazione binario naturale, detto anche semplicemente **sistema binario** è un sistema di numerazione di fondamentale importanza per le ragioni che vedremo nei paragrafi successivi.

Le regole di conversione dal sistema binario al sistema decimale, e quelle di conversione dal sistema decimale al sistema binario, si desumono da quelle enunciate nel paragrafo precedente per un sistema a base B qualunque, ponendo $B = 2$.

Esempio P1_C1.5.1 **Trasformare nel sistema decimale i numeri:**

$$(101100100)_2 \;=\; (1 \cdot 256 + 1 \cdot 64 + 1 \cdot 32 + 1 \cdot 4)_{10} \;=\; (356)_{10}$$

$$(1000110011)_2 \;=\; (512 + 32 + 16 + 2 + 1)_{10} \;=\; (563)_{10}$$

$$(10011010010)_2 \;=\; (1024 + 128 + 64 + 16 + 2) \;=\; (1234)_{10}$$

Esempio P1_C1.5.2 **Trasformare nel sistema binario i numeri**

$$\begin{aligned} (24)_{10} &= 12 \cdot 2 + 0 \\ 12 &= 6 \cdot 2 + 0 \\ 6 &= 3 \cdot 2 + 0 \\ 3 &= 1 \cdot 1 + 1 \\ 1 &= 1 \end{aligned} \qquad (24)_{10} = (11000)_2$$

$$\begin{aligned} (764)_{10} &= 382 \cdot 2 + 0 \\ 382 &= 191 \cdot 2 + 0 \\ 191 &= 95 \cdot 2 + 1 \\ 95 &= 47 \cdot 2 + 1 \\ 47 &= 23 \cdot 2 + 1 \\ 23 &= 11 \cdot 2 + 1 \\ 11 &= 5 \cdot 2 + 1 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned} \qquad (764)_{10} = (1011111100)_2$$

Possiamo introdurre le operazioni di **somma, sottrazione, prodotto e divisione** tra numeri in binario.

Introduciamo a tale scopo la:

ARITMETICA BINARIA -

Prendiamo in esame prima il caso di operazioni tra numeri ad una sola cifra

ADDIZIONE

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 0 \quad \textit{con riporto di } 1 \end{aligned}$$

SOTTRAZIONE

$$\begin{aligned} 0 - 0 &= 0 \\ 0 - 1 &= 1 \quad \textit{con prestito di } 1 \\ 1 - 0 &= 1 \\ 1 - 1 &= 0 \end{aligned}$$

PRODOTTO

$$\begin{aligned} 0 \cdot 0 &= 0 \\ 0 \cdot 1 &= 0 \\ 1 \cdot 0 &= 0 \\ 1 \cdot 1 &= 1 \end{aligned}$$

DIVISIONE

$$\begin{array}{ll} 0:0 & non\ definita \\ 0:1=0 & \\ 1:0 & non\ definita \\ 1:1=1 & \end{array}$$

Le regole sono simili a quelle per il sistema decimale.

Prendiamo ora in esame le regole delle quattro operazioni *tra numeri a più cifre e positivi*, rimandando alla letteratura in bibliografia quelle tra numeri con segno.

ADDIZIONE: si esegue come per il sistema decimale, tenendo conto del "riporto".

Esempio P1_C1.5.3 **Eseguire le seguenti somme nel sistema binario:**

$$\begin{array}{ccccccccl} 1 & & 1 & 1 & & 1 & & & \leftarrow Riporto \\ & & & & & & & & \\ & 1 & 0 & 1 & 1 & 0 & 1 & + & \rightarrow (45)_{10} + \\ & & 1 & 1 & 1 & 0 & 1 & = & \rightarrow (29)_{10} = \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 0 & & \rightarrow (74)_{10} \end{array}$$

$$\begin{array}{cccccccccl} 1 & & 1 & 1 & 1 & & & & & \leftarrow Riporto \\ & & & & & & & & & \\ & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \ + & \rightarrow (185)_{10} + \\ & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \ = & \rightarrow (188)_{10} = \\ \hline 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & \rightarrow (373)_{10} \end{array}$$

SOTTRAZIONE: si esegue come per il sistema decimale, tenendo conto dei "prestiti".

Esempio P1_C1.5.4 **Eseguire le seguenti sottrazioni nel sistema binario:**

$$\begin{array}{ccccccccl} 1 & 1 & 1 & 1 & & 1 & & & \leftarrow Prestiti \\ & & & & & & & & \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & + & \rightarrow (74)_{10} + \\ & 1 & 0 & 1 & 1 & 0 & 1 & = & \rightarrow (45)_{10} = \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 & & \rightarrow (29)_{10} \end{array}$$

$$\begin{array}{ccccccccl} 1 & 1 & 1 & 1 & & 1 & & & \leftarrow Prestiti \\ & & & & & & & & \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & + & \rightarrow (74)_{10} + \\ & & 1 & 1 & 1 & 0 & 1 & = & \rightarrow (29)_{10} = \\ \hline 0 & 1 & 0 & 1 & 1 & 0 & 1 & & \rightarrow (45)_{10} \end{array}$$

MOLTIPLICAZIONE: si esegue come per il sistema decimale, tenendo conto delle regole della moltiplicazione e della addizione viste per tali operazioni tra numeri ad una sola cifra.

Esempio P1_C1.5.5 Eseguire le seguenti moltiplicazioni nel sistema binario

$$
\begin{array}{cccccccccc}
 & & 1 & 0 & 1 & 1 & 1 & 0 & \times & \rightarrow (46)_{10}\times \\
 & & & & & & 1 & 1 & = & \rightarrow (3)_{10}= \\
\cline{3-8}\cline{10-10}
 & & 1 & 0 & 1 & 1 & 1 & 0 & & \\
 & 1 & 0 & 1 & 1 & 1 & 0 & - & & \\
\cline{1-8}
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & & \rightarrow (138)_{10} \\
 & & & & & & & & & \\
 & & 1 & 0 & 1 & 1 & 1 & 1 & \times & \rightarrow (47)_{10}\times \\
 & & & & & 1 & 0 & 0 & = & \rightarrow (4)_{10}= \\
\cline{3-8}\cline{10-10}
 & & 0 & 0 & 0 & 0 & 0 & 0 & & \\
 & 0 & 0 & 0 & 0 & 0 & 0 & - & & \\
1 & 0 & 1 & 1 & 1 & 1 & - & & & \\
\cline{1-8}
1 & 0 & 1 & 1 & 1 & 1 & - & & & \rightarrow (188)_{10}
\end{array}
$$

DIVISIONE: si esegue come per il sistema decimale, tenendo conto delle regole della sottrazione e della moltiplicazione viste per tali operazioni tra numeri ad una sola cifra

Esempio P1_C1.5.6 Eseguire le seguenti divisioni nel sistema binario:

$$
\begin{array}{cccccccccccccc}
1 & 0 & \overset{\backslash}{0} & \dot{0} & \dot{1} & \dot{0} & \dot{1} & \dot{0} & \vert 1 & 1 & & & & \\
\cline{9-14}
0 & 1 & 1 & & & & & & 1 & 0 & 1 & 1 & 1 & 0 \\
\cline{1-3}
0 & 0 & 1 & 0 & 1 & & & & & & & & & \\
 & & 0 & 1 & 1 & & & & & & & & & \\
\cline{3-5}
 & & 0 & 1 & 0 & 0 & & & & & & & & \\
 & & & 0 & 1 & 1 & & & & & & & & \\
\cline{4-6}
 & & & 0 & 0 & 1 & 1 & & & & & & & \\
 & & & & & 1 & 1 & & & & & & & \\
\cline{6-8}
 & & & & & 0 & 0 & 0 & & & & & &
\end{array}
$$

$(138)_{10} : (3)_{10} = (46)_{10}$

$$
\begin{array}{ccccccccccccc}
1 & 0 & 0 & \dot{0} & \dot{1} & \dot{0} & \dot{1} & \dot{0} & & & & & \\
 & 1 & 1 & 1 & & & & & & & & & \\
\cline{1-4}
0 & 0 & 0 & 1 & 1 & 0 & 1 & & & & & & \\
 & & & & 1 & 1 & 1 & & & & & & \\
\cline{4-7}
 & & & 0 & 1 & 1 & 0 & 0 & & & & & \\
 & & & & & 1 & 1 & 1 & & & & & \\
\cline{4-8}
 & & & 0 & 1 & 0 & 1 & 0 & & & & & \\
 & & & & & 1 & 1 & 1 & & & & & \\
\cline{4-9}
 & & & 0 & 0 & 1 & 1 & 0 & 0 & & & & \\
 & & & & & & 1 & 1 & 1 & & & & \\
\cline{6-10}
 & & & & & 0 & 1 & 0 & 1 & 0 & & & \\
 & & & & & & & 1 & 1 & 1 & & & \\
\cline{7-10}
 & & & & & & 0 & 0 & 1 & 1 & 0 & 0 & \\
 & & & & & & & & & 1 & 1 & 1 & \\
\cline{9-13}
 & & & & & & & & 0 & 1 & 0 & 1 & 0 \\
 & & & & & & & & & & 1 & 1 & 1 \\
\cline{10-13}
 & & & & & & & & & 0 & 0 & 1 & 1
\end{array}
\qquad
\begin{array}{|l}
1\ 1\ 1 \\
\hline
1\ 0\ 0\ 1\ 1,\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0
\end{array}
$$

$$(138)_{10} : (3)_{10} = (46)_{10}$$

dove :

$(10011, 10110110)_2 = (2^4{+}2^1{+}2^0{+}1.2^{-1}{+}0.2^{-2}{+}1.2^{-3}{+}1.2{-}4{+}0.2^{-5}{+}1.2^{-6}{+}1.2^{-7}{+}0.2^{-8})_{10} = 19,71$

P1_C1.6 Sistema di numerazione binario riflesso

DEF. P1_C1.6.1 Si definisce SISTEMA DI NUMERAZIONE BINARIO RIFLESSO un sistema di numerazione con:

1. base $B = 2$
2. la seguente regola di codificazione:
   - Il peso di ogni $n-esima$ cifra, da destra a sinistra vale (2^{n+1}) in modulo; (per la prima cifra a destra, $n = 0$).
   - Il peso ha segno alterno $(+, -, +, -, \ldots)$ operando da sinistra a destra, qualora si tenga conto solo di quei pesi che corrispondono alle cifre dove compare 1.

Esempio P1_C1.6.1 Trasformare nel sistema decimale i numeri scritti in binario riflesso:

$(1111)_{2R} = (1 \cdot 15 - 1 \cdot 7 + 3 \cdot 1 - 1 \cdot 1)_{10} = (10)_{10}$
$(11000)_{2R} = (1 \cdot 31 - 1 \cdot 15)_{10} = (16)_{10}$
$(1101011101)_{2R} = (1023 - 511 + 127 - 31 + 15 - 7 + 1)_{10} = (1129)_{10}$

Per scrivere un numero decimale nel sistema binario riflesso conviene trasformarlo prima nel sistema binario naturale, poi trasformarlo nel sistema binario riflesso mediante la seguente regola.

Per scrivere nel sistema binario riflesso un numero scritto nel sistema binario naturale, si trascrive da destra a sinistra, cifra per cifra:

- *lo stesso simbolo* (0 *o* 1)*, se la cifra precedente (a sinistra) contiene lo zero.*
- *il complemento del simbolo, se la cifra precedente contiene 1.*

Esempio P1_C1.6.2 Scrivere nel sistema binario riflesso i seguenti numeri decimali

$$
\begin{aligned}
(10)_{10} &= (1010)_2 \\
&| \\
&= (1111)_{2R} \\
(16)_{10} &= (10000)_2 \\
&| \\
&= (11000)_{2R} \\
(1129)_{10} &= (1001101001)_2 \\
&| \\
&= (1101011101)_{2R}
\end{aligned}
$$

Riportiamo ora una tabella in cui compaiono i primi quindici numeri scritti nel sistema binario e accanto, gli stessi numeri scritti nel sistema binario riflesso.

	8	4	2	1	← peso →	15	7	3	1
0	0	0	0	0		0	0	0	0
1	0	0	0	1		0	0	0	1
2	0	0	1	0		0	0	1	1
3	0	0	1	1		0	0	1	0
4	0	1	0	0		0	1	1	0
5	0	1	0	1		0	1	1	1
6	0	1	1	0		0	1	0	1
7	0	1	1	1		0	1	0	0
8	1	0	0	0		1	1	0	0
9	1	0	0	1		1	1	0	1
10	1	0	1	0		1	1	1	1
11	1	0	1	1		1	1	1	0
12	1	1	0	0		1	0	1	0
13	1	1	0	1		1	0	1	1
14	1	1	1	0		1	0	0	1
15	1	1	1	1		1	0	0	0

0110.....
00111100.....
0000111111110000.....
00000000111111111111111100000000...

01......
0011....
00001111....
0000000011111111......

Tale tabella ci permette di fare alcune importanti considerazioni:

Ogni colonna di numeri 0 e 1, corrispondente ad una certa cifra dei sistemi binario naturale e riflesso ha un suo "modulo di ripetitività", che è indicato nella tabella. Ad esempio per la seconda colonna, a peso 2, del sistema binario il modulo è 0011.

Ogni numero scritto nel sistema binario riflesso si ottiene da quello che lo precede o da quello che lo segue variando il simbolo 0 o 1 di una sola cifra.

Considerando ad esempio i numeri a 4 cifre in binario riflesso come *quadruple* ordinate sull'insieme di elementi 0, 1 si può dire che ogni quadrupla si ottiene da quella che la precede o da quella che la segue variando un solo elemento (vedi P1_C1.3).

Questa proprietà del sistema binario riflesso viene chiamata **proprietà di adiacenza**.

P1_C1.7 Codifica della informazione. Codici

Il concetto di **codice** è legato alla teoria della informazione.

Ogniqualvolta si vuole memorizzare o trasferire un MESSAGGIO contenente una informazione, si deve ricorrere ad una rappresentazione formale di tale messaggio.

Ogni metodo di rappresentazione formale di messaggi si chiama CODICE.

È interessante leggere a mo' di esempio di concetto di informazione, messaggio e codice, un passo del volume di Ross Ashby "Introduzione alla Cibernetica".

"*UBIQUITÀ DELLA CODIFICAZIONE. Per avere un'idea della quantità di codificazioni che si hanno durante l'ordinaria interazione tra organismo ed ambiente, considereremo abbasanza dettagliatamente ciò che accade quando un bollettino meteorologico viene diffuso per radio. La sequenza si inizia con un qualche processo strutturato entro i neuroni del meteorologo che viene tradotto in un corrispondente insieme di movimenti muscolari quando egli scrive il testo del bollettino, che diviene quindi una configurazione di segni sulla carta. Il bollettino si traduce in un alternarsi di chiaro e di scuro sulla retina dell'annunciatore, poi, in una configurazione di eccitazione neuronica e quindi in una di impulsi nervosi attraverso il nervo ottico fino alla corteccia cerebrale. Si traduce quindi in un insieme corrispondente di movimenti ben determinati delle labbra e della lingua e viaggia nell'aria sotto forma di un treno d'onde che raggiunge il microfono e si trasforma in una configurazione di variazioni del potenziale elettrico che viene sottoposto ad ulteriori cambiamenti mentre viene amplificato, modulato e diffuso. A questo punto è un treno d'onde elettromagnetiche che diventa una configurazione nel radioricevitore e tradotto di nuovo in un treno d'onde sonore, diviene un insieme di vibrazioni che attraversa i padiglioni auricolari degli ascoltatori, gli ossicini, la coclea e infine, si traduce ancora in una configurazione d'impulsi nervosi che si propagano lungo il nervo acustico. A questo punto possiamo fermarci facendo solo notare che questo resoconto molto breve nomina non meno di sedici trasformazioni principali attraverso ognuna delle quali qualcosa è stato conservato benchè in apparenza tali trasformazioni abbiano reso questo qualcosa quasi irriconoscibile*".

DEF. P1_C1.7.1 Definire un **codice** $\mathcal{C}$ significa fissare:

- un insieme $\mathcal{A}$ di **caratteri (o simboli)** detto **alfabeto** del codice.
- l'insieme $\mathcal{D}$ di tutte le possibili combinazioni di caratteri dell'insieme alfabeto che hanno un significato (PAROLE). Possiamo chiamare l'insieme $\mathcal{D}$ **dizionario** del codice.
- una legge di trasformazione $\mathcal{T}$ **(codifica)** che associa ad ogni elemento di un insieme $\mathcal{O}$ di "oggetti" uno ed un solo elemento del dizionario del codice. La legge di trasformazione $\mathcal{T}$ è in genere una applicazione biiettiva di $\mathcal{O}$ su $\mathcal{D}$.

Se $\mathcal{O}$ è costituito da tutti gli oggetti e da tutti i concetti formulabili dal pensiero umano, il codice $\mathcal{C}$ è un linguaggio e l'operazione di applicazione $\mathcal{T}$ è la **codificazione** del linguaggio.

Un codice si dice **non ambiguo** quando $\mathcal{T}$ è una applicazione biiettiva. In tal caso esiste la trasformazione inversa di $\mathcal{T}$, $\mathcal{T}$ ed essa viene chiamata **decodifica**.

Se la legge di codifica $\mathcal{T}$ di un codice $\mathcal{C}$ di dizionario $\mathcal{D}$ è una applicazione da $\mathcal{D}$ ad $\mathcal{A}_1$, dove $\mathcal{A}_1$ è l'alfabeto d'un codice $\mathcal{C}_1$, il codice $\mathcal{C}$ viene chiamato **cifrario**. Un codice è semantico, un cifrario è visivo o fonetico. Il cosiddetto codice Morse con l'alfebeto $\mathcal{A} = \{\cdot, -\}$ è in realtà un cifrario. Ogni sua parola rappresenta in realtà una lettera dell'alfabeto d'una lingua e non ha un significato in sè stessa. Un codice può essere usato da un SISTEMA (nella accezione da noi data a questa parola nella introduzione) sia a trasferire informazione, sia ad elaborarla, se è in grado di farlo.

Il trasferimento di informazione tra due sistemi che non comunichino mediante lo stesso codice comporta la necessità di una traduzione del messaggio dal codice del primo sistema a quello del secondo e viceversa. Tale operazione viene chiamata **transcodificazione**. L'uomo ha creato un gran numero di codici, sia per le comunicazioni tra uomo e uomo, sia per le comunicazioni tra macchine e uomo, sia per le comunicazioni tra macchine e macchine.

I codici per le comunicazioni tra uomo e uomo posseggono in genere alfabeti con un numero di caratteri talvolta molto elevato (si pensi all'alfabeto cinese, ad es.), il che comporta parole molto compatte. Ciò perchè l'uomo presenta una grande facilità a riconoscere le forme.

I codici invece che l'uomo ha creato per le macchine hanno un numero assai limitato di simboli (nella maggioranza dei casi 2) e tali da essere nettamente differenziati tra loro per il minimo rischio di errore. La ragione di ciò sta nella scarsa capacità delle macchine a riconoscere senza errore forme complesse.

Un sistema di numerazione in base B (vedi P1_C1.3) definisce un codice. Fissato ad esempio un sistema di numerazione in base B, viene fissato il suo insieme di simboli $\mathcal{A}$ $= (0, 1, ...B-1)$ (**alfabeto del codice**). Fissate n cifre, possiamo costruire B^n disposizioni con ripetizioni di classe n con i B elementi dell'insieme $\mathcal{A}$ (vedi appendice A-4), dette **configurazioni** (parole del codice). Fissata una regola ponderale, è fissata la legge di trasformazione $\mathcal{T}$.

Esempio P1_C1.7.1 **Se B=3, n=2 le parole del codice tra loro distinte sono le 3^2 configurazioni:**

0 0	1 0	2 0
0 1	1 1	2 1
0 2	1 2	2 2

La $(B^n) - upla$ di configurazioni può dar luogo a $(B^n)!$ permutazioni, quindi a $(B^n)!$ $(B^n) - uple$ ordinate. Ad ogni $k - mo$ elemento di ognuna di queste $(B^n) - uple$ ordinate si associ il numero naturale k $(k = 0, ..., B^n)$. Ciò vuol dire eseguire una CODIFICAZIONE. Dal momento che $(B^n)!$ è il numero delle $(B^n) - uple$ ordinate, il numero di codificazioni possibile è $(B^n)!$.

Esempio P1_C1.7.2 **Sia $B = 2$, $n = 3$. Il numero di configurazioni (parole del codice) è 8, il numero di $8 - uple$ ordinate possibili è $8!$. Vengono riportati due esempi di codificazione tra parole del codice e i primi 8 numeri naturali**

0	0	0	$\leftrightarrow$	0	0	0	1	$\leftrightarrow$	0
0	0	1	$\leftrightarrow$	1	0	0	0	$\leftrightarrow$	1
0	1	0	$\leftrightarrow$	2	0	1	0	$\leftrightarrow$	2
0	1	1	$\leftrightarrow$	3	0	1	1	$\leftrightarrow$	3
1	0	0	$\leftrightarrow$	4	1	0	0	$\leftrightarrow$	4
1	0	1	$\leftrightarrow$	5	1	0	1	$\leftrightarrow$	5
1	1	0	$\leftrightarrow$	6	1	1	0	$\leftrightarrow$	6
1	1	1	$\leftrightarrow$	7	1	1	1	$\leftrightarrow$	7

Esempio P1_C1.7.3 La regola ponderale fissata per un sistema in base B (vedi P1_C1.3) e che associa ad ogni numero in base B una quantità, e la regola di trasformazione inversa, costituiscono una regola di CODIFICA e DECODIFICA. Tale codifica associa ad ognuna delle infinite parole del codice un numero naturale e viceversa.

Esempio P1_C1.7.4 L'alfabeto del sistema decimale è l'insieme $\mathcal{A} = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$. Le PAROLE del codice sono tutte le possibili configurazioni ad $n(n = 1, .., \infty)$ cifre ottenute mediante i 10 simboli elementi di $\mathcal{A}$.

P1_C1.8 Il codice BCD (Binary-Coded Decimal)

Hanno notevole importanza quei codici con simboli legati al sistema di numerazione binario e che si propongono di rappresentare i numeri decimali codificandone le cifre indipendentemente le une dalle altre.

Uno dei più importanti fra questi è il codice BCD. I dieci simboli del codice decimale sono associati a 10 delle 16 possibili configurazioni a 4 cifre del codice binario nel modo seguente :

$$\begin{array}{cccccc}
0 & 0 & 0 & 0 & \leftrightarrow & 0 \\
0 & 0 & 0 & 1 & \leftrightarrow & 1 \\
0 & 0 & 1 & 0 & \leftrightarrow & 2 \\
0 & 0 & 1 & 1 & \leftrightarrow & 3 \\
0 & 1 & 0 & 0 & \leftrightarrow & 4 \\
0 & 1 & 0 & 1 & \leftrightarrow & 5 \\
0 & 1 & 1 & 0 & \leftrightarrow & 6 \\
0 & 1 & 1 & 1 & \leftrightarrow & 7 \\
1 & 0 & 0 & 0 & \leftrightarrow & 8 \\
1 & 0 & 0 & 1 & \leftrightarrow & 9
\end{array}$$

L'insieme delle 10 configurazioni di tabella costituisce l'alfabeto del CODICE BCD; mediante le parole di tale codice possono essere rappresentati tutti i numeri decimali.

Esempio P1_C1.8.1 Rappresentare in codice BCD, i numeri decimali 4, 15, 92, 153.

$$\begin{array}{rcccccccccccc}
4 & 0 & 1 & 0 & 0 \\
15 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
92 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
153 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1
\end{array}$$

P1_C1.9 Importanza del sistema di numerazione binario

L'importanza del sistema di numerazione binario naturale è fondamentale per la realizzazione di macchine calcolatrici elettroniche. Infatti ogni numero binario ad n cifre è rappresentato da una successione ordinata di zeri o di uni. Se associamo ad ogni cifra un filo (o un terminale di un circuito) che possa assumere due stati di tensione, ed associamo, ad uno di questi stati lo zero e all'altro l'uno, possiamo, tramite gli n fili, rappresentare un numero qualsiasi ad n cifre, espresso in codice binario.

Esempio P1_C1.9.1 Ai 4 morsetti della scatola nera compaiono le tensioni segnate in figura: associando l'elemento 0 alla tensione V=0 Volt, l'elemento 1 alla tensione V=5 Volt, leggere il numero in binario associato ai quattro morsetti.

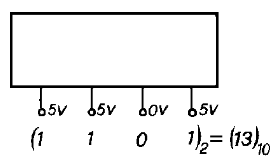


Figura P1_C1.9.1

Abbiamo parlato di associare ad ogni cifra un filo che può presentare due stati di tensione. Questa non è che una possibilità (elettronica) per esprimere un numero binario. Si può associare ad ogni cifra il terminale di uscita di un qualsiasi dispositivo fisico (a fluido magnetico, superconduttivo, ecc., vedi bibliogr.(9)(10)), che abbia la possibilità di assumere due strati distinti. Ma ritorniamo nell'ambito dell'elettronica. Abbiamo visto che, nel sistema binario si possono eseguire le quattro operazioni tra due numeri e che il risultato è, in decimale, il numero che si otterrebbe eseguendo la corrispondente operazione, tra i due numeri, nel sistema decimale. Possiamo quindi pensare di costruire circuiti elettronici con ingressi ed uscite a due stati logici che eseguano le operazioni fra numeri in binario. I circuiti elettronici infatti, che assumono due stati all'uscita e che siano pilotati da due stati di tensione (0V, 5V ad esempio), sono di gran lunga più affidabili di quanto non siano circuiti che assumano più stati di tensione discreti o addirittura stati di tensione continui "analogici". I due stati di tensione possono esser compresi tra due fascie di tolleranza abbastanza ampia di tensioni, naturalmente separate da una fascia di interdizione. Tali circuiti elettronici si chiamano **circuiti elettronici a scatto** o **circuiti elettronici logici.** essi sono basati generalmente sul funzionamento ON/OFF dei transistori.

Parte 1

Capitolo 1

Parte B. Algebra di Boole

P1_C1.10 Introduzione. Necessità di un'algebra

Supponiamo ora di voler eseguire il prodotto di due numeri qualsiasi C e D, ad una sola cifra, scritti nel sistema binario mediante un qualche dispositivo fisico basato sulla possibilità di avere ingressi ed uscite a due stati. Un blocco logico di questo tipo deve eseguire il prodotto come definito in P1_C1.5, qualsiasi siano i valori di C e D. Questi, a coppie, possono assumere i valori riportati in tabella. A fianco, nella tabella, viene riportato il valore del prodotto E relativo a ciascuna delle 4 possibili coppie di valori che i numeri C e D possono assumere.

C	D	E
0	0	0
0	1	0
1	0	0
1	1	1

Tabella P1_C1.10.1

Il sistema logico quindi che esegue il prodotto $C \cdot D$ deve, ad ogni coppia di valori C,D agli ingressi, dare in uscita il corrispondente valore E. Supponiamo di voler associare agli stati di C,D,E due tensioni elettriche, ad esempio la tensione zero allo stato 0 e la tensione V allo stato 1. Supponiamo di voler adoperare come dispositivo fisico fondamentale di commutazione il relais: questo è un dispositivo che:

- chiude il contatto di un interruttore quando al suo ingresso è presente una tensione,

Figura P1_C1.10.1

- mentre tiene questo contatto normalmente aperto quando al suo ingresso non c'è tensione.

Per semplicità rappresenteremo graficamente il relais con un interruttore ed un simbolo C,D,... che rappresenta l'ingresso al dispositivo e che, se assume il valore 1 (tensione V all'ingresso) fa chiudere l'interruttore, se assume il valore 0 (tensione 0 all'ingresso) fa aprire l'interruttore. Ma veniamo ora alla realizzazione pratica del nostro blocco logico moltiplicatore. Utilizzando i relais definiti sopra, un blocco logico che realizzi le condizioni della tabella P1_C1.10.1 (che potremo definire tabella del comportamento del blocco), è quello disegnato in figura P1_C1.10.2.

Figura P1_C1.10.2

Infatti, ai capi dei terminali d'uscita E c'è tensione V se e soltanto se, contemporaneamente, C=1, D=1 e quindi i contatti sono chiusi.

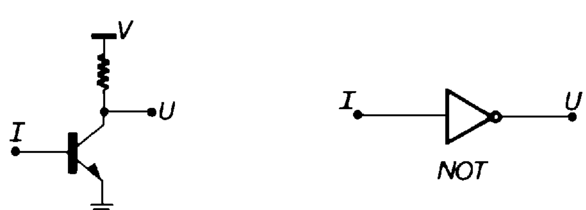


Figura P1_C1.10.3

Questo è uno dei blocchi logici fondamentali e si chiama blocco AND (nel nostro caso a 2 ingressi) ed è indicato dal simbolo in fig. P1_C1.10.2. Supponiamo ora, sempre restando nella interpretazione elettrica degli stati logici, di scegliere come elemento fondamentale di commutazione il transistore, nelle sue condizioni di funzionamento **ON-OFF**, che schematizzeremo come in figura P1_C1.10.3, trascurando la rete di polarizzazione. Una tensione V (nel nostro caso positiva) all'ingresso I (stato 1 dell'ingresso) porta l'uscita ad una tensione 0 V (stato 0 dell'uscita).

Più in generale, un certo stato di ingresso provoca lo stato opposto all'uscita. Questo elemento fondamentale si chiama **invertitore** e si indica con il simbolo logico in fig. P1_C1.10.3, chiamato **NOT**.

Un blocco logico a transistori che realizzi la condizione della tabella P1_C1.10.1 è quello in fig. P1_C1.10.4.

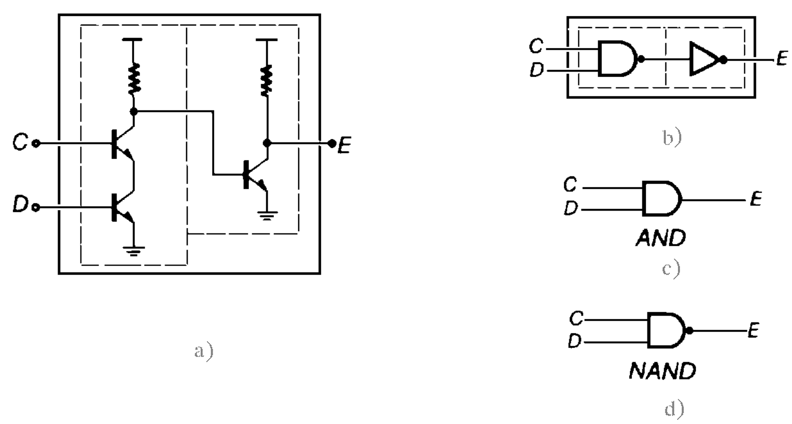


Figura P1_C1.10.4

Notiamo che il primo blocco tratteggiato è costituito da due blocchi invertitori in serie e realizza la tabella P1_C1.10.2, che ha i valori di E complementati rispetto a quelli della tabella P1_C1.10.1 da realizzare.

C	D	E
0	0	1
0	1	1
1	0	1
1	1	0

Tabella P1_C1.10.2

Esso è un blocco logico **AND complementato**, o **NAND (=NOT AND)**, il cui simbolo è indicato accanto (si differenzia dal simbolo dell'AND per il pallino all'uscita, simbolo di inversione o di complemento). Il secondo blocco tratteggiato è un invertitore (NOT) che, connesso all'uscita del primo blocco NAND, realizza il blocco (composto) AND. Il circuito dunque di fig. P1_C1.10.4 esegue il prodotto, secondo le definizioni della tabella P1_C1.10.1 di due numeri binari qualunque C e D. Infatti, il numero prodotto E è nello stesso stato logico 1 se e soltanto se ambedue C e D sono nello stato logico 1.

Supponiamo ora di voler eseguire la somma senza riporto di due numeri qualsiasi C e D, ad una cifra, scritti nel sistema binario, mediante un qualche blocco logico basato sulla possibilità di avere ingressi e uscite a due stati.

Un blocco logico di questo tipo deve eseguire la somma come definito in P1_C1.5, con l'unica differenza che 1+1=1, cioè deve soddisfare la tabella P1_C1.10.3

C	D	E
0	0	0
0	1	1
1	0	1
1	1	1

Tabella P1_C1.10.3

Adoperando una logica a relais, possiamo realizzare un addizionatore mediante lo schema di fig. P1_C1.10.5.

Figura P1_C1.10.5

Ai capi dei terminali d'uscita E infatti c'è una tensione V se C oppure D, oppure entrambi sono nello stato 1.

Un blocco logico che realizzi la tabella P1_C1.10.3 è un altro blocco logico fondamentale chiamato OR (nel nostro caso a due ingressi) ed è indicato dal simbolo in fig. P1_C1.10.5 b). Adoperando una logica a transistori invece che a relais, un blocco logico OR è realizzabile mediante lo schema in fig. P1_C1.10.6 a).

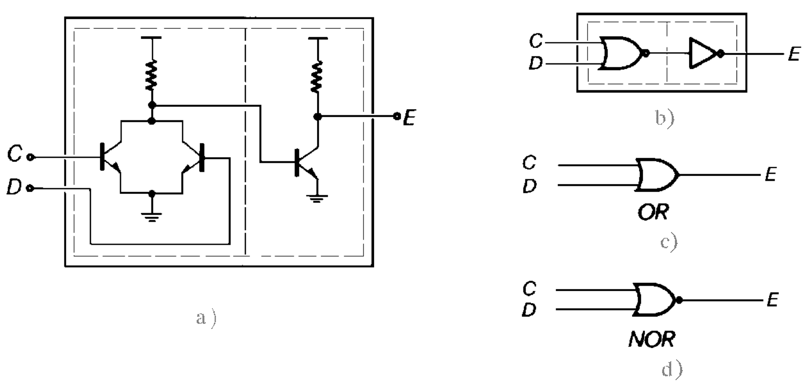


Figura P1_C1.10.6

Il primo circuito entro il tratteggio è un circuito che realizza la tabella P1_C1.10.4, la quale ha i valori di E complementati rispetto a quelli della tabella P1_C1.10.3 relativa alla operazione di somma.

C	D	E
0	0	1
0	1	0
1	0	0
1	1	0

Tabella P1_C1.10.4

Una tale tabella rappresenta il comportamento di un blocco logico chiamato **OR complementato** o **NOR (=NOT OR)**, ed il cui simbolo si differenzia da quello dell'OR per il pallino nero all'uscita che indica una complementazione dell'uscita stessa (figura P1_C1.10.7 b). Il secondo blocco entro il tratteggio è un invertitore (NOT) che, connesso all'uscita del primo blocco NOR forma il blocco composto OR che realizza la tabella P1_C1.10.3. I blocchi logici NOT, AND, OR sono blocchi fondamentali con cui si possono realizzare blocchi più complessi.

Notiamo esplicitamente che abbiamo sempre parlato di blocchi logici, di simboli:

Figura P1_C1.10.7

ed abbiamo parlato di circuiti solo come un esempio di materializzazione di tali blocchi. In realtà infatti i blocchi logici possono essere realizzati con elementi fondamentali non elettronici, purchè questi siano elementi che assumono due stati soltanto qualora sollecitati da ingressi a due soli valori. Notiamo che si possono rappresentare blocchi OR o AND ad un numero di ingressi superiore a 2 aggiungendo elementi fondamentali, in parallelo o, rispettivamente, in serie ai due dell'OR o dell'AND a 2 ingressi.

Mettiamo ora in evidenza una metodologia fondamentale comune ai due esempi precedenti. Ci siamo in essi proposti di realizzare un blocco logico che soddisfasse a certe condizioni la cui descrizione era contenuta in una tabella (vedi tabella P1_C1.10.1 e tabella P1_C1.10.3).

Scelto poi un elemento fondamentale fisico con comportamento binario (vedi relais o transistore), mediante un ragionamento intuitivo basato sulla tabella, abbiamo realizzato il blocco logico che la soddisfa.

Procediamo ora con un altro esempio: supponiamo di porci il problema che si pone ad un elettricista che deve collegare ad una lampada, due interruttori i quali devono accendere e spegnere la lampada indipendentemente. Scriviamo come prima cosa le condizioni cui deve soddisfare il blocco logico. A e B siano le variabili associate agli interruttori, L sia la variabile dipendente d'uscita. Le condizioni sono contenute nella tabella P1_C1.10.5.

A	B	L
0	0	0
0	1	1
1	0	1
1	1	0

Tabella P1_C1.10.5

La lampada deve essere accesa quando uno degli interruttori è chiuso e l'altro aperto, deve essere spenta quando ambedue sono aperti, deve essere spenta anche quando ambedue gli interruttori sono chiusi (altrimenti la lampada non si spegnerebbe più, a meno di non aprirli entrambi contemporaneamente). Risolvendo il problema in modo generale, cioè con blocchi AND, OR, NOT, si ottiene lo schema in fig. P1_C1.10.8.

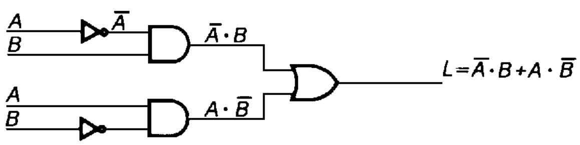


figura P1_C1.10.8:

Chiamando $\bar{A}$ e $\bar{B}$ i complementi di A e di B ($\bar{A}$ =0 quando A=1, $\bar{A}$ =1 quando A=0), si può interpretare il comportamento dello schema in fig. P1_C1.10.8 mediante l'equazione:

$$L = \bar{A} \cdot B + A \cdot \bar{B}$$

Da quest'ultima si può vedere che:
L=1 quando:

A=0($\bar{A}$ =1) e B=1   OPPURE   A=1 e B=0 ($\bar{B}$ =1)

mentre L=0 quando:

A=0($\bar{A}$ =1) e B=0   OPPURE   A=1 e B=1 ($\bar{B}$ =0)

Notiamo che il nostro elettricista, per risolvere il problema dovrà montare due commutatori come in fig. P1_C1.10.9

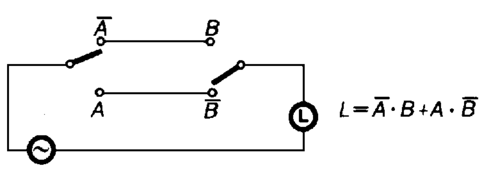


figura P1_C1.10.9:

e chiamare:

- A uno dei contatti mobili del primo com mutatore, $\bar{A}$ l'altro;
- B uno dei contatti mobili del secondo commutatore, $\bar{B}$ l'altro.

Alla fine l'elettricista avrà realizzato uno schema che realizza la equazione:

$$L = \bar{A} \cdot B + A \cdot \bar{B}$$

Tiriamo ora una importante conclusione. In tutti e tre gli esempi abbiamo realizzato un blocco logico con due ingressi ed una uscita, che in funzione degli ingressi (VARIABILI INDIPENDENTI A e B) fornisce una uscita (VARIABILE DIPENDENTE).

Abbiamo risolto intuitivamente questi tre problemi solo perchè la loro semplicità e il loro numero esiguo di ingressi (2) e di uscite (1) ce lo ha consentito.

Ma se il numero di ingressi e di uscite aumentano, i metodi intuitivi non ci sorreggono più. Si sente perciò l'esigenza di un metodo sistematico che ci permetta di risolvere sistemi logici più complessi; di un metodo, ad esempio, che ci permetta di esprimere la tabella delle condizioni mediante una relazione algebrica tra le variabili indipendenti e le variabili dipendenti, relazione algebrica che può essere materializzata mediante combinazioni dei tre blocchi logici fondamentali AND, OR, NOT.

Un metodo che ci permetta tutto ciò, ci è fornito dalla **algebra di Boole**.

P1_C1.11 Algebra di Boole. Generalità

L'Algebra di Boole[1] nasce con la pubblicazione, nel 1854 dell'opera di George Boole intitolata: AN INVESTIGATION OF THE LAWS OF THOUGHT ON WHICH ARE FOUNDED THE MATHEMATICAL THEORIES OF LOGIC AND PROBABILITIES. (vedi Bibl.(2),(1)).

Per capire il contenuto e la finalità di quest'opera, basta leggerne il primo capoverso del capitolo primo:

" NATURA E SCOPO DI QUEST'OPERA. Lo scopo del seguente trattato è di indagare sulle leggi fondamentali di quelle operazioni della mente umana mediante le quali vengono formulati i ragionamenti;

dare a queste una espressione nel linguaggio simbolico del calcolo e in queste basi fondare la scienza della logica e costruirne il metodo; fare di questo stesso metodo le basi di un metodo generale per l'applicazione della dottrina matematica delle probabilità;

e, infine, mettere insieme, dai vari elementi di verità portati alla luce nel corso di questa analisi, alcune probabili idee sulla costituzione e la natura della mente umana".

Nei primi 12 dei 24 capitoli del suo volume, Boole costruisce, con eccezionale chiarezza, l'algebra delle proposizioni logiche; nei capitoli dal 13-esimo al 15-esimo dà una rappresentazione algebrica di una parte dell'opera di Clarke "Demonstration of the being and attributes of God", di una parte dell'opera di Spinoza "Ethica ordine geometrico demonstrata" e di una parte della logica aristotelica.

Nei capitoli 16-21, Boole prende in esame la teoria del calcolo delle probabilità e le relazioni di causa-effetto. Nell'ultimo capitolo, dal titolo ON THE NATURE OF SCIENCE AND THE CONSTITUTION OF INTELLECT, Boole indaga su quelli che sono i rapporti fra la scienza come prodotto dell'intelletto umano e l'intelletto stesso.

[1] G. Boole (1815-1864), professore di matematica al Queen's College, Cork.

L'algebra di Boole è basata su un insieme di due elementi, il VERO (simbolo 1), il FALSO (simbolo 0), stati questi delle proposizioni logiche che quest'algebra analizza.

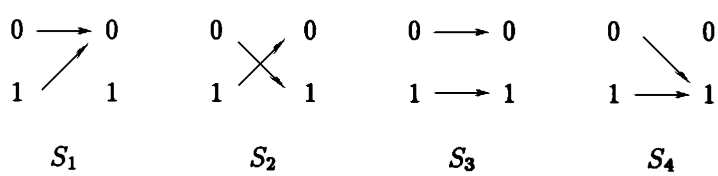
Questa teoria rimase a lungo applicata solo nell'ambito della logica finchè nel 1938 **Claude Shannon** (4) non l'applicò allo studio dei circuiti di commutazione. Da quel momento essa è diventata lo strumento essenziale per lo studio dei sistemi digitali.

L'idea della applicazione dell'Algebra di Boole alla elettronica digitale consiste nell'associare ai suoi elementi 0 ed 1 l'apertura e la chiusura di un contatto o la assenza e la presenza di una tensione ai capi di un filo o ai terminali di un circuito a scatto.

In tal modo, con l'ausilio di questo potente strumento matematico, possono essere analizzati e sintetizzati i più complessi sistemi digitali combinatori e sequenziali.

P1_C1.12 Operazioni su un solo elemento dell'insieme 0,1 (operazioni unarie)

Cercheremo, nel presente e nel successivo paragrafo quante e quali sono le possibili operazioni (e le loro proprietà) unarie e binarie sugli elementi dell'insieme B={0,1}, che chiameremo, per convenzione, insieme di Boole. Ogni operazione unaria sugli elementi dell'insieme B={0,1} è una applicazione da B a B. Il numero quindi di queste possibili operazioni è $2^2 = 4$, pari al numero delle disposizioni con ripetizioni di classe 2 costruibili con i 2 elementi di B={0,1}. Ciascuna delle operazioni e quindi ciascuno degli operatori associati S_i, sono definiti da una delle quattro applicazioni:



Chiamando X una entità che può assumere solamente i valori 0,1, possiamo rappresentare sinteticamente le 4 operazioni unarie mediante la tabella che segue.

X	$S_1(X)$	$S_2(X)$	$S_3(X)$	$S_4(X)$
0	0	1	0	1
1	0	0	1	1

S_1 trasforma ogni elemento nell'elemento 0	$S_1(X) = 0$
S_2 trasforma ogni elemento nel suo complemento	$S_2(X) = X$
S_3 trasforma ogni elemento in sè stesso	$S_3(X) = X$
S_4 trasforma ogni elemento nell'elemento 1	$S_4(X) = 1$

DEF. P1_C1.12.1 Definiamo l'operatore S_2 **operatore di inversione** o **complementazione** e l'elemento X, ottenuto applicando S_2 all'elemento X, l'**inverso** di X o il **complemento** di X.

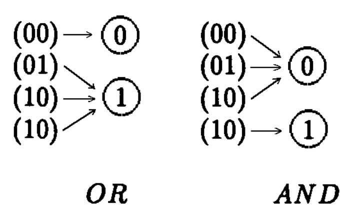
P1_C1.13 Operazioni su due elementi dell'insieme {0,1} (operazioni binarie)

Vediamo ora quante e quali operazioni binarie si possono definire sugli elementi dell'insieme B= { 0,1 }. Una operazione binaria associa ad ogni coppia ordinata di valori (0,1) un elemento dell'insieme B. È cioè una applicazione da B^2 a B, dove:

$$B^2 = \{0,1\}^2 = (0,0),(0,1),(1,0),(1,1)$$

Il numero di tutte le applicazioni possibili da B^2 a B è $(2^2)^2 = 16$, pari al numero delle disposizioni con ripetizioni a 4 o 4 che si possano ottenere con i 2 elementi di B={0,1}.

Esempio P1_C1.13.1 **Rappresentiamo graficamente due delle 16 operazioni binarie possibili**



Chiamando ora X_1 e X_2 due entità che possono assumere solamente i valori 0,1, possiamo rappresentare le 16 operazioni binarie $O_i (i = 0, ..., 15)$ in modo sintetico mediante la tabella di figura P1_C1.13.1.

X_1	X_2	OPERAZIONI															
		O_0	O_1	O_2	O_3	O_4	O_5	O_6	O_7	O_8	O_9	O_{10}	O_{11}	O_{12}	O_{13}	O_{14}	O_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
Simboli		0	$X_1 \cdot X_2$	$X_1 \cdot \overline{X_2}$ $X_1 (X_2$	X_1	$\overline{X_1} \cdot X_2$ $X_1) X_2$	X_2	$X \oplus X_2$	$X_1 + X_2$	$\overline{X_1 + X_2}$ op $X_1 \downarrow X_2$	$\overline{X_1 \oplus X_2}$ op $X_1 \odot X_2$	$\overline{X_2}$	$\overline{X_1 \cdot X_2}$ op $X_1 \leftarrow X_2$	$\overline{X_1}$	$\overline{X_1 \cdot X_2}$ op $X_1 \rightarrow X_2$	$\overline{X_1 \cdot X_2}$ op $X_1 \mid X_2$	1
Nomi delle operazioni		ZERO	AND	INIBIZIONE 1	X_1	INIBIZIONE 2	X_2	OR ESCLUSIVO	OR	NOR	AND ESCLUSIVO	$\overline{X_2}$	IMPLICAZIONE 1	$\overline{X_1}$	IMPLICAZIONE 2	NAND	UNITÀ

Figura P1_C1.13.1

Nella tabella di figura P1_C1.13.1 vengono anche associati, ad ogni operazione O_i, i simboli ed i nomi più usati nella letteratura.

Esempio P1_C1.13.2 L'operazione AND, tra due elementi di B, x_1, x_2, di simbolo

$$x_1 \cdot x_2$$

comporta come risultato:

$$\begin{array}{llll} 0 & se & x_1 = 0 & x_2 = 0 \\ 0 & se & x_1 = 0 & x_2 = 1 \\ 0 & se & x_1 = 1 & x_2 = 0 \\ 1 & se & x_1 = 1 & x_2 = 1 \end{array}$$

La tabella di figura P1_C1.13.1 non ha bisogno di commento. L'unica osservazione da fare è che le ultime otto operazioni $(O_8, \ldots, O_{15})$ forniscono risultati complementari rispetto a quelli delle prime otto $(O_0, \ldots, O_7)$ secondo la:

$$O_{15-i} = \overline{O_i} \qquad (i = 0, \ldots, 15)$$

Le operazioni O_0 e O_{16} portano ad un risultato indipendente dalle due variabili tra cui avviene l'operazione. Le operazioni O_3, O_5, O_{10}, O_{12} conducono invece a risultati che dipendono da una sola delle variabili. Le proprietà (vedi App. B-6) delle operazioni O_1, O_7, O_6, O_9, O_8, O_{14}, O_2, O_4, O_{11}, O_{13} sono mostrate nelle tabelle seguenti.

	OR $(+)$	AND $(\cdot)$
ASSOC.	$x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$	$x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2)x_3$
COMMUT.	$x_1 + x_2 = x_2 + x_1$	$x_1 \cdot x_2 = x_2 \cdot x_1$
IDEMP.	$x_1 + x_1 = x_1$	$x_1 \cdot x_1 = x_1$
DISTR.	$x_1 + (x_2 \cdot x_3) = (x_l + x_2) + (x_1 + x_3)$	$x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$
ASSORB.	$x_1 + (x_1 \cdot x_2) = x_1$	$x_1 \cdot (x_1 + x_2) = x_1$
EL. NEU.	0	1

	OR ESC. $(\oplus)$	*AND ESC.* $(\odot)$
ASSOC.	$x_1 \oplus (x_2 \oplus x_3) = (x_1 \oplus x_2) \oplus x_3$	$x_1 \odot (x_2 \odot x_3) = (x_1 \odot x_2) \odot x_3$
COMMUT.	$x_1 \oplus x_2 =_x 2 \oplus x_l$	$x_1 \oplus x_2 = x_2 \oplus x_1$
IDEMP.		
DISTR.		
ASSORB.		
EL. NEU.	0	1

	NOR $(\downarrow)$	*NAND* $(\vert)$
ASSOC.		
COMMUT.	$x_1 \downarrow x_2 = x_2 \downarrow x_1$	$x_1 \mid x_2 = x_2 \mid x_1$
IDEMP.		
DISTR.		
ASSORB.		
EL. NEU.		

	INIBIZIONE $(x_1 \cdot \bar{x_2})$ $(x_1 \overset{/}{\vert} x_2)$	*INIBIZIONE* $(x_1 \cdot x_2)$ $(x_1 \overset{\backslash}{\vert} x_2)$
ASSOC.		
COMMUT.		
IDEMP.		
DISTR.		$x_1 \overset{\backslash}{\vert} (x_2 \overset{/}{\vert} x_3) = (x_2 \overset{\backslash}{\vert} x_2) \overset{/}{\vert} (x_1 \overset{\backslash}{\vert} x_3)$
ASSORB.	$x_1 \overset{/}{\vert} (x_1 \overset{\backslash}{\vert} x_2) = x_1$	
EL. NEU.	0	

	IMPLICAZIONE $(x_1 \leftarrow x_2)$	*IMPLICAZIONE* $(x_1 \rightarrow x_2)$
ASSOC.		
COMMUT.		
IDEMP.		
DISTR.		
ASSORB.	$x_1 \leftarrow (x_1 \rightarrow x_2) = x_1$	
EL. NEU.	1	

P1_C1.14 Strutture algebriche sull'insieme di elementi (0,1)

Riportiamo in questo paragrafo alcune possibili strutture algebriche sull'insieme booleano E di elementi (0,1).

Ciò sia perchè è importante avere una visione più vasta della collocazione dell'algebra di Boole nell'ambito dell'Algebra moderna, sia perchè quest'ultima è, nella sua eleganza formale, talmente semplice da non richiedere, almeno nel nostro caso, nozioni di matematica più approfondite di quelle date dal biennio propedeutico.

Per una più chiara comprensione dei concetti matematici richiamati nel paragrafo, si è riportata in Appendice B una sintesi di quelle parti dell'Algebra moderna che hanno attinenza con l'argomento del paragrafo stesso.

Tutto ciò non è strettamente necessario per la comprensione dell'algebra di Boole e quindi della logica combinatoria e sequenziale, in quanto l'algebra di Boole può essere costruita semplicemente partendo da un certo numero di assiomi. Perciò si consiglia al lettore che durasse fatica alla lettura del paragrafo successivo, di passare al paragrafo P1_C1.18 dove l'algebra booleana è costruita per postulati.

P1_C1.15 Gruppi, campi e reticoli sull'insieme di Boole

Ricordiamo che, dato un insieme $\mathcal{E}$, definire alcune operazioni su quell'insieme e definire alcune proprietà di quelle operazioni significa definire una **struttura algebrica** (vedi App. B.10). Vediamo quali strutture algebriche si possono costruire con il nostro insieme $\mathcal{E}$ dotato dei due soli elementi (0 e 1) e delle 16 operazioni possibili tra i due elementi dell'insieme.

P1_C1.15.1 Struttura algebrica sull'insieme di Boole come gruppo abeliano $(\mathcal{E}, \oplus)$, $(\mathcal{E}, \odot)$

Ricordando che un **gruppo abeliano** è una struttura algebrica $(\mathcal{G}; *)$ in cui l'operazione * è associativa e commutativa, in cui esiste un elemento neutro, ed ogni elemento dell'insieme $\mathcal{G}$ ha il suo simmetrico (vedi Appendice B,16),

possiamo concludere che l'insieme binario $\mathcal{E}$ di elementi $\{0, 1\}$ e l'operazione $\oplus$ formano un gruppo abeliano $(\mathcal{E}, \oplus)$.

Infatti l'operazione $\oplus$ è commutativa e associativa, inoltre ammette come elemento neutro lo 0. Ogni elemento dell'insieme $\mathcal{E}$ poi, ha il suo simmetrico, ricavato dalle:

$$\begin{array}{lll} 0 \oplus 0' = 0 & \rightarrow 0' = 0 & \{0 \oplus 0 = 0 \\ 1 \oplus 1' = 0 & \rightarrow 1' = 1 & \{1 \oplus 1 = 0 \end{array}$$

da dove si desume che gli elementi simmetrici dell'insieme sono gli elementi stessi, visto che $0 = 0 \oplus 0, \quad 0 = 1 \oplus 1$.

Possiamo anche concludere però che anche l'insieme $\mathcal{E}$ binario di elementi 0,1 e l'operatore $\odot$ formano un gruppo abeliano $(\mathcal{E}; \odot)$.

Infatti anche l'operazione $\odot$ è commutativa e associativa e ammette come elemento neutro 1. Ogni elemento dell'insieme $\mathcal{E}$ ha quindi il suo simmetrico che è sè stesso, come si vede dalle:

$$\begin{array}{lll} 0 \odot 0' = 1 & \to 0' = 0 & \{0 \odot 0 = 1 \\ 1 \odot 1' = 1 & \to 1' = 1 & \{1 \odot 1 = 1 \end{array}$$

ricordando che $1 = 0 \odot 0, \quad 1 = 1 \odot 1$.

Esempio P1_C1.15.1 Dimostrare che $(\mathcal{E};+)$ e $(\mathcal{E};\cdot)$ non sono gruppi. Notiamo che, scegliendo come operazione * l'operazione AND o la operazione OR non si potrebbe costruire un gruppo. Infatti l'operazione OR ha come elemento neutro t=0. Infatti dalla definizione

$$0 + t = 0 \qquad \to t = 0$$

$$1 + t = 1 \qquad \to t = 0$$

Vediamo ora quali sono gli elementi simmetrici di 0 ed 1: dalla definizione:

$$0 + 0' = t = 0$$

$$1 + 1' = t = 0$$

Dalla seconda relazione si vede che nessun elemento dell'insieme può essere il simmetrico di 1. Non esiste il simmetrico di 1 rispetto alla operazione OR, ergo la struttura $(\mathcal{E};+)$ non è un gruppo. Considerando ora l'operazione AND, che ha come elemento neutro t=1. Con ragionamento analogo al precedente possiamo vedere che l'insieme $\mathcal{E}$ non possiede il simmetrico di 0, ergo $(\mathcal{E};\cdot)$ non è un gruppo.

P1_C1.15.2 Struttura algebrica sull'insieme di Boole come corpo di Galois: $(\mathcal{E};\oplus,\cdot)$ oppure $(\mathcal{E};\oplus,+)$

> Ricordando ora che un **corpo** è una struttura algebrica $(\mathcal{K};+,-)$ che è un gruppo abeliano rispetto alla operazione + su $\mathcal{K}$, mentre è un gruppo rispetto alla operazione $\cdot$ su $\mathcal{K}$- $\{0\}$, dove $\{0\}$ è l'elemento neutro della operazione + (vedi App. B.19),
> **possiamo dire che l'insieme binario $\mathcal{E}$ di elementi 0,1 e le operazioni $\oplus$ e $\cdot$ (AND) formano un corpo di Galois $(\mathcal{E};\oplus,\cdot)$.**

Infatti le operazioni $\oplus$ ed $\cdot$ sono ambedue associative e commutative (la proprietà commutativa per l'operazione $\cdot$ non è richiesta per un corpo; la sua esistenza fa trasformare il corpo in un corpo commutativo).

Esiste l'elemento neutro $t_{\oplus} = 0$ rispetto all'operazione $\oplus$ in $\mathcal{E}$ e l'elemento neutro $t_{\odot} = 1$ rispetto all'operazione in $\mathcal{E}$-$\{0\}$=$\{1\}$.

Esistono gli elementi simmetrici rispetto all'operazione $\cdot$ in $\mathcal{E}$-$\{0\}$ (l'elemento simmetrico dell'elemento 1 è l'uno stesso).

Ne deduciamo che $(\mathcal{E};\oplus)$ è un corpo commutativo e finito. È un **corpo di Galois** .

Possiamo anche dire che l'insieme binario $\mathcal{E}$ di elementi 0,1 e le operazioni $\oplus$ e +(OR) formano un corpo di Galois $(\mathcal{E};\oplus,+)$.

Infatti le operazioni $\oplus$ e $+$ sono ambedue associative e commutative. Esiste l'elemento neutro $t_\odot = 1$ rispetto all'operazione $\odot$ e l'elemento neutro $t_+ = 0$ rispetto all'operazione $+$.

Esistono gli elementi simmetrici rispetto all'operazione $\odot$; essi sono gli elementi stessi di $\mathcal{E}$. Esiste l'elemento simmetrico dell'unico elemento (0) dell'insieme $\mathcal{E}$-$\{1\}$ rispetto alla operazione $+$, che è lo zero stesso. Il corpo poi è finito.

Si può vedere, a titolo di esempio, come la struttura $(\mathcal{E},\mathcal{OR},\mathcal{AND}) = (\mathcal{E};+,\cdot)$ non possa essere un corpo. Pur essendo infatti rispettate le condizioni sulle proprietà delle operazioni imposte dalla struttura di gruppo, l'insieme $\mathcal{E}$, rispetto alla operazione $+$ (di elemento neutro 0) non possiede il simmetrico dell'elemento 1. Difatti $1 + 1' = 0$ non possiede nessuna soluzione $1' \in \mathcal{E}$.

P1_C1.15.3 Struttura algebrica sull'insieme di Boole come reticolo $(\mathcal{E};+,\cdot)$.

Ricordando ora che un **reticolo** è una struttura algebrica $(R;\triangle,\nabla)$ costituita da un insieme R sul quale siano definite due operazioni interne $\triangle$, e ∇ che godono delle proprietà associativa, commutativa, di idempotenza e di assorbimento (vedi appendice B.10)

possiamo dire che l'insieme binario $\mathcal{E}$ di elementi $\{0,1\}$ e le operazioni $\triangle = OR$ e $\nabla = AND$ formano un reticolo e in più che il reticolo è **completo, complementato e distributivo** .

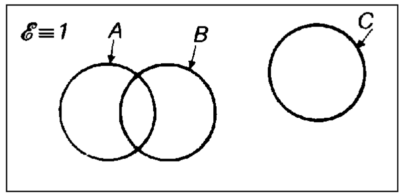
Notiamo che con nessun'altra coppia di operazioni fra tutte le altre 14 che sono state definite sull'insieme $\{0,1\}$ (P1_C1.13) possono costituire un reticolo. Infatti nessun'altra operazione che non sia l'AND e l'OR possiede, al contempo, proprietà di idempotenza e di assorbimento (vedi tabelle a fine paragrafo P1_C1.13).

Si può dimostrare che, tra la struttura reticolare formata della classe $C(S)$ dei sottinsiemi di un insieme totale S (vedi appendice B) più le operazioni di unione e intersezione $(C(S);\cup,\cap)$, e la struttura al gebrica $(B;+,\cdot)$ formata dall'insieme delle variabili booleane, più le operazioni booleane somma e prodotto, esiste un isomorfismo.

Ciò permette una rappresentazione grafica assai suggestiva delle proprietà della struttura $(\mathcal{B};+,\cdot)$. Infatti, le proprietà della struttura $(\mathcal{B};+,\cdot)$ sono le medesime proprietà della struttura $(C(S);\cup,\cap)$ che sono rappresentabili mediante i diagrammi di Eulero-Venn[2].

Possiamo associare all'insieme S una figura geometrica piana, ad esempio un rettangolo $\mathcal{E}$ (vedi figura). Possiamo poi associare agli elementi A,B,C,..., di C(S), sottinsiemi di $\mathcal{E}$, ad esempio cerchi (cerchi di Eulero) A,B,C. Associamo ora ad ogni variabile booleana A,B,C,..., i sottinsiemi A,B,C,...,e quindi i cerchi A,B,C,....

[2]LEONHARD EULER (1707-1783)
JOHN VENN (1834-1923) matematico inglese, per primo adottò i cerchi di Eulero per raffigurare le funzione booleane.



Associamo infine alla operazione ∪ (unione) l'operazione OR ed alla ∩ (intersezione) l'operazione AND. Otteniamo un diagramma del tipo in figura (**diagramma di Venn**) mediante il quale possiamo rappresentare graficamente tutte le leggi e le proprietà del reticolo.

Esempio P1_C1.15.2 Dimostriamo coi diagrammi di Venn che la struttura algebrica in questione è:

1. **un RETICOLO**
2. **un RETICOLO COMPLETO**
3. **un RETICOLO COMPLEMENTATO**
4. **un RETICOLO DISTRIBUTIVO**

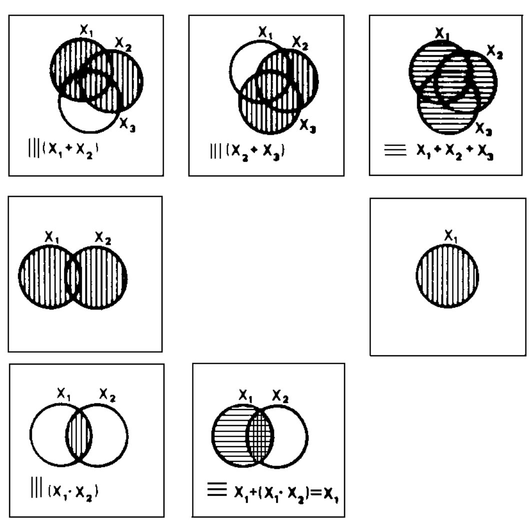
1) bisogna dimostrare che le operazioni $(\cup \leftrightarrow +, \cap \leftrightarrow .)$ definite sugli elementi A, B, C di $\mathcal{E}$ (che chiameremo d'ora in poi per uniformare i simboli: x_1, x_2, x_3) sono associative, commutative, idempotenti, e dotate di proprietà di assorbimento. Dimostriamo l'esistenza di tali proprietà per l'operazione $+$.

Associativa: $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$

Commutativa: $x_1 + x_2 = x_2 + x_1$

Idempotente: $x_1 + x_1 = x_1$

Assorbimento: $x_1 + (x_1 \cdot x_2) = x_1$

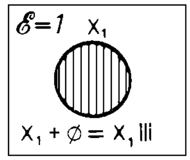


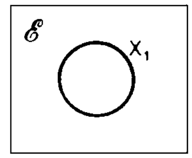
Invocando la legge di dualità potremmo ritenere dimostrate le stesse proprietà per l'operazione duale · (AND).

2) Il reticolo possiede un minimo maggiorante universale O $= 0$ ed un massimo minorante universale 1$=\mathcal{E}$, esso è dunque completo e valgono le relazioni:

$$\boldsymbol{x_1 + 0 = x_1} + 0 = \boldsymbol{x_1}$$

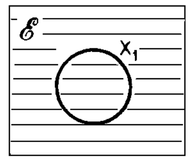
$$\boldsymbol{x_1 + 1 = x_1} + 1$$

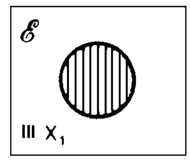




$$\boldsymbol{x_1 \cdot 0 = x}.0 = 0$$

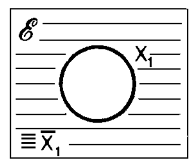
$$\boldsymbol{x_1 \cdot 1 = x_1} \cdot 1 = \boldsymbol{x_1}$$



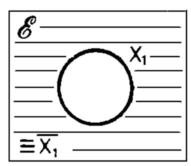


3) Il reticolo è complementato: ogni $x_1, x_2, \ldots$ possiede il suo complemento $x_1', x_2', \ldots$, o meglio, per uniformare i simboli, $\overline{x_1}, \overline{x_2}, \ldots$

$$\boldsymbol{x_1 + \overline{x_1} = 1} \equiv \mathcal{E}$$

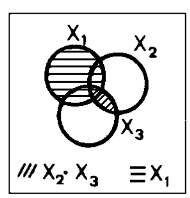


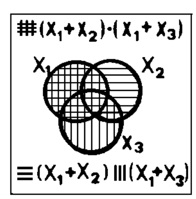
$$\boldsymbol{x_1 \cdot \overline{x_1} = \mathrm{O}} \equiv \emptyset$$



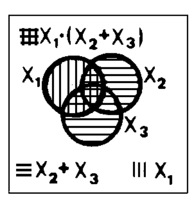
4) Il reticolo è distributivo, cioè le operazioni OR ed AND godono della proprietà distributiva l'una rispetto all'altra:

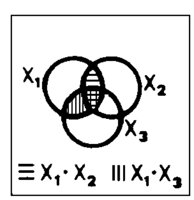
$$\boldsymbol{x_1 + (x_2 \cdot x_3) = (x_1 + x_2) \cdot (x_l + x_3)}$$





$$\boldsymbol{x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)}$$

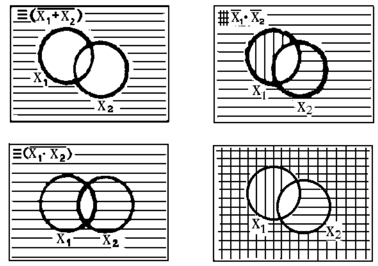




Esempio P1_C1.15.3 Dimostriamo, come esempio di applicazione dei diagrammi di Venn, il seguente TEOREMA DI DE MORGAN nelle sue due espressioni duali :

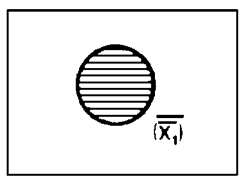
$\overline{(x_1 + x_2)} = \overline{x_1} \cdot \overline{x_2}$

$\overline{(x_1 \cdot x_2)} = \overline{x_1} + \overline{x_2}$



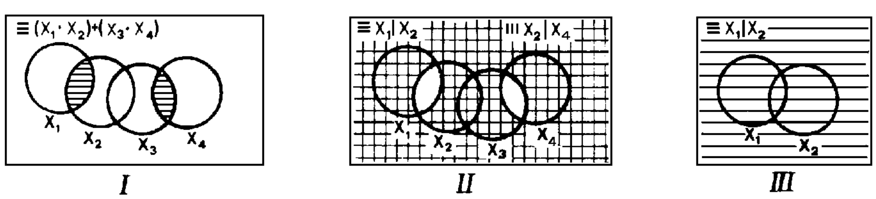
Esempio P1_C1.15.4 **Dimostriamo la LEGGE DELL'INVOLUZIONE**

$\overline{\overline{(x_1)}} = x_1$



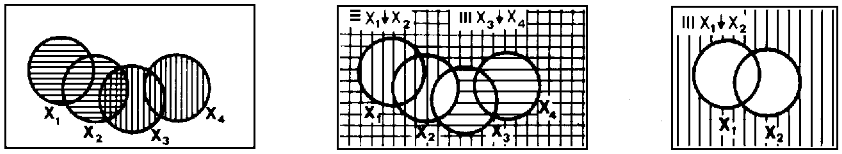
Esempio P1_C1.15.5 **Dimostriamo mediante i diagrammi di Venn, il seguente teorema:**

$\boxed{(x_1 \cdot x_2) + (x_3 \cdot x_4) = (x_1 \mid x_2) \mid (x_3 \mid x_4)}$ $\{x_1 \mid x_2 = \overline{x_1} \cdot \overline{x_2}$



Esempio P1_C1.15.6 **Dimostriamo, mediante i diagrammi di Venn, il seguente teorema:**

$\boxed{(x_1 + x_2) \cdot (x_3 + x_4) = (x_1 \downarrow x_2) \downarrow (x_3 \downarrow x_4)}$ $\{x_1 \downarrow x_2 = \overline{x_1 + x_2}$



I *II* *III*

Esempio P1_C1.15.7 **Dimostrare che, mediante l'operatore NAND, si possono costruire gli operatori NOT, AND, OR:**

$\overline{x_1} = x_1 \mid x_1$, **vedi fig. III dell'Es.(32-I)**

$x_1 \cdot x2 = (x_1 \mid x_2) \mid (x_1 \mid x_2)$, **vedi teorema dell'Es.P1_C1.15.5 ponendo** $x_3 = x_1, x_4 = x_2$

$x + y = (x \mid x) \mid (y \mid y)$, **vedi teorema dell'Es. P1_C1.15.5 ponendo** $x = x_1 = x_2, y = x_3 = x_4$.

Esempio P1_C1.15.8 **Dimostrare che, mediante l'operatore NOR, si possono costruire gli operatori NOT, AND, OR:**

$\overline{x_1} = x_1 \downarrow x_1$, **vedi tabella III dell'Es.P1_C1.15.6**

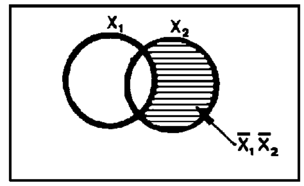
$x_1 \cdot x2 = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2)$, **vedi teorema dell'Es.P1_C1.15.6 ponendo** $x = x_1 = x_2, \quad y = x_3 = x_4$

$x + y = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2)$, **vedi teorema dell'Es.P1_C1.15.6 ponendo** $x_3 = x_1, \quad x_4 = x_2$.

Esempio P1_C1.15.9 **Dimostrare i seguenti teoremi di assorbimento**

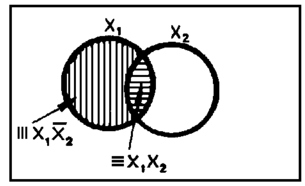
$$x_1 + \overline{x_1}x_2 = x_1 + x_2$$

$$x_1 \cdot (\overline{x_1} + x_2) = x_1 \cdot x_2$$



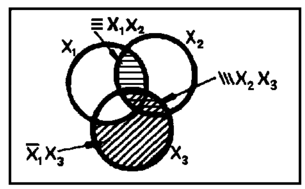
$$x_1 \cdot x_2 + x_1\overline{x_2} = x_1$$

$$(x_1 + x_2) \cdot (x_1 + \overline{x_2}) = x_1$$



$$x_1 \cdot x_2 + x_2 \cdot x_3 + \overline{x_1} \cdot x_3 = x_1 \cdot x_2 + \overline{x_1} \cdot x_3$$

$$(x_1 + x_2) \cdot (x_2 + x_3) \cdot (\overline{x_1} + x_3) = (\overline{x_1} + x_3) \cdot (x_1 + x_2)$$



Abbiamo dimostrato i primi teoremi delle 3 coppie di teoremi: i secondi sono i teoremi duali e si ritengono dimostrati invocando la legge di dualità.

P1_C1.16 Generalizzazione del concetto di algebra di Boole

DEF. P1_C1.16.1 Un reticolo $(B; \leq)$ oppure $(B; \triangle, \nabla)$ complementato, distributivo, con $0 \neq$ (vedi App.B.10), si definisce un'**algebra di Boole** e si indica, in generale mediante la sestupla:

$$B = (B, \cup, \cap, \bar{}, 1, 0)$$

dove:

- B è L'INSIEME SU CUI È ERETTA L 'ALGEBRA
- $\cup$ è L'OPERAZIONE BINARIA INTERNA PRIMA
- $\cap$ è L'OPERAZIONE BINARIA INTERNA SECONDA
- $^{-}$ è L'OPERAZIONE UNARIA COMPLEMENTO
- 0 è IL MASSIMO MINORANTE UNIVERSALE DI B, **O**
- 1 è IL MINIMO MAGGIORANTE DI B, **I**

DEF. P1_C1.16.2 Si dice algebra B^* duale dell'algebra di Boole B, l'algebra:

$$B^* = (B, \cap, \cup, \bar{}, 0, 1)$$

Nella quale viene scambiato, rispetto a B, $\cap$ con $\cup$, 0 con 1 e viceversa.

TEOREMA P1_C1.16.1 L'algebra B^* è anch'essa un'algebra di Boole. Infatti la applicazione $\Phi(x) = \bar{x}$, per ogni $x \in B$ è un isomorfismo (App.B.14) tra B e B^* e le due algebre sono isomorfe. Infatti:

$$\forall x \in B, \;\; \Phi(x) = \bar{x} \in B$$

$$a \cup b = c \;\; \rightarrow \;\; \Phi(a \cup b) = \Phi(a) \cap \Phi(b) \;\; \{\forall a, b \in B$$

$$\overline{a \cup b} = \bar{a} \cap \bar{b}$$

$$a \cap b = d \;\; \rightarrow \;\; \Phi(a \cap b) = \Phi(a) \cup \Phi(b) \;\; \{\forall a, b \in B$$

$$\overline{a \cap b} = \bar{a} \cup \bar{b}$$

P1_C1.17 Principio di dualità

Possiamo ora enunciare un principio assai importante per le Algebre di Boole, il principio di dualità (che in realtà è un teorema).

TEOREMA P1_C1.17.1 Una identità booleana T rimane ancora una identità se si scambiano i simboli $\cup$ con $\cap$, e $\cap$ con $\cup$, 1 con 0 e 0 con 1. L'identità T^* che si ottiene, si definisce identità duale di T. Infatti una identità Booleana T è vera per un'algebra Booleana se e soltanto se è vera T^* per la sua algebra duale B^* (B e B^* sono isomorfe)

Esempio P1_C1.17.1

$$\begin{array}{ll} T: & A \cdot (B + C) = AB + AC \\ T^*: & A + (B \cdot C) = (A + B) \cdot (A + C) \end{array}$$

P1_C1.18 Costruzione dell'algebra di Boole mediante postulati

Abbiamo visto nel paragrafo precedente, come l'algebra di Boole possa essere derivata dall'Algebra Astratta. In questo capitolo mostriamo come quella struttura che è denominata RETICOLO DI BOOLE possa essere definita mediante postulati. Partendo dalle operazioni AND($\cdot$) e OR(+) definite nel paragrafo P1_C1.13, poniamo i postulati contenuti nella tabella alla pagina seguente:

I	$\begin{cases} x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3 \\ x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3 \end{cases}$	*PROPRIETA' ASSOCIATIVA*
II	$\begin{cases} x_1 + x_2 = x_2 + x_1 \\ x_1 \cdot x_2 = x_2 \cdot x_1 \end{cases}$	*PROPRIETA' COMMUTATIVA*
III	$\begin{cases} x_1 + x_1 = x_1 \\ x_1 \cdot x_1 = x_1 \end{cases}$	*PROPRIETA' DI IDEMPOTENZA*
IV	$\begin{cases} x_1 + x_1 \cdot x_2 = x_1 \\ x_1 \cdot (x_1 + x_2) = x_1 \end{cases}$	*PROPRIETA' DI ASSORBIMENTO*
V	$\begin{cases} x_1 + (x_2 \cdot x_3) = (x_1 + x_2) \cdot (x_1 + x_3) \\ x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3) \end{cases}$	*PROPRIETA' DISTRIBUTIVA*
VI	$\begin{cases} 0 + x = 0 \\ 1 \cdot x = x \end{cases}$	*DEFINIZIONE ELEMENTI NEUTRI*
VII	$\begin{cases} x + \bar{x} = 1 \\ x \cdot \bar{x} = 0 \end{cases}$	*DEFINIZIONE DEL COMPLEMENTO*
VIII	$\{ \overline{(\bar{x})} = x$	*LEGGE DELL'INVOLUZIONE*
IX	$\begin{cases} \overline{(x_1 + x_2)} = \bar{x_1} \cdot \bar{x_2} \\ \overline{(x_1 \cdot x_2)} = \bar{x_1} + \bar{x_2} \end{cases}$	*TEOREMA DI DE MORGAN*

Mediante questi postulati possiamo dimostrare algebricamente tutti i teoremi che abbiamo dimostrato mediante i diagrammi di Venn. I teoremi dimostrati ci saranno utili nel seguito.

Bibliografia

ALGEBRA, ALGEBRA DI BOOLE (A)
SISTEMI DI NUMERAZIONE, CODICI (B)

A (l) Boole G., *The Mathematical Analysis of Logic*, Cambridge, 1847.

A (2) Boole G., *An Investigation of the Laws of Though*, London, 1854, ristampa Dover, 1954.

A (3) Huntington E.W., *Sets of Independent Postulates for the Algebra of Logic*, Trans. Am. Math. Soc., 5, 1904.

A (4) Shannon C.E., *A Symbolic Analysis of Relay and Switching Circuits*, Transactions OA AIEE, 57, 1938.

A (5) Birkhoff G., Mc Lane S., *A Survey of Modern Algebra*, Mc Millan, New York, 1953.

A (6) Kaufmann A., Precigout M., *Cours de mathematiques nouvelles*, Dunod, Paris, 1966.

A (7) Kuntzman J., *Algebre de Boole*, Dunod, Paris, 1968.

A (8) Hoernes G., Heilweilm., *Introduction a l'algebre de Boole e aux dispositifs logiques*, Dunod, Paris, 1969,

A (9) Naslin P., *Circuits logiques et automatismes a sequence*, Dunod, Paris, 1970.

AB (10) Lagasse J., *Logique combinatoire et sequentielle*, Dunod, Paris, 1971.

A (11) Lombardo Radice L., *Istituzioni di algebra astratta*, Feltrinelli, Torino, 1973.

A (12) Mendelson E., *Algebra di Boole e circuiti di commutazione*, Schaum Etas libri, 1977.

B (13) Falzone V., *Tecniche digitali*, ed. Siderea, Roma, 1979.

CIBERNETICA (C)

C 1) Wiener, N., *Cybernetics*, M.I.T. Press and J. Wiley, N.Y., 1961

C 2) Wiener, N., *Introduzione alla cibernetica*, Boringhieri, 1976.

C 3) Ashby, W.R., *Introduzione alla cibernetica*, Einaudi, Torino, 1971.

TEORIA DEI SISTEMI (S)

S 1) Rinaldi, S., *Teoria dei sistemi*, Clup, Milano, 1977.

S 2) Ruberti, A., Isidori, A., *Teoria dei sistemi*, Patron, Bologna, 1979.

S 3) Marro, G., *Fondamenti di teoria dei sistemi*, Patron, Bologna, 1979.

S 4) Emery, L.E., *La teoria dei sistemi*, Angeli, Milano, 1980.

Parte 2

Appendice 1

Elementi di calcolo combinatorio

A.1 Generalità

In questa Appendice cercheremo di sintetizzare quegli elementi fondamentali del calcolo combinatorio che possano avere attinenza con la materia trattata in questo o in altri capitoli.

A.2 N-uple ordinate

DEF. A.2.1 Consideriamo un raggruppamento di n "posti" o "posizioni" ordinate dall'uno ad n, suscettibili di contenere ciascuna un oggetto

$$((\ldots)_1, (\ldots)_2, \ldots, (\ldots)_n)$$

Definiamo un tale raggruppamento **ennupla ordinata** (o $n - upla$ ordinata). Sia dato ora un insieme $\mathcal{E}$ di elementi $\{a, b, c, \ldots\}$.

DEF. A.2.2 Una $n - upla$ ordinata contenente in ognuno dei suoi "posti" un elemento qualsiasi ed uno solo dell'insieme $\mathcal{E}$ si chiama **ennupla ordinata di elementi di** $\mathcal{E}$ e si indica con

$$(a_1, a_2, \ldots, a_n)$$

nella quale $a_i (i = 1, \ldots, n)$ si chiama **elemento** $i - esimo$ **della ennupla ordinata di elementi** di $\mathcal{E}$.

Possiamo quindi pensare una $n - upla$ ordinata di elementi di $\mathcal{E}$ come n caselle ordinate dall'uno all'n (annupla ordinata) in ciascuna delle quali è stato introdotto un qualsiasi elemento di $\mathcal{E}$. Non è escluso che la $n - upla$ sia costituita da n elementi tutti eguali.

A.3 Permutazioni combinazioni e disposizioni semplici

Sia dato un insieme $\mathcal{E}$ contenente n oggetti tutti diversi l'uno dall'altro (distinti) e sia data una $n - upla$ ordinata.

DEF. A.3.1 Una $n-upla$ ordinata di elementi $\mathcal{E}$ che contenga tutti gli elementi di $\mathcal{E}$ si dice **permutazione semplice**.

TEOREMA A.3.1 Il numero di permutazioni semplici che si possono ottenere con gli n elementi di $\mathcal{E}$

$$P_n = n!$$

dove $n!$ significa il prodotto dei primi n numeri naturali $(n! = 1, 2, 3, \ldots, (n - 1), n)$.

Le permutazioni sono chiamate semplici perchè nelle $n - ple$ ogni elemento di $\mathcal{E}$ compare una sola volta.

Esempio A.3.1 Sia $\mathcal{E}$ l'insieme costituito dai primi 3 numeri naturali. Sono permutazioni semplici le $n - ple$:

$$\begin{array}{ccc} (1,2,3) & (2,1,3) & (3,1,2) \\ (1,3,2) & (2,3,1) & (3,2,1) \end{array}$$

Esse sono $3! = 6$.

Sia dato un insieme $\mathcal{E}$ con n elementi distinti.

DEF. A.3.2 Si definisce **combinazione semplice di classe** k $(k < n)$ di quegli elementi un raggruppamento non ordinato di k di quegli elementi.

TEOREMA A.3.2 Il numero di combinazioni semplici di classe k che si possono ottenere con gli n elementi di $\mathcal{E}$ è:

$$C_{n,k} = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Esempio A.3.2 **Sia $\mathcal{E}$ l'insieme che ha come elementi i primi 3 numeri naturali $1, 2, 3$. Le combinazioni semplici di classe 2 (dette a due a due) ottenibili sono** $\left(\begin{array}{c} 3 \\ 2 \end{array} \right) = \frac{3!}{2!(3-2)!} = 3$ **e sono:**

$$(1,2) \quad (2,3) \quad (1,3)$$

Sia dato un insieme $\mathcal{E}$ con n elementi distinti.

DEF. A.3.3 Si chiama **Disposizione semplice di classe** k di quegli n elementi $(k < n)$ ogni $k - upla$ ordinata di elementi di $\mathcal{E}$.

TEOREMA A.3.3 Il numero di disposizioni semplici di classe k che si possono ottenere con gli n elementi di $\mathcal{E}$ è:

$$D_{n,k} = \quad k! \left(\begin{array}{c} n \\ k \end{array} \right) = \quad k! \frac{n!}{k!(n-k)!}$$

Esempio A.3.3 **Sia $\mathcal{E}$ l'insieme che ha come elementi i primi tre numeri naturali $1, 2, 3$. Le disposizioni semplici di classe 2 ottenibili sono in numero di** $2! \left(\begin{array}{c} 3 \\ 2 \end{array} \right) = 6$ **e sono:**

$$\begin{array}{ccc} (1,2) & (2,3) & (1,3) \\ (2,1) & (3,2) & (3,1) \end{array}$$

A.4 Permutazioni combinazioni e disposizioni con ripetizioni

Abbiamo finora supposto che $\mathcal{E}$ contenesse n elementi distinti tra loro e che, nelle permutazioni, combinazioni, disposizioni semplici ogni elemento di $\mathcal{E}$ comparisse una sola volta.

Supponiamo ora di considerare il caso più generale in cui $\mathcal{E}$ contenga n elementi distinti, ma in cui le permutazioni, le combinazioni e le disposizioni possano contenere più volte uno stesso elemento di $\mathcal{E}$. In questo caso allora può verificarsi la condizione $k > n$.

Le permutazioni, combinazioni e disposizioni si chiamano in questo caso **permutazioni, combinazioni, disposizioni con ripetizioni**.

TEOREMA A.4.1 Il numero di permutazioni con ripetizioni che si possono costruire mediante gli n elementi dell'insieme $\mathcal{E}\{\beta_\infty, \beta_\in, \ldots, \beta_\backslash\}$ dei quali $alpha_1$ sono eguali a β_1, α_r sono eguali a β_n $(\alpha_1 + \alpha_2 + \ldots + \alpha_n = m)$ è:

$$P_n^r = \quad m! \frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_n!}$$

TEOREMA A.4.2 Il numero di combinazioni con ripetizioni di classe k che si possono ottenere con gli n elementi di $\mathcal{E}$ è:

$$C_{n,k}^r = \quad \begin{pmatrix} n+k-1 \\ k \end{pmatrix}$$

TEOREMA A.4.3 Il numero di disposizioni con ripetizioni di classe k che si possono ottenere con gli n elementi di $\mathcal{E}$ è:

$$D_{n,k}^r = n^k$$

Esempio A.4.1 Si abbia un insieme $\mathcal{E}$ che abbia come elementi i due numeri 0 ed 1. Quante sono le $3-uple$ che si possono costruire con gli elementi di $\mathcal{E}$?

Se ne possono costruire tante quante sono le disposizioni con ripetizioni di classe $k = 3$ che si possono costruire con gli $n = 2$ elementi $0, 1$ cioè 2^3. Esse sono:

$$\begin{array}{c} (000) \\ (001) \\ (010) \\ (011) \\ (100) \\ (101) \\ (110) \\ (111) \end{array}$$

Parte 2

Appendice 2

Complementi di algebra

B.1 Premessa

Lo scopo di questa appendice è raccogliere quei concetti dell'Algebra Moderna che sono utili sia nello studio dell'Algebra di Boole applicata ai sistemi di commutazione, sia nello studio di alcune particolari metodologie di sintesi dei sistemi digitali combinatori e sequenziali.

Questi complementi quindi non hanno alcuna pretesa di essere un trattato, se pur parziale, di Algebra, ma vogliono essere una sorta di tabella sinottica dei concetti sopradetti.

Vengono qui riportate, o meglio "ricordate", le definizioni necessarie, vengono generalmente omesse le dimostrazioni che possono essere reperite nei testi citati nella bibliografia.

B.2 Insiemi

I concetti di INSIEME, di ELEMENTO di un insieme, di APPARTENENZA di un elemento ad un insieme, vengono assunti come concetti primitivi.

Per insieme si intende ogni aggregato, famiglia, raccolta, classe, collezione di oggetti o entità che possono avere caratteristiche in comune. Ogni oggetto si dice elemento dell'insieme.

Esempio B.2.1

- **1) L'insieme degli oggetti contenuti in una stanza.**
- **2) L'insieme dei mobili contenuti in quella stanza.**
- **3) L'insieme delle sedie contenute in quella stanza.**
- **4) L'insieme dei numeri naturali.**
- **5) L'insieme dei numeri reali.**

Se un insieme $\mathcal{X}$ è costituito dagli elementi x_1, x_2, x_3, x_n ciò viene espresso simbolicamente dalla:

$$\mathcal{X} \ = \ \{x_1, x_2, \ldots, x_n\}$$

e si indica simbolicamente l'appartenenza all'insieme X dell'elemento x_i mediante la notazione:

$$x_i \in \mathcal{X}$$

DEF. B.2.1 Si definisce CARDINALITÀ d'un insieme $\mathcal{X}$ $(\mid \mathcal{X} \mid)$ il numero di elementi dell'insieme.

Un insieme può avere cardinalità finita o cardinalità infinita a seconda che il numero dei suoi elementi sia finito oppure no.

DEF. B.2.2 Un insieme $\mathcal{X}$ si definisce EGUALE ad un insieme $\mathcal{Y}$ quando ambedue sono costituiti dagli stessi elementi. $(\mathcal{X} = \mathcal{Y})$.

DEF. B.2.3 Un insieme $\mathcal{X}$ non eguale ad un insieme $\mathcal{Y}$ si definisce DIVERSO da $\mathcal{Y}$ $(\mathcal{X} \neq \mathcal{Y})$.

DEF. B.2.4 Un insieme $\mathcal{X}$ si dice essere un SOTTOINSIEME dell'insieme $\mathcal{A}$, quando ogni elemento di $\mathcal{X}$ è anche elemento di $\mathcal{A}$ e si scrive $\mathcal{X} \subseteq \mathcal{A}$.

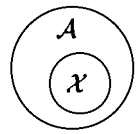
Il simbolo $\subseteq$ viene chiamato SIMBOLO DI INCLUSIONE.

Indicando col simbolo $\forall x$ la frase "per ogni x", si esprime simbolicamente la definizione precedente mediante la scrittura:

$$\mathcal{X} \subseteq \mathcal{A} \ \ \mathit{se} \ \ \forall x \in \mathcal{X}, x \in \mathcal{A}$$

Esempio B.2.2 **L'insieme 3) dell'esempio 1 è un sottinsieme dell'insieme 2) il quale, a sua volta, è un sottinsieme dell'insieme 1); l'insieme 4) è un sottinsieme dell'insieme 5).**

Esempio B.2.3 **Siano $\mathcal{A}$ ed $\mathcal{X}$ insiemi di punti contenuti in due cerchi nel piano (cerchi di EULERO) come in figura:**



$\mathcal{X}$ è un sottinsieme di $\mathcal{A}$.

Notiamo che, nell'esempio precedente, $\mathcal{X}$ è contenuto in $\mathcal{A}$ ($\mathcal{X} \subset \mathcal{A}$) cioè $\mathcal{X}$ è un sottinsieme di $\mathcal{A}$, ma $\mathcal{X} \neq \mathcal{A}$. Gli elementi di un insieme possono essere anch'essi degli insiemi.

DEF. B.2.5 si definisce CLASSE DEI SOTTINSIEMI di un insieme $\mathcal{A}$, l'insieme di tutti i sottinsiemi di $\mathcal{A}$ o INSIEME DELLE PARTI DI $\mathcal{A}$, $\mathcal{C}(\mathcal{A})$.

Notiamo che la classe dei sottinsiemi di $\mathcal{A}$, contiene $\mathcal{A}$ stesso. $\mathcal{A}$ è infatti un possibile sottinsieme di $\mathcal{A}$: vedi definizione di sottinsieme.

Vi sono due insiemi di grande importanza e che ora definiremo:

DEF. B.2.6 Si definisce INSIEME TOTALE o INSIEME UNIVERSO o SPAZIO DI INSIEMI, l'insieme che contiene tutti gli insiemi che si prendano in considerazione.

DEF. B.2.7 Si definisce INSIEME VUOTO quell'insieme che non contiene elementi e si denota col simbolo $\emptyset$.

L'insieme vuoto è chiaramente sottinsieme di qualunque insieme.

Dato l'insieme totale $\mathcal{T}$ ed un insieme $\mathcal{X}$,

DEF. B.2.8 Si definisce INSIEME COMPLEMENTARE di $\mathcal{X}$ (in simboli $\overline{\mathcal{X}}$), l'insieme che è costituito dagli elementi dell'insieme totale $\mathcal{T}$ che non appartengono ad $\mathcal{X}$.

Prendiamo in esame un altro tipo di insieme che riveste una certa importanza nella teoria dei sistemi digitali sequenziali.

Sia dato un insieme $\mathcal{A}$.

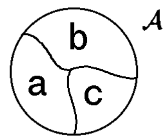
DEF. B.2.9 Si dice PARTIZIONE Π su $\mathcal{A}$, $\Pi(\mathcal{A})$, un insieme di sottinsiemi disgiunti (tali che le loro intersezioni siano l'insieme vuoto $\emptyset$) di $\mathcal{A}$, tali che la loro unione sia l'insieme $\mathcal{A}$. Gli elementi della partizione $\Pi(\mathcal{A})$ prendono il nome di BLOCCHI DELLA PARTIZIONE. Si scriverà :

$$\Pi(\mathcal{A}) = \{\mathcal{B}_1, \ldots, \mathcal{B}_n\}$$

se n sono i blocchi di partizione $\mathcal{B}_i$.

Dato quindi un insieme $\mathcal{A}$, si possono costruire più partizioni su $\mathcal{A}$. Notiamo che in una partizione gli elementi (blocchi di partizione) sono a due a due disgiunti per definizione, nella classe dei sottinsiemi invece, gli elementi sono non necessariamente a due a due disgiunti.

Esempio B.2.4 **Sia dato l'insieme $\mathcal{A} = \{a, b, c\}$: costruire le possibili partizioni $\Pi_i(\mathcal{A})$:**



$$\begin{aligned}
\Pi_1(\mathcal{A}) &= \{\{a\}, \{b\}, \{c\}\} \\
\Pi_2(\mathcal{A}) &= \{\{a, b\}, \{c\}\} \\
\Pi_3(\mathcal{A}) &= \{\{a, c\}\{b\}\} \\
\Pi_4(\mathcal{A}) &= \{\{a\}, \{b, c\}\} \\
\Pi_5(\mathcal{A}) &= \{\{a, b, c\}\}
\end{aligned}$$

DEF. B.2.10 Definiremo INSIEME DELLE PARTIZIONI su $\mathcal{A}$ l'insieme i cui elementi sono costituiti da tutte le possibili partizioni su $\mathcal{A}$.

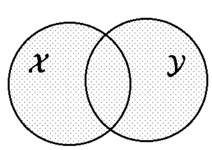
$$\mathcal{P}(\mathcal{A}) = \{\Pi_1(\mathcal{A}), ..., \Pi_n(\mathcal{A})\}$$

B.3 Operazioni tra insiemi.

Definiremo qui alcune operazioni tra insiemi e cioè la UNIONE, la INTERSEZIONE, la DIFFERENZA. (leggi di composizione binarie).

DEF. B.3.1 Si definisce UNIONE (o SOMMA, simbolo $\cup$) di due insiemi $\mathcal{X}$ e $\mathcal{Y}$, l'insieme costituito dagli elementi che appartengono o ad $\mathcal{X}$ o ad $\mathcal{Y}$.

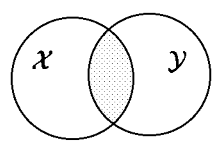
Esempio B.3.1 **Siano $\mathcal{X}$ e $\mathcal{Y}$ rappresentati da due cerchi di Eulero; l'unione è rappresentata dall'insieme ombreggiato:**



$\mathcal{X} \cup \mathcal{Y}$

DEF. B.3.2 Si definisce INTERSEZIONE (o PRODOTTO, simbolo $\cap$) di due insiemi $\mathcal{X}$ e $\mathcal{Y}$, l'insieme costituito dagli elementi che appartengono sia ad $\mathcal{X}$ che a $\mathcal{Y}$.

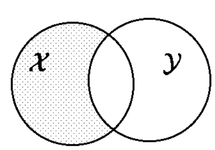
Esempio B.3.2 **Siano $\mathcal{X}$ e $\mathcal{Y}$ rappresentati dai due cerchi di Eulero in figura; l'intersezione è rappresentata dall'insieme ombreggiato:**



$\mathcal{X} \cap \mathcal{Y}$

DEF. B.3.3 Si definisce DIFFERENZA di due insiemi $\mathcal{X}$ e $\mathcal{Y}$ (nell'ordine), l'insieme costituito dagli elementi di $\mathcal{X}$ che non appartengono a $\mathcal{Y}$.

Esempio B.3.3 **Siano $\mathcal{X}$ ed $\mathcal{Y}$ rappresentati dai due cerchi di Eulero in figura; la differenza tra $\mathcal{X}$ ed $\mathcal{Y}$ è rappresentata dall'insieme ombreggiato:**



$\mathcal{X} - \mathcal{Y}$

B.4 Prodotto cartesiano tra insiemi.

Per poter dare la definizione di prodotto cartesiano tra insiemi, dobbiamo prima dare le definizioni di coppia, coppia ordinata, n-upla, n-upla ordinata.

DEF. B.4.1 Si definisce COPPIA di elementi di un insieme $\mathcal{E} = \{a, b, c, \ldots\}$ un insieme di due suoi elementi, ad esempio:

$$\{a, b\}$$

DEF. B.4.2 Si definisce COPPIA ORDINATA, una coppia $\{a, b\}$ in cui si definisce il primo elemento ed il secondo elemento. La coppia $\{a, b\}$ in cui a viene definito primo elemento, si indica simbolicamente con:

$$(a, b)$$

Estendendo le due definizioni:

DEF. B.4.3 Si dice n-UPLA, un insieme di n elementi di un insieme $\mathcal{E}$:

$$\{a_1, \ldots, a_n\}$$

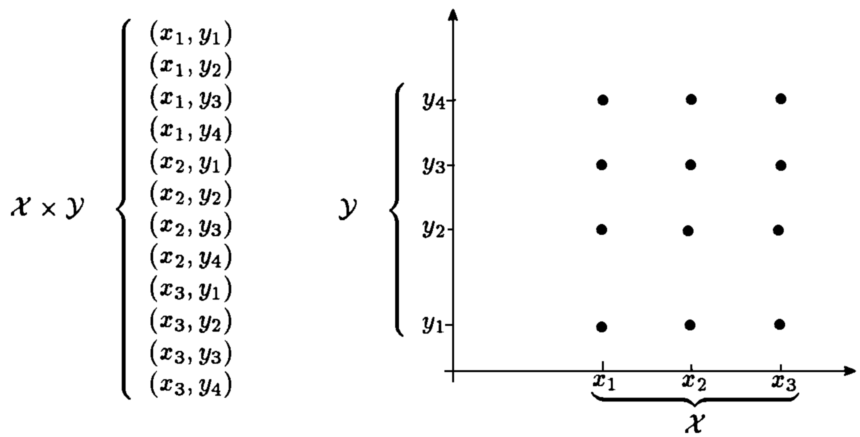
DEF. B.4.4 Si dice n-UPLA ORDINATA una n-upla tra i cui elementi si stabilisca un ordine:

$$(a_1, \ldots, a_n)$$

Possiamo ora definire il prodotto cartesiano tra n insiemi, iniziando con $n = 2$.

DEF. B.4.5 Si definisce PRODOTTO CARTESIANO DI DUE INSIEMI (non necessariamente distinti) $\mathcal{X}$ e $\mathcal{Y}$ (che si indica col simbolo $\mathcal{X} \times \mathcal{Y}$) l'insieme di tutte le coppie ordinate (x,y), dove $x \in \mathcal{X},\ y \in \mathcal{Y}$.

Esempio B.4.1 Fissata una coppia d'assi cartesiani e due versori degli assi, sia $\mathcal{X}$ l'insieme costituito dai 3 valori di ascissa x_1, x_2, x_3, sia $\mathcal{Y}$ l'insieme costituito dai 4 valori di ordinate y_1, y_2, y_3, y_4. Il prodotto cartesiano $\mathcal{X} \times \mathcal{Y}$ è l'insieme delle coppie ordinate di coordinate dei punti in figura:



Notiamo che, se $\mathcal{X}$ ha cardinalità N_x, e se $\mathcal{Y}$ ha cardinalità N_y , la cardinalità di $\mathcal{X} \times \mathcal{Y}$ vale $N_x \times N_y$.

Estendendo la definizione precedente al caso in cui $n > 2$,

DEF. B.4.6 Si dice PRODOTTO CARTESIANO DI n INSIEMI, non necessariamente distinti $\mathcal{X}_1, \ldots, \mathcal{X}_n$, $(\mathcal{X}_1 \times \mathcal{X}_2, \ldots \times \mathcal{X}_n)$, l'insieme di tutte le n-uple ordinate ($x_{1i}, x_{2i}, \ldots, x_{nk}$) dove $x_{1i} \in \mathcal{X}_1, \ldots, x_{nk} \in \mathcal{X}$.

B.5 Relazione tra due insiemi.

Il concetto di relazione tra due insiemi è fondamentale nella teoria degli insiemi, in quanto è da questo concetto che derivano quello di funzione, di applicazione.

Una relazione tra due insiemi $\mathcal{A}$ e $\mathcal{B}$ (non necessariamente distinti ma in questo preciso ordine) è una legge che associa ad elementi di $\mathcal{A}$, elementi di $\mathcal{B}$.

DEF. B.5.1 Si dice RELAZIONE $\mathbf{R}$ tra l' insieme $\mathcal{A}$ e l'insieme $\mathcal{B}$ (nell'ordine) l'insieme di coppie ordinate (a, b) con $a \in \mathcal{A}$, $b \in \mathcal{B}$ che verifichino la relazione

$$a \; \mathbf{R} \; b$$

Una relazione è un sottinsieme del prodotto cartesiano $\mathcal{A} \times \mathcal{B}$.

Siano dati due insiemi $\mathcal{A}$ e $\mathcal{B}$ ed una relazione $\mathbf{R}$ tra $\mathcal{A}$ e $\mathcal{B}$ (nell'ordine) o relazione $\mathbf{R}$ da $\mathcal{A}$ a $\mathcal{B}$.

DEF. B.5.2 Si dice DOMINIO DI $\mathbf{R}$ il sottinsieme di $\mathcal{D}$ di $\mathcal{A}$ costituito dagli elementi di $\mathcal{A}$ per i quali esiste almeno un elemento $b \in \mathcal{B}$ talchè:

$$a \,\mathbf{R}\, b$$

DEF. B.5.3 Si dice CODOMINIO DI $\mathbf{R}$ il sottinsieme $\mathcal{C}$ di $\mathcal{B}$ costituito dagli elementi di $\mathcal{B}$ per i quali esiste almeno un elemento $a \in \mathcal{A}$ talchè:

$$a \,\mathbf{R}\, b$$

Se tra un elemento $a' \in \mathcal{A}$ ed un elemento $b' \in \mathcal{B}$ non sussiste la relazione $\mathbf{R}$, ciò viene espresso dal simbolismo $a' \not\!\mathbf{R}\; b'$. Notiamo che tutte le definizioni date valgono anche nel caso che sia $\mathcal{A} = \mathcal{B}$. In tal caso si parla di relazione di $\mathcal{A}$ su $\mathcal{A}$.

Sia $\mathbf{R}$ una relazione tra due insiemi $\mathcal{A}$ e $\mathcal{B}$ e sia $a \in \mathcal{A}$.

DEF. B.5.4 Si dice SEZIONE DI $\mathbf{R}$ PER MEZZO DI a, $(\mathbf{R}(a))$, l'insieme di tutti gli elementi b di $\mathcal{B}$ tali che:

$$a \,\mathbf{R}\, b.$$

Notiamo che $\mathbf{R}(a)$ può anche coincidere con l'insieme vuoto.

<u>RAPPRESENTAZIONE DI UNA RELAZIONE</u>.

Una relazione tra un insieme $\mathcal{X}$ ed un insieme $\mathcal{Y}$, nell'ordine, può essere rappresentata mediante:

- a) una tabella.
- b) una sezione per mezzo degli elementi di $\mathcal{X}$.
- c) un grafo.
- d) una rappresentazione sul piano cartesiano.

Esempio B.5.1 Siano dati due insiemi $\mathcal{X}$, $\mathcal{Y}$, una relazione $\mathbf{R}$ tra loro, con dominio $\mathcal{D}$ e codominio $\mathcal{C}$ come specificato sotto:

$$\mathcal{X} = \{x_1, x_2, x_3, x_4\} \qquad \mathcal{Y} = \{y_1, y_2, y_3, y_4\}$$

$$\mathcal{X} \;\mathbf{R}\; \mathcal{Y}$$

$$\mathcal{D} = \{x_1, x_2, x_3\} \subset \mathcal{X} \qquad \mathcal{C} = \{y_1, y_2, y_3, y_4\} \subseteq \mathcal{Y}$$

$$\mathbf{R} = \{(x_1, y_1), (x_1, y_2), (x_2, y_1), (x_2, y_3), (x_3, y_4)\}$$

Rappresentiamo la relazione nelle forma a),b),c),d)

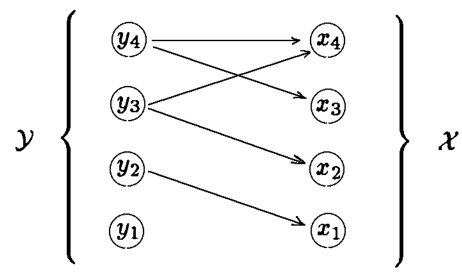
a) <u>TABELLA</u>

	x_1	x_2	x_3	x_4
y_1	$\surd$	$\surd$		
y_2	$\surd$			
y_3		$\surd$		
y_4			$\surd$	

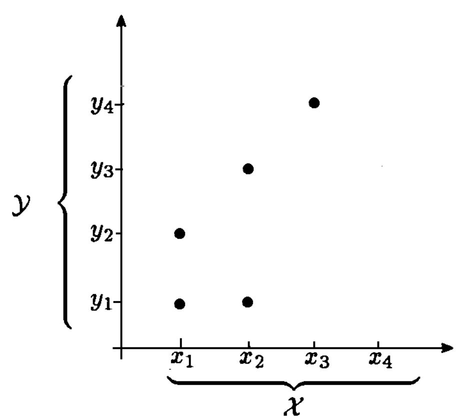
b) **<u>SEZIONI</u>**

x_1	x_2	x_3	x_4
$\{y_1, y_2\}$	$\{y_1, y_3\}$	$\{y_4\}$	$\emptyset$

c) **<u>GRAFO</u>**



d) **<u>PIANO CARTESIANO</u>**



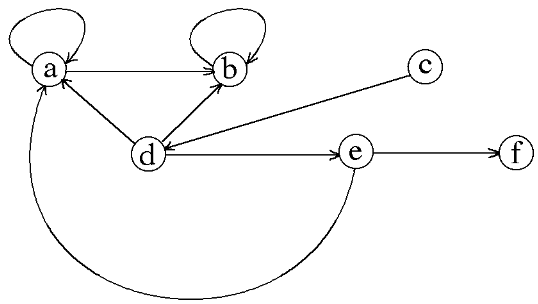
Esempio B.5.2 **Si abbia una relazione di $\mathcal{A}$ su $\mathcal{A}$ definita come sotto specificato:**

$$\mathcal{A} = \{a, b, c, d, e, f\}$$

	a	b	c	d	e	f
a	$\surd$			$\surd$	$\surd$	
b	$\surd$	$\surd$		$\surd$		
c						
d			$\surd$			
e				$\surd$		
f					$\surd$	$\surd$

Rappresentarla mediante la sezione ed il grafo.

a	b	c	d	e	f
$\{a, b\}$	$\{b\}$	$\{d\}$	$\{a, b, e\}$	$\{a, f\}$	$\emptyset$



B.6 Funzioni, applicazioni iniettive, suriettive, biiettive.

Siano dati due insiemi $\mathcal{A}$ e $\mathcal{B}$. Sia data una relazione $\mathbf{R}$ da $\mathcal{A}$ a $\mathcal{B}$. Sia $\mathcal{D} \subseteq \mathcal{A}$ il dominio della relazione. Sia $\mathcal{C} \subseteq \mathcal{B}$ il codominio della relazione.

DEF. B.6.1 Se per ogni $d \in \mathcal{D}$ esiste uno ed un solo elemento $c \in \mathcal{C}$ talchè $d\,\mathbf{R}\,c$, allora la relazione $\mathbf{R}$ si chiama una MAPPA DELL'INSIEME A NELL'INSIEME B o FUNZIONE f da $\mathcal{D}$ a $\mathcal{C}$ $(c = f(d))$.

DEF. B.6.2 Se nella mappa di $\mathcal{A}$ in $\mathcal{B}$, $\mathcal{D} = \mathcal{A}$ (se per ogni $a \in \mathcal{A}$ esiste uno ed un solo $c \in \mathcal{C}$ talchè $a\mathbf{R}c$), la mappa si chiama APPLICAZIONE DI $\mathcal{A}$ in $\mathcal{B}$ (o CORRISPONDENZA UNIVOCA DA $\mathcal{A}$ a $\mathcal{B}$)

DEF. B.6.3 Se una applicazione di $\mathcal{A}$ in $\mathcal{B}$ è tale che a due elementi distinti di $\mathcal{A}$ corrispondono due elementi distinti di $\mathcal{B}$, la applicazione si dice APPLICAZIONE INIETTIVA o INIEZIONE DI $\mathcal{A}$ in $\mathcal{B}$.

Il codominio $\mathcal{C} \subseteq \mathcal{B}$ dell'applicazione iniettiva ha elementi a due a due distinti ed ha cardinalità eguale a quella di $\mathcal{D} = \mathcal{A}$. Può avere cardinalità $\leq$ alla cardinalità di $\mathcal{B}$.

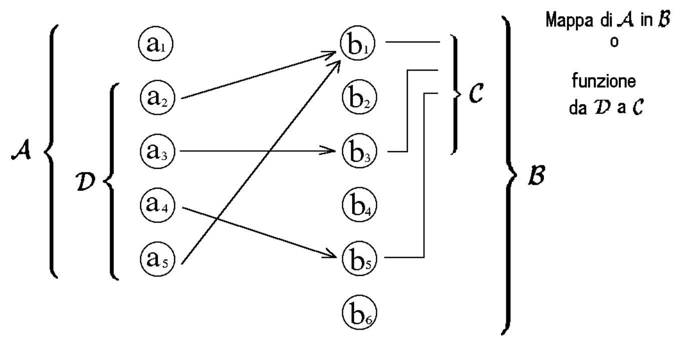
DEF. B.6.4 Se una applicazione di $\mathcal{A}$ in $\mathcal{B}$ è tale che $\mathcal{C} = \mathcal{B}$ la applicazione si dice APPLICAZIONE SURIETTIVA O SURIEZIONE DI $\mathcal{A}$ su $\mathcal{B}$.

Il codominio $\mathcal{C} = \mathcal{B}$ della suriezione ha cardinalità $\leq$ alla cardinalità di A, in quanto, dato un $b \in \mathcal{B}$, più di un elemento a, $(a \in \mathcal{A})$ può soddisfare la relazione a **R** b.

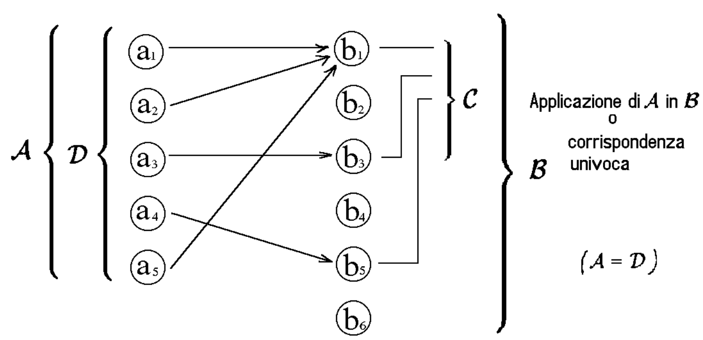
DEF. B.6.5 Se una applicazione di $\mathcal{A}$ su $\mathcal{B}$ è nel contempo iniettiva e suriettiva, si dice APPLICAZIONE BIIETTIVA o BIIEZIONE o CORRISPONDENZA BIUNIVOCA DA $\mathcal{A}$ a $\mathcal{B}$.

Il codominio $\mathcal{C} = \mathcal{B}$ ed il dominio $\mathcal{D} = \mathcal{A}$ della biiezione hanno la medesima cardinalità.

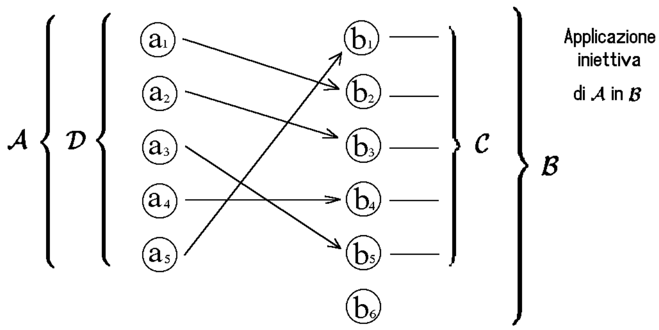
Esempio B.6.1 .



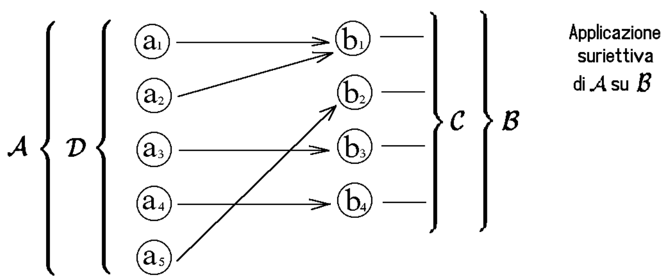
Esempio B.6.2 .



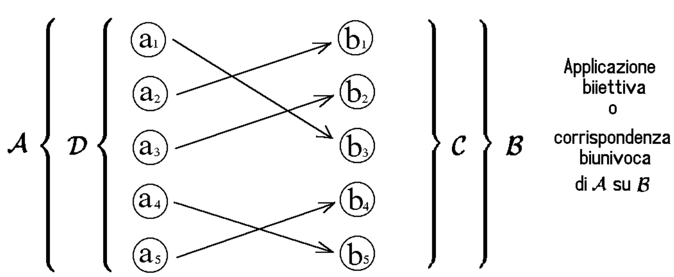
Esempio B.6.3 .



Esempio B.6.4 .



Esempio B.6.5 .



B.7 Leggi di composizione su un insieme; legge di composizione unaria (operazione unaria)

DEF. B.7.1 Si dice LEGGE DI COMPOSIZIONE UNARIA o OPERAZIONE UNARIA SU UN INSIEME $\mathcal{E}$, OGNI APPLICAZIONE DI $\mathcal{E}$ in $\mathcal{E}$.

Una operazione unaria è una corrispondenza univoca tra elementi di $\mathcal{E}$.

Esempio B.7.1 **Sia $\mathcal{E}$ l'insieme dei numeri interi relativi e sia $x \in \mathcal{E}$. Il passaggio da x a $\mid x \mid$ è una operazione unaria.**

Esempio B.7.2 **Sia $\mathcal{C}(\mathcal{E})$ l'insieme dei sottinsiemi di $\mathcal{E}$. Il passaggio dall'insieme $\mathcal{A} \subseteq \mathcal{E}$ al suo complementare è una operazione unaria.**

LEGGE DI COMPOSIZIONE BINARIA INTERNA (OPERAZIONE INTERNA BINARIA).

DEF. B.7.2 Si dice LEGGE DI COMPOSIZIONE o OPERAZIONE BINARIA INTERNA su $\mathcal{E}$ ogni applicazione di $\mathcal{E} \times \mathcal{E}$ in $\mathcal{E}$, (simbolo $*$, ad esempio).

Ad ogni coppia ordinata (a, b) con $a, b, \in \mathcal{E}$ viene associato uno ed un solo elemento c di $\mathcal{E}$.

Esempio B.7.3 **L'operazione di addizione nel caso che $\mathcal{E}$ rappresenti l'insieme dei numeri interi, reali, complessi, l'insieme dei vettori in uno spazio tridimensionale, l'insieme delle matrici quadrate e dello stesso ordine, ecc.**

Esempio B.7.4 **L'operazione di unione e intersezione nel caso che $\mathcal{E}$ rappresenti l'insieme dei sottinsiemi di $\mathcal{A}$ (classe dei sottinsiemi di $\mathcal{A}$).**

LEGGE DI COMPOSIZIONE BINARIA ESTERNA (OPERAZIONE BINARIA ESTERNA).
Siano dati due insiemi, $\mathcal{M}$ ed $\mathcal{E}$.

DEF. B.7.3 Si dice LEGGE DI COMPOSIZIONE o OPERAZIONE BINARIA ESTERNA (simbolo O, ad esempio) su $\mathcal{E}$ con $\mathcal{M}$ (insieme degli operatori) ogni applicazione di $\mathcal{M} \times \mathcal{E}$ in $\mathcal{E}$. Ad ogni coppia (m, a) ordinata $m \in \mathcal{M}, a \in \mathcal{E}$ viene associato uno ed un solo elemento b di $\mathcal{E}$.

$$m \; O \; a \; = \; b$$

Esempio B.7.5 **Sia $\mathcal{E}$ l'insieme dei vettori nello spazio tridimensionale, $\mathcal{M}$ il campo reale; l'operazione prodotto di un vettore $\vec{v}$ $(\in \mathcal{E})$ per un numero reale $m \in \mathcal{M}$, $(mO\vec{v} = \vec{u})$, è una operazione binaria esterna.**

PROPRIETÀ DELLE LEGGI DI COMPOSIZIONE BINARIA INTERNA

Le leggi di composizione binaria interna (operazioni binarie interne) su un insieme $\mathcal{E}$ possono godere (o non godere) delle seguenti proprietà:

Commutativa

DEF. B.7.4 Una operazione $*$ interna su $\mathcal{E} = \{x_1, \ldots, x_n\}$ si dice COMMUTATIVA quando, per due qualsiasi elementi x_i e x_j di $\mathcal{E}$:

$$x_i * x_j = x_j * x_i$$

Associativa

DEF. B.7.5 Una operazione $*$ interna su $\mathcal{E} = \{x_1, \ldots, x_n\}$ si dice ASSOCIATIVA quanto per ogni elemento x_i, x_j, x_k di $\mathcal{E}$:

$$(x_i * x_j) * x_k = x_i * (x_j * x_k)$$

Idempotenza

DEF. B.7.6 Una operazione $*$ interna su $\mathcal{E} = \{x_1, \ldots, x_n\}$ si dice IDEMPOTENTE quando per ogni x_i di $\mathcal{E}$:

$$x_i * x_i = x_i$$

Assorbimento

DEF. B.7.7 Date due operazioni interne $*, \cdot$ su $\mathcal{E} = \{x_1, \ldots, x_n\}$, si dice che godono della PROPRIETÀ DI ASSORBIMENTO, quando per ogni x_i, x_j di $\mathcal{E}$:

$$x_i * (x_i \cdot x_j) = x_i$$

$$x_i \cdot (x_i * x_j) = x_i$$

Distributiva

DEF. B.7.8 Date due operazioni interne $*, \cdot$ su $\mathcal{E} = \{x_1, \ldots, x_n\}$ si dice che godono della PROPRIETÀ DISTRIBUTIVA D'UNA RISPETTO ALL'ALTRA quando, per ogni x_i, x_j, x_k di $\mathcal{E}$:

$$x_i * (x_j \cdot x_k) = (x_i * x_j) \cdot (x_i * x_k)$$

$$x_i \cdot (x_j * x_k) = (x_i \cdot x_j) * (x_i \cdot x_k)$$

Elemento neutro

DEF. B.7.9 Data una operazione (binaria) interna $*$ su $\mathcal{E} = \{x_1, \ldots, x_n\}$, un elemento $t \in \mathcal{E}$ si dice ELEMENTO NEUTRO rispetto alla operazione $*$, quando per ogni $x_i \in \mathcal{E}$:

$$t * x_i = x_i * t = x_i$$

Elementi simmetrici

DEF. B.7.10 Data una operazione interna $*$ su $\mathcal{E} = \{x_1, \ldots, x_n\}$, due elementi $x_i, x_j, \in \mathcal{E}$ si dicono tra loro SIMMETRICI se esiste l'elemento neutro t e se:

$$x_i * x_j = x_j * x_i = t$$

B.8 Relazioni tra un insieme e sè stesso. Equivalenza, preordine, ordine parziale, ordine totale.

Sia dato un insieme $\mathcal{E} = \{x_1, \ldots, x_n\}$ Sia data una relazione $\mathbf{R}(\preceq)$ tra $\mathcal{E}$ ed $\mathcal{E}$, talchè:

$$\mathbf{R} = \{(x_i, x_j); \quad x_i \preceq x_j\}$$

dove $x_i \preceq x_j$ va inteso come "x_i precede x_j" e la $\preceq$ va intesa come una relazione di ordinamento.

Gli elementi di $\mathcal{E}$ che, a coppie formano gli elementi di $\mathbf{R}$ si dicono ELEMENTI CONFRONTABILI.

Se per $x_p, x_q \in \mathcal{E}$ non vale nè la $x_p \preceq x_p$, nè la $x_q \preceq x_p$, i due elementi x_p ed x_q si dicono NON CONFRONTABILI.

Una relazione $\mathbf{R}$ tra un insieme $\mathcal{E}$ e sè stesso è un sottinsieme di $\mathcal{E} \times \mathcal{E}$. Il dominio $\mathcal{D}$ ed il codominio $\mathcal{C}$ della relazione sono inclusi in E. La relazione $\mathbf{R} = \{(x_i, x_j); x_i \preceq x_j\}$ permette di correlare o confrontare, (se sono confrontabili), tra loro gli elementi di $\mathcal{E}$.

Esempio B.8.1 La notazione $\preceq$ può rappresentare la relazione di minore o eguale ($\leq$) tra elementi dell'insieme dei numeri interi, o dell'insieme di numeri reali; può rappresentare la relazione di inclusione tra gli elementi di un insieme di insiemi, ecc, ecc.

La relazione può possedere qualcuna delle seguenti proprietà:

- 1) RIFLESSIVA $x_i \preceq x_i, \forall x_i \in \mathcal{E}$
- 2) SIMMETRICA $x_i \preceq x_j \quad \rightarrow \quad x_j \preceq x_i$
- 3) TRANSITIVA $x_i \preceq x_j, x_j \preceq x_p \quad \rightarrow \quad x_i \preceq x_p$
- 4) ASIMMETRICA $x_i \preceq x_j, x_j \preceq x_i \quad \rightarrow \quad x_i = x_j$
- 5) DI TOTALITÀ $\forall x_i, x_j \in$E $vale\ la:\ x_i \preceq x_j,\ o\ la:\ x_j \preceq x_i$

Notiamo che la proprietà di totalità di una relazione (relazione d'ordine) tra un insieme $\mathcal{E}$ e sè esso è soddisfatta quando tutti gli elementi di $\mathcal{E}$ sono confrontabili. Neppure in quest'ultimo caso la relazione $\mathbf{R}$ coincide con $\mathcal{E} \times \mathcal{E}$ (infatti se $x\mathbf{R}x', neconsegueche\ x' \not\mathbf{R}x$ e la coppia $(x', x) \notin \mathbf{R}$, mentre $(x', x) \in \mathcal{E} \times \mathcal{E}$).

DEF. B.8.1 Un insieme $\mathcal{E}$ più una relazione d'ordine $\mathbf{R}$ tra $\mathcal{E}$ e sè stesso si dicono formare una STRUTTURA D'ORDINE:

$$(E; \preceq)$$

DEF. B.8.2 Una relazione $\preceq$ che possieda le tre proprietà 1),2),3) RIFLESSIVA, SIMMETRICA, TRANSITIVA, si chiama RELAZIONE DI EQUIVALENZA.

DEF. B.8.3 Una relazione $\preceq$ che possieda le proprietà RIFLESSIVA E TRANSITIVA 1),3) si dice RELAZIONE DI PREORDINE.

DEF. B.8.4 L'insieme $\mathcal{E}$ dotato di una relazione di preordine si definisce INSIEME QUASI ORDINATO.

DEF. B.8.5 Una relazione $\preceq$ che possieda le proprietà 1),3),4) RIFLESSIVA TRANSITIVA ANTISIMMETRICA, si dice RELAZIONE D'ORDINE PARZIALE.

DEF. B.8.6 L'insieme $\mathcal{E}$ dotato di una relazione d'ordine parziale si definisce INSIEME PARZIALMENTE ORDINATO.

DEF. B.8.7 Una relazione $\preceq$ che possieda le proprietà 1),3),4),5), RIFLESSIVA, TRANSITIVA, ANTISIMMETRICA, DI TOTALITÀ, si dice RELAZIONE D'ORDINE TOTALE.

DEF. B.8.8 L'insieme $\mathcal{E}$ dotato d'una relazione d'ordine totale si definisce INSIEME TOTALMENTE ORDINATO o CATENA.

B.9 Equivalenza. Partizione d'un insieme in classi di equivalenza

Sia $\mathcal{E}$ un insieme dotato di una relazione di equivalenza (vedi par. B.8) $\mathbf{R}$.

Se $a, b \in \mathcal{E}$, diremo che a è EQUIVALENTE a b se $a\ \mathbf{R}\ b$. In tal caso potremo dire anche che b è equivalente ad a, vista la proprietà simmetrica della equivalenza. ($a\ \mathbf{R}\ b\ \rightarrow\ b\ \mathbf{R}\ a$).

Date le proprietà (RIFLESSIVA, SIMMETRICA e TRANSITIVA) della relazione di EQUIVALENZA, due elementi equivalenti $a, b \in \mathcal{E}$ generano la identica sezione di $\mathbf{R}$; $\mathbf{R}(a) = \mathbf{R}(b)$.

Così pure due elementi $a, b \in \mathcal{E}$, che generano la stessa sezione sono equivalenti. In sintesi:

La sezione $\mathbf{R}(a)$ coincide con la sezione $\mathbf{R}(b)$ se e solo se a è equivalente a b ($a\ \mathbf{R}\ b$). Tutte le sezioni $\mathbf{R}(x)$, ottenibili da tutti gli elementi x di $\mathcal{E}$, tra loro distinte, formano un insieme $\mathcal{P}$ di sottinsiemi di $\mathcal{E}$ DISGIUNTI; la loro unione coincide con $\mathcal{E}$. L'insieme $\mathcal{P}$ è quindi una PARTIZIONE (vedi paragrafo B.2) di $\mathcal{E}$ detta PARTIZIONE DI $\mathcal{E}$ IN CLASSI DI EQUIVALENZA.

Una relazione d'equivalenza su $\mathcal{E}$ induce quindi una PARTIZIONE di $\mathcal{E}$ in CLASSI DI EQUIVALENZA.

B.10 Strutture algebriche.

Sia dato un insieme $\mathcal{E}$ sul quale siano definite una o più leggi di composizione interna $(*_1, *_2, *_3, \ldots)$ e leggi di composizione esterna $(O_1, O_2, O_3, \ldots\ )$ con insiemi di operatori $(M_1, M_2, M_3, \ldots)$ eventualmente provvisti di leggi di composizione interna, tutte queste leggi essendo provviste di varie proprietà; l'entità definita in tal modo:

$$(\mathcal{E}, *_1, *_2, *_3, \ldots;\ (M_1, *_1, *_2, *_3, \ldots), O_1;\ (M_2, *_1, *_2, *_3, \ldots), O_2; \ldots)$$

si definisce STRUTTURA ALGEBRICA.

B.11 Reticolo

Prima di definire il reticolo, abbiamo bisogno di definire il concetto di minimo maggiorante e di massimo minorante di un sottinsieme di un insieme dato. Sia $\mathcal{E}$ un insieme PARZIALMENTE ORDINATO ed $\mathcal{X}$ un suo sottinsieme $\mathcal{X} \subset \mathcal{E}$:

DEF. B.11.1 Si dice che $u \in \mathcal{E}$ è un MINIMO MAGGIORANTE DI $\mathcal{X}$ ($mM(\mathcal{X})$) se e solo se:

$$\forall x \in \mathcal{X}, \quad x \preceq u$$

$$\forall u' \in \mathcal{E},\ talche' :\ x \ \preceq u' \ \rightarrow \ u \preceq u'$$

Il $mM(\mathcal{X})$ è dunque, tra gli elementi di $\mathcal{E}$ che "seguono" tutti gli elementi di $\mathcal{X}$, il primo nell'ordine dato dalla $\preceq$.

DEF. B.11.2 Si dice che $v \in \mathcal{E}$ è un MASSIMO MINORANTE di $\mathcal{X}$ ($Mm(\mathcal{X})$) se e solo se:

$$\forall x \in \mathcal{X}, \quad v \preceq x$$

$$\forall v' \in \mathcal{E},\ talche' :\ v' \ \preceq x \ \rightarrow \ v' \preceq v$$

Il $Mm(\mathcal{X})$ è dunque, tra tutti gli elementi di $\mathcal{E}$ che "precedono" tutti gli elementi di $\mathcal{X}$, l'ultimo nell'ordine dato dalla $\preceq$.

Noti i concetti di insieme parzialmente ordinato, di operazione interna, di massimo minorante e minimo maggiorante, possiamo dare la definizione di reticolo.

DEF. B.11.3 Una struttura algebrica costituita da:

- un insieme $\mathcal{E}$ parzialmente ordinato, per ogni coppia di elementi (x, y) del quale esiste $mM(x, y)$ e $Mm(x, y)$,
- e da due operazioni interne $\triangle e \bigtriangledown$ definite dalle:

$$mM(x, y) = x \triangle y$$

$$Mm(x, y) = x \bigtriangledown y,$$

si definisce RETICOLO $R = (\mathcal{E}; \triangle, \bigtriangledown)$.

Si può dare anche un'altra definizione di reticolo, equivalente a quella data.

DEF. B.11.4 Si dice RETICOLO una struttura algebrica $(\mathcal{E}; \triangle, \bigtriangledown)$ costituita da un insieme $\mathcal{E}$ e da due operazioni interne su $\mathcal{E}$, dotate delle proprietà:

- 1) ASSOCIATIVA
- 2) COMMUTATIVA
- 3) IDEMPOTENTE
- 4) DI ASSORBIMENTO (vedi paragrafo B.7).

DEF. B.11.5 Un reticolo $R = (\mathcal{E}; \triangle, \bigtriangledown)$ si dice COMPLETO se ogni sottinsieme di $\mathcal{E}$ ammette mM e Mm.

Se un reticolo è completo esiste il minimo maggiorante di $\mathcal{E}$, $mM(\mathcal{E})$, denotato dal simbolo **I** e chiamato MINIMO MAGGIORANTE UNIVERSALE, ed esiste il massimo minorante di $\mathcal{E}$, $Mm(\mathcal{E})$, denotato dal simbolo **O** e chiamato MASSIMO MINORANTE UNIVERSALE.

DEF. B.11.6 Se un reticolo $R = (\mathcal{E}; \triangle, \bigtriangledown)$ è completo, si dice COMPLEMENTO DI $x \in \mathcal{E}$, qualora esista, un elemento y di $\mathcal{E}$ talchè:

$$x \triangle y = \mathbf{I}, \qquad x \bigtriangledown y = \mathbf{O}$$

DEF. B.11.7 Un reticolo $R = (\mathcal{E}; \triangle, \bigtriangledown)$ si dice COMPLEMENTATO se per ogni elemento $x \in \mathcal{E}$ esiste il suo complemento.

DEF. B.11.8 Un reticolo $R = (\mathcal{E}; \triangle, \bigtriangledown)$ si dice DISTRIBUTIVO se le operazioni $\triangle$, e $\bigtriangledown$ godono della proprietà distributiva.

Vedremo nel prossimo paragrafo alcuni esempi di reticolo.

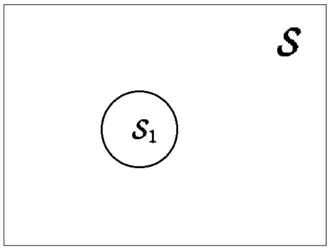
B.12 Esempi di reticoli

B.12.1 Classe dei sottinsiemi di $\mathcal{S}$

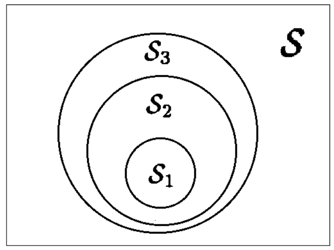
Vogliamo qui dimostrare che la classe dei sottinsiemi di un insieme $\mathcal{S}$ (vedi paragrafo B.2) e le due operazioni di unione e intersezione costituiscono un reticolo:

$$R = (\mathcal{C}(\mathcal{S}); \cup, \cap)$$

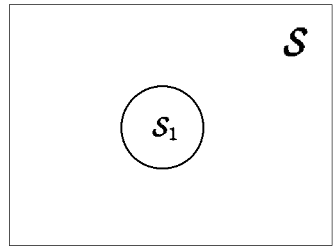
- A) La classe dei sottinsiemi di $\mathcal{S}$, $\mathcal{C}(\mathcal{S})$ è un insieme PARZIALMENTE ORDINATO, se si considera come relazione d'ordine la relazione d'inclusione $\subseteq$. Infatti la relazione di inclusione è una relazione d'ordine parziale, in quanto possiede le proprietà RIFLESSIVA, TRANSITIVA, ANTISIMMETRICA.



$\mathcal{S}_1 \subseteq \mathcal{S}_1$



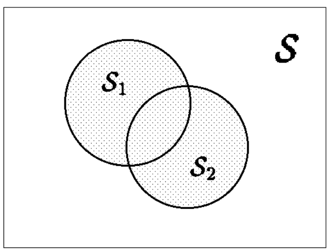
$\mathcal{S}_1 \subseteq \mathcal{S}_2, \mathcal{S}_2 \subseteq \mathcal{S}_3$
$\rightarrow\ \mathcal{S}_1 \subseteq \mathcal{S}_3$



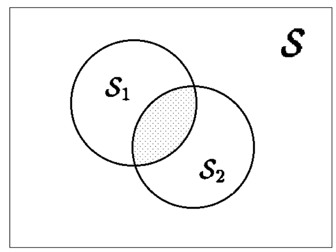
$\mathcal{S}_1 \subseteq \mathcal{S}_2, \mathcal{S}_2 \subseteq \mathcal{S}_1$
$\rightarrow\ \mathcal{S}_1 \equiv \mathcal{S}_2$

- B) Ogni coppia, $\mathcal{S}_1, \mathcal{S}_2$ di elementi di $\mathcal{S}$ possiede un $mM(\mathcal{S}_1, \mathcal{S}_2)$ e un $Mm(\mathcal{S}_1, \mathcal{S}_2)$. Il $mM(\mathcal{S}_1, \mathcal{S}_2)$ si può vedere essere l'unione dei due insiemi $\mathcal{S}_1$ ed $\mathcal{S}_2$.

  Il $Mm(\mathcal{S}_1, \mathcal{S}_2)$ si può vedere esser l'intersezione di $\mathcal{S}_1$ ed $\mathcal{S}_2$.

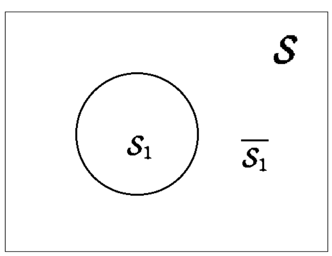


$mM(\mathcal{S}_1, \mathcal{S}_2) = \mathcal{S}_1 \cup \mathcal{S}_2$



$Mm(\mathcal{S}_1, \mathcal{S}_2) = \mathcal{S}_1 \cap \mathcal{S}_2$

L'insieme $\mathcal{C}(\mathcal{S})$ dunque e le due operazioni $\triangle = \cup$, $\triangledown = \cap$ costituiscono un RETICOLO. Tale reticolo è pure COMPLETO: infatti $mM(\mathcal{C}(\mathcal{S})) = \mathbf{I} = \mathcal{S}$ mentre il $Mm(\mathcal{C}(\mathcal{S})) = \mathbf{O} = \emptyset$ Il reticolo è COMPLEMENTATO.

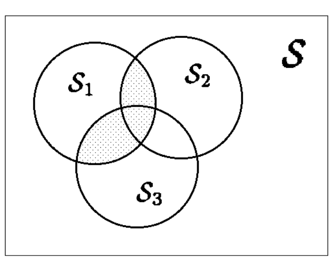


Infatti dato un qualunque elemento $\mathcal{S}_1 \subset \mathcal{S}$, esiste un $\overline{\mathcal{S}}_1 \in \mathcal{S}$ talchè:

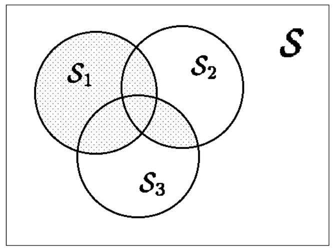
$$\mathcal{S}_1 \cup \overline{\mathcal{S}}_1 = \mathbf{I} = \mathcal{S}$$

$$\mathcal{S}_1 \cap \overline{\mathcal{S}}_1 = \mathbf{O} = \emptyset$$

Il reticolo è anche DISTRIBUTIVO.



$$\mathcal{S}_1 \cap (\mathcal{S}_2 \cup \mathcal{S}_3) = (\mathcal{S}_1 \cap \mathcal{S}_2) \cup (\mathcal{S}_1 \cap \mathcal{S}_3)$$



$$\mathcal{S}_1 \cup (\mathcal{S}_2 \cap \mathcal{S}_3) = (\mathcal{S}_1 \cup \mathcal{S}_2) \cap (\mathcal{S}_1 \cup \mathcal{S}_3)$$

B.12.2 Insieme di Boole $\mathcal{E}\{0,1\}$

Dimostriamo che l'insieme $\mathcal{E} = \{0,1\}$ e le due operazioni somma e prodotto Booleano $(+,\cdot)$ costituiscono un reticolo:

$$R = (\mathcal{E};+,\cdot)$$

- A) L'insieme $\mathcal{E}$ è parzialmente ordinato se si considera come relazione d'ordine la relazione di minore o eguale $(\leq)$. Infatti tale relazione di $\mathcal{E}$ su $\mathcal{E}$ gode delle proprietà

$$\begin{array}{cc}
RIFLESSIVA & x \leq x \quad \forall \in \mathcal{E} \\
TRANSITIVA & x \leq y,\ \ y \leq z \rightarrow x \leq z, \quad x,y,z \in \mathcal{E} \\
ANTISIMMETRICA & x \leq y,\ \ y \leq x \rightarrow x = y, \quad x,y \in \mathcal{E}
\end{array}$$

- B) Ogni coppia x, y di elementi di $\mathcal{E}$ possiede $mM(x,y)$ e $Mm(x,y)$:

COPPIA	mM	Mm
0,0	u=0=0$\triangle$ 0	v=0=0$\triangledown$0
0,1	u=1=0$\triangle$ 1	v=0=0$\triangledown$1
1,1	u=1=1$\triangle$ 1	v=1=1$\triangledown$1
1,0	u=1=1$\triangle$ 0	v=0=1$\triangledown$0

Dalla tabella sopra scritta per tutte le possibili coppie di elementi di E si può dedurre che le operazioni $\triangle e \triangledown$ coincidono con le operazioni booleane $+$ e $-$.

L'insieme $\mathcal{E} = \{0,1\}$ dunque, e le due operazioni $+$ e $-$ costituiscono una struttura algebrica reticolare:

$$R = (\mathcal{E} = \{0,1\};+,\cdot)$$

Il reticolo è COMPLETO: esiste il $mM(\mathcal{E}) = \mathbf{I} = 1$ ed il $Mm(\mathcal{E}) = \mathbf{O} = \emptyset$.

Il reticolo è COMPLEMENTATO: infatti per ogni $x \in \mathcal{E}$ esiste il suo complemento $\overline{x}$ talchè $x + \overline{x} = \mathbf{I} = 1, \quad x \cdot \overline{x} = \mathbf{O} = \emptyset$

Il reticolo è DISTRIBUTIVO: infatti le operazioni $+$ e $\cdot$ godono della proprietà distributiva.

B.13 Insieme delle partizioni su A

Consideriamo l'insieme di tutte le partizioni (vedi paragrafo B.2) su un insieme $\mathcal{A}$

$$\mathcal{C} = \{\Pi_1(\mathcal{A}), \Pi_2(\mathcal{A}), \ldots\}$$

DEF. B.13.1 Definiamo come relazione d'ordine $\preceq$ di C in C, mediante la:

$$\Pi_i \preceq \Pi_j$$

se ogni blocco di Π_i è contenuto in un blocco di Π_j.

1) L'insieme $\mathcal{C}$ è un insieme parzialmente ordinato: infatti la relazione d'ordine $\preceq$ soddisfa alle proprietà RIFLESSIVA, TRANSITIVA, ANTISIMMETRICA.

2) Per ogni coppia di elementi di $\mathcal{C}(\Pi_i)$, (Π_i, Π_j) esiste un $mM(\Pi_i, \Pi_j)$ ed un $Mm(\Pi_i, \Pi_j)$

$$\Pi_i = \{B_{i,l}\}$$

$$\Pi_j = \{B_{j,m}\}$$

$$mM(\Pi_i, \Pi_j) = \Pi_i \bigtriangleup \Pi_j = \{B_{i,l}, B_{j,m}\} \quad \forall l, m$$

$$Mm(\Pi_i, \Pi_j) = \Pi_i \bigtriangledown \Pi_j = \{B_{i,l}, B_{j,m}\} \quad \forall l, m$$

L'insieme $\mathcal{C}$ di tutte le partizioni su $\mathcal{A}$ è un RETICOLO.

Il mM universale del reticolo, $\mathbf{I}$, se $\mathcal{A} = \{a_1, \ldots . a_n\}$ è:

$$\mathbf{I} = \Pi_{\mathbf{I}} = \{(a_1, \ldots, a_n)\}$$

Il Mm universale del reticolo, $\mathbf{O}$ è:

$$\mathbf{O} = \Pi_{\mathbf{O}} = \{(a_1), (a_2), \ldots, (a_n)\}$$

B.14 Isomorfismo

Siano $(\mathcal{E}, *)$ ed $(\mathcal{F}; \perp)$ due strutture algebriche con:

$$\mathcal{E} = \{x, y, \ldots\},$$

$$\mathcal{F} = \{x', y', \ldots\},$$

e con $*$ *e* $\perp$ due operazioni interne rispettivamente di $\mathcal{E}$ e di $\mathcal{F}$,

DEF. B.14.1 Sia F una applicazione di $\mathcal{E}$ su $\mathcal{F}$ tale che:

$$x \stackrel{F}{\rightarrow} = x' = F(x),$$

e che, per ogni $x, y \in \mathcal{E}$

$$x * y = z \;\rightarrow\; F(z) = x' \perp y'$$

cioè

$$F(x * y) = F(x) \perp F(y),$$

allora l'applicazione F di $\mathcal{E}$ su $\mathcal{F}$ si dice MORFISMO

DEF. B.14.2 Se l'applicazione è iniettiva, F si dice MORFISMO INIETTIVO

DEF. B.14.3 Se l'applicazione è suriettiva, F si dice MORFISMO SURIETTIVO o OMOMORFISMO.

DEF. B.14.4 Se l'applicazione è biiettiva, F si dice ISOMORFISMO.

Due strutture algebriche in isomorfismo sono sostanzialmente la stessa struttura.

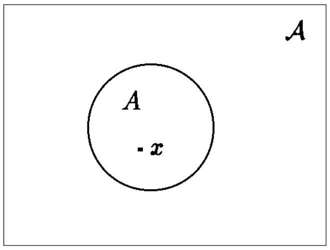
B.15 Isomorfismo tra particolari strutture algebriche

Vogliamo dimostrare l'esistenza di un isomorfismo tra la struttura algebrica reticolare formata dalla classe dei sottinsiemi $\mathcal{C}(\mathcal{A})$ di un insieme totale $\mathcal{A}$ più le operazioni di unione e intersezione $(\mathcal{C}(\mathcal{A}); \cup, \cap)$, e la struttura algebrica formata dall'insieme di tutte le variabili booleane $\mathcal{B}$ più le operazioni booleane di somma e prodotto $(\mathcal{B}; +, -)$.

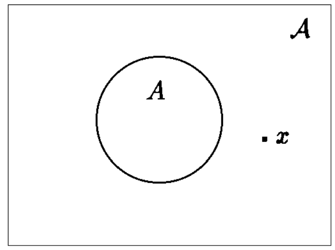
A tale scopo, dato un insieme $\mathcal{A}$ ed un punto $x \in \mathcal{A}$, associamo ad ogni sottinsieme A di $\mathcal{A}$ una funzione (detta funzione caratteristica di A), la quale può assumere il valore 1 o 0, a seconda che x sia contenuto o no in A.

$$A, x \stackrel{F}{\rightarrow} f_A(x)$$

$$F(A; x) = f_A(x) = \begin{array}{l} 1 \; se \; x \in A \\ \\ 0 \; se \; x \in A \end{array}$$

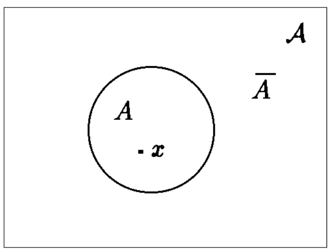


$$F(A;x) = f_A(x) = 1$$

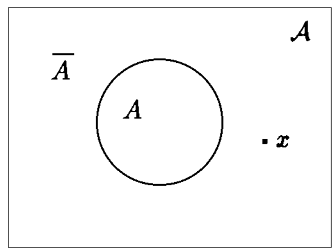


$$F(A;x) = f_A(x) = 0$$

Nella figura vengono rappresentate le costruzioni della funzione caratteristica mediante i diagrammi di Eulero-Venn. La funzione caratteristica del complementare di A si ricava dalla definizione di $\overline{A}$:



$$F(\overline{A};x) = 0$$
$$f_A(x) = 1$$



$$F(\overline{A};x) = 1$$
$$f_A(x) = 0$$

$$F(\overline{A};x) = 1 - f_A(x) = 1 - F(A;x)$$

$$F(\overline{A};x) = 1 - F(A;x) \qquad f_{\overline{A}}(x) = \overline{f}_A(x)$$
$$f_{\overline{A}}(x) = 1 - f_A(x)$$

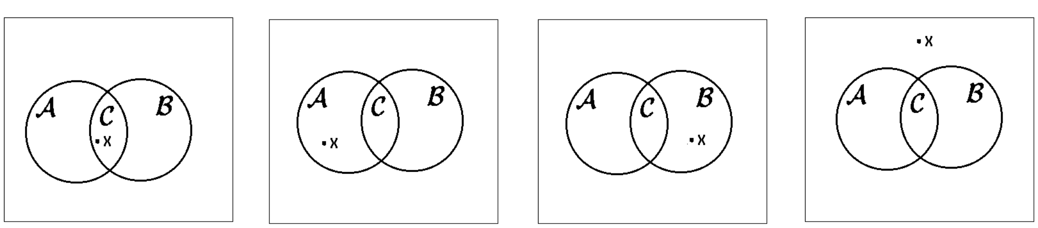
Per dimostrare che le due strutture sono isomorfe bisogna dimostrare che la applicazione F sopra definita (funzione caratteristica) è tale che:

$$F(A;x) = f_A(x), \qquad \forall A \subseteq \mathcal{A}$$

e che $\forall A, B \subseteq \mathcal{A}$:

$$1)\forall C = A \cap B, , \forall x \subseteq \mathcal{A}, \quad C, x \xrightarrow{F} f_C(x) = f_A(x) \cdot f_B(x)$$
$$2)\forall D = A \cup B, , \forall x \subseteq \mathcal{A}, \quad D, x \xrightarrow{F} f_D(x) = f_A(x) + f_B(x)$$

Possiamo dimostrare le proprietà 1) e 2) della funzione caratteristica usando i diagrammi di Eulero Venn:



$$\begin{array}{cccc}
\mathcal{A} \cap \mathcal{B} = \mathcal{C} & \mathcal{A} \cap \mathcal{B} = \mathcal{C} & \mathcal{A} \cap \mathcal{B} = \mathcal{C} & \mathcal{A} \cap \mathcal{B} = \mathcal{C} \\
f_A(x) = 1 & f_A(x) = 1 & f_A(x) = 0 & f_A(x) = 0 \\
f_B(x) = 1 & f_B(x) = 0 & f_B(x) = 1 & f_B(x) = 0 \\
F(\mathcal{C}; x) = f_C(x) & F(\mathcal{C}; x) = f_C(x) & F(\mathcal{C}; x) = f_C(x) & F(\mathcal{C}; x) = f_C(x) \\
= 1 = f_A(x) \cdot f_B(x) & = 0 = f_A(x) \cdot f_B(x) & = 0 = f_A(x) \cdot f_B(x) & = 0 = f_A(x) \cdot f_B(x)
\end{array}$$

$$\begin{array}{cccc}
\mathcal{A} \cup \mathcal{B} = \mathcal{D} & \mathcal{A} \cup \mathcal{B} = \mathcal{D} & \mathcal{A} \cup \mathcal{B} = \mathcal{D} & \mathcal{A} \cup \mathcal{B} = \mathcal{D} \\
F(\mathcal{D}; x) = f_D(x) & F(\mathcal{D}; x) = f_D(x) & F(\mathcal{D}; x) = f_D(x) & F(\mathcal{D}; x) = f_D(x) \\
= 1 = f_A(x) + f_B(x) & = 1 = f_A(x) + f_B(x) & = 1 = f_A(x) + f_B(x) & = 0 = f_A(x) + f_B(x)
\end{array}$$

L'insieme delle funzioni caratteristiche $f_A(x)$ rappresenta l'insieme di tutte le variabili.

La applicazione F è una applicazione biiettiva quindi le due strutture algebriche sono isomorfe, come ci eravamo proposti di dimostrare.

Facciamo notare in particolare come $F(\mathcal{A}; x) = 1$ e come $F(0; x) = 0$.

B.16 Configurazioni

Consideriamo l'insieme di Boole $\mathcal{B} = \{0, 1\}$, i prodotti cartesiani $\mathcal{B} \times \mathcal{B} = \mathcal{B}^2$, $\quad \mathcal{B} \times \mathcal{B} \times \mathcal{B} = \mathcal{B}^3, \ldots$, ed i loro elementi:

$$\mathcal{B}^2 = \left\{ \begin{array}{c} (0\ 0) \\ (0\ 1) \\ (1\ 0) \\ (1\ 1) \end{array} \right\} \qquad \mathcal{B}^3 = \left\{ \begin{array}{c} (0\ 0\ 0) \\ (0\ 0\ 1) \\ (0\ 1\ 0) \\ (0\ 1\ 1) \\ (1\ 0\ 0) \\ (1\ 0\ 1) \\ (1\ 1\ 0) \\ (1\ 1\ 1) \end{array} \right\} \qquad \ldots$$

$$\mathcal{B}^2 = \{(x, y)\} \qquad \mathcal{B}^3 = \{(x, y, z)\} \qquad \ldots$$

Si può pensare $\mathcal{B}^n$ come un insieme che ha come elemento una n-upla ordinata di variabili booleane.

Ogni $n - pla$ ordinata di valori ottenibili dalle n variabili si chiama configurazione delle n variabili booleane: le configurazioni sono nel numero di 2^n (vedi appendice A.4).

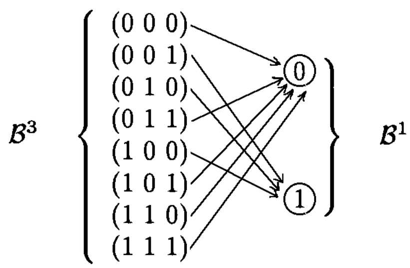
B.17 Funzioni booleane

Consideriamo una applicazione di $\mathcal{B}^n$ su $\mathcal{B}$. Questa dà origine ad una funzione booleana F:

$$(F(x_1, \ldots, x_n) = A)$$

Esempio B.17.1 Supponiamo n=3

x	y	z	A
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0



In generale una applicazione di $\mathcal{B}^n$ su $\mathcal{B}^p$ è una funzione booleana ad n variabili d'ingresso e p d'uscita (multipolo booleano).

Esempio B.17.2 **Supponiamo** $n = 3, p = 2$

x	y	z	A	B
0	**0**	**0**	**0**	**1**
0	**0**	**1**	**0**	**0**
0	**1**	**0**	**1**	**1**
0	**1**	**1**	**1**	**0**
1	**0**	**0**	**0**	**0**
1	**0**	**1**	**1**	**0**
1	**1**	**0**	**0**	**1**
1	**1**	**1**	**1**	**1**

B.18 Gruppi

DEF. B.18.1 Si dice MONOIDE una struttura algebrica del tipo $(\mathcal{E}; *)$ nella quale la composizione interna $*$ è associativa, cioè:

$$(x_i * x_j) * x_k = x_i * (x_j * x_k) \quad \forall x_i, x_j, x_k \in \mathcal{E}$$

Se l'operazione $*$ è anche commutativa, il MONOIDE è ABELIANO.

DEF. B.18.2 Si dice GRUPPO un monoide $(\mathcal{G}; *)$ che contenga, tra gli elementi di $\mathcal{G}$, un elemento neutro t e il simmetrico x_i' di ogni elemento x_i di $\mathcal{G}$, cioè se:

$$(x_i * x_j) * x_k = x_i * (x_j * x_k) \qquad \forall x_i, x_j, x_k \ \in \mathcal{G}$$

$$x_i * t = t * x_i = x_i \qquad \forall x_i \in \mathcal{G}$$

$$x_i * x_i' = x_i' * x_i = t \qquad \forall x_i \in \mathcal{G}$$

Se l'operazione $*$ è commutativa, il gruppo si dice GRUPPO ABELIANO.

Esempio B.18.1 L'insieme dei numeri interi relativi $(... -3, -2, -1, 0, 1, 2, 3, ...)$ assieme alla operazione somma, costituisce una struttura algebrica che è un GRUPPO ABELIANO $(\mathcal{N}; +)$.

Infatti l'operazione $+$ è associativa e commutativa

$$\begin{array}{lll} \mathcal{G} = \mathcal{N} & (a+b)+c = a+(b+c) & \forall a,b,c, \in \mathcal{N} \\ * \equiv + & a+b = b+a & \forall a,b \in \mathcal{N} \\ t \equiv 0 & a+0 = a & \forall a \in \mathcal{N} \\ a' \equiv (-a) & (-a)+a = 0 & \forall a \in \mathcal{N} \end{array}$$

Esempio B.18.2 L'insieme dei numeri interi relativi, privato dell'elemento zero assieme alla operazione prodotto, costituisce un gruppo abeliano $(\mathcal{N} - \{O\}; \cdot)$ con elemento neutro $t = 1$ ed elemento simmetrico di a pari a $\frac{1}{a} = a'$.

$$\begin{array}{ll} \mathcal{G} \equiv (\mathcal{N} - \{0\}) & (a \cdot b).c = a.(b.c) \\ * \equiv \cdot & a \cdot b = b \cdot a \\ t \equiv 1 & a \cdot 1 = a \\ a' \equiv \frac{1}{a} & a \cdot \frac{1}{a} = 1 \end{array}$$

Bisogna eliminare da $\mathcal{N}$ l'elemento zero perchè non è definito il suo simmetrico.

B.19 Corpi

DEF. B.19.1 Dicesi CORPO una struttura algebrica del tipo $(\mathcal{K}; +, -)$ che è un gruppo abeliano in $\mathcal{K}$ rispetto alla operazione $+$, mentre è un gruppo in $\mathcal{K} - \{O\}$ (cioè nell'insieme $\mathcal{K}$ privato dello zero) rispetto alla operazione $\cdot$.

DEF. B.19.2 Dicesi CAMPO NUMERICO un corpo che sia un gruppo abeliano in $\mathcal{K}$ rispetto a $+$ ed un corpo abeliano in $K - \{O\}$ rispetto alla operazione $\cdot$.

DEF. B.19.3 Dicesi CORPO DI GALOIS (CAMPO DI GALOIS) un campo numerico finito.

Bibliografia

1) G. Birkhoff, S. Mc Lane, *A Survey of Modern Algebra*, Macmillan, New York, 1953.

2) A. Kaufmann, M. Precigout, *Cours de mathèmatiques nouvelles*, Dunod, Paris, 1966.

3) J. Kuntzman, *Algèbre de Boole*, Dunod, Paris 1968.

4) L. Lombardo Radice, *Istituzioni di algebra astratta*, Feltrinelli, Torino, 1973.

5) E. Mendelson, *Algebra di Boole e circuito di commutazione*, Shaum Etas libri, 1977.