APPUNTI PER UN CORSO DI MATEMATICA DISCRETA

Nell'espressione "Matematica discreta", l'aggettivo "discreto" va inteso in contrapposizione all'aggettivo "continuo": senza pretesa di dare definizioni rigorose di queste due nozioni (che sono di pertinenza della branca della matematica detta topologia) possiamo dire che laddove la seconda descrive oggetti come una retta o una curva nel piano, la prima descrive insiemi di punti isolati.
Nel caso degli oggetti continui, i matematici hanno sviluppato metodi come il calcolo infinitesimale che, sfruttando il fatto che in un oggetto continuo ha senso considerare punti "sempre più vicini" a un punto dato, possono definire nozioni come quella di limite o derivata e studiare problemi come la determinazione della tangente a una curva o la lunghezza della curva stessa. Tali metodi costituiscono quindi una sorta di "matematica del continuo", e quindi le branche della matematica che non usano tali metodi possiamo pensarle come una sorta di "matematica discreta". In questo senso, è matematica discreta ad esempio lo studio dei numeri interi e delle loro proprietà, ma più in generale l'algebra nelle sue varie accezioni.
In questo corso non solo ricorderemo i fatti fondamentali dell'algebra dei numeri interi (e a dispetto della sua apparente semplicità ne vedremo importanti applicazioni, ad esempio in crittografia), ma anche la cosiddetta algebra vettoriale (fondamentale nella grafica ma non solo), o l'algebra di Boole, una sorta di formulazione algebrica della logica, di fondamentale importanza nell'informatica.
Alla base di tutte queste nozioni (ma in generale di ogni teoria matematica) sta la nozione di insieme, il cui studio sarà oggetto dei primi due capitoli di questi appunti.

Chapter 1

Teoria degli insiemi e algebra booleana

1.1 Insiemi, elementi, uguaglianza tra insiemi

Un *insieme* è una collezione di oggetti (concreti o astratti) detti i suoi *elementi*.

Osservazione 1.1. Quella che abbiamo appena dato è una definizione molto intuitiva, sufficiente per questo corso ma chiaramente insoddisfacente se si vuole rendere rigorosa fino in fondo la teoria. A questo scopo, è stata elaborata la cosiddetta *teoria assiomatica degli insiemi* che (analogamente a quanto succede in geometria euclidea con le nozioni di punto e retta) evita di dare le definizioni di insieme e elemento, assumendole come nozioni primitive non definite e basando la teoria su un insieme di affermazioni di partenza (gli assiomi, appunto) che devono essere soddisfatte da questi oggetti e che in un certo senso li definiscono implicitamente. Non tratteremo la teoria assiomatica degli insiemi, che è oltre gli scopi di questo corso.

Per indicare che x è un elemento di un insieme A, scriveremo

$$x \in A$$

che si legge "x è un elemento di A" oppure "x appartiene a A".

Dare un insieme significa quindi specificare chi sono i suoi elementi: questo può essere fatto o elencandoli esplicitamente (convenzionalmente all'interno di parentesi graffe), ad esempio

$$A = \{0, 1, 2, 3\}$$

oppure caratterizzando gli elementi dell'insieme mediante una loro proprietà: ad esempio, lo stesso insieme A appena definito può essere descritto anche come l'insieme dato dai numeri naturali[1] minori di 4, in simboli

$$A = \{x \in \mathbb{N} \mid x < 4\}.$$

In generale, useremo spesso la notazione

$$\{x \mid P(x)\}$$

per denotare l'insieme degli x dotati di una certa proprietà P.
Tale modo di definire un insieme è chiaramente l'unico possibile se l'insieme è infinito, nel qual caso chiaramente non possiamo scrivere tutti i suoi elementi.

Osservazione 1.2. Accettare che per ogni proprietà P che possiamo enunciare esista l'insieme degli x con la proprietà P può però portare a contraddizioni: un celebre esempio, dovuto a Russell e che fu tra i motivi per cui emerse la necessità di una più rigorosa teoria assiomatica degli insiemi, si ottiene scegliendo come proprietà P quella di "non appartenere a se stessi": prendendo l'insieme degli x con tale proprietà, ovvero

$$A = \{x \mid x \notin x\}$$

otterremmo una contraddizione chiedendoci se A appartiene a se stesso o no: se infatti $A \in A$, allora non soddisfa la proprietà scelta e quindi $A \notin A$; se viceversa $A \notin A$, allora A soddisfa esattamente la proprietà richiesta per appartenere ad A, e quindi $A \in A$: qualunque ipotesi facciamo, arriviamo a una contraddizione.
Nella teoria assiomatica degli insiemi, si mostra che la contraddizione appena trovata si evita se ogni volta che si vuole definire un insieme mediante una certa proprietà, si precisa che gli elementi x che soddisfano tale proprietà devono appartenere a un insieme già esistente: quindi solo con una formula del tipo $\{x \in A \mid P(x)\}$, dove P è una qualunque proprietà e A è un insieme dato, si definisce correttamente un insieme senza rischiare contraddizioni.
Tuttavia, noi continueremo a scrivere $\{x \mid P(x)\}$ sottointendendo che gli x che stiamo considerando appartengano a un insieme che contiene tutti gli oggetti

[1] Ricordiamo che si tratta dei numeri $0, 1, 2, 3, 4, 5...$ che si usano per contare: l'insieme di tali numeri si denota $\mathbb{N}$. Si indicano invece con il simbolo $\mathbb{Z}$ i *numeri interi*, ovvero $0, \pm 1, \pm 2...$, con $\mathbb{Q}$ i *numeri razionali*, ovvero le frazioni (esprimibili anche come numeri decimali con numero finito di cifre dopo a virgola o periodici) e con $\mathbb{R}$ i *numeri reali*, ovvero tutti i numeri decimali (anche quelli con una sequenza infinita non periodica di cifre dopo la virgola, detti irrazionali: ad esempio $\sqrt{2}$ o π).

e gli enti di cui abbiamo bisogno in questo corso: tale ipotetico insieme lo chiameremo *insieme universo* e lo denoteremo U.
Si badi tuttavia che l'insieme universo non è l'insieme di tutti gli insiemi possibili: si può vedere che anche tale nozione porterebbe a una contraddizione.

Dal momento che un insieme è determinato dai suoi elementi, verificare che due insiemi dati sono uguali significa verificare che questi hanno esattamente gli stessi elementi: ad esempio, se come sopra

$$A = \{0, 1, 2, 3\}, \quad B = \{x \in \mathbb{N} \mid x < 4\}$$

per verificare che effettivamente $A = B$ dobbiamo verificare innanzitutto che ogni elemento di A appartiene anche a B: ad esempio, 0 è un elemento di A, e poiché $0 < 4$ si ha che 0 soddisfa la proprietà che definisce B, quindi $0 \in B$; allo stesso modo si procede con $1, 2, 3$ e si dimostra che ogni elemento di A sta anche in B.
Questo non è però sufficiente: infatti, la stessa cosa sarebbe vera anche se avessimo preso $B = \{x \in \mathbb{N} \mid x < 5\}$, tuttavia in tal caso A non è uguale a B in quanto $B = \{0, 1, 2, 3, 4\}$.
Questo perché per dimostrare che $A = B$ non basta dimostrare che ogni elemento di A sta anche in B, ma anche che viceversa che ogni elemento di B sta anche in A.
La verifica di uno solo di questi due fatti, per esempio che ogni elemento di A appartiene anche a B, ci dice solo che A *è contenuto in* B: in tal caso, si scrive $A \subseteq B$. Diremo anche che A *è un sottoinsieme di* B.

1.2 Intersezione, unione e complementare

Siano A e B due insiemi dati. Possiamo allora considerare

(1) l'insieme, denotato $A \cap B$ (e detto *intersezione di* A *e* B) costituito dagli elementi comuni a A e B, ovvero, in simboli,

$$\{x \mid x \in A \text{ e } x \in B\}$$

dove, come nel significato usuale della congiunzione "e", si intende che $x \in A$ e $x \in B$ è verificata solo quando sono verificate sia $x \in A$ che $x \in B$, cioè solo per gli elementi x che stanno sia in A che in B.

Ad esempio, se $A = \{0, 1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$, si ha $A \cap B = \{2, 3\}$: infatti, $2 \in A$ e $2 \in B$ sono entrambe vere; e lo stesso per $3 \in A$, $3 \in B$; mentre ad esempio, 0 non appartiene a $A \cap B$ perché $0 \in A$ è vera ma

$0 \in B$ è falsa; analogamente, 5 non appartiene a $A \cap B$ perché $5 \in B$ è vera ma $5 \in A$ è falsa.

(2) l'insieme che si ottiene mettendo insieme gli elementi di A e gli elementi di B, ovvero, in simboli,

$$\{x \mid x \in A \text{ o } x \in B\}$$

dove la congiunzione "o" è usata nel senso che $x \in A$ o $x \in B$ è verificata quando è vera almeno una delle due tra $x \in A$ e $x \in B$ (quindi eventualmente anche entrambe: non va inteso come un "o" esclusivo, significato che tale congiunzione ha spesso nel linguaggio comune, nel quale deve valere l'una o l'altra ma non entrambe)

Ad esempio, se, come sopra, $A = \{0, 1, 2, 3\}$ e $B = \{2, 3, 4, 5\}$, si ha $A \cup B = \{0, 1, 2, 3, 4, 5\}$: infatti, per $x = 0$ e $x = 1$ si ha che $x \in A$ o $x \in B$ è verificata in quanto è vera $x \in A$ (come abbiamo detto, basta una sola delle due); per $x = 4$ e $x = 5$ invece $x \in A$ o $x \in B$ è verificata in quanto è vera $x \in B$ (pur non essendo vera $x \in A$); infine, per $x = 2$ e $x = 3$ sono vere sia $x \in A$ che $x \in B$ e quindi, in virtù del fatto che la congiunzione "o" non va intesa in senso esclusivo, $x \in A$ o $x \in B$ è verificata.

Il significato non esclusivo della congiuzione "o" che abbiamo definito e usato sopra è esattamente quello che aveva in latino la congiunzione "vel" (contrapposta a "aut" che invece significava un "o" esclusivo: o l'uno o l'altro, ma non entrambi): per questo motivo, tale congiunzione viene anche indicata con il simbolo $\vee$; in questa notazione, la congiunzione "e" viene indicata con il simbolo $\wedge$. Tale notazione ha il vantaggio di usare simboli universali (comprensibili anche ai non italiani), quindi da ora la seguiremo

Come ulteriore esempio di intersezione, consideriamo $A = \{0, 1, 2, 3\}$ e $B = \{4, 5\}$: in tal caso, l'affermazione $x \in A \wedge x \in B$ non è mai verificata, in quanto non esiste nessun elemento x per cui siano vere sia $x \in A$ che $x \in B$: quindi l'insieme $A \cap B = \{x \mid x \in A \wedge x \in B\}$ non ha elementi, ovvero è quello che si chiama l'*insieme vuoto*, che si denota $\emptyset$.
Quando $A \cap B = \emptyset$, si dice anche che gli insiemi A e B sono *disgiunti*.

Un'altra operazione che si può fare, in questo caso a partire da un solo insieme A, è quella del *complementare* $\bar{A}$, definito come

$$\bar{A} = \{x \mid x \notin A\} \tag{1.1}$$

ovvero l'insieme degli elementi che *non* appartengono ad A.

In effetti, la (1.1), come abbiamo detto all'inizio del capitolo, sta più precisamente per $\bar{A} = \{x \in U \mid x \notin A\}$. Volendo, si può definire anche il complementare di un insieme A dato *in un altro insieme* X, che non sia necessariamente l'insieme universo U, come $\{x \in X \mid x \notin A\}$: ad esempio, se A è l'insieme dei numeri naturali pari, ovvero $A = \{x \in \mathbb{N} \mid x \text{ è pari }\}$, il complementare di A in $\mathbb{N}$ è $\{x \in \mathbb{N} \mid x \text{ non è pari }\}$, ovvero l'insieme dei numeri dispari.

Così come le operazioni di intersezione e unione sono definite da simboli logici (rispettivamente $\wedge$ e $\vee$) anche il complementare è definito applicando un'operazione logica, ovvero la *negazione*, all'affermazione $x \in A$.
Il simbolo che si usa per indicare la negazione è $\neg$, oppure $\sim$.

L'intersezione e l'unione appena introdotte costituiscono a tutti gli effetti due operazioni che dati due insiemi ce ne danno un terzo, analogamente alla somma e alla moltiplicazione tra numeri, che ci danno un numero a partire da due numeri dati; analogamente, il complementare può essere pensato come un'operazione che a partire da un insieme ce ne dà un altro, analogamente a quello che succede ad esempio con l'opposto di un numero che manda a in $-a$ o l'inverso che manda a in a^{-1}.
Proseguendo con questa analogia, così come per fare calcoli e manipolare espressioni numeriche è necessario conoscere le proprietà di tali operazioni (es. la proprietà commutativa, per cui $a + b = b + a$ e $ab = ba$, oppure la proprietà distributiva, per cui $a(b+c) = ab+ac$ etc.) anche per l'intersezione, l'unione e il complementare è importante sapere quali proprietà valgono.
Ad esempio, l'intersezione gode della proprietà distributiva rispetto all'unione? ovvero ci chiediamo se dati comunque tre insiemi A, B, C, valga sempre l'uguaglianza

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{1.2}$$

In base alla definizione di uguaglianza tra insiemi, dobbiamo verificare se dato $x \in A \cap (B \cup C)$ si ha allora $x \in (A \cap B) \cup (A \cap C)$ e viceversa.
Ora, da una parte $x \in A \cap (B \cup C)$ significa per definizione di intersezione "$x \in A \wedge x \in B \cup C$", che a sua volta per definizione di unione si legge

$$x \in A \wedge (x \in B \vee x \in C) \tag{1.3}$$

Dall'altra, $x \in (A \cap B) \cup (A \cap C)$ significa $x \in (A \cap B) \vee x \in (A \cap C)$" cioè

$$\text{“}(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\text{''} \tag{1.4}$$

Quindi, per dimostrare la (1.2) bisogna dimostrare che se l'affermazione (1.3) è vera, allora lo è anche la (1.4), e viceversa.

È chiaro che la verifica di ciò richiede un approfondimento delle proprietà delle congiunzioni $\wedge$ e $\vee$, che ci consenta di manipolare espressioni logiche come la (1.3) e la (1.4).
Più precisamente, possiamo interpretare anche le congiunzioni $\wedge$ e $\vee$ come operazioni che date due affermazioni o proposizioni P e Q (nel caso di sopra che riguardano l'appartenenza di un elemento a un insieme, ma possiamo considerare anche proposizioni più generali) ci danno una terza proposizione "$P \wedge Q$" oppure "$P \vee Q$": a questo punto, la verifica delle proprietà di queste operazioni può essere pensata come una sorta di "algebra della logica" o di "algebra delle proposizioni", che si chiama più precisamente *algebra booleana* e che studieremo nel prossimo paragrafo.

1.3 Algebra booleana

L'algebra usuale studia espressioni nelle quali compaiono delle incognite x, y, z etc. che rappresentano numeri reali e ci dà formule e identità che coinvolgono queste incognite e che sono vere qualunque siano i numeri reali che sostituiamo ad esse. Ad esempio, quando l'algebra ci dice che

$$(x + y)^2 = x^2 + 2xy + y^2$$

ci sta dicendo che tale uguaglianza è verificata qualunque siano i valori numerici che sostituiamo al posto delle incognite x e y. In altre parole, scelti un valore numerico di x e un valore numerico di y e sostituendoli a primo e a secondo membro della formula otterremo lo stesso valore.

L'algebra booleana si comporta esattamente in maniera analoga: qui le incognite P, Q, R etc. rappresentano proposizioni che possono essere o vere o false, cioè possono assumere solo due valori "V" o "F", che possiamo per avere un'analogia ancora più stretta con l'algebra usuale rappresentare tramite i valori numerici rispettivamente 1 e 0.
Le formule dell'algebra booleana sono quindi formule che coinvolgono le incognite P, Q, R e le operazioni $\wedge$ e $\vee$, ad esempio

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R) \tag{1.5}$$

e la validità di una tale formula significa, esattamente come nell'algebra usuale, che qualunque valore numerico sostituiamo alle incognite (che può essere solo 0 o 1 a seconda che l'incognita rappresenti una proposizione vera o falsa rispettivamente) otteniamo lo stesso valore numerico (sempre 0 o 1) a primo e a secondo membro.

A questo scopo, iniziamo con il racchiudere in tabelle le proprietà base delle operazioni $\wedge$ e $\vee$ che abbiamo implicitamente usato nelle definizioni di intersezione e unione.
Abbiamo detto che un'affermazione come $P \wedge Q$ può essere vera solo se sono vere tutte e due le proposizioni P e Q, ed è falsa negli altri casi. Possiamo rappresentare questo in una tabella nella quale in corrispondenza dei vari possibili valori (0 o 1) di P e Q scriviamo il corrispondente valore di verità di $P \wedge Q$.

P	Q	P $\wedge$ Q
0	0	0
0	1	0
1	0	0
1	1	1

La tabella dice esattamente quanto abbiamo detto sopra: $P \wedge Q$ è vera (cioè assume valore 1) solamente quando sia P che Q hanno valore 1, cioè solo quando sono entrambe vere, e in tutti gli altri casi è falsa (cioè vale 0).
Una tabella come quella che abbiamo appena scritto prende il nome di *tavola di verità*.

Passiamo ora alla tavola di verità della congiunzione $\vee$: abbiamo detto che affinchè un'affermazione del tipo $P \vee Q$ sia vera è sufficiente che sia vera almeno una tra P e Q: quindi la tavola di verità è

P	Q	P $\wedge$ Q
0	0	0
0	1	1
1	0	1
1	1	1

La tabella dice esattamente quanto abbiamo detto sopra: $P \vee Q$ è vera (cioè assume valore 1) quando almeno una tra P e Q ha valore 1, cioè è vera.

A questo punto diamo anche la tavola di verità della negazione:

P	$\neg$ P
0	1
1	0

che rappresenta semplicemente che se P è vera, la sua negazione è falsa e viceversa.

A questo punto siamo pronti a verificare la validità della formula (1.5): ci basterà considerare tutti i possibili valori di verità di P,Q e R e vedere se per ogni scelta di valori il primo e il secondo membro ci danno lo stesso risultato: prima di tutto, i possibili valori delle tre incognite coinvolte sono

P	Q	R
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Visto che a secondo membro della (1.5) compaiono $P \wedge Q$ e $P \wedge R$, aggiungiamo due colonne con i valori di verità di queste due affermazioni (in corrispondenza dei valori che vediamo nelle prime tre colonne):

P	Q	R	$P \wedge Q$	$P \wedge R$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

A questo punto, possiamo scrivere la colonna di valori di $(P \wedge Q) \vee (P \wedge R)$ (cioè il secondo membro della (1.5)), usando la tavola di verità di $\vee$ che ci dice che $(P \wedge Q) \vee (P \wedge R)$ vale 0 solo quando sia $P \wedge Q$ che $P \wedge R$ valgono 0:

P	Q	R	P e Q	P e R	$(P \wedge Q) \vee (P \wedge R)$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

Fino a questo punto, la tabella che abbiamo scritto ci dice che valori assume il secondo membro della (1.5) in funzione di tutti i valori possibili di P, Q, R: ora dobbiamo fare la stessa cosa per il primo membro della (1.5), cioè $P \wedge (Q \vee R)$ e vedere se otteniamo esattamente gli stessi valori. Iniziamo con lo scrivere la colonna di $Q \vee R$

P	Q	R	P e Q	P e R	$(P \wedge Q) \vee (P \wedge R)$	Q $\vee$ R
0	0	0	0	0	0	0
0	0	1	0	0	0	1
0	1	0	0	0	0	1
0	1	1	0	0	0	1
1	0	0	0	0	0	0
1	0	1	0	1	1	1
1	1	0	1	0	1	1
1	1	1	1	1	1	1

e finalmente, guardando la prima e l'ultima colonna e usando la tavola di verità di $\wedge$, scriviamo la colonna con i valori di $P \wedge (Q \vee R)$, cioè il secondo membro della (1.5):

P	Q	R	P e Q	P e R	$(P \wedge Q) \vee (P \wedge R)$	Q $\vee$ R	P $\wedge$ (Q $\vee$ R)
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	0	1	0
0	1	1	0	0	0	1	0
1	0	0	0	0	0	0	0
1	0	1	0	1	1	1	1
1	1	0	1	0	1	1	1
1	1	1	1	1	1	1	1

Vediamo allora che la sesta e l'ottava colonna, corrispondenti rispettivamente al primo e al secondo membro della (1.5), sono uguali: quindi le espressioni corrispondenti assumono lo stesso valore qualunque siano i valori che assegniamo a P,Q, R: questo dimostra la validità dell'uguaglianza (1.5).

La (1.5) ci dice che nell'algebra booleana vale la proprietà distributiva di $\wedge$ rispetto a $\vee$.

Si noti che se usiamo la notazione (che si trova spesso in letteratura) della somma $+$ per indicare la congiunzione $\vee$ e del prodotto $\cdot$ per indicare $\wedge$, la (1.5) può essere scritta

$$P \cdot (Q + R) = P \cdot Q + P \cdot R$$

che ha il fascino di essere formalmente identica alla analoga proprietà distributiva valida nell'algebra usuale.
Tuttavia, non tutte le proprietà dell'algebra booleana risultano avere la forma di identità valide anche nell'algebra usuale: ad esempio, analogamente a quanto fatto sopra, si può dimostrare che vale anche la distributività di $\vee$ rispetto a $\wedge$, ovvero

$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

(la dimostrazione di questa identità è proposta come esercizio alla fine del capitolo). Nella notazione con somma e prodotto usata sopra, questa formula diventa

$$P + Q \cdot R = (P + Q) \cdot (P + R)$$

che è chiaramente falsa nell'algebra usuale, ma è un'identità valida nell'algebra booleana.

Ispirandoci alle proprietà delle operazioni somma e prodotto dell'algebra usuale e in particolare alle proprietà commutativa ($a + b = b + a$ e $ab = ba$) e associativa ($(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$), ci chiediamo se tali proprietà sono vere anche rispetto a $\vee$ e $\wedge$ in algebra booleana, ovvero

$$P \vee Q = Q \vee P, \quad P \wedge Q = Q \wedge P$$
$$(P \vee Q) \vee R = P \vee (Q \vee R)$$
$$(P \wedge Q) \wedge R = P \wedge (Q \wedge R)$$

La risposta è sì, e la validità di tali formule è facile da verificare (ad esempio, la $P \vee Q = Q \vee P$ si dimostra ricordando che $\vee$ è falsa solo se P e Q sono entrambe false, e questo non dipende chiaramente dall'ordine in cui le scriviamo).
Si osservi che se come P, Q, R prendiamo rispettivamente $x \in A, x \in B, x \in C$, dove A, B, C sono tre insiemi dati, allora le uguaglianze di sopra si riscrivono rispettivamente

$$x \in A \vee x \in B = x \in B \vee x \in A, \quad x \in A \wedge x \in B = x \in B \wedge x \in A$$
$$(x \in A \vee x \in B) \vee x \in C = x \in A \vee (x \in B \vee x \in C)$$
$$(x \in A \wedge x \in B) \wedge x \in C = x \in A \wedge (x \in B \wedge x \in C)$$

La validità di queste uguaglianze significa che se il loro primo membro vale 1 (cioè è vero) allora lo è anche il secondo membro, e viceversa: ma allora, ricordando le definizioni di unione e intersezione, esse dimostrano le uguaglianze

$$A \cup B = B \cup A, \quad A \cap B = B \cap A$$
$$(A \cup B) \cup C = A \cup (B \cup C), \quad (A \cap B) \cap C = A \cap (B \cap C)$$

Osservazione 1.3. Le prime due uguaglianze ci dicono che sia per l'unione che per l'intersezione vale la proprietà commutativa; la terza e la quarta ci dicono che vale per entrambe le operazioni la proprietà associativa, ovvero è indifferente dove scriviamo le parentesi tonde: tale proprietà ci consente quindi di omettere le parentesi e di scrivere semplicemente $A \cup B \cup C$ e $A \cap B \cap C$, senza ambiguità[2].

Così come in una espressione dell'algebra usuale possono comparire anche numeri reali (ad esempio $2x + 3y$), ovvero delle costanti, rispetto alle incognite che possono assumere qualunque valore reale, anche in algebra booleana possono comparire valori numerici costanti, in questo caso solo 0 e 1: si ha ad esempio la seguente identità algebrica base:

$$P \wedge 1 = P$$

dimostrata dalla tavola seguente, dove si vede che la colonna di $P \wedge 1$ è uguale alla colonna di P

P	1	P $\wedge$1
0	1	0
1	1	1

Analogamente, abbiamo le

$$P \wedge 0 = 0$$
$$P \vee 0 = P$$
$$P \vee 1 = 1$$

dimostrate rispettivamente dalle tabelle

[2]In un'operazione non associativa, invece, le parentesi sono necessarie: ad esempio l'espressione $2 : 2 : 2$ è ambigua in quanto se la interpretiamo come $2 : (2 : 2)$ essa vale 2, mentre se la interpretiamo come $(2 : 2) : 2$ essa vale $\frac{1}{2}$.

P	0	P $\wedge$0
0	0	0
1	0	0

P	0	P $\vee$0
0	0	0
1	0	1

P	1	P $\vee$1
0	1	1
1	1	1

Si noti che nella notazione con somma $+$ per $\vee$ e prodotto $\cdot$ per $\wedge$, le identità di sopra diventano

$$P \cdot 1 = P$$

$$P \cdot 0 = 0$$

$$P + 0 = P$$

$$P + 1 = 1$$

Con questa notazione, vediamo che le prime tre sono vere anche nell'algebra usuale, mentre la quarta vale solo nell'algebra booleana.

Vediamo ora anche alcune identità che coinvolgono la negazione $\neg$: la prima è

$$\neg(\neg P) = P$$

la cui validità è dimostrata dalla tabella

P	$\neg$ P	$\neg(\neg P)$
0	1	0
1	0	1

Come esempio di altre due formule che valgono in algebra booleana ma non in algebra usuale, diamo le seguenti:

$$P \wedge P = P$$

$$P \vee P = P$$

Si dice che le operazioni $\wedge$ e $\vee$ sono *idempotenti*. Nella notazione con somma e prodotto tali proprietà si scrivono rispettivamente $P \cdot P = P$ e $P + P = P$. La loro verifica mediante tavole di verità è immediata:

P	$P \wedge P$
0	0
1	1

P	$P \vee P$
0	0
1	1

Altre due identità molto importanti in algebra booleana sono le seguenti:

$$\neg(P \wedge Q) = \neg P \vee \neg Q$$
$$\neg(P \vee Q) = \neg P \wedge \neg Q$$

dette *leggi di De Morgan.*
La loro validità è dimostrata dal fatto che la quarta e l'ultima colonna in ognuna delle seguenti tabelle sono uguali:

P	Q	P $\wedge$ Q	$\neg(P \wedge Q)$	$\neg P$	$\neg Q$	$\neg P \vee \neg Q$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0	1	1
1	1	1	0	0	0	0

P	Q	P $\vee$ Q	$\neg(P \vee Q)$	$\neg P$	$\neg Q$	$\neg P \wedge \neg Q$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

1.4 L'implicazione

Oltre a "e" e "o" c'è un terzo modo di ottenere una proposizione combinandone due date P e Q, ovvero l'implicazione "se P allora Q", denotata con il simbolo $P \Rightarrow Q$.
Ad esempio, se P è la proposizione "piove" e Q è la proposizione "prendo l'ombrello" allora $P \Rightarrow Q$ è la nuova proposizione "se piove allora prendo l'ombrello.
Nell'espressione $P \Rightarrow Q$ (che si legge anche "P implica Q") P si dice *antecedente* e Q *conseguente.*

Così come fatto per $\wedge$ e $\vee$, anche l'implicazione $\Rightarrow$ viene definita mediante una tavola di verità, che è la seguente:

P	Q	P $\Rightarrow$ Q
0	0	1
0	1	1
1	0	0
1	1	1

Tale tavola implica ad esempio che affermazioni come "se 1=2 allora Parigi è la capitale dell'Italia" o "se 1=2 allora Roma è la capitale dell'Italia" sono vere (la prima per la prima riga della tavola, in cui sia antecedente che conseguente sono falsi, e la seconda per la seconda riga, in cui l'antecedente è falso e il conseguente è vero): a parte l'impressione di spaesamento provocato dal fatto che in queste affermazioni antecedente e conseguente non hanno nessun legame di tipo causale o temporale tra loro (come invece succede quando si usa l'implicazione nel linguaggio comune), si potrebbe comprensibilmente avere qualche difficoltà nell'accettare che sia vera un'implicazione in cui l'antecedente è falso e il conseguente è vero oppure in cui sia antecedente che conseguente sono falsi.
Tuttavia, ci sono dei motivi precisi per cui i logici (a partire da quelli dell'antichità per arrivare, attraverso i logici medievali, a quelli moderni) hanno assegnato all'implicazione la tavola di verità data sopra. Noi ne riportiamo due:

(1) la prima giustificazione alla tavola di verità dell'implicazione è che vogliamo che essa sia l'operazione logica che corrisponde all'inclusione tra insiemi. Più precisamente, dati due insiemi A e B vogliamo che $A \subseteq B$ esattamente quando l'implicazione

$$x \in A \Rightarrow x \in B \tag{1.6}$$

è vera per ogni x, cioè qualunque cosa sostituiamo a x.

Ad esempio, prendiamo $A = \{1, 2, 3\}$ e $B = \{1, 2, 3, 4, 5\}$, per i quali chiaramente vale $A \subseteq B$: quindi vogliamo che (1.6) sia vera qualunque cosa sostituiamo a x.

Ad esempio, poniamo $x = 4$: vogliamo che l'implicazione

$$4 \in A \Rightarrow 4 \in B$$

(nella quale l'antecedente è falso e il conseguente è vero) sia vera: questa è esattamente la situazione descritta dalla seconda riga della tavola di verità di $\Rightarrow$.

Ponendo invece ad esempio $x = 8$, vogliamo che anche l'implicazione

$$8 \in A \Rightarrow 8 \in B$$

(nella quale sia l'antecedente che il conseguente sono falsi) sia vera: questa è la situazione descritta dalla prima riga della tavola di verità di $\Rightarrow$.

Questo giustifica la prima e la seconda riga della tavola di verità data per $\Rightarrow$, che sono solitamente quelle di più difficile comprensione.

(2) una seconda giustificazione della tavola di verità dell'implicazione è che $P \Rightarrow Q$ va letto come un sinonimo di

$$\neg(P \wedge \neg Q)$$

(che potremmo leggere e interpretare come "non è possibile che valgano contemporaneamente P e la negazione di Q", che è un'interpretazione ragionevole del fatto che P implichi Q). Se si accetta tale equivalenza, allora la tavola di verità di $P \Rightarrow Q$ è esattamente quella di $\neg(P \wedge \neg Q)$, che ricaviamo subito:

P	Q	$\neg Q$	$P \wedge \neg Q$	$\neg(P \wedge \neg Q)$
0	0	1	0	1
0	1	0	0	1
1	0	1	1	0
1	1	0	0	1

e che come si vede coincide con quella data sopra per $\Rightarrow$.

Osserviamo che per l'operazione di implicazione non vale la proprietà commutativa, ovvero l'uguaglianza $(P \Rightarrow Q) = (Q \Rightarrow P)$ non è vera: basta verificare che le due espressioni non hanno la stessa tavola di verità (ad esempio, quando P vale 0 e Q vale 1, l'implicazione $P \Rightarrow Q$ vale 1 mentre l'implicazione opposta $Q \Rightarrow P$ vale 0); si dimostra invece che vale l'uguaglianza

$$(P \Rightarrow Q) = (\neg Q \Rightarrow \neg P)$$

come si vede calcolando la tavola di verità di $\neg Q \Rightarrow \neg P$

P	Q	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
0	0	1	1	1
0	1	0	1	1
1	0	1	0	0
1	1	0	0	1

che risulta essere la stessa di $P \Rightarrow Q$.
La $\neg Q \Rightarrow \neg P$ si dice *contronominale* di $P \Rightarrow Q$. Il fatto che ogni implicazione sia logicamente equivalente alla sua contronominale è spesso usato per riformulare in maniera alternativa un teorema da dimostrare: ad esempio, per dimostrare il teorema "se x è dispari allora x^2 è dispari" si può equivalentemente dimostrare l'affermazione "se x^2 è pari allora x è pari", che è esattamente la sua contronominale.

Osservazione 1.4. Se vale l'implicazione $P \Rightarrow Q$, si dice che P *è condizione sufficiente per* Q mentre Q *è condizione necessaria per* P: questo è in accordo con l'uso di tali espressioni nel linguaggio ordinario, ad esempio il fatto che l'implicazione "se x è veneto allora x è italiano" sia vera ci dice che essere veneti è condizione sufficiente per essere italiani (ma non necessaria: si può essere italiani anche essendo sardi, per esempio) e che essere italiani è condizione necessaria per essere veneti (ma non sufficiente: esistono italiani che non sono veneti, per esempio i sardi).

Un altro simbolo logico che si può definire a partire dall'implicazione è quello della *doppia implicazione* $\Leftrightarrow$: scriveremo $P \Leftrightarrow Q$ per intendere

$$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$$

Ricavando la tavola di verità di questa espressione come segue

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

ovvero la tavola di verità della doppia implicazione è

P	Q	$P \Leftrightarrow Q$
0	0	1
0	1	0
1	0	0
1	1	1

Quindi una doppia implicazione è vera solamente quando le due proposizioni che la compongono hanno lo stesso valore di verità.

Osservazione 1.5. Dal momento che due insiemi A e B sono uguali esattamente quando per ogni x si ha $x \in A \Rightarrow x \in B$ e viceversa $x \in B \Rightarrow x \in A$, possiamo unire queste due condizioni usando la doppia implicazione e dire che due insiemi A e B sono uguali quando per ogni x si ha $x \in A \Leftrightarrow x \in B$.

1.5 Tautologie e contraddizioni

Consideriamo l'espressione $P \vee \neg P$ e ricaviamone la tavola di verità:

P	$\neg P$	$P \vee \neg P$
0	1	1
1	0	1

Notiamo che tale espressione assume sempre valore 1 (cioè è sempre vera) indipendentemente dal valore di P: espressioni di questo tipo si chiamano *tautologie*.
Il fatto che la $P \vee \neg P$ sia una tautologia risulta comprensibile se la si interpreta come "o vale P o non vale P", che rende più evidente il fatto che essa è sicuramente e sempre vera (si tratta del cosiddetto *principio del terzo escluso*).

Consideriamo ora invece l'espressione $P \wedge \neg P$ e ricaviamone la tavola di verità:

P	$\neg P$	$P \wedge \neg P$
0	1	0
1	0	0

Notiamo stavolta che tale espressione assume sempre valore 0 (cioè è sempre falsa) indipendentemente dal valore di P: espressioni di questo tipo si chiamano *contraddizioni*.
Il fatto che la $P \wedge \neg P$ sia una contraddizione risulta comprensibile se la si interpreta come "si ha contemporaneamente P e non P", che rende più evidente il fatto che essa si contraddice ed è quindi sicuramente sempre falsa.
Proporremo negli esercizi altri importanti esempi di tautologie e contraddizioni.

Osservazione 1.6. Si osservi che grazie alla doppia implicazione possiamo riformulare tutte le identità logiche viste sopra come tautologie, ad esempio il fatto che vale la (1.5)

$$P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$$

può essere riformulato dicendo che la

$$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$$

è una tautologia: infatti, nella prima forma l'uguaglianza significa che il primo e il secondo membro assumono lo stesso valore per qualunque assegnazione dei valori di verità di P, Q, R: dal momento che, come si vede nella sua tavola di verità, la doppia implicazione $P_1 \Leftrightarrow P_2$ è vera solamente quando P_1 e P_2 hanno lo stesso valore di verità, la seconda forma risulta essere una tautologia.

Osservazione 1.7. L'algebra booleana che abbiamo discusso prevede che le incognite (che rappresentano proposizioni) possano assumere solo due valori 0 e 1 (ovvero essere o false o vere). Logici e matematici hanno però provato a sviluppare anche algebre nelle quali ci siano più valori di verità, ad esempio 0, 1, $\frac{1}{2}$: una tale algebra vuole modellizzare una logica nella quale le proposizioni oltre a essere false o vere possono essere anche "possibili" (e assumono quindi un valore di verità intermedio, per l'appunto $\frac{1}{2}$).
Quando si aggiungono valori di verità, bisogna però stare attenti a definire le nuove tavole di verità (ovvero bisogna dire che valori assumono $P \wedge Q$, $P \vee Q$ e $\neg P$ in funzione dei vari valori di verità di P e Q, per i quali ora è ammesso anche $\frac{1}{2}$) in modo da mantenere alcune delle proprietà alle quali in nessuna logica si vuole rinunciare, ad esempio il fatto che $P \vee \neg P$ sia una tautologia o che $P \wedge \neg P$ sia una contraddizione.
Ad esempio, Lukasiewicz nel 1920 ha proposto di definire $P \wedge Q$ come il minimo dei valori di P e Q (quindi ad esempio se P vale $\frac{1}{2}$ e Q vale 1, allora $P \wedge Q$ vale $\frac{1}{2}$), $P \vee Q$ come il massimo dei valori di P e Q (quindi ad esempio se P vale $\frac{1}{2}$ e Q vale 1, allora $P \vee Q$ vale 1) e $\neg P$ come 0 non solo se P vale 1 ma anche se vale $\frac{1}{2}$.
Il problema di tali definizioni, che sembrano sensate (ad esempio, la negazione di una proposizione possibile è ragionevole che sia falsa) è che mentre $P \wedge \neg P$ rimane una contraddizione (se P vale $\frac{1}{2}$ allora $\neg P$ in base alla scelta di Lukasiewicz vale 0, e quindi sempre in base alle sue scelte $P \wedge \neg P$ è sempre zero) si ha che $P \vee \neg P$ non è più una tautologia! Infatti, se P vale $\frac{1}{2}$, si ha che $\neg P$ vale 0 e quindi $P \vee \neg P$, che è per la definizione di Lukasiewicz il massimo dei valori di verità di P e $\neg P$ vale $\frac{1}{2}$ (e non 1, quindi non è una tautologia).

Esistono anche le cosiddette *logiche fuzzy*, nelle quali le proposizioni possono assumere come valore di verità qualunque numero reale compreso tra 0 e 1

(l'idea è rendere infinite sfumature di verità): i problemi da affrontare in tali costruzioni sono gli stessi che abbiamo ilustrato nel caso della logica a 3 valori, ma omettiamo ulteriori dettagli.

1.6 I quantificatori universali

Introduciamo ora altri due importanti simboli della logica, detti quantificatori universali:

(1) il simbolo $\forall$, che va letto "per ogni" (ad esempio, data una proprietà P, la formula $\forall x \in X\ P(x)$ significa "per ogni elemento x di X, x ha la proprietà P", ovvero "tutti gli elementi di X hanno la proprietà P.

(2) il simbolo $\exists$, che va letto "esiste" (ad esempio, data una proprietà P, la formula $\exists x \in X\ P(x)$ significa "esiste un elemento x di X tale che x ha la proprietà P", ovvero "almeno un elemento di X ha la proprietà P.

Osserviamo che la negazione di $\forall x \in X\ P(x)$ è $\exists x \in X\ \neg P(x)$: infatti, se non è vero che tutti gli elementi di X hanno la proprietà P, questo significa che ne esiste almeno uno che non ce l'ha (e non, come in un tipico errore, che non ce l'abbia nessuno); analogamente, la negazione di $\exists x \in X\ P(x)$ è $\forall x \in X\ \neg P(x)$: infatti, se non è vero che esiste un elemento di X che ha la proprietà P, questo significa che nessun elemento di X ce l'ha (ovvero per ogni x, x non ce l'ha).

I quantificatori universali possono essere usati per estendere le definizioni di intersezione e unione di due insiemi a qualunque numero di insiemi, anche infinito.
Più precisamente, iniziamo con l'osservare con lo scegliere una notazione opportuna per unioni e intersezioni che comprendano più di due insiemi: l'uso delle lettere dell'alfabeto A, B, C per indicare questi ultimi è estremamente limitante in quanto non ci consente ad esempio di scrivere l'unione o l'intersezione di più insiemi di quante siano le lettere dell'alfabeto: tuttavia, tale problema si risolve semplicemente denotando tutti gli insiemi con la stessa lettera ma aggiungendo un indice che ci dica se si tratta del primo insieme, del secondo, del terzo e così via: A_1, A_2, A_3, etc.
In questo modo, possiamo scrivere l'unione e l'intersezione di un qualunque numero di insiemi (diciamo n insiemi, dove n rappresenta un qualunque numero naturale) con le notazioni seguenti:

$$A_1 \cap A_2 \cap \cdots \cap A_n, \quad A_1 \cup A_2 \cup \cdots \cup A_n$$

(si noti che non abbiamo bisogno di parentesi quando uniamo o intersechiamo o uniamo più di due insiemi grazie alla proprietà associativa di tali operazioni, come visto nell'Osservazione 1.3).
Per evitare di scrivere più volte il simbolo di intersezione, una notazione efficace per indicare le stesse cose è la seguente

$$\cap_{j=1}^{n} A_j, \quad \cup_{j=1}^{n} A_j$$

che significano esattamente che stiamo facendo l'intersezione (o l'unione) degli insiemi A_j con j che va da 1 a n.
In base alla definizione di intersezione, che usa la congiunzione "e", si ha quindi che $x \in \cap_{j=1}^{n} A_j$ solo se $x \in A_j$ è vera per tutti gli indici j da 1 a n, mentre in base alla definizione di unione, che usa la congiunzione "o", si ha quindi che $x \in \cup_{j=1}^{n} A_j$ solo se $x \in A_j$ è vera per almeno un indice j da 1 a n, cioè se esiste almeno un j compreso tra 1 e n per cui si ha $x \in A_j$.
In questa riformulazione, l'intersezione e l'unione di insiemi si estende immediatamente a una qualunque famiglia di insiemi, anche infinita: più precisamente, data una famiglia A_i di insiemi, dove i è un indice che appartiene a una certo insieme di indici I (ad esempio, potrebbe essere $I = \mathbb{N}$ e allora la famiglia è data da $A_0, A_1, A_2, A_3, \ldots$ e così via): l'intersezione di tutti gli insiemi di questa famiglia si denota $\cap_{i \in I} A_i$ ed è definita come

$$\cap_{i \in I} A_i = \{x \mid \forall i \in I \ x \in A_i\}$$

ovvero l'insieme degli x che appartengono ad A_i per tutti gli indici $i \in I$.
Analogamente, l'unione di tutti gli insiemi di questa famiglia si denota $\cup_{i \in I} A_i$ ed è definita come

$$\cup_{i \in I} A_i = \{x \mid \exists i \in I \ x \in A_i\}$$

ovvero l'insieme degli x che appartengono ad A_i per almeno un indice $i \in I$.

Esercizi

(1) si dimostri la distributività di $\vee$ rispetto a $\wedge$, cioè la seguente identità in algebra booleana:

$$P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$$

(2) Si dimostri che le seguenti sono tautologie

$$P \wedge (P \Rightarrow Q) \Rightarrow Q$$
$$(\neg P \Rightarrow P) \Rightarrow P$$
$$P \wedge Q \Rightarrow P$$
$$P \Rightarrow P \vee Q$$

(le prime due si chiamano rispettivamente *modus ponens* e *consequentia mirabilis*) mentre non lo sono

$$P \Rightarrow P \wedge Q$$
$$P \vee Q \Rightarrow P$$

(3) Si dimostrino le seguenti uguaglianze:

$$A \cap \emptyset = \emptyset$$
$$A \cup \emptyset = A$$
$$\emptyset \subseteq A$$

(la terza afferma che l'insieme vuoto è sottoinsieme di qualunque insieme A).

Chapter 2

Insiemi, relazioni e funzioni