Metodi Matematici per l'Informatica - Dispensa 1
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Combinatoria = arte/tecnica del contare insiemi finiti. Alcune domande tipiche della Combinatoria:

- Quante targhe è possibile formare nel sistema attualmente in uso in Italia (ogni targa è composta da una sequenza di 2 lettere, 3 cifre, 2 lettere)? Quante di queste targhe contengono almeno una T e almeno un 9?
- Quanti numeri primi esistono tra 1 e 1 milione?
- Quanti sono gli esiti del lancio di 2 dadi a 6 facce, distinguendo il risultato del primo dado da quello del secondo? E quanti sono gli esiti se non distinguiamo tra i due dadi?
- Quanti modi ho di vestirmi se il mio guardaroba è composto da 3 giacche, 2 camicie, 4 pantaloni e 3 paia di scarpe, assumendo che uso un capo di ogni tipo e non mescolo scarpe di paia diverse? Quanti modi ho di vestirmi se assumo di usare al più un capo di ogni tipo? Quanti modi ho di vestirmi per la giornata "mezzi nudi", in cui è regola mettere o la camicia o il pantalone (e un capo di ogni altro tipo)?
- Se in una elezione si presentano 15 liste ciascuna composta di 8 candidati e il voto consiste nello scegliere una lista e nell'indicare al più 3 preferenze tra i candidati di quella lista, quanti sono gli esiti possibili del voto?
- Quanti modi ho di ottenere il numero 30 come somma di 4 numeri interi non negativi, contando l'ordine degli addendi? Quanti modi ho di ottenere 30 con numeri interi positivi senza contare l'ordine degli addendi?

1 Principio Moltiplicativo

Il Principio Moltiplicativo è un principio estremamente intuitivo che permette di risolvere un numero sorprendente di problemi di conteggio anche non banali.

> Principio Moltiplicativo: Se scelgo un oggetto tra m oggetti e un oggetto tra n oggetti, quante sono le possibili scelte?

Si vede facilmente che le scelte possibili sono $m \times n$. Ho infatti m possibili scelte per il primo oggetto e, per ciascuna di queste, ho n possibili scelte per il secondo oggetto.

Esempio 1 *Se ho 5 cani e 4 gatti, quante coppie cane/gatto posso formare? La risposta è* 5×4. *Si osservi che ci interessa contare tutte le possibili coppie, non solo quelle che posso formare simultaneamente.*

Il Principio Moltiplicativo (PM) si generalizza facilmente a più di due scelte.

Esempio 2 *Se ho 5 cani e 4 gatti e 8 topi, quanti trio cane/gatto/topo posso formare? La risposta è* $5 \times 4 \times 8$.

Principio Moltiplicativo Generale (PMG): Se scelgo un primo oggetto tra m_1, un secondo oggetto tra m_2, ... un ultimo oggetto tra m_t, ho $m_1 \times m_2 \times \cdots \times m_t$ possibili scelte.

Esempio 3 *Quanti modi ho di vestirmi se il mio guardaroba è composto da 3 giacche, 2 camicie, 4 pantaloni e 3 paia di scarpe, assumendo che uso un capo di ogni tipo e non mescolo scarpe di paia diverse? Ho* $3 \times 2 \times 4 \times 3$ *modi di vestirmi.*

Esempio 4 *Quante targhe è possibile formare nel sistema attualmente in uso in Italia (ogni targa è composta da una sequenza di 2 lettere, 3 cifre, 2 lettere)? Assumendo di usare l'alfabeto latino (composto di 26 lettere) le targhe possibili sono*

$$26 \times 26 \times 10 \times 10 \times 10 \times 26 \times 26 = 26^2 \times 10^3 \times 26^2 = 456976000.$$

Esempio 5 *Se da un'urna contenente i numeri* $1, 2, 3, \ldots, 10$ *estraggo in successione due numneri quante sono le possibili estrazioni? Sono* $10 \times 9 = 90$. *Abbiamo applicato il PM, osservando che scelgo il primo numero tra 10 mentre il secondo numero è scelto tra 9 (tutti i numeri di partenza tranne quello estratto per primo).*

Esempio 6 *Quante stringhe/parole di 5 lettere posso scrivere usando le lettere* $A, B, C, D, E, F, G, H, I, J$ *che non iniziano con H e che non contengo due cifre consecutive identiche? La risposta è* 9^5*, applicando il PMG: ho infatti 9 scelte per la prima lettera (tutte tranne la H, 9 scelte per la seconda (tutte tranne la precedente), 9 scelte per la terza (tutte tranne la precedente) e così via.*

Consideriamo il seguente problema: ho una collezione di lettere A, M, Q, T, U , Z e voglio contare tutti i modi possibili per selezionare una sottocollezione, ossia scegliere alcune lettere e altre no. Non mi interessa l'ordine degli elementi, ma solo quali elementi sono selezionati (ossia non distinguo tra una scelta M, Q, Z e Q, M, Z). Più in generale suppongo di avere una collezione di n oggetti distinti e di voler contare tutte le possibili scelte di alcuni tra essi, senza contare l'ordine.

Potrei pensare di approcciare il problema così: a priori, posso selezionare una collezione di m oggetti tra i miei n totali, dove m varia tra $0, 1, 2, 3, \ldots, n-1, n$ (0 corrisponde a non scegliere alcun oggetto, e n a sceglierli tutti). Posso quindi provare a spezzare il problema come segue: conto quante scelte ho di m oggetti tra i miei n totali e sommo tutti i risultati. Per $m = 0$ la domanda: quanti modi ho di scegliere m oggetti tra n ha una risposta ovvia; ossia 1. Stessa cosa per $m = 1$: ho infatti n modi di scegliere m elementi tra n. Analogamente si può rispondere facilmente alla domanda per $m = n$ e anche per $n - 1$ (la risposta è n). Ma quanti modi ho di scegliere m elementi tra n per $m = 2$? E per $m = 3$? La risposta non è immediata, e il solo PM non ci aiuta.

Proviamo quindi ad aggirare il problema. A questo scopo definiamo una traduzione (o associazione, o riduzione), descrivendo una regola per trasformare uno degli oggetti che vogliamo contare (ossia una scelta di m oggetti tra gli n totali) in un oggetto di tipo diverso. In questo caso associamo a una scelta arbitraria di m oggetti tra gli n totali una stringa binaria (ossia composta di 0 e di 1) di lunghezza n.

Consideriamo l'esempio di sopra. Ho 6 oggetti di partenza, A, M, Q, T, U, Z. Una scelta di alcuni tra questi è per esempio M, T, Z. A questa scelta associamo la stringa 010101. Come abbiamo ottenuto questa stringa? Abbiamo messo in sequenza le risposte alle domande: A è nella scelta (se sì, metto 1; se no, metto 0)? M è nella scelta? Q è nella scelta? T è nella scelta? U è nella scelta? Z è nella scelta? Con questa regola possiamo associare a una scelta arbitraria di lettere tra A, M, Q, T, U, Z una stringa binaria di lunghezza 6. Per esempio, alla scelta di nessuna lettera corrisponde la stringa 000000; alla scelta di tutte le lettere corrisponde la stringa 111111; alla scelta delle lettere U, Z corrisponde la stringa 000011, e così via.

Si osserva che una stringa binaria di lunghezza 6 descrive completamente una delle possibili scelte di lettere tra A,M,Q,T,U,Z, nel senso che a ogni scelta di questo tipo corrisponde una e una sola stringa binaria

di lunghezza 6 e, viceversa, a ogni stringa binaria di lunghezza 6 corrisponde una scelta: per es. alla stringa 101010 corrisponde la scelta A, Q, U.

Questo ci permette di concludere (almeno intuitivamente) che le stringhe binarie di lunghezza 6 sono tante quante le scelte di lettere tra A, M, Q, T, U, Z, ossia la collezione di oggetti che volevamo contare. [Torneremo più avanti, in modo formale, su questo principio che qui usiamo intuitivamente].

Qual è il vantaggio? Il vantaggio è che sappiamo contare le stringhe binarie di lunghezza 6 usando il PMG: infatti ho 2 scelte (0 o 1) per il primo elemento, due per il secondo e così via. In tutto sono quindi $2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^6$.

Per l'osservazione di sopra concludiamo che anche le scelte possibili di lettere tra A,M,Q,T,U,Z sono 2^6.

Il ragionamento di sopra si generalizza a una collezione generica di n oggetti, siano $a_1, a_2, \ldots, a_n$. Una scelta di alcuni di questi oggetti ha la forma $a_{i_1}, \ldots, a_{i_m}$ per un qualche m tra 0 e n, dove gli indici $i_1, \ldots, i_m$ variano tra 1 e n, e per convenzione supponiamo di averli scritti in ordine crescente, ossia $i_1 < i_2 < \cdots < i_m$. A un oggetto di questo tipo associamo la stringa binaria $b_1 b_2 \ldots b_n$ definita così: $b_1 = 0$ se 1 non è uno degli $i_1, \ldots, i_m$, $= 1$ altrimenti; $b_2 = 0$ se 2 non è uno degli $i_1, \ldots, i_m$, $=1$ altrimenti; etc. In altre parole stiamo segnando, per ogni elemento $a_1, \ldots, a_n$ della collezione di partenza, la sua presenza (1) o assenza (0) nella scelta $a_{i_1}, \ldots, a_{i_m}$. Per esempio alla scelta di elementi a_2, a_4, a_6 associamo la stringa 010101.

Per il PMG il numero di stringhe binarie di lunghezza n è 2^n. Concludiamo che il numero di scelte di oggetti in una collezione di n oggetti è pure 2^n.

Teorema 1 *Ci sono 2^n modi diversi di selezionare elementi in una collezione di n oggetti.*

Il risultato esposto sopra si può più rigorosamente esprimere usando il linguaggio della Teoria degli Insiemi (cfr. libro di testo A1); e anzi illustra la naturalezza e la convenienza di introdurre le nozioni elementari di tale teoria. Della collezione di partenza ci interessa soltanto che consista di n elementi distinti (e non, per esempio, del loro ordine), e analogamente vale per le scelte di alcuni tra questi elementi. In termini insiemistici il risultato di sopra si esprime, equivalentemente, così:

- Il numero di sottinsiemi di un insieme di n elementi è 2^n.
- L'insieme potenza (o insieme della parti) di un insieme di n elementi contiene 2^n elementi.
- Se $A = \{a_1, \ldots, a_n\}$ allora $P(A) = \{X \ : \ X \subseteq A\}$ ha 2^n elementi.

Metodi Matematici per l'Informatica - Dispensa 2
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Figure fondamentali della Combinatoria.

1 Disposizioni semplici

Esempio 1 *Sia A l'insieme di tre elementi $\{a, b, c\}$. Quanti modi ci sono di formare sequenze ordinate di lunghezza $1, 2, 3$? Le sequenze di lunghezza 1 sono solo tre:*

$$a, b, c.$$

Le sequenze di lunghezza 2 sono 6:

$$ab, ac, ba, bc, ca, cb$$

Le sequenze di lunghezza 3 sono 6:

$$abc, acb, bac, bca, cab, cba$$

Per contarle possiamo usare il PGM: per il caso di lunghezza 2 ho 3 scelte per la prima posizione, 2 scelte per la seconda, dunque $3 \times 2 = 6$. Per il caso di lunghezza 3 ho 3 scelte per la prima posizione, 2 scelte per la seconda, 1 scelta per la terza, dunque $3 \times 2 \times 1 = 6$.

L'esempio si generalizza facilmente.

Definizione 1 *Sia $1 \leq k \leq n$. Chiamiamo disposizione semplice di ordine k di n oggetti una sequenza ordinata $(x_1, \ldots, x_k)$ di k oggetti distinti scelti tra gli n totali.*

Posso usare il PM per contare le disposizioni semplici di ordine k di n oggetti:

Ordine 1: n scelte.
Ordine 2: $n \times (n-1)$ scelte
Ordine 3: $n \times (n-1) \times (n-2)$ scelte
...
Ordine k: $n \times (n-1) \times (n-2) \times \cdots \times (n-(k-1))$ scelte.

Indicando con $D_{n,k}$ il numero delle disposizioni semplici di ordine k di n oggetti abbiamo dunque che

$$D_{n,k} = n \times (n-1) \times (n-2) \times \cdots \times (n-(k-1))$$

Per ricordarsi l'espressione basti ricordare che consiste di k fattori. L'espressione è ovviamente strettamente legata al fattoriale, dove con fattoriale di n intendiamo il prodotto dei fattori n, $(n-1)$, $(n-2)$, ..., 2, 1:

$$n! = n \times (n-1) \times (n-2) \times \ldots 2 \times 1$$

(per convenzione $0! = !$). Dall'espressione di sopra per $D_{n,k}$ si ottiene quindi

$$D_{n,k} = \frac{n!}{(n-k)!}.$$

Un caso particolare è quando $n = k$. In questo caso parliamo di *permutazioni* e il loro numero è:

$$P_n = D_{n,n} = n!$$

Esempio 2 *Quanti sono i possibili ordini di arrivo (non simultanei) in una gara con 10 partecipanti (assumendo che tutti gli atleti arrivino al traguardo)? Sono esattamente quante le permutazioni di 10 elementi, ossia* $10! = 3628800$.

Quante sono le possibili salite sul podio (primi tre posti)? Sono $D_{10,3} = 10 \times 9 \times 8 = 720$.

Esempio 3 *Se a un torneo partecipano 8 squadre scelte tra 15 e l'ordine di partenza è a sorte, quanti sono i possibili schieramenti di partenza? La domanda può distinguersi in due modi: se so quali delle 8 squadre partecipano la risposta è* $8!$. *Se invece non lo so, la risposta è* $D_{15,8} = 15 \times 14 \times 13 \times 12 \times 11 \times 10 \times 9 \times 8$.

2 Disposizioni con ripetizione

Esempio 4 *Consideriamo l'insieme* $A = \{a, b, c\}$. *Vogliamo contare le sequenze ordinate di lunghezza 2 di elementi scelti in A con possibili ripetizioni. Sono*

$$aa, ab, ac, ba, bb, bc, ca, cb, cc$$

Contandole con il PM abbiamo che sono $3 \times 3 = 9$, *perché abbiamo* 3 *scelte per il primo elemento e* 3 *scelte per il secondo.*

L'esempio si generalizza facilmente.

Definizione 2 *Chiamiamo disposizione con ripetizione di ordine* k *di* n *oggetti una sequenza ordinata* $(x_1, \ldots, x_k)$ *di* k *oggetti scelti tra gli* n *totali.*

Per contarle applichiamo il PMG. Indicando con $D'_{n,k}$ il numero delle disposizioni con ripetizione di ordine k di n oggetti, abbiamo che

$$D'_{n,k} = n \times n \times n \times \cdots \times n = n^k.$$

Si noti bene che in questo caso la nozione ha senso anche se k è maggiore di n.

Esempio 5 *Quante sono le sequenze di 5 lettere scelte tra A, B, C? Sono* $3^5 = D'_{3,5}$.

3 Combinazioni semplici

Esempio 6 *Consideriamo ancora l'insieme* $A = \{a, b, c, d\}$. *Vogliamo contare quanti sono i sottinsiemi di* 3 *elementi. Si vede facilmente che sono 4:*

$$\{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}.$$

Che idea possiamo usare per contarli? Confrontiamoli con le disposizioni semplici di ordine 3*:*

$$abc, acb, bac, bca, cab, cba$$
$$abd, adb, bad, bda, dab, dba$$
$$adc, acd, dac, dca, cad, cda$$
$$dbc, dcb, bdc, bcd, cdb, cbd$$

Cosa si può osservare? Si può osservare che il sottinsieme $\{a, b, c\}$ corrisponde alle 6 sequenze abc, acb, bac, cab, cba formate con i suoi elementi; il sottinsieme $\{a, b, d\}$ corrisponde alle 6 sequenze abd, adb, bad, bda, dba formate con i suoi elementi, e analogamente per $\{a, c, d\}$ e $\{b, c, d\}$. Dunque ogni sottinsieme di 3 elementi corrisponde a 6 disposizioni semplici di lunghezza 3. Dato che sappiamo contare queste ultime, possiamo contare i sottinsiemi, usando la cosidetta

Regola del Pastore: Per contare le pecore in un gregge, conta le zampe e dividi per 4.

Nel nostro caso gni pecora (sottinsieme di 3 elementi tra 6) ha 6 zampe (disposizioni semplici di lunghezza 3). Si nota che è fondamentale che l'associazione sopra descritta tra sottinsiemi di 3 elementi e disposizioni semplici soddisfi le seguenti condizioni: (1) a ogni sottinsieme di 3 elementi viene associato lo stesso numero (=6) di disposizioni semplici; (2) se due sottinsiemi di 3 elementi sono distinti allora l'insieme delle disposizioni semplici associate al primo non ha elementi in comune con l'insieme delle disposizioni semplici associato al secondo; (3) l'associazione esaurisce l'insieme delle disposizioni semplici di ordine 3 su 4, ossia ogni disposizione semplice di ordine 3 sui 4 elementi $\{a, b, c, d\}$ appartiene all'insieme di disposizioni semplici associato a un qualche sottinsieme di 3 elementi in $\{a, b, c, d\}$. Queste condizioni ci permettono di contare quante sono le combinazioni semplici di ordine 3 su $\{a, b, c, d\}$ se sappiamo contare quante sono le disposizioni semplici di ordine 3 su $\{a, b, c, d\}$: ogni volta che contiamo (o togliamo) un insieme di 3 elementi scelti in $\{a, b, c, d\}$ stiamo contando (o togliendo) 6 disposizioni semplici di ordine 3 su $\{a, b, c, d\}$. Il procedimento esaurisce l'insieme dei sottinsiemi di ordine 3 in $\{a, b, c, d\}$ esattamente quando è esaurito l'insieme delle disposizioni semplici di ordine 3 su $\{a, b, c, d\}$.

Abbiamo dunque che

$$C_{4,3} = \frac{D_{4,3}}{6}$$

Per ottenere una formula generale dobbiamo chiederci cosa è 6 come funzione di n o di k. Si vede facilmente che 6 è il numero delle permutazioni di 3 elementi ($6 = 3!$) e che ogni sottinsieme corrisponde a tante disposizioni semplici quante sono le permutazioni dei suoi elementi: infatti ogni disposizione semplice di ordine 3 composta dagli elementi di un sottinsieme $\{x, y, z\}$ è determinata/determina/corrisponde a una permutazione di x, y, z.

In generale dunque abbiamo

$$C_{n,k} = \frac{D_{n,k}}{k!} = \frac{n!}{(n-k)!k!} = \frac{n \times (n-1) \times (n-2) \times \cdots \times (n-k+1)}{k!}.$$

Per ricordarsi l'espressione è comodo pensare che ha k fattori partendo da n al numeratore e k fattori partendo da k al denominatore.

La quantità $C_{n,k}$ è molto importante in Combinatoria e si merita un nome – coefficiente binomiale – e una notazione a sé:

$$C_{n,k} := \binom{n}{k}.$$

Combinazioni semplici e sottinsiemi Rivisitiamo il problema di contare i sottinsiemi di un insieme di n elementi. Con la formula per $C_{n,m}$ posso contare quanti sono i sottinsiemi contenenti esattamente m elementi, per ogni $m = 0, 1, \ldots, n$. Dato che so già che in totale i sottinsiemi sono 2^n, ho la seguente identità:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Intuitivamente stiamo contando i sottinsiemi di un insieme di n elementi suddividendoli in gruppi distinti, ossia i sottinsiemi di 0 elementi, di 1 elemento, di 2 elementi, etc, fino ai sottinsiemi di n elementi. Si osserva che abbiamo ottenuto una identità algebrica contando i due modi lo stesso insieme, ossia l'insieme dei sottinsiemi di un insieme di n elementi.

Ragionando sul significato insiemistico delle quantità $\binom{n}{k}$ è possibile dedurre alcune identità puramente numeriche. Consideriamo dapprima la seguente:

$$\binom{n}{k} = \binom{n}{n-k}$$

In base al significato dei coefficienti binomiali l'identità di sopra dice che i sottinsiemi di k elementi scelti tra n sono tanti quanti i sottinsiemi di $n-k$ elementi scelti tra n. Proviamo a dimostrare che è così.

Usiamo una corrispondenza: fissiamo un insieme $A = \{a_1, \ldots, a_n\}$ di n elementi. A un generico sottinsieme$B$ di A di k elementi associamo l'unico sottinsieme di A di $n-k$ elementi che contiene tutti e soli gli elementi di A che non sono contenuti in B.

Si osserva facilmente che l'associazione sopra definita è tale che: due sottinsiemi diversi di k elementi di A vengono associati a due sottinsiemi diversi di $n-k$ elementi di A; e ogni sottinsieme di $n-k$ elementi di A si ottiene da un sottinsieme di k elementi di A mediante l'associazione. In questo caso possiamo concludere che gli elementi del primo tipo sono tanti quanti gli elementi del secondo tipo.

Dunque: i sottinsiemi di k elementi di A sono tanti quanti i sottinsiemi di $n-k$ elementi di A.

NB: Dall'identità sopra dimostrata segue che per calcolare $\binom{10}{7}$, che sarebbe $\frac{10\times9\times8\times7\times6\times5\times4}{7!}$, posso calcolare equivalentemente $\binom{10}{3}$, che è $\frac{10\times9\times8}{3\times2}$.

Consideriamo la seguente identità, per $n \geq k > 0$:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

In base al significato dei coefficienti binomiali, l'identità di sopra equivale a dire che i sottinsiemi di k elementi scelti tra n sono tanti quanti i sottinsiemi di $k-1$ elementi scelti tra $n-1$ più i sottinsiemi di k elementi scelti tra $n-1$. Proviamo a dimostrare che è proprio così.

Fissiamo $A = \{a_1, \ldots, a_n\}$ con n elementi, e supponiamo $n > 0$. Dato che A è non vuoto, contiene almeno un elemento a. Fissiamo un tale elemento $a \in A$ arbitrariamente. Sia B il sottinsieme di A che contiene tutti gli elementi di A eccetto a. Ovviamente B ha $n-1$ elementi. Sia $k > 0$. Formiamo due gruppi con i sottinsiemi di A di k elementi.

Gruppo 1: Tutti e soli i sottinsiemi di A di k elementi che contengono l'elemento a.

Gruppo 2: Tutti e soli i sottinsiemi di A di k elementi che non contengono l'elemento a.

Osservo quanto segue: Gli insiemi nel Gruppo 1 possono ottenersi aggiungendo l'elemento a a un sottinsieme di $k-1$ elementi di B. Gli insiemi nel Gruppo 2 sono esattamente i sottinsiemi di k elementi di B.

Questo è sufficiente a dimostrare l'identità desiderata.

Metodi Matematici per l'Informatica - Dispensa 3
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Dimostrazioni per doppio conteggio e binomiale

La proprietà già dimostrata usando una corrispondenza, ossia

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

può dimostrarsi anche, più intuitivamente, con una tecnica detta del doppio conteggio. Si tratta di contare in due modi la stessa quantità, deducendo l'identità tra i risultati ottenuti con i due conteggi.

In questo caso stiamo contando i sottinsiemi di k elementi di un insieme di n elementi.

Un primo modo di contarli è quello che abbiamo già visto, ossia $C_{n,k} = \binom{n}{k}$.

Proviamo ora a contare la stessa quantità in un altro modo. Distinguiamo due tipi di sottinsieme di k elementi di un generico insieme di n elementi $A = \{a_1, \ldots, a_n\}$.

- Tipo 1: Sottinsiemi di k elementi di A che contengono l'elemento a_1.
- Tipo 2: Sottinsiemi di k elementi di A che non contengono l'elemento a_1.

Se sappiamo contare gli elementi di tipo 1 e quelli di tipo 2 la loro somma ci darà la quantità desiderata.

Gli elementi di tipo 2 sono tanti quanti le scelte di k elementi tra gli elementi di A tolto a_1 (che è vietato). Quindi sono tanti quanti i sottinsiemi di k elementi scelti in un insieme di $n-1$ elementi, ossia $\binom{n-1}{k}$.

Gli elementi di tipo 1 si ottengono scegliendo $k-1$ elementi tra gli elementi di A diversi da a_1: infatti ognuno di questi insiemi ha la forma $\{a_1, a_{j_1}, \ldots, a_{j_{k-1}}\}$ dove gli a_{j_i} sono scelti tra gli $n-1$ elementi di A diversi da a_1. In tutto sono $\binom{n-1}{k-1}$.

Dunque tutti i sottinsiemi di k elementi scelti in A sono $\binom{n-1}{k} + \binom{n-1}{k-1}$.

Abbiamo così dimostrato l'identità desiderata.

Triangolo di Tartaglia-Pascal Dalla proprietà appena dimostrata segue, per esempio, che

$$\binom{3}{1} = \binom{2}{1} + \binom{2}{0}$$

$$\binom{4}{1} = \binom{3}{1} + \binom{3}{0}$$

$$\binom{4}{2} = \binom{3}{2} + \binom{3}{1}$$

$$\binom{4}{3} = \binom{3}{3} + \binom{3}{2}$$

Ricordando che $\binom{n}{0} = \binom{n}{n} = 1$, queste identità suggeriscono di organizzare i binomiali nella seguente tabella, nella quale otteniamo tutti i valori diversi da quelli della prima colonna e della diagonale (tutti = 1) usando

l'identità sopra dimostrate: il valore nella colonna c-esima riga n-esima deriva dalla somma dei valori nella colonna c-esima riga $(n-1)$-esima e colonna $c-1$-esima riga $(n-1)$-esima. Otteniamo il cosidetto triangolo di Tartaglia-Pascal, di cui si mostrano qui sotto le prime otto righe:

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$
0	1							
1	1	1						
2	1	2	1					
3	1	3	3	1				
4	1	4	6	4	1			
5	1	5	10	10	5	1		
6	1	6	15	20	15	6	1	
7	1	7	21	35	35	21	7	1

Dall'osservazione del triangolo di Tartaglia-Pascal è possibile individuare alcune proprietà dei coefficienti binomiali, delle loro somme e dei loro prodotti.

Esempio. Per esempio, la proprietà già dimostrata per cui $\binom{n}{k} = \binom{n}{n-k}$ corrisponde alla simmetria del triangolo di Tartagli-Pascal.

Consideriamo per esempio il valore $\binom{6}{4} = 15$ e quello nella cella immediatamente in alto a sinistra ossia $\binom{5}{3} = 10$. Che rapporto intercorre tra 15 e 10? Abbiamo:

$$15 \times \frac{4}{6} = 10$$

ossia

$$15 \times 4 = 6 \times 10$$

ossia

$$\binom{6}{4} \times 4 = 6 \times \binom{5}{3}.$$

Proviamo ancora partendo da $\binom{5}{3}$. Il valore immediatamente in alto a sinistra è $\binom{4}{2} = 6$. Abbiamo

$$10 \times 3 = 5 \times 6$$

ossia

$$\binom{5}{3} \times 3 = 5 \times \binom{4}{2}.$$

Queste osservazioni suggeriscono di formulare la seguente identità generale:

$$\binom{n}{k} \times k = n \times \binom{n-1}{k-1}.$$

Proviamo a dimostrarla con un doppio conteggio. Osserviamo che $\binom{n}{k} \times k$ conta, per esempio, i modi di scegliere una commissione di k rappresentanti tra n studenti e successivamente di scegliere un portavoce all'interno della commissione (per il Principio Moltiplicativo). Questo è equivalente a scegliere prima un portavoce tra gli n studenti ($= n$ scelte) e successivamente i restanti membri per formare la commissione di k elementi, ossia $k-1$ altri studenti tra gli $n-1$ restanti una volta scelto il portavoce. Ma quest'ultimo numero di scelte è (per il Principio Moltiplicativo e per il significato del binomiale) proprio $n \times \binom{n-1}{k-1}$. Abbiamo così dimostrato la validità dell'identità generale.

Esempio Consideriamo la seguente identità (anch'essa si può derivare per osservazione dal Triangolo di Tartaglia-Pascal): siano $0 \leq k \leq m \leq n$. Allora

$$\binom{n}{m} \times \binom{m}{k} = \binom{n}{k} \times \binom{n-k}{m-k}.$$

Proviamo a dimostrare l'identità con un doppio conteggio. La quantità a sinistra, ossia $\binom{n}{m} \times \binom{m}{k}$ rappresenta una scelta di m elementi tra n seguita da una scelta di k tra m. Conta quindi, per esempio, i modi di scegliere una commissione di m rappresentanti tra n studenti e successivamente una sottocommissione di k delegati tra gli m membri della commissione scelta. Ma queste scelte equivalgono a scegliere prima i k membri della sottocommissione tra tutti gli n studenti e successivamente i restanti membri necessari per formare una commissione di m rappresentanti (dunque $m-k$ altri membri) tra gli studenti restanti dopo aver scelto i k della sottocommissione, ossia tra $n-k$ studenti. Questo numero di scelte è proprio il membro destro dell'identità, ossia $\binom{n}{k} \times \binom{n-k}{m-k}$.

Esempio Un'altra proprietà notevole delle somme dei coefficienti binomiali si ottiene osservando le colonne del triangolo di Tartaglia-Pascal. Consideriamo per esempio la seconda colonna e sommiamo i primi 4 valori: 1+2+3+4 = 10. Si osserva che il valore di questa somma appare nella cella immediatamente in basso a destra dell'ultima cella sommata. Ossia

$$\binom{1}{1} + \binom{2}{1} + \binom{3}{1} + \binom{4}{1} = \binom{5}{2}.$$

Provando su altre colonne si ottiene un risultato analogo. Vale infatti la seguente identità: sia $k \geq 0$ (una colonna), e $n \geq 0$ (il numero dei termini della colonna che vogliamo sommare) allora:

$$\sum_{i=0}^{n} \binom{i}{k} = \binom{n+1}{k+1}.$$

Esempio Partiamo ora da una riga arbitraria r, colonna 0 e sommiamo i termini lungo la diagonale che scende verso Sud-Est, fermandoci quando vogliamo. Per esempio, partendo dalla riga $r = 2$ abbiamo $1 + 3 + 6 + 10$ fermandoci dopo quattro celle. Il valore della somma appare nella cella immediatamente sotto l'ultimo termine, in questo caso nella riga 6 colonna 3.

$$\binom{2}{0} + \binom{3}{1} + \binom{4}{2} + \binom{5}{3} = \binom{6}{3}.$$

In generale abbiamo

$$\sum_{i=0}^{k} \binom{r+i}{i} = \binom{r+k+1}{k}.$$

Le ultime identità possono essere dimostrate, come vedremo, per induzione o con risoluzione algebrica, mentre è più laborioso darne una prova per doppio conteggio.

Metodi Matematici per l'Informatica - Dispensa 4
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

1 Coefficiente binomiale - altre proprietà e applicazioni

Alcuni esempi

Esempio 1 *L'uso delle combinazioni semplici può risolvere anche problemi apparentemente legati all'ordine. Quante sono le sequenze di 7 numeri tra 1 e 12? La domanda apparentemente si riferisce all'ordine ma il conteggio può eseguirsi con il binomiale. Infatti le sequenze in questione sono tante quante i sottinsiemi di 7 elementi dell'insieme* $\{1, 2, 3, \ldots, 12\}$*, ossia sono* $C_{12,7} = \binom{12}{7} = 792$*. Basta infatti considerare i sottinsiemi enumerati in ordine crescente.*

Esempio 2 *Quanti sono i modi di formare con 12 giocatori 3 squadre da 4? Posso provare a ragionare così: scelgo un sottinsieme di 4 elementi dei 12 totali, poi scelgo un sottinsieme da 4 tra gli 8 giocatori restanti. L'ultima squadra è obbligatoriamente composta dai 4 giocatori restanti. Per il PM ho allora che le scelte possibili sono* $\binom{12}{4} \times \binom{8}{4}$*. Questo numero conta davvero quello che ci interessa? Siano A, B, C tre squadre da 4. Nella quantità* $\binom{12}{4} \times \binom{8}{4}$ *sto contando come distinte le scelte* $ABC, ACB, BAC, BCA, CAB, CBA$ *mentre esse rappresentano la stessa ripartizione in squadre del mio insieme di giocatori! Devo quindi dividere per* 3!*, e ottengo*

$$\frac{\binom{12}{4} \times \binom{8}{4}}{3!} = 5775.$$

Esempio 3 *Quanti sono i modi di formare con 12 giocatori 3 squadre da 4? Posso provare a ragionare così: scelgo un sottinsieme di 4 elementi dei 12 totali, poi scelgo un sottinsieme da 4 tra gli 8 giocatori restanti. L'ultima squadra è obbligatoriamente composta dai 4 giocatori restanti. Per il PM ho allora che le scelte possibili sono* $\binom{12}{4} \times \binom{8}{4}$*. Questo numero conta davvero quello che ci interessa? Siano A, B, C tre squadre da 4. Nella quantità* $\binom{12}{4} \times \binom{8}{4}$ *sto contando come distinte le scelte* $ABC, ACB, BAC, BCA, CAB, CBA$ *mentre esse rappresentano la stessa ripartizione in squadre del mio insieme di giocatori! Devo quindi dividere per* 3!*, e ottengo*

$$\frac{\binom{12}{4} \times \binom{8}{4}}{3!} = 5775.$$

In termini tecnico insiemistici abbiamo contato le partizioni di un insieme di 12 elementi in 3 parti (o classi).

Esempio 4 *Quante partite in un campionato (andata e ritorno) di 18 squadre?*

Esempio 5 *In quanti modi posso dividere una classe di 30 studenti in 3 gruppi da 10 assegnando a ciascun gruppo un compito diverso? In quanti modi posso farlo se devo assegnare un compito uguale?*

Combinazioni semplici e potenze del binomio Il termine coefficiente binomiale per $\binom{n}{k}$ è giustifiato da una stretta connessione con lo sviluppo delle potenze di un binomio. Consideriamo l'identità

$$(a + b)^2 = a^2 + 2ab + b^2$$

e

$$(a+b)^3 = a^3 + a^2b + a^2b + a^2b + ab^2 + ab^2 + ab^2 + b^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Ci interessa contare il numero di occorrenze dei termini di questa somma, o in altre parole i coefficienti moltiplicativi, che nell'ultimo esempio sono 1 per il termina a^3 e b^3, e 2 per i termini a^2b e ab^2.

In generale vale il seguente Teorema.

Teorema 1 *Siano a, b numeri reali, e sia n un intero positivo. Allora*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

Si ricorda che la sommatoria qui sopra è un'abbreviazione per la somma seguente:

$$\binom{n}{0}a^0b^{n-0} + \binom{n}{1}a^1b^{n-1} + \binom{n}{2}a^2b^{n-2} + \cdots + \binom{n}{n-1}a^{n-1}b^{n-(n-1)} + \binom{n}{n}a^ib^{n-n}.$$

Dimostrazione. La potenza $(a+b)^n = \underbrace{(a+b)(a+b)\dots(a+b)}_{n}$ si ottiene sommando tutti i possibili prodotti di n fattori $p_1 \times \cdots \times p_n$ dove ogni p_i è uguale ad a o a b.

Applicando distributività e commutatività posso dire che ogni addendo ha la forma a^ib^{n-i}, corrispondente allo scegliere i volte a e le restanti volte b nel fattore $(a+b)$ di $(a+b)^n$.

Fissiamo $i \in [0, n]$. Gli addendi di forma a^ib^{n-i} sono tutti e soli i prodotti $p_1 \dots p_n$ in cui l'insieme $\{j : p_j = a\}$ è un sottinsieme di i elementi di $\{1, \dots, n\}$. Dunque sono in quantità di $\binom{n}{i}$. **QED**

Binomiale e scritture additive Quanti sono i modi di scrivere il numero 3 come somma di 2 interi non-negativi, tenendo conto dell'ordine degli addendi?

$$3 = 0+3 = 3+0 = 1+2 = 2+1.$$

Ci stiamo chiedendo quante coppie ordinate (i_1, i_2) di numeri non negativi esistono tali che $i_1 + i_2 = 3$.

Quanti sono i modi di scrivere il numero 7 come somma di 6 addendi non negativi, tenendo conto dell'ordine degli addendi?

$$0+7+0+0+0+00 = 1+1+1+1+1+2 = 5+0+0+1+0+1 = \dots$$

Vogliamo contare le sequenze ordinate $(i_1, \dots, i_6)$ di numeri non negativi tali che $i_1 + \cdots + i_6 = 7$. Come contarle? Cerchiamo di astrarre dalla specificità numerica del problema, in favore di una rappresentazione astratta. Osserviamo che ogni soluzione sarà composta di esattamente 6 simboli $+$. Inoltre, ovviamente, la somma totale delle unità presenti nella soluzione sarà 7. Immaginiamo di rappresentare una singola unità con una pallina $\odot$, e di disporre queste 7 palline in fila. Una soluzione è allora completamente determinata dalla posizione dei 5 simboli $+$ tra queste unità. Tra quante posizioni è possibile scegliere? Dato che i simboli $+$ possono essere consecutivi (se la soluzione ha zeri consecutivi) e trovarsi anche a destra o a sinistra di tutte le unità o palline, le posizioni possibili sono esattamente 7+5=12.

Per esempio,

$$+ + + + + \odot \odot \odot \odot \odot \odot\odot$$

corrisponde alla soluzione

$$0+0+0+0+0+7$$

la configurazione

$$\odot \odot + + \odot + \odot + \odot + \odot\odot$$

corrisponde alla soluzione

$$2+0+1+1+1+2$$

etc.

Come al solito osserviamo che due soluzioni distinte danno luogo a due configurazioni distinte e che ogni configurazione corrisponde a una soluzione. Le soluzioni richieste sono dunque **tante quante** le configurazioni considerate.

Il numero delle soluzioni è dunque identico al numero di sottinsiemi di 5 elementi scelti tra 12.

Il ragionamento è completamente generale, e permette di dimostrare il seguente Teorema.

Teorema 2 *Il numero di modi di scrivere un intero non negativo m come somma di t interi non negativi, contando l'ordine, è $\binom{m+t-1}{t-1}$.*

Esempio 6 *Il numero di modi di scrivere 7 come somma di 6 interi non negativi è $\binom{7+6-1}{6-1} = \binom{7+5}{5} = \binom{12}{5} = \frac{12\times11\times10\times9\times8}{5\times4\times3\times2}$.*

2 Combinazioni con ripetizioni

Esempio 7 *Consideriamo l'insieme $A = \{a, b, c, d\}$. Vogliamo contare i modi scegliere 6 elementi in A con possibili ripetizioni, senza contare l'ordine. Per esempio una scelta è: 2 copie di a, 3 copie di c, 1 copia di d (6 oggetti in tutto). Una rappresentazione tabulare è molto conveniente:*

a	b	c	d
2	0	3	1

Dove abbiamo $2 + 0 + 3 + 1 = 6$.

Definizione 1 *Chiamiamo combinazione con ripetizione di ordine k di n oggetti un raggruppamento di k oggetti scelti tra n con possibili ripetizioni.*

Useremo le tabelle per denotare una combinazione di ordine k con ripetizione:

a_1	a_2	$\dots$	a_{n-1}	a_n
m_1	m_2	$\dots$	m_{n-1}	m_n

Dobbiamo avere $k = m_1 + m_2 + \cdots + m_n$.

Per contare le combinazioni con ripetizione è comodo usare una traduzione! Consideriamo la combinazione con ripetizione data dalla tabella seguente:

Associamo una stringa (ordinata) di zeri e di uni:

110010

Come ho ottenuto questa stringa? Partendo da sinistra ho messo tanti 1 quante sono le copie di a, ho aggiunto uno 0 come separatore, ho messo tanti 1 quante sono le copie di b (ossia zero), un altro 0 come separatore, e così via.

Si osserva facilmente che a ogni combinazione con ripetizione corrisponde una e una sola sequenza di 0 e di 1 di lunghezza $3 + (4 - 1)$: infatti secondo la regola di associazione una stringa associata a una combinazione con ripetizione di ordine 3 di 4 elementi avrà 3 occorrenze di 1 e $4 - 1$ occorrenze di 0.

Dunque le combinazioni con ripetizione di ordine $k = 3$ di $n = 4$ elementi sono tante quante le stringhe binarie di lunghezza 6 con esattamente 3 occorrenze di 1. Ma queste ultime sono esattamente i sottinsiemi di 3 elementi di un insieme di 6 elementi. E quest'ultima quantità sappiamo già contarla!

$$C'_{4,3} = C_{4+3-1,3} = C_{6,3} = \frac{6 \times 5 \times 4}{3 \times 2}.$$

Il ragionamento di sopra è del tutto generale. Dunque abbiamo:

$$C'_{n,k} = C_{n+k-1,k} = \binom{n+k-1}{k}.$$

3 Anagrammi

Esempio 8 *Quanti sono gli anagrammi della parola PADRE? Per il PMG sono* $5! = 120$.

Esempio 9 *Quanti sono gli anagrammi della parola NONNA? In questo caso* $5! = 120$ *non è la quantità desiderata, perché sta contando le N come se fossero tutte distinte, ossia come se si trattasse degli anagrammi della parola* $N_1ON_2N_3A$, *dove* N_1, N_2, N_3 *vengono considerate lettere distinte. Ovviamente vogliamo invece considerare identici e contare una sola volta gli anagrammi* $N_1AN_2N_3O$, $N_2AN_1N_3O$, $N_1AN_3N_2O$, $N_2AN_3N_1O$, $N_3AN_1N_2O$ *e* $N_3AN_2N_1O$. *Per la Regola del Pastore devo quindi dividere per* $3!$ *ossia per il numero delle permutazioni di* $\{N_1, N_2, N_3\}$. *Ottengo quindi* $\frac{5!}{3!} = 20$ *anagrammi.*

Esempio 10 *Quanti sono gli anagrammi della parola NONNO? In questo caso non voglio contare né le 3 occorrenze di N né le 2 occorrenze di O come distinte. Ragionando per passi ho:* $5! = 120$ *permutazioni di* $\{N_1, O_1, N_2, N_3, O_3\}$, $\frac{5!}{3!} = 20$ *parole di 5 lettere nell'alfabeto* $\{N, O_1, O_2\}$ *e infine, ancora per la Regola del Pastore,* $\frac{5!}{3!2!} = 10$ *anagrammi di NONNO.*

Riassumendo: se voglio formare gli anagrammi di una parola formata da n occorrenze di lettere di cui n_1 sono identiche, ho $\frac{n!}{n_1!}$ possibilità. Se ci sono n_1 lettere identiche di un tipo e n_2 di un altro tipo, ho $\frac{n!}{n_1!n_2!}$ possibilità, etc. In generale: gli anagrammi di una parola lunga n in cui compaiono t gruppi di $n_1, \ldots, n_t$ lettere ripetute, sono

$$\frac{n!}{n_1! \times n_2! \times \cdots \times n_t!}$$

Esempio 11 *Quante sono le sequenze lunghe 6 composte da due 0, tre 1 e un 2? Sono gli anagrammi di 110002. Dunque sono* $\frac{6!}{2!3!} = \frac{720}{12} = 60$.

Esempio 12 *Quanti sono gli anagrammi di MISSISSIPPI? Sono* $\frac{11!}{4!4!2!}$.

Esempio 13 *Quanti sono gli ordinamenti di 5 persone di cui 3 uomini e 2 donne se mi interessa soltanto distinguere tra uomini e donne? Mentre gli ordinamenti totali sono 5! gli ordinamenti che identificano gli uomini tra loro e le donne tra loro sono* $\frac{5!}{3!2!}$.

Metodi Matematici per l'Informatica - Dispensa 5
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

1 Combinazioni con ripetizioni - Osservazioni aggiuntive

Il metodo usato per dimostrare le due seguenti proposizioni:

- I modi per scrivere un intero non-negativo m come somma di r interi non-negativi sono $\binom{m+r-1}{r-1}$,
- Le combinazioni con ripetizione di ordine k su n elementi sono $C'_{n,k} = \binom{k+n-1}{k}$,

usando una traduzione con pallini e stanghette è un metodo molto generale che permette di risolvere un gran numero di problemi di conteggio anche senza ricordare la formula per $C'_{n,k}$ (si osservi che $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$ usando la proprietà di simmetria – quindi le due formule sopra sono identiche).

Le seguenti sono due formulazioni tipiche di problemi che si possono risolvere con questo metodo.

Problema dei Biscotti Quanti modi ci sono di distribuire m biscotti tra r bambini (ammettendo di poter scegliere di non dare nessun biscotto a qualche bambino)?

Problema di scrittura additiva Quante sono le soluzioni (intere) **non-negative** dell'equazione seguente?

$$x_1 + x_2 + \cdots + x_r = m$$

Si vede facilmente che i due problemi sono identici, e la risposta è $\binom{m+r-1}{r-1}$.
Una variante di questi problemi può ancora risolversi con lo stesso metodo. Consideriamo le seguenti domande:

Problema Quanti modi ci sono di distribuire 10 biscotti tra 5 bambini **dando almeno un biscotto a ciascun bambino**?

Problema Quante sono le soluzioni (intere) **positive** dell'equazione seguente?

$$x_1 + x_2 + \cdots + x_5 = 10$$

Un primo modo di risolvere il problema è il seguente: se consideriamo le espressioni con $\cdot$ e $|$ associate alle soluzioni del problema originale (senza vincolo di dare almeno un biscotto a ciascuno o, equivalentemente, che ogni x_i sia > 0), ci accorgiamo che vogliamo escludere dal conteggio le espressioni che iniziano con $|$, quelle che finiscono con $|$ e quelle che contengono due $|$ adiacenti. Queste e solo queste corrispondono a soluzioni in cui qualche bambino non riceve biscotti. Il problema è quindi ridotto a contare in quante posizioni possiamo mettere gli $5 - 1 = 4$ separatori nelle posizioni tra le unità (i pallini). Queste posizioni sono ovviamente $10 - 1 = 9$. Dunque dobbiamo contare i sottinsiemi di 4 elementi scelti tra 9, che sono $\binom{9}{4}$.

Un secondo modo di ragionare è il seguente, in cui riduciamo il problema a un problema senza il vincolo aggiunto: distribuiamo per iniziare un biscotto a ciascun bambino, quindi 5 biscotti, soddisfacendo subito il

vincolo. Restano da assegnare $10-5=5$ biscotti tra 5 bambini, ma questa volta senza il vincolo aggiuntivo di dare almeno un biscotto ciascuno. Sappiamo già contare questa quantità, che è $\binom{5+5-1}{5-1}=\binom{9}{4}$. In termini di soluzioni di una equazione, assegnamo a ognuna delle 5 variabili il valore 1. Quello che ci resta da contare sono le soluzioni dell'equazione

$$y_1+y_2+y_3+y_4+y_5=10-5,$$

dove gli y_i possono essere 0. Sappiamo già contare questa quantità.

I ragionamenti di sopra sono perfettamente generali e otteniamo che i modi di dare m biscotti a r bambini dando almeno un biscotto a ciascuno, e il numero delle soluzioni positive dell'equazione

$$x_1+x_2+\cdots+x_r=m$$

è $\binom{m-1}{r-1}$.

Combinazioni con ripetizioni e Anagrammi Per calcolare $C'_{n,k}$ abbiamo contato il numero delle parole di lunghezza $m+r-1$ composte di $r-1$ lettere $|$ e di m lettere $\cdot$. Possiamo vedere il problema come un problema di anagrammi. Sappiamo già contare gli anagrammi della parola composta da $r-1$ lettere $|$ e m lettere $\cdot$, e sono

$$\frac{(m+r-1)!}{m!(r-1)!}.$$

D'altra parte sappiamo che il numero delle espressioni in questione è esattamente $C'_{r,m}$, dunque possiamo concludere che

$$C'_{r,m}=\binom{m+r-1}{r-1}=\frac{(m+r-1)!}{m!(r-1)!}.$$

Abbiamo così dedotto una identità algebrica con un doppio conteggio combinatorio.

Per esempio,

$$\binom{10}{3}=\frac{10!}{7!3!},$$

come si può anche verificare svolgendo i calcoli.

Principio Additivo

Abbiamo usato implicitamente diverse volte il seguente principio: se gli oggetti di una collezione sono di due tipi distinti e mutualmente esclusivi, allora il loro numero è la somma degli oggetti del primo tipo e degli oggetti del secondo tipo.

Per esempio abbiamo usato questo principio quando abbiamo dimostrato

$$\binom{n}{k}=\binom{n-1}{k}+\binom{n-1}{k-1},$$

dividendo i sottinsiemi di k elementi tra n in due tipi (quelli contenenti un certo elemento fissato a e quelli non conteneti a).

Questo principio elementare, detto Principio Additivo, funziona bene in molte situazioni. Ad esempio:

Esempio Quanti sono le possibili cene complete in un menu composto da 3 antipasti, 4 primi, 3 secondi di pesce, 2 secondi di carne, 3 dessert? (Per cena completa intendiamo un antipasto un primo un secondo un dessert). Sono ovviamente, per il PM:

$$3\times 4\times(3+2)\times 3.$$

Qui abbiamo implicitamente usato il Principio Additivo per contare il totale dei secondi. Anche in questo caso il ragionamento è corretto perché i due tipi di secondi sono esclusivi (nessun secondo di carne è di pesce e viceversa).

Esempio Se ho 80 animali terrestri e 100 animali acquatici, in tutto ho $80 + 100$ animali.

Dal punto di vista logico siamo nella situazione seguente: ho una collezione di oggetti, X, e gli oggetti in X possono essere di due tipi, A e B. Nessun oggetto di tipo A è di tipo B e viceversa (diciamo che i tipi sono esclusivi). Allora gli oggetti di tipo A oppure B sono $\#(A) + \#(B)$ (il numero degli oggetti di tipo A più il numero degli oggetti di tipo B). In termini di scelte: se devo scegliere un oggetto tra oggetti di due tipi come sopra, il numero di scelte è la somma.

Osservazione Si osserva facilmente che il PA si generalizza a più di due tipi. Se ho m_1 èesche, m_2 susine, m_3 arance e m_4 mandarini ovviamente ho $m_1 + m_2 + m_3 + m_4$ frutti.

Esempio Il Principio Additivo, generalizzato a tre tipi esclusivi A, B, C, si può esare per rispondere a una delle domande nella lista iniziale del corso: quanti sono i modi possibili di votare se il voto consiste nello scegliere tra 12 liste di 10 candidati ciascuna dando al massimo 2 preferenze tra i candidati della lista scelta. Per il PM il conto è 12 moltiplicato il numero di modi di dare al massimo 2 preferenze. Quest'ultimo posso contarlo suddividendo in tre tipi esclusivi: $A =$ nessuna preferenza, $B =$ una preferenza, $C =$ due preferenze. I modi di dare al massimo 2 preferenze all'interno della lista scelta sono dunque, per il PA,

$$1 + 10 + 45,$$

dove 45 è $\binom{10}{2}$, i modi di scegliere 2 candidati da una lista di 10. Il numero di voti possibili è dunque

$$12 \times (1 + 10 + 45).$$

Consideriamo ora le varianti seguenti degli esempi visti sopra.

Esempio Quanti sono le possibili cene complete in un menu composto da 3 antipasti, 4 primi, 3 secondi al forno, 2 secondi di carne, 3 dessert? In questo caso non possiamo dire quanti sono i secondi, perché qualche secondo di carne potrebbe essere cotto al forno! Quindi usare la somma $3 + 2$ non è corretto!

Esempio Se ho 80 animali terrestri e 100 animali acquatici, non necessariamente ho in tutto $80 + 100$ animali. Potrebbero esserci dei deflini o delle balene tra gli animali acquatici.

Posso senz'altro dire che, nel primo esempio, i secondi sono $\leq 3 + 2 = 5$ e nel secondo esempio gli animali sono $\leq 80 + 100 = 180$.

In generale posso dire che se ho una collezione di oggetti di due tipi A e B, ma i due tipi non sono necessariamente esclusivi, allora il numero totale di oggetti è $\leq \#(A) + \#(B)$.

Posso dire qualcosa di più: nella somma $3+2$ per il primo esempio, sto contando esattamente 2 volte tutti e soli i secondi che sono di carne e cotti al forno. Per avere il totale esatto di secondi devo quindi sottrarre la loro quantità alla somma $3 + 2$.

Analogamente nel secondo esempio nella somma $80 + 100$ sto contando esattamente 2 volte tutti e soli gli animali che sono mammiferi e acquatici. Il totale degli animali è dato dalla somma *meno* la quantità di questo tipo di animali.

In termini astratti, il numero di oggetti di tipo A oppure B (il totale) è dato dalla somma del numero di oggetti di tipo A più il numero di oggetti di tipo B meno il numero di oggetti di tipo A e B. In formule possiamo scrivere

$$\#(A \text{ o } B) = \#(A) + \#(B) - \#(A \text{ e } B).$$

Chiamiamo questo principio Principio Additivo, o Principio di Inclusione-Esclusione. Si osserva facilmente che la forma del Principio Additivo considerata sopra, in cui i tipi A e B sono esclusivi è un caso particolare della forma più generale, perché se i tipi sono esclusivi il termine $\#(A \text{ e } B)$ è uguale a 0.

Esempio
Consideriamo una classe con 24 studenti, sottoposti a due test di valutazione. Supponiamo che

- 18 studenti superano il primo test,
- 15 studenti superano il secondo test,
- 12 studenti superano entrambi i test.

Vogliamo contare quanti studenti superano **almeno un test**. Osserviamo subito che il costrutto *almeno* è parente stretto dell'*oppure*: almeno in questo caso significa superare il primo test *oppure* superare il secondo test. Possiamo quindi applicare il Principio Additivo. Gli studenti di tipo A sono quelli che superano il primo test, gli studenti di tipo B quelli che superano il secondo test. Nella somma $18 + 15$ stiamo contando esattamente due volte tutti e soli gli studenti che superano sia il primo che il secondo test, ossia gli studenti che sono simultaneamente di tipo A e di tipo B. Come visto sopra, dobbiamo sottrarti alla somma. In questo caso sappiamo esattamente quanti sono, ossia 12. Gli studenti di tipo A o di tipo B, ossia gli studenti che superano almeno un test, sono dunque

$$18 + 15 - 12 = 21.$$

Metodi Matematici per l'Informatica - Dispensa 6
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Principio di Inclusione-Esclusione

Riformulazione insiemistica - PIE a 2 termini Abbiamo formulato il Principio Additivo (o Principio di Inclusione-Esclusione - PIE) a due termini come segue:

Caso 1: Le proprietà A e B sono esclusive (ossia nessun A è un B). In questo caso

$$\#(A \text{ oppure } B) = \#A + \#B.$$

Caso 2: Le proprietà A e B non sono necessariamente esclusive (ossia qualche A puòà essere un B). In questo caso

$$\#(A \text{ oppure } B) = \#A + \#B - \#(A \text{ e } B).$$

Il Principio Additivo (o Principio di Inclusione-Esclusione - PIE) a due termini può formularsi in termini di insiemi anziché di proprietà.

Invece di considerare due proprietà o tipi A, B, e di considerare quanti sono gli oggetti che le soddisfano, consideriamo direttamente gli insiemi di oggetti che le soddisfano (in termini tecnici: la lore *estensione*). Siano quindi A e B due insiemi. Analogamente invece di considerare la proprietà "A o B" consideriamo l'insieme degli oggetti che la soddisfano, ossia l'insieme degli oggetti di tipo A o di tipo B ossia l'insieme degli oggetti che sono elementi di A oppure elementi di B:

$$\{x : x \in A \text{ oppure } x \in B\}.$$

Chiamiamo questo insieme **l'unione** di A e di B e lo denotiamo con $A \cup B$. Si badi che usiamo la disgiunzione *oppure* nel suo senso *inclusivo*, ossia non escludiamo il caso che l'oggetto x appartenga sia ad A che a B.

La domanda: quanti sono gli oggetti che hanno la proprietà A o B (o: quanti sono gli oggetti di tipo A o B) si traduce adesso in: Quanti sono gli elementi dell'insieme unione $A \cup B$, ossia quanto vale $\#(A \cup B)$.

Il PIE ci dice che dobbiamo sommare il numero di elementi di A, il numero di elementi di B e sottrarre il numero di oggetti che hanno sia la proprietà A che la proprietà B. In termini insiemistici quest'ultimo è il numero di oggetti nell'insieme i cui elementi sono sia elementi di A che elementi di B:

$$\{x : x \in A \text{ e } x \in B\}.$$

Chiamiamo questo insieme **l'intersezione** di A e di B e lo denotiamo con $A \cap B$.

Il PIE per due termini si traduce in questo nuovo linguaggio come segue:

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

Si osservi che questa formulazione include anche il Caso 1 del PIE a due termini: la richiesta che le proprietà A e B sono esclusive si traduce in linguaggio insiemistico con: $A \cap B = \emptyset$, che è un modo sintetico di dire che A e B non hanno elementi in comune. In questo caso (e solo in questo caso) l'ultimo termine nella formula di sopra, ossia $\#(A \cap B)$ è uguale a 0.

Esempio Una classe di 24 studenti viene sottoposta a 2 test di valutazione. I risultati sono i seguenti:

- 18 superano il primo test
- 17 superano il secondo test
- 14 superano entrambi i test

Quanti studenti superano almeno un test? Possiamo applicare il PIE a 2 termini. Dichiariamo i seguenti insiemi

$$A = \{ \text{ studenti che superano il primo test} \}$$

$$B = \{ \text{ studenti che superano il secondo test} \}$$

Importante: in A stiamo contando gli studenti che superano il primo test, senza specificare se superano anche il secondo o meno. Analogamente in B stiamo contando gli studenti che superano il secondo test, senza specificare se superano anche il primo o meno.

Rispondere alla domanda significa contare quanti studenti superano "il primo test o il secondo". In termini insiemistici si tratta di valutare la grandezza dell'unione $A \cup B$. Per questo ci basta conoscere la grandezza di A, di B e di $A \cap B$.

$$A \cap B = \{\text{studenti che superano il primo test e il secondo test}\}.$$

Sappiamo dai dati che $\#(A \cap B) = 14$. Possiamo quindi applicare il PIE:

$$18 + 17 - 14 = 21$$

Gli studenti che superano **almeno** un test sono 21.

Esempio In una città esistono solo due circoli: il circolo del Tennis, che conta 20 iscritti, e il circolo del Golf che ne conta 15. Sappiamo anche che il numero di persone iscritti a qualche circolo è 25. Quante persone sono iscritte sia al circolo del Tennis che a quello del Golf?

Poniamo:

$$T = \{ \text{ persone iscritte al circolo del Tennis } \}$$

$$G = \{ \text{ persone iscritte al circolo del Golf } \}$$

Abbiamo che

$$T \cup G = \{ \text{ persone iscritte al circolo Tennis o al circolo Golf} \} = \{ \text{ persone iscritte ad almeno un circolo} \},$$

che sappiamo essere 25, e

$$T \cap G = \{ \text{ persone iscritte al circolo Tennis e al circolo Golf} \}$$

che è la quantità che ci interessa scoprire.

Sappiamo (per PIE) che:

$$\#(T \cup G) = \#T + \#G - \#(T \cap G),$$

dunque

$$25 = 20 + 15 - \#(T \cap G),$$

e dunque

$$\#(T \cap G) = 20 + 15 - 25 = 10.$$

PIE a 3 termini Consideriamo un caso in cui i nostri dati sono divisi in 3 tipi. Consideriamo una classe di 41 studenti sottoposti a tre test di valutazione: Combinatoria (C), Induzione (I) e Logica (L). I risultati dei test a nostra disposizione sono i seguenti:

- 12 studenti superano I
- 5 studenti superano L
- 8 studenti superano C
- 2 studenti superano sia I che L
- 6 studenti superano sia I che C
- 3 studenti superano sia L che C
- 1 studente supera sia I che L che C

Si osserva che, come sopra, i dati vanno di norma interpretati così: il numero degli studenti che supera I conta quelli che superano solo I, I e anche L, I e anche C, I e L e C; e analogamente per gli altri dati.

Quanti studenti hanno superato **almeno** un test?

Ponendo

$$I = \{ \text{ studenti che superano Induzione} \}$$

$$L = \{ \text{ studenti che superano Logica} \}$$

$$C = \{ \text{ studenti che superano Combinatoria} \}$$

possiamo vedere il problema come un problema di unione. Denotiamo, generalizzando la notazione per l'unione, con $I \cup L \cup C$ l'insieme degli studenti che sono sia in I che in C che in L, detto unione di I, C, L.

Proviamo a procedere così: consideriamo la somma

$$\#I + \#L + \#C$$

In questa somma stiamo contando due volte gli studenti che superano almeno due esami. Infatti in $\#I$ stiamo contando quelli che superano solo I e anche quelli che superano I e L; in $\#L$ contiamo quelli che superano solo L ma anche quelli che superano I e L – risulta così che gli studenti che superano I e L sono stati contati due volte. Dobbiamo quindi sottrarli.

Stessa cosa se consideriamo gli studenti che superano L e C, che sono contati una volta in $\#L$ e una in $\#C$ quindi due volte; o gli studenti che superano I e C, contati una volta in $\#I$ e una volta in $\#C$.

Abbiamo che dobbiamo sottrarre le quantità $\#(I \cap L)$, $\#(I \cap C)$ e $\#(L \cap C)$.

Otteniamo così

$$\#I + \#L + \#C - \#(I \cap L) - \#(I \cap C) - \#(L \cap C)$$

Dobbiamo ancora aggiustare il risultato: in ciascuno dei primi tre addendi abbiamo infatti contato una volta gli studenti che superano tutti e tre i test. Ma questi ultimi sono stati anche sottratti in ciascuno dei tre sottraendi. Infatti in $\#(I \cap C)$ contiamo sia gli studenti che superano solo I e C ma anche quelli superano I e C e L. Analogamente in $\#(I \cap L)$ e in $\#(L \cap C)$. Generalizzando la notazione per l'intersezione, denotiamo con $I \cap L \cap C$ l'insieme degli elementi che sono sia in I che in C che in L. Risulta che dobbiamo aggiungere la quantità $\#(I \cap C \cap L)$ perché non l'abbiamo contata.

Otteniamo così l'espressione:

$$\#I + \#L + \#C - \#(I \cap L) - \#(I \cap C) - \#(L \cap C) + \#(I \cap C \cap L)$$

Il ragionamento di sopra è del tutto generale e possiamo formulare il PIE a 3 termini: siano A, B, C tre insiemi finiti. Allora

$$\#(A \cup B \cup C) = \#A + \#B + \#C - \#(A \cap B) - \#(A \cap C) - \#(B \cap C) + \#(A \cap B \cap C).$$

Esempio Consideriamo il problema di distribuire 11 biscotti tra 3 bambini, con il vincolo aggiuntivo che nessun bambino riceve più di 4 biscotti. In termini di equazioni stiamo chiedendo il numero di soluzioni dell'equazione

$$x + y + z = 11$$

con il vincolo $x, y, z \leq 4$.

In questo come in altri casi, per contare gli oggetti con una certa proprietà P, conviene contare gli oggetti con la proprietà "non P". In questo caso

$$P = \text{ essere una soluzione in cui nessun bambino ha più di 4 biscotti}$$

e dunque

$$\text{non } P = \text{ essere una soluzione in cui almeno un bambino ha più di 4 biscotti.}$$

Proviamo a contare queste ultime, riformulandolo come un problema di unione. Poniamo

$$A = \{ \text{ soluzioni in cui il primo bambino ha più di 4 biscotti}\}.$$
$$B = \{ \text{ soluzioni in cui il secondo bambino ha più di 4 biscotti}\}.$$
$$C = \{ \text{ soluzioni in cui il terzo bambino ha più di 4 biscotti}\}.$$

La risposta che ci interessa è data dal numero di elementi dell'unione

$$A \cup B \cup C.$$

Per applicare il PIE a 3 termini dobbiamo contare $\#A$, $\#B$, $\#C$, $\#(A \cap B)$, $\#(A \cap C)$, e $\#(B \cap C)$.

$\#A$: diamo subito 5 biscotti al primo bambino. Per contare gli elementi in A ci resta da contare i modi di distribuire i restanti 6 biscotti tra i 3 bambini (senza vincoli). Sappiamo che questi sono $\binom{6+3-1}{3-1} = \binom{8}{2}$.

$\#B$: diamo subito 5 biscotti al secondo bambino. Per contare gli elementi in A ci resta da contare i modi di distribuire i restanti 6 biscotti tra i 3 bambini (senza vincoli). Sappiamo che questi sono $\binom{6+3-1}{3-1} = \binom{8}{2}$.

$\#C$: perfettamente identico.

$\#(A \cap B)$: diamo subito 5 biscotti al primo bambino e al secondo. Per contare gli elementi in $A \cap B$ ci resta da contare i modi di distribuire il restant biscotto tra i 3 bambini (senza vincoli). Ovviamente ci sono solo 3 modi. Usando la formula delle combinazioni con ripetizione abbiamo $\binom{1+3-1}{3-1} = \binom{3}{2} = 3$.

I conteggi di $\#(A \cap C)$ e $\#(B \cap C)$ sono identici.

$\#(A \cap B \cap C)$: stiamo contando i modi di dare 11 biscotti a tre bambini dando a ciascun bambino più di 4 biscotti. Il vincolo è insoddisfacibile quindi queste soluzioni sono 0.

Applicando il PIE a 3 termini abbiamo che le soluzioni che **non hanno** la proprietà P sono:

$$\binom{8}{2} + \binom{8}{2} + \binom{8}{2} - \binom{3}{2} - \binom{3}{2} - \binom{3}{2} + 0 = 75.$$

Per rispondere alla domanda iniziale sottraiamo questa quantità dal totale di tutte le soluzioni. Tutte le soluzioni possibili sono $\binom{11+3-1}{3-1} = \binom{13}{2} = 78$. Dunque le soluzioni con la proprietà P sono

$$78 - 75 = 3.$$

Il metodo sopra illustrato è generale per problemi su soluzioni di equazioni additive con un vincolo sul valore massimo delle variabili.

PIE a più termini Il tipo di ragionamento usato per ottenere le formule del PIE a 2 e 3 termini si generalizza facilmente a più termini. Consideriamo un esempio.

Esempio Consideriamo il seguente problema delle madri degeneri. Abbiamo 4 madri ciascuna con un neonato, decisamente stufe del proprio pargolo. In quanti modi le madri degeneri possono scambiarsi i figli in modo che a nessuna madre capiti il proprio figlio?

Si vede facilmente che possiamo rappresentare il problema fissando un ordine delle madri 1,2,3,4 e un ordine dei rispettivi pargoli a, b, c, d, e che siamo interessati alle permutazioni dell'insieme $\{a, b, c, d\}$ (ciascuna delle quali rappresenta un possibile riassegnamento di un pargolo a ogni madre) in cui nessuna lettera rimane al suo posto. Per esempio (b, a, d, c) è una soluzione buona mentre (b, c, a, d) non lo è (d è rimasta al suo posto – la quarta madre ha riavuto il suo pargolo).

Anche qui conviene contare gli oggetti che **non** hanno la proprietà che ci interessa: in questo caso si tratta delle soluzioni (o permutazioni) in cui **almeno** una lettera rimane al suo posto. Dunque possiamo ragionare come sopra.

Vogliamo contare le soluzioni che fissano almeno un elemento, dunque l'unione delle soluzioni che fissano a unite a quelle che fissano b unite a quelle che fissano c unite a quelle che fissano d.

Proviamo a contare gli elementi di tipo 1 o 2 o 3 o 4: consideriamo prima la somma

#{soluzioni che fissano a}+#{soluzioni che fissano b}+#{soluzioni che fissano c}+#{soluzioni che fissano d}

Si osserva che nel primo termine ho contato anche le soluzioni che fissano a e b, quelle che fissano a e c, quelle che fissano a e d. Nel secondo termine ho contato anche quelle che fissano b e a (quindi contate due volte!), quelle che fissano b e c, e quelle che fissano b e d. Continuando l'analisi dei casi osserviamo che nella somma di sopra ho contato una volta di troppo esattamente tutte quelle soluzioni che fissano almeno 2 lettere. Dunque devo sottrarle:

$-$#{soluzioni che fissano a e b} $-$ #{soluzioni che fissano a e c} $-$ #{soluzioni che fissano a e d} $- \ldots$

Ci accorgiamo ora di aver aggiunto e sottratto tutte le soluzioni che fissano 3 lettere: per esempio le soluzioni che fissano a,b e c sono contate nelle soluzioni che fissano a, nelle soluzioni che fissano b e nelle soluzioni che fissano c, ma sono sottratte una volta sottranedo le soluzioni che fissano a e b, un'alta volta sottraendo a e c e un'altra volta sottranedo c e d. Dunque in definitiva, non le abbiamo contate: dobbiamo aggiungerle! Continuiamo quindi la somma con

+#{soluzioni che fissano a e b e c}+#{soluzioni che fissano a e c e d}+#{soluzioni che fissano b e c e d}+...

Ci accorgiamo ora di aver contato alcune soluzioni una volta di troppo: sono le soluzioni che fissano tutte e quattro le lettere a, b, c, d: si tratta di una unica soluzione. Dobbiamo quindi sottrarre la loro quantità, ossia aggiungere il termine

$$-\#\{\text{ soluzioni che fissano a, b, c, d}\}.$$

Sappiamo ora quali quantità ci interessa contare e come metterle insieme. Per il conteggio possiamo procedere così.

Caso 1. Contiamo le soluzioni che tengono fissa almeno una lettera: ci sono 4 scelte di quale lettera fissare e per ogni scelta devo contare tutte le permutazioni dei restanti 3 elementi, che sono 3!. In tutto ho quindi

$$4 \times 3!$$

Caso 2. Contiamo le soluzioni che tengono fissi almeno due lettere: ci sono $\binom{4}{2}$ modi di scegliere 2 elementi tra i 4 e per ciascun modo devo contare tutte le permutazioni dei restanti 2 elementi, che sono 2!. In tutto ho quindi

$$\binom{4}{2} \times 2!$$

Caso 3. Contiamo le soluzioni che tengono fisse almeno tre lettere: ci sono $\binom{4}{3}$ modi di scegliere i 3 elementi da fissare e per ciascuna scelta ho 1 modo di permutare l'unico elemento restante. Quindi ho in tutto

$$\binom{4}{3} \times 1$$

Caso 4. Contiamo infine le soluzioni che tengono fissi almeno quattro lettere, ossia tutte le lettere: ovviamente c'è un'unica soluzione di questo tipo!

Osserviamo che le espressioni ottenute nei casi analizzati hanno una certa forma regolare:

$$4 \times 3! = \binom{4}{1} \times 3!$$

$$\binom{4}{2} \times 2!$$

$$\binom{4}{3} \times 1 = \binom{4}{3} \times 1!$$

$$1 = \binom{4}{4} \times 0!$$

(0! è per convenzione uguale a 1).

Usando la formula suggerita dal procedimento descritto sopra abbiamo che le soluzioni che fissano almeno una lettera sono in numero di:

$$\binom{4}{1} \times 3! + \binom{4}{2} \times 2! + \binom{4}{1} \times 1! + \binom{4}{4} \times 0!.$$

Le soluzioni che fanno contente le madri degeneri sono dunque

$$4! - \left(\binom{4}{1} \times 3! + \binom{4}{2} \times 2! + \binom{4}{1} \times 1! + \binom{4}{4} \times 0! \right).$$

Si evince dal caso di sopra che si può sviluppare una formula per il PIE per unioni di 4 insiemi. Con analogo ragionamento si ottiene una formula per unioni arbitrarie di n insiemi.

Teorema 1 *Siano $A_1, A_2, \ldots, A_n$ insiemi finiti. La loro unione contiene esattamente*

$$\sum_{i=1}^{n} \#A_i - \sum_{1 \le i_1 < i_2 \le n} \#(A_{i_1} \cap A_{i_2}) + \sum_{1 \le i_1 < i_2 < i_3} \#(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \cdots + (-1)^{n-1} \#(A_1 \cap A_2 \cap \cdots \cap A_n).$$

Alcune considerazioni sulla formula: la sommatoria $\sum_{1 \le i_1 < i_2 \le n} \#(A_{i_1} \cap A_{i_2})$ è un'espressione sintetica per variare su tutte le possibili coppie di due insiemi scelte tra gli n a disposizione. Va letta così: per ogni scelta di i_1 e i_2 cha variano tra 1 e n e tali che $i_1 < i_2$ ho un certo addendo dipendente da i_1 e i_2, in questo caso è il numero di elementi nell'intersezione di A_{i_1} con A_{i_2}. In termini informatici può leggersi come un doppio *for*. Analogo discorso per $\sum_{1 \le i_1 < i_2 < i_3 \le n} \#(A_{i_1} \cap A_{i_2} \cap A_{i_3})$, che va letta come: per ogni scelta di $i_1 < i_2 < i_3$ che variano tra 1 e n ho l'addendo $\#(A_{i_1} \cap A_{i_2} \cap A_{i_3})$, ossia come un triplo *for*. Il termine $(-1)^{n-1}$ non è che un trucchetto per scrivere uniformemente il segno dell'ultiomo termine della formula che è un - se n è pari (cfr. caso $n = 2$) e un + se n è dispari (cfr. caso $n =$). Diamo ora una dimostrazione combinatoria del Teorema.

Dimostrazione Consideriamo un arbitrario elemento a nell'unione $A_1 \cup \ldots A_n$. Questo elemento ovviamente contribuisce una unità al conto del numero di elementi dell'unione (termine sinistro dell'identità da dimostrare). Chiediamoci ora quanto contribuisce al termine destro dell'identità. In altre parole: in quante

delle intersezioni che compaiono nella parte destra dell'identità nel Teorema viene contato il termine a. Ovviamente in tutte e sole quelle che coinvolgono insiemi ai quali a appartiene! Sia dunque i il numero degli insiemi in $A_1, \ldots, A_n$ di cui a è un elemento. Rinominiamo per comodità la nostra lista di insiemi in modo che gli i insiemi che contengono a compaiano per primi, ossia in modo tale che a sia in $A_1, A_2, \ldots, A_i$ e in nessun insieme con indice più grande. L'elemento a compare nelle intersezioni di ogni k-pla di insiemi scelti tra questi. Dunque compare in $\binom{i}{k}$ intersezioni. Queste intersezionio vengono aggiunte o sottratte a seconda della parità di k: infatti vengono contate con segno $(-1)^{k-1}$ nella formula a destra dell'identità del PIE. Dunque il contribuito dell'elemento a alla parte destra dell'identità è di

$$\binom{i}{1} - \binom{i}{2} + \binom{i}{3} - \cdots + (-1)^{i-1}\binom{i}{i}.$$

Per concludere basta osservare che questa espressione vale esattamente 1. Dunque un arbitrario elemento a contribuisce una unità a sinistra e una unità a destra dell'identità e il Teorema è dimostrato.

Esercizio Dimostrare che

$$\binom{i}{1} - \binom{i}{2} + \binom{i}{3} - \cdots + (-1)^{i-1}\binom{i}{i} = \sum_{j=1}^{i}\binom{i}{j}.$$

(Suggerimento: dimostrare che

$$\binom{i}{0} - \binom{i}{1} + \binom{i}{2} - \cdots + (-1)^{i}\binom{i}{i} = \sum_{j=1}^{i}\binom{i}{j} = 0,$$

usando lo sviluppo di un binomio $(a+b)^n$ per una scelta opportuna di a e b – ricordandosi che vale per a, b numeri reali non necessariamente positivi)

Metodi Matematici per l'Informatica - Dispensa 7
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Figure della Combinatoria e Funzioni

Le funzioni da A in B con $\#(A) = k$ e $\#(B) = n$ (e.g. $A = \{1, \ldots, k\}$ e $B = \{1, \ldots, n\}$) sono esattamente le disposizioni con ripetizioni di ordine k su n elementi. Il loro numero è $D'_{n,k} = n^k$.

Le funzioni iniettive da A in B con $\#(A) = k$ e $\#(B) = n$ (e.g. $A = \{1, \ldots, k\}$ e $B = \{1, \ldots, n\}$) sono esattamente le disposizioni semplici di ordine k su n elementi. Il loro numero è $D_{n,k} = \frac{n!}{(n-k)!}$.

Le funzioni biiettive da A in A con $\#(A) = n$ (e.g. $A = \{1, \ldots, n\}$) sono esattamente le permutazioni di n elementi. Il loro numero è $P_n = n!$.

Le combinazioni con ripetizione di ordine k su n elementi possono identificarsi con le funzioni

$$f : A \to \{0, 1, 2, \ldots\}$$

tali che

$$\sum_{a_i \in A} f(a_i) = k,$$

dove $A = \{a_1, a_2, \ldots, a_n\}$. Il loro numero è $C'_{n,k}$.

Proprietà della Composizione

Proposizione 1 *Siano $f : X \to Y$ e $g : Y \to Z$. Allora*

1. *Se f e g sono iniettive allora $g \circ f$ è iniettiva.*
2. *Se f e g sono suriettive allora $g \circ f$ è suriettiva.*
3. *Se f e g sono biiettiva allora $g \circ f$ è biiettiva.*

Dimostrazione
Punto (2).Diamo una dimostrazione diretta. La tesi è $g \circ f$ è suriettiva, ossia per ogni $z \in X$ esiste $x \in X$ tale che $(g \circ f)(x) = z$. Le ipotesi sono due: f è suriettiva e g è suriettiva, ossia: per ogni $y \in Y$ esiste $x \in X$ tale che $f(x) = y$; e per ogni $z \in Z$ esiste $y \in Y$ tale che $g(y) = z$.
Sia $z \in Z$ arbitrario. Per ipotesi su g esiste $y \in Y$ tale che $g(y) = z$. Fissiamo un tale $y \in Y$. Per ipotesi su f esiste $x \in X$ tale che $f(x) = y$. Dunque per ogni $z \in Z$ esiste un $x \in X$ tale che

$$(g \circ f)(x) = g(f(x)) = z,$$

dunque $(g \circ f)$ è suriettiva.

Punto (1). La tesi è $g \circ f$ è iniettiva, ossia per ogni $x, x' \in X$, se $x \neq x'$ allora $g(f(x)) \neq g(f(x'))$. Le ipotesi sono che f è iniettiva e g è iniettiva, ossia: per ogni $x, x' \in X$, se $x \neq x'$ allora $f(x) \neq f(x')$, e per ogni $y, y' \in Y$ se $y \neq y'$ allora $g(y) \neq g(y')$.

Ragioniamo per assurdo. Ipotizziamo che la tesi sia falsa e andiamo a contraddizione con una delle ipotesi. La tesi è falsa significa che $(g \circ f)$ non è iniettiva, dunque che esistono $x, x' \in X$ tali che $x \neq x'$ ma $(g \circ f)(x) = (g \circ f)(x')$, ossia $g(f(x)) = g(f(x'))$. Ragioniamo per casi. Caso 1: $f(x) \neq f(x')$. Allora g non è iniettiva, contro una delle ipotesi. Caso 2: g è iniettiva. Allora f non è iniettiva, poiché abbiamo $x \neq x'$ per ipotesi ma $f(x) = f(x')$ dato che g è iniettiva e vale $g(f(x)) = g(f(x'))$. Ma f è iniettiva per ipotesi. Contraddizione.

Il punto (3) segue dai punti precedenti. **QED**

Esercizio Siano $f : X \to Y$ a $g : Y \to Z$. Se $(g \circ f) : X \to Z$ è iniettiva, è vero che f è iniettiva? E g?

Dimostriamo che f deve essere iniettiva. Altrimenti (ragionamento per assurdo) abbiamo che esistono $x, x' \in X$ tali che $x \neq x'$ e $f(x) = f(x')$. Ma allora $g(f(x)) = g(f(x'))$ (g non può separare ciò che f ha unito...) e dunque la composta $(g \circ f)$ non è iniettiva, contro l'iportesi.

g può essere non iniettiva: è sufficiente osservare che $f(X)$ non coincide necessariamente col codominio Y ma con un suo sottinsieme. La funzione g può essere non iniettiva su elementi che non appartengono all'immagine di X via f, ossia a $f(X)$ (fornire un semplice esempio esplicito per esercizio).

Esercizio Siano $f : X \to Y$ a $g : Y \to Z$. Se $(g \circ f) : X \to Z$ è suriettiva, è vero che f è suriettiva? E g?

Dimostriamo che g deve essere suriettiva. Se non lo fosse, esisterebbe $z \in Z$ tale che per nessun $y \in Y$ si ha $g(y) = z$. D'altra parte sappiamo che $(g \circ f)$ è suriettiva, dunque per ogni $z \in Z$ esiste $x \in X$ tale che

$$(g \circ f)(x) = g(f(x)) = z.$$

Fissiamo un elemento z di Z che testimonia che g non è suriettiva, ossia tale che per nessun $y \in Y$ vale $g(y) = z$. Per questo z esiste (dato che $(g \circ f)$ è suriettiva) un $x \in X$ tale che $(g \circ f)(x) = z$. Ma $f(x) \in Y$ e abbiamo che $g(f(x)) = z$. Dunque esiste un $y \in Y$ tale che $g(y) = z$, contro l'ipotesi per assurdo.

f può essere non suriettiva: il motivo è simile a quello dell'esercizio precedente (dare un esempio esplicito per esercizio).

Esercizio Siano $g : X \to Y$ e $h : X \to Y$ due funzioni distinte. Sia $f : Y \to Z$ tale che per ogni $x \in X$:

$$(f \circ g)(x) = (f \circ h)$$

f può essere iniettiva?

La risposta è no: g e h sono distinte, dunque esiste almeno un $x \in X$ tale che

$$g(x) \neq h(x).$$

D'altro canto abbiamo per ipotesi che

$$f(g(x)) = f(h(x)).$$

Dunque f non è iniettiva, perché manda i due argomenti $g(x)$ e $h(x)$ distinti nello stesso valore.

Esercizio Se $f : A \to B$ è iniettiva allora per ogni $X, Y \subseteq A$

$$f(X \cap Y) = f(X) \cap f(Y).$$

Dobbiamo dimostrare una identità tra i due insiemi $f(X \cap Y)$ e $f(X) \cap f(Y)$. Cominciamo scrivendo le loro definizioni.

$f(X \cap Y) = \{b \in B : \text{ esiste } a \in X \cap Y (f(a) = b))\}$.

$f(X) \cap f(Y) = \{b \in B : b \in f(X) \text{ e } b \in f(Y)\}$, ossia

$= \{b \in B : \text{ esiste } a \in X (f(a) = b) \text{ ed esiste } a' \in Y (f(a') = b)\}$.

Dimostriamo $f(X \cap Y) \subseteq f(X) \cap f(Y)$. Se $b \in f(X \cap Y)$ allora esiste un $a \in X \cap Y$ tale che $f(a) = b$. Dunque a fortiori (ossia: a maggior ragione) esiste un $a \in X$ tale che $f(a) = b$ ed esiste un $a' \in Y$ tale che $f(a') = b$ (nella fattispecie sono lo stesso elemento). Dunque $b \in f(X) \cap f(Y)$. Si osservi che non abbiamo usato alcuna ipotesi su f.

Dimostriamo che $f(X) \cap f(Y) \subseteq f(X \cap Y)$: Se $b \in f(X) \cap f(Y)$ allora esiste un $a \in X$ tale che $f(a) = b$ ed esiste un $a' \in Y$ tale che $f(a') = b$. In generale questi due elementi possono essere distinti. Ma dato che f è iniettiva, se $a \neq a'$ dovremmo avere $f(a) \neq f(a')$, mentre entrambi sono uguali a b. Dunque $a = a'$ e abbiamo che esiste un elemento $a \in X \cap Y$ tale che $f(a) = b$, ossia $b \in f(X \cap Y)$.

Cardinalità nel finito

Per un insieme finito A indichiamo con $\#(A)$ il numero degli elementi di A.

Si osserva facilmente che se $f : A \to B$ allora $\#(A)$ è uguale al numero di frecce nel diagramma a frecce della funzione. D'altro canto, se $f : A \to B$ è suriettiva, allora ogni elemento di B ha almeno una freccia entrante, dunque $\#(B)$ è al massimo uguale al numero di frecce nel diagramma. In conclusione:

$$\#(A) = \text{ numero di frecce da } A \geq \#(B).$$

Se $f : A \to B$ è iniettiva, allora ogni elemento di B ha al più una freccia entrante (mentre ogni elemento di A ha una e una sola freccia uscente), dunque $\#(A) \leq \#(B)$.

Riassumendo abbiamo la seguente proposizione.

Proposizione 2 *Siano A e B insiemi finiti.*

1. *Se esiste una $f : A \to B$ suriettiva allora $\#(A) \geq \#(B)$.*
2. *Se esiste una $f : A \to B$ iniettiva allora $\#(A) \leq \#(B)$.*
3. *Se esiste una $f : A \to B$ biiettiva allora $\#(A) = \#(B)$.*

L'ultimo punto si ottiene ovviamente dai primi due.

Osserviamo che le implicazioni si invertono. Sia $\#(A) \geq \#(B)$. Allora esiste una suriezione di A su B. Se $A = \{a_1, a_2, \ldots, a_n\}$ e $B = \{b_1, b_2, \ldots, b_,m\}$ con $n \geq m$ basta associare

$$a_1 \mapsto b_1, a_2 \mapsto b_2, \ldots, a_m \mapsto b_m, a_{m+1} \mapsto b_{m+1}, \ldots, a_n \mapsto b_m$$

per ottenere una suriezione da A a B.

D'altro canto se $\#(A) \leq \#(B)$ è facile vedere che esiste una iniezione da A in B.

Proposizione 3 *Siano A e B insiemi finiti.*

1. *Se $\#(A) \geq \#(B)$ allora esiste una $f : A \to B$ suriettiva.*
2. *Se $\#(A) \leq \#(B)$ allora esiste una $f : A \to B$ iniettiva.*
3. *Se esiste $\#(A) = \#(B)$ allora esiste una $f : A \to B$ biiettiva.*

NB: Per dimostrare l'ultimo punto occorre assicurarsi che per A e B insiemi finiti, se esiste una suriezione da A su B e una iniezione di A in B allora esiste una biiezione tra A e B (Esercizio: provare a dimostarlo).

Metodi Matematici per l'Informatica - Dispensa 8
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Teorema di Cantor

Teorema 1 *Sia A un insieme qualunque. Non esiste una biiezione tra A e $\mathcal{P}(A)$.*

Dimostrazione Dimostriamo che non esiste una suriezione da A su $\mathcal{P}(A)$. Ragioniamo per assurdo. Sia dunque $f : A \to \mathcal{P}(A)$ una suriezione. La funzione f manda elementi di A in sottinsiemi di A. In generale, dato un elemento a di A e un sottinsieme S di A, ha senso chiedersi se $a \in S$ oppure no. Questa domanda ha senso anche per un arbitrario elemento a di A e la sua immagine $f(a)$ tramite f. Distinguiamo dunque in due tipi gli elementi di A:

Tipo 1 Elementi $a \in A$ tali che $a \in f(a)$.

Tipo 2 Elementi $a \in A$ tali che $a \notin f(a)$.

Consideriamo ora l'insieme di tutti e soli gli elementi $a \in A$ del secondo tipo, ossia

$$X = \{a \in A : a \notin f(a)\}.$$

X è un sottinsieme di A, ossia $X \in \mathcal{P}(A)$. Dato che f per ipotesi è suriettiva, deve esiste un elemento $x \in A$ tale che $f(x) = X$. Fissiamo un tale x.

Chiediamoci ora di che tipo è questo x.

Se x è di tipo 1, allora $x \in f(x)$. Dato che $f(x) = X$ abbiamo $x \in X$. Ma per definizione di X, questo implica che $x \notin f(x)$. Abbiamo dunque che: se $x \in f(x)$ allora $x \notin f(x)$. Questo è impossibile dunque x non è di tipo 1.

Se x è di tipo 2, allora $x \notin f(x)$, ossia $x \notin X$. Per definizione di X questo implica che $x \notin f(x)$ è falso, dunque $x \in f(x)$. Abbiamo dunque che: se $x \notin f(x)$ allora $x \in f(x)$.

Unendo le due parti del ragionamento abbiamo che $x \in f(x)$ se e solo se $x \notin f(x)$, il che è ovviamente contraddittorio. Dunque la nostra ipotesi per assurdo è falsa: non esiste una suriezione f da A su $\mathcal{P}(A)$.

Q.E.D.

Dal Teorema di sopra segue facilmente che per ogni insieme A, vale

$$\#(A) < \#(\mathcal{P}(A)).$$

Per definizione questa diseguaglianza significa che:

1. esiste una iniezione da A in $\mathcal{P}(A)$, ma
2. non esiste una suriezione da A su $\mathcal{P}(A)$ (o, equivalentemente, non esiste una iniezione da $\mathcal{P}(A)$ in A).

Il secondo punto è proprio quello che abbiamo dimostrato nel Teorema. Per il primo punto: si vede facilmente che la seguente mappa è una iniezione da A in $\mathcal{P}(A)$: basta associare a un elemento $a \in A$ il sottinsieme $\{a\}$.

Iterando il Teorema, a partire da $A = \mathbb{N}$, abbiamo una successione infinita di cardinalità infinite l'una strettamente maggiore della precedente:

$$\#(\mathbb{N}) < \#(\mathcal{P}(\mathbb{N})) < \#(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \#(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))) < \dots$$

In altre parole, esistono infiniti numeri infiniti (detti *numeri transfiniti*).

Metodi Matematici per l'Informatica - Dispensa 9
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Alcuni risultati aggiuntivi sulle relazioni.

Relazioni di equivalenza e partizioni

Teorema 1 *Sia $R \subseteq A \times A$ una relazione di equivalenza. Per $a \in A$ definiamo*

$$R[a] = \{b \in A : aRb\}$$

detta classe di equivalenza di a. Valgono i seguenti punti:

1. *Per ogni $a \in A$, $R[a] \neq \emptyset$.*
2. *Per ogni $a, b \in A$ si ha che $R[a] \cap R[b] = \emptyset$ oppure $R[a] = R[b]$.*

Dimostrazione Dato che R è riflessiva, per ogni $a \in A$ vale aRa. Dunque $a \in R[a]$. Questo dimostra il primo punto.

Siano $a, b \in A$. O aRb oppure no. Ragioniamo per casi.

(Caso 1) aRb. Dimostriamo che $R[a] = R[b]$. Cominciamo dimostrando che $R[a] \subseteq R[b]$. Sia $c \in R[a]$. Per definizione vale aRc. Per simmetria vale cRa. Dato che per ipotesi del caso vale aRb, per transitività abbiamo cRb. Per simmetria vale bRc e dunque per definizione $c \in R[b]$. L'inclusione $R[b] \subseteq R[a]$ si dimostra analogamente.

(Caso 2) Non vale aRb. Supponiamo per assurdo che valga $R[a] \cap R[b] \neq \emptyset$. Sia c nell'intersezione di $R[a]$ e $R[b]$. Per definizione di $R[a]$ segue che cRa e per definizione di $R[b]$ segue che bRc. Per simmetria da cRa segue aRc; e da bRc segue cRb. Per transitività, da aRc e cRb segue aRb, contro l'ipotesi del caso. **Q.E.D.**

Il risultato appena dimostrato mostra che ogni relazione di equivalenza su A determina una cosidetta *partizione* di A, ossia una scomposizione di A come unione di sottinsiemi di A due a due disgiunti.

Vale anche il viceversa: ogni partizione determina una relazione di equivalenza.

Definizione 1 (Partizione) *Una partizione di un insieme A è una famiglia $\{C_i : i \in I\}$ di insiemi non vuoti $C_i \subseteq A$, dove I è un insieme qualunque (anche infinito, detto insieme di indici), tali che*

1. *per ogni $a \in A$ esiste un $i \in I$ tale che $a \in C_i$, e*
2. *per $i, j \in I$ se $i \neq j$ allora $C_i \cap C_j = \emptyset$ (ossia le classi C_i sono due a due disgiunte).*

Si osserva che $\bigcup_{i \in I} C_i \subseteq A$ dato che ogni C_i è sottinsieme di A; dal primo punto della definizione di partizione segue invece che $A \subseteq \bigcup_{i \in I} C_i$. Dunque $A = \bigcup_{i \in I} C_i$. (La notazione $\bigcup_{i \in I} C_i$ generalizza la notazione di unione e indica l'insieme che contiene tutti e soli gli elementi x per cui esiste (almeno) un $i \in I$ tale che $x \in C_i$).

Teorema 2 *Sia $\{C_i : i \in I\}$ una partizione di A. Allora la relazione $R \subseteq A \times A$ definita ponendo aRb sse esiste un $i \in I$ tale che $a, b \in C_i$ è una relazione di equivalenza su A.*

Dimostrazione Dimostriamo che R è riflessiva simmetrica e transitiva. Per ogni a esiste un $i \in I$ tale che $a \in C_i$. Per definizione di R questo implica aRa. Siano $a, b \in A$ tali che aRb. Per definizione di R esiste $i \in I$ tale che $a, b \in C_i$, che implica anche che bRa. Siano $a, b, c \in A$ tali che aRb e bRc. Da aRb segue che esiste $i \in I$ tale che $a, b \in C_i$. Da bRc segue che esiste $j \in C_j$ tale che $b, c \in C_j$. Dall'ipotesi che C_i e C_j sono disgiunte per $i \neq j$, deve essere $i = j$ dunque $a, c \in C_i$ e dunque aRc. **Q.E.D.**

Si vede facilmente che le classi di equivalenza della relazione definita in base alla partizione sono classi della partizione. Si osserva che se $R \subseteq A \times A$ e $S \subseteq A \times A$ determinano le stesse classi di equivalenza allora sono la stessa relazione (esercizio).

Ordini (parziali)

Abbiamo visto come rappresentare un ordine parziale finito con diagrammi di Hasse. L'idea è semplicemente di non indicare le frecce riflessive e quelle che seguono per transitività e di indicare l'orientamento della relazione usando la direzione dal basso verso l'alto. Alcuni esempi:

Diagramma dei sottinsiemi di $\{a, b, c\}$ ordinati per inclusione.

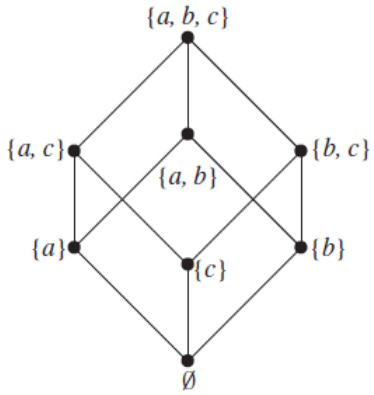
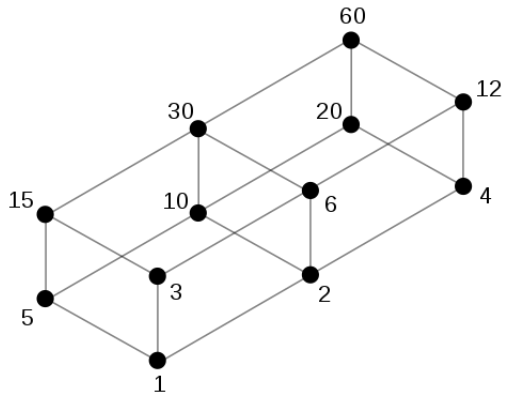


Diagramma dei divisori di 60:



Definizione 2 (Immersione tra ordini) *Siano $\leq$ un ordine (parziale) su un insieme X e sia $\leq^*$ un ordine (parziale) su un insieme X^*. Una funzione $f : X \to X^*$ è una* **immersione** *di $(X, \leq)$ in $(X^*, \leq^*)$ se è iniettiva e se vale*

$$f(x) \leq^* f(y) \text{ se e solo se } x \leq y.$$

Teorema 3 *Sia X un insieme e $\leq$ una relazione d'ordine su X. Esiste una immersione in $\mathcal{P}(X)$ ordinato da $\subseteq$.*

Dimostrazione Definiamo una funzione $f : X \to \mathcal{P}(\mathcal{X})$ come segue:

$$f(x) = \{y \in X \,:\, y \leq x\}.$$

Dimostriamo che è una immersione.

Dimostriamo che f è iniettiva. Siano $x, y \in X$ tali che $f(x) = f(y)$. Dato che $x \leq x$ e $y \leq y$ abbiamo che $x \in f(x)$ e $y \in f(y)$. Dunque $x \in f(y)$ e segue $x \leq y$; $y \in f(x)$ e segue $y \leq x$. Per antisimmetria segue $x = y$.

Dimostriamo che è una immersione. Sia $x \leq y$. Se $z \in f(x)$ allora $z \leq x$ e per transitività segue $z \leq y$ e dunque $z \in f(y)$. Questo dimostra $f(x) \subseteq f(y)$. Supponiamo ora che $f(x) \subseteq f(y)$ e dimostriamo che $x \leq y$. Dato che $x \in f(x)$ per riflessività di $\leq$, segue che $x \in f(y)$ e dunque $x \leq y$. **Q.E.D.**

Il risultato di sopra dimostra che gli ordini di tipo $(\mathcal{P}(X), \subseteq)$ sono universali nel senso che contengono una copia di qualunque insieme ordinato!

Ordini totali e sottosuccessioni monotone

Teorema 4 *Sia $n \geq 1$. Sia $(x_1, \ldots, x_{n^2+1})$ una successione di elementi distinti scelti in insieme X su cui $\preceq$ è un ordine totale. Allora esiste una sottosuccessione strettamente crescente lunga $n+1$ oppure esiste una sottosuccessione strettamente decrescente lunga $n+1$.*

NB X non è necessariamente un insieme di numeri ma è un insieme arbitrario! La relazione denotata con $\preceq$ è un arbitrario ordine totale su X. Le sottosuccessioni sono ordinate rispetto all'ordine $\preceq$. Denotiamo con $\prec$ l'ordine stretto ottenuto da $\preceq$ (ossia $x \prec y$ sse $x \preceq y$ e $x \neq y$). Una sottosuccessione strettamente crescente di lunghezza $\ell \leq n^2+1$ è una sequenza $(x_{a_1}, x_{a_2}, \ldots, x_{a_\ell})$ con $x_{a_1} \prec x_{a_2} \prec \cdots \prec x_{a_\ell}$, per qualche $a_1 < \cdots < a_\ell$ in $\{1, \ldots, n^2+1\}$. Analogamente una sottosuccessione strettamente decrescente di lunghezza $\ell \leq n^2+1$ è una sequenza $(x_{a_1}, x_{a_2}, \ldots, x_{a_\ell})$ con $x_{a_\ell} \prec x_{a_\ell} \prec \cdots \prec x_{a_1}$, per qualche $a_1 < \cdots < a_\ell$ in $\{1, \ldots, n^2+1\}$.

Per capire la dimostrazione può essere utile pensare a un ordine totale famigliare, per es. l'ordine $\leq$ sui naturali, e a valori concreti di n.

Dimostrazione Ragioniamo per assurdo. La Supponiamo quindi che non esista **né** una sottosuccessione strettamente crescente di lunghezza $n+1$ **né** una sottosuccessione strettamente decrescente di lunghezza $n+1$. Consideriamo la funzione

$$f : \{1, \ldots, n^2+1\} \to \{1, \ldots n\}$$

definita ponendo $f(i) =$ lunghezza massima di una successione strettamente crescente che termina con x_i. La funzione f ha dominion $\{1, \ldots, n^2+1\}$ e, per l'ipotesi per assurdo, codominio $\{1, \ldots, n\}$.

Dato che il dominio è più grande del codominio, diversi elementi del dominio assumeranno lo stesso valore tramite f. In particolare almeno $n+1$ elementi del dominio assumono lo stesso valore. Altrimenti ognuno degli n valori del codominio viene assunto al massimo da n elementi del dominio. Ma dunque al massimo $n + \cdots + n = n \times n = n^2$ elementi di $\{1, 2, \ldots, n^2+1\}$ ricevono un valore. Contraddizione.

Esistono dunque indici $i_1 < \cdots < i_{n+1}$ in $\{1, \ldots, n^2+1\}$ tali che

$$f(i_1) = f(i_2) = \cdots = f(i_{n+1}).$$

Sia ℓ il valore comune in $\{1, \ldots, n\}$ assunto dagli elementi $x_{i_1}, \ldots, x_{i_{n+1}}$.

Consideriamo i primi due elementi x_{i_1} e x_{i_2}. Dato che $\preceq$ è un ordine totale, abbiamo che $x_{i_1} \prec x_{i_2}$ oppure $x_{i_2} \prec x_{i_1}$. Dimostriamo che deve essere $x_{i_2} \prec x_{i_1}$. Supponiamo che valga $x_{i_1} \prec x_{i_2}$. Dato che $f(x_{i_1}) = \ell$, esiste una sottosuccessione strettamente crescente lunga ℓ con ultimo termine x_{i_1}. Ossia esistono $j_1 < \cdots < j_{\ell-1} < i_1$ tali che

$$x_{j_1} \prec x_{j_2} \prec \cdots \prec x_{j_{\ell-1}} \prec x_{i_1}.$$

Ma allora la successione

$$x_{j_1} \prec x_{j_2} \prec \cdots \prec x_{j_{\ell-1}} \prec x_{i_1} \prec x_{i_2}$$

è una sottosuccessione strettamente crescente di lungezza $\ell + 1$ che termina con x_{i_2}, contraddicendo l'ipotesi che la massima sottosuccessione di questo tipo è lunga ℓ.

Lo stesso ragionamento dimostra che $x_{i_3} \prec x_{i_2}$, $x_{i_4} \prec x_{i_3}$ etc. fino a $x_{i_{n+1}} \prec x_{i_n}$. Dunque la successione $(x_{i_1}, x_{i_2}, \ldots, x_{i_{n+1}})$ è una sottosuccessione strettamente decrescente (rispetto all'ordine $\prec$) di lunghezza $n+1$. Contro l'ipotesi per assurdo che ogni successione di questo tipo ha lunghezza al più n. **Q.E.D.**

Metodi Matematici per l'Informatica - Dispensa 10
(a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)

Alcune integrazioni su Principio del Minimo Numero e Induzione Forte.

Principio del Minimo Numero

Principio del Minimo Numero Ogni insieme non vuoto di interi non-negativi ha un elemento minimo.

Questo principio è molto elementare ma molto potente.

Esempio Ogni frazione $\frac{a}{b}$ può scriversi in termini minimi, ossia esistono $a', b' > 0$ con senza fattori primi comuni tali che $\frac{a}{b} = \frac{a'}{b'}$.

Supponiamo per assurdo che esista una frazione che non ammette una scrittura in termini minimi. Siano $a, b > 0$ tali che $\frac{a}{b}$ non ammette una scrittura in termini minimi. Consideriamo l'insieme

$$C = \{n \ : \ n > 0 \text{ è numeratore di una frazione che non ammette scrittura in termini minimi}\}.$$

Intuitivamente C è l'insieme dei numeratori dei controesempi alla proprietà che vogliamo dimostrare. Sappiamo che C è non vuoto perché $a \in C$. Per il PMN esiste m minimo elemento in C. Per definizione di C esiste $d > 0$ tale che $\frac{m}{d}$ non ammette una scrittura in termini minimi. Dunque esiste un primo $p > 1$ fattore comune di m e d (altrimenti la frazione è già in termini minimi). Ma allora $\frac{m/p}{d/p}$ è una frazione equivalente a $\frac{m}{d}$. Dunque per ipotesi su $\frac{m}{d}$, sappiamo che $\frac{m/p}{d/p}$ non è in termini minimi. Dunque $m/p \in C$. Ma ovviamente $m/p < m$, il che contraddice la minimalità di m in C.

Esempio Dimostriamo con il PMN la formula di Gauss: per ogni $n > 0$

$$1 + 2 + \cdots + n = \frac{n \times (n+1)}{2}.$$

Per assurdo supponiamo che la formula non sia vera. Dunque per qualche $n > 0$,

$$1 + 2 + \cdots + n \neq \frac{n \times (n+1)}{2}.$$

Dunque l'insieme dei controesempi,

$$C = \{n \ : \ 1 + 2 + \cdots + n \neq \frac{n \times (n+1)}{2}\}$$

è non-vuoto. Per il PMN sia $m = \min(C)$. Si osserva facilmente che per $n = 1$ l'equazione è vera: $1 = \frac{1\times 2}{2}$- Dunque deve essere $m > 1$.

Dato che m è il minimo controesempio, per $m - 1$ l'equazione è valida:

$$1 + 2 + \cdots + (m-1) = \frac{(m-1)times(m-1+1)}{2}.$$

Ma allora, aggiungendo m a entrambi i lati:

$$1 + 2 + \cdots + (m-1) + m = \frac{(m-1) \times (m-1+1)}{2} + m.$$

Un semplice calcolo mostra che

$$\frac{(m-1) \times (m-1+1)}{2} + m = \frac{m^2 - m + 2m}{2} = \frac{m^2 + m}{2} = \frac{m \times (m+1)}{2}.$$

Dunque

$$1 + 2 + \cdots + (m-1) + m = \frac{m \times (m+1)}{2}$$

e l'equazione è vera anche per m. Contraddizione.

Teorema 1 *Ogni intero positivo può scriversi come prodotto di numeri primi.*

Dimostrazione Per assurdo, supponiamo che la tesi non sia vera. Dunque l'insieme dei controesempi

$$C = \{n \ : \ n \text{ non è fattorizzabile in primi}\}$$

non è vuoto. Per il PMN esiste $m = \min(C)$.

m può essere primo? Ovviamente no, altrimenti avrebbe una scrittura come prodotto di primi (se stesso!). Dunque devono esistere a, b tali che $m = a \times b$, e $1 < a, b < m$. Dato che a e b sono minori di m, a e b non sono in C dunque non sono controesempi dunque ammettono ciascuno una fattorizzazione in primi:

$$a = p_1 \times \cdots \times p_k$$

$$b = q_1 \times \cdots \times q_\ell$$

dove i p_i e i q_j sono primi (non necessariamente distinti). Ma allora possiamo scrivere

$$m = a \times b = p_1 \times \cdots \times p_k \times q_1 \times \cdots \times q_\ell$$

e m ammette una fattorizzazione in primi. Contraddizione a $m \in C$. **Q.E.D.**

Esempio Ho a disposizione francobolli da 8 e da 5 centesimi. Quali affrancature postali posso realizzare? Dimostriamo che per ogni $n \geq 28$ posso usare francobolli da 8 e da 5 per ottenere una affrancatura di valore complessivo n.

Per assurdo, supponiamo che la tesi sia falsa. Dunque l'insieme dei controesempi

$$C = \{n \ : \ n \geq 20 \ \& \ n \text{ non si può ottenere con francobolli da 8 e da 5}\}$$

è non-vuoto. Per il PMN esiste $m = \min(C)$.

Si osserva prima di tutto che $m > 28$: infatti posso ottenere una affrancatura di valore 28 usando 4 francobolli da 5 e una da 8.

Considero allora $m-1$. Dato che $m-1 \geq 28$, è un valore che rientra nel dominio di variazione della nostra tesi (Per ogni $n \geq 28$...). Dato che $m-1 \notin C$, ma $m-1 \geq 28$, deve essere vero che $m-1$ **si può ottenere** usando francobolli da 8 e da 5 (altrimenti verificherebbe entrambe le condizioni che definiscono l'insieme C). Possiamo dunque assumere che esista una scelta di francobolli da 5 e da 8 che somma a $m-1$ (NB: non sappiamo nulla su quale sia questa scelta!!).

Caso 1: Per ottenere $m-1$ usiamo almeno 3 francobolli da 5. Ma allora per ottenere m basta sostituire, nella combinazione che somma a $m-1$, tre francobolli da 5 con due da 8:

$$m - 1 = \ldots \cdots + 5 + 5 + 5 + \ldots\ldots$$

$$m = \ldots\cdots + 8 + 8 + \ldots\ldots$$

Contraddizione a $m \in C$.

Caso 2: Per ottenere $m-1$ usiamo al massimo 2 francobolli da 5. Dato che $m-1 \geq 28$, dobbiamo usare almeno 3 francobolli da 8 ($m-1 \geq 28$ allora $m-1-10 \geq 18 > 16$). Ma allora sostituendo due francobolli da 8 con 5 francobolli da 5 nella combinazione che dà $m-1$ otteniamo il valore m. Contraddizione.

Osservazione Si consideri la seguente formulazione insiemistica del Principio di Induzione: Sia $S \subseteq \mathbb{N}$. Se

1. $1 \in S$, e
2. per ogni $n \in \mathbb{N}$: Se $n \in S$ allora anche $n+1 \in S$,

Allora $S = \mathbb{N}$.

Mostriamo che il PMN implica il Principio di Induzione: Supponiamo per assurdo che il Principio di Induzione sia falso. Dunque esiste un insieme $S \subseteq \mathbb{N}$ che verifica le due condizioni ($1 \in S$ e $n \in S \Rightarrow n+1 \in S$) ma non soddisfa la conclusione, ossia $S \neq \mathbb{N}$ (S non coincide con $\mathbb{N}$). Dunque $\mathbb{N} - S$ è non-vuoto. Per il PMN sia m il minimo di questo insieme. Dato che $1 \in S$, deve essere $m > 1$. Dunque $m-1 \notin (\mathbb{N} - S)$ ossia $m-1 \in S$. Ma per ipotesi su S se $m-1 \in S$ allora anche $m \in S$. Contraddizione. **Q.E.D.**

Principio di Induzione Forte

Se proviamo a tradurre la dimostrazione del Teorema di fattorizzazione in numeri primi in una dimostrazione per Induzione incontriamo qualche difficoltà: infatti in quel caso non abbiamo ragionato soltanto sul predecessore $m-1$ del minimo dei controesempi, m. Ci siamo invece ritrovati a ragionare su due elementi più piccoli del minimo dei controesempi, ossia i due fattori a, b tali che $a \times b = m$. In termini di induzione questo significa supporre che l'Ipotesi Induttiva vale non soltanto per il predecessore immediato del numero che stiamo considerando, ma per tutti i numeri più piccoli di lui.

Principio di Induzione Forte Sia P una proprietà di interi non-negativi e sia k un intero non-negativo. Se valgono i seguenti punti

1. (Base) P vale di k,
2. (Passo) Se P vale di $k, k+1, k+2, \ldots, n-1$ allora vale di n (per $n > k$ arbitrario),

allora posso concludere che per ogni $n \geq k$ vale $P(n)$.

Il caso classico è $k = 0$, utile a dimostrare proprietà che valgono per tutti gli interi non-negativi. L'Induzione Forte va usata tutte le volte che nell'analisi del passo induttivo, ci troviamo a ragionare su arbitrari elementi più piccoli del caso in esame.

Esempio Diamo una dimostrazione del Teorema di fattorizzazione usando l'Induzione Forte. La tesi è che per ogni $n > 1$ esiste una fattorizzazione in numeri primi.

La base è $n = 2$, e ovviamente vale la tesi perché 2 è primo.

Il passo induttivo consiste nell'assumere, per un arbitrario $n > 2$, che per ogni $2 \leq k < n$ vale la tesi e dimostrare che vale per n.

Se n è primo, la tesi è dimostrata. Se n non è primo allora $n = a \times b$ con $1 < a, b < n$. Dunque per a e per b vale la tesi (Ipotesi Induttiva) ossia a è fattorizzabile e b è fattorizzabile. Allora anche n è fattorizzabile.

Esempio Consideriamo la sequenza di Fibonacci definita come segue:

$$F_0 = 0; F_1 = 1$$

e, per $n \geq 0$,

$$F_{n+2} = F_n + F_{n+1}.$$

Sia $\phi = \frac{1+\sqrt{5}}{2}$. Dimostriamo per Induzione Forte che per ogni $n \geq 2$ vale $F_n \geq \phi^{n-2}$.

Base: $n = 2$. $F_2 \geq \phi^{2-2} = \phi^0 = 1$.

Passo: Sia $n > 2$ e assumiamo che la tesi valga per ogni k tale che $2 \leq k < n$. Dimostriamo che vale per n. $n = m + 2$ per qualche $m \geq 0$ e per definizione ho $F_{m+2} = F_m + F_{m+1}$. Per Ipotesi Induttiva Forte vale la tesi per F_m e per F_{m+1}. Dunque

$$F_n = F_{m+2} = F_m + F_{m+1} \geq \phi^{m-2} + \phi^{m-1} = \phi^{m-2}(\phi + 1).$$

Si osserva che $\phi^2 = (\phi + 1)$ e dunque

$$F_n \geq \phi^{m-2}\phi^2 = \phi^m = \phi^{n-2}$$

.

Esempio Abbiamo una barra di Toblerone con n quadratini. Ci chiediamo quante mosse di spezzatura (lungo le linee che separano i quadratini) sono necessarie per dividere il Toblerone in n quadratini distinti (monoporzioni). Si dimostra facilmente, usando l'Induzione Forte, che la risposta è $n - 1$.

Base: $n = 1$. Ovviamente mi servono 0 mosse.

Passo: n arbitrario maggiore di 0. NB: dobbiamo dimostrare che non si può ridurre in porzioni singole il Toblerone usando meno di $n - 1$ mosse. Possiamo quindi ragionare così: lasciamo la prima mossa a un avversario, che può decidere di spezzare il Toblerone in un punto a sua scelta tra gli $n - 1$ possibili. Dimostreremo poi, usando l'ipotesi induttiva forte, che qualunque sia la scelta dell'avversario, non potrà far meglio di fare $n - 1$ spezzature totali.

La mossa dell'avversario divide il Toblerone in due parti A_1 e A_2, di n_1 e n_2 quadratini rispettivamente. Di questi valori so soltanto che $n_1 + n_2 = n$, con $1 \leq n_1, n_2 < n$. Per ipotesi induttiva forte sappiamo che per dividere la prima parte, A_1, sono necessarie $n_1 - 1$ mosse e che per dividere la seconda parte, A_2, sono necessarie $n_2 - 1$ mosse. Dunque la strategia dell'avversario non potrà fare a meno di fare

$$n_1 - 1 + n_2 - 1 + 1 = n_1 + n_2 - 1 = n - 1$$

mosse.

METODI MATEMATICI PER L'INFORMATICA

ANNO ACCADEMICO 2019/2020

SOMMARIO. Sintassi e semantica della logica proposizionale. Tavole di verità. soddisfacibilità, valitdità, conseguenza logica. Teoremi di sostituzione. verità logiche notevoli. Completezza funzionale. Forme Normali CNF e DNF. Principio di dualità AND/OR.

N.B. Ho in ROSSO le parti di questo documento che non sono state viste a lezione (ma possono essere lette a piacere per approfondimento).

1. Linguaggio e proposizioni formali

Definizione 1.1 (Linguaggio proposizionale)**.** Un linguaggio proposizionale è un insieme $\mathcal{L}$ di simboli contenente

(1) I seguenti simboli, detti connettivi logici: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$,
(2) Le parentesi tonde chiuse e aperte,
(3) Una quantità finita o infinita numerabile di simboli (distinti dai connettivi e dalle parentesi) detti variabili proposizionali, il cui insieme viene indicato con $\mathsf{VAR}_{\mathcal{L}}$.

Definizione 1.2 (Proposizioni)**.** Sia $\mathcal{L}$ un linguaggio proposizionale. L'insieme delle proposizioni (o formule ben formate) in $\mathcal{L}$ è il minimo insieme X di stringhe finite di simboli in $\mathcal{L}$ tale che

(1) Tutte le variabili proposizionali di $\mathcal{L}$ sono in X, e
(2) Se A è in X allora $(\neg A)$ è in X, e
(3) Se A e B sono in X allora $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ sono in X.

Denotiamo con $\mathrm{PROP}_{\mathcal{L}}$ (o $\mathsf{FML}_{\mathcal{L}}$) l'insieme delle proposizioni (o formule) nel linguaggio $\mathcal{L}$. Se $\mathcal{L}$ è chiaro dal contesto, scriviamo PROP.

Osservazione 1.3. Cosa significa nella Definizione precedente che PROP è *il minimo insieme tale che...*? Quello che si intende è che, se Y è un qualunque insieme che soddisfa (1)(2)(3), allora $\mathrm{PROP} \subseteq Y$. Come sappiamo che un tale Y esiste? Possiamo argomentare come segue.

Chiamiamo *chiuso* un insieme X che soddisfa (1)(2)(3). Assumiamo che esiste un insieme chiuso (questo si pu* dimostrare usando i normali assiomi della teoria degli insiemi), e dimostriamo che esiste un minimo insieme chiuso. Osserviamo che se X e Y sono insiemi chiusi, allora anche $X \cap Y$ è un insieme chiuso, e più in generale che se S è un insieme non vuoto di insiemi chiusi, allora anche l'intersezione $\bigcap S = \{Z \text{ tali che } (\forall W \in S)(Z \subseteq W)\}$ è un insieme chiuso.

Sia X un insieme chiuso. Sia ora S l'insieme di tutti i sottinsiemi chiusi di X. Allora $\bigcap S$ è un insieme chiuso, ed è minimo nel senso di sopra. Sia infatti Y un insieme chiuso qualunque. Allora per ogni $W \in S$, anche $Y \cap W$ è un sottinsieme chiuso di X. Dunque se $x \in \bigcap S$ allora $x \in Y \cap W$ e dunque $x \in Y$, che dimostra $\bigcap S \subseteq Y$.

Definizione 1.4 (Sottoformula)**.** Una proposizione B è una sottoformula di una proposizione A se è verificato uno dei seguenti casi.

(1) A è identica a B.
(2) A è $(\neg C)$ e B è sottoformula di C.
(3) A è $(C \square D)$ e B è sottoformula di C oppure è sottoformula di D.

Se A è $(\neg C)$, C è detta sottoformula immediata di A. Se A è $(C \square D)$, C e D sono dette sottoformule immediate di A, dove usiamo il simbolo $\square$ come un segnaposto per uno dei connettivi $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

Note preparate da Lorenzo Carlucci, carlucci@di.uniroma1.it.

2. Induzione e Ricorsione sulle Proposizioni

Proposizione 2.1 (Principio di Induzione Strutturale su Formule)**.** *Sia $\mathcal{L}$ un linguaggio proposizionale. Sia $\mathcal{A}$ una proprietà di stringhe. Se valgono i tre punti seguenti allora $\mathcal{A}$ vale di tutte le proposizioni nel linguaggio $\mathcal{L}$.*

(1) *$\mathcal{A}$ vale di tutte le variabili proposizionali,*
(2) *Se $\mathcal{A}$ vale di una stringa A, allora vale di $(\neg A)$,*
(3) *Se $\mathcal{A}$ vale delle stringhe A e B, allora vale della stringa $(A\square B)$, dove usiamo il simbolo $\square$ come un segnaposto per uno dei connettivi $\{\wedge, \vee, \to, \leftrightarrow\}$.*

Dimostrazione. Consideriamo l'insieme X di tutte le stringhe nel linguaggio $\mathcal{L}$ che soddisfano la proprietà $\mathcal{A}$. Tale insieme soddisfa le tre condizioni nella definizione dell'insieme $\mathrm{PROP}_{\mathcal{L}}$ (ossia è un insieme chiuso). Dunque $\mathrm{PROP}_{\mathcal{L}} \subseteq X$, perché $\mathrm{PROP}_{\mathcal{L}}$ è per definizione il minimo insieme che soddisfa le tre condizioni in questione. □

Possiamo condurre dimostrazioni per induzione sull'insieme delle proposizioni anche usando la comune induzione matematica completa. Vediamo come.

Definizione 2.2. Sia $\mathcal{L}$ un linguaggio proposizionale e siano $\{p_1, p_2, \dots\}$ le sue variabili proposizionali. Definiamo una famiglia di insiemi di stringhe, per ricorsione su n.

$$\mathbf{F}_0 = \{p_1, p_2, \dots\}$$
$$\mathbf{F}_{n+1} = \mathbf{F}_n \cup \{(\neg A) \ : \ A \in \mathbf{F}_n\} \cup \{(A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B) \ : \ A, B \in \mathbf{F}_n\}$$
$$\mathbf{F} = \bigcup_{n \in \mathbf{N}} \mathbf{F}_n$$

Si può dimostrare che $\mathbf{F}$ coincide con l'insieme delle proposizioni nel linguaggio $\mathcal{L}$ (Esercizio). Definiamo l'altezza $h(A)$ di una proposizione A nel linguaggio $\mathcal{L}$ come il minimo n tale che $A \in \mathbf{F}_n$.

Per dimostrare che una proprietà $\mathcal{A}$ vale di tutte le proposizioni possiamo allora usare la usuale induzione matematica completa, dimostrando che per ogni $n \in \mathbf{N}$, $\mathcal{A}$ vale di tutte le proposizioni di altezza n.

Per esempio possiamo dimostrare il Principio di Induzione Strutturale usando l'induzione completa sull'altezza.

Dimostriamo la Proposizione seguente.

Proposizione 2.3. *Se X è un insieme che soddisfa le tre condizioni del Principio di Induzione Strutturale allora* $\mathrm{PROP} \subseteq X$.

Dimostrazione. Supponiamo il contrario, e sia $A \in \mathrm{PROP} - X$ di altezza minima. Allora non può essere $h(A) = 0$, perché tutte le variabili proposizionali sono in X. Dunque $h(A) = n + 1$ per qualche $n \in \mathbf{N}$. Abbiamo due casi.

(Caso 1) Esiste una proposizione B tale che $h(B) = n$ e $A = (\neg B)$. Dato che A è stata scelta come proposizione non contenuta in X di altezza minimale, abbiamo che $B \in X$. Ma allora per ipotesi su X vale anche $(\neg B) \in X$. Contraddizione.

(Caso 2) Esistono due proposizioni B e C tali che $h(B), h(C) \leq n$ tali che $A = (B\square C)$. Ancora per la minimalità di $h(A)$, vale che $B, C \in X$ e per ipotesi su X vale $(A\square C) \in X$. Contraddizione. □

Le definizioni per ricorsione sono definizioni in cui i valori di una funzione su un certo argomento sono espressi come funzione dei valori della stessa funzione su argomenti più piccoli. Esempi elementari sono i seguenti.

$$x^0 = 1, \quad x^{n+1} = x^n \cdot x.$$
$$(x + 0) = x, \quad (x + (n + 1)) = (x + n) + 1.$$
$$(x + 1)! = x!(x + 1).$$

Dimostriamo che si possono definire funzioni per ricorsione sull'insieme delle proposizioni. Sia X un insieme. Si possono definire per ricorsione funzioni di tipo $\mathrm{PROP} \to X$.

Proposizione 2.4 (Principio di Definizione per Ricorsione su Formule)**.** *Sia X un insieme. Siano*

$$f : X \times X \to X,$$
$$g : X \to X,$$
$$h : \mathrm{VAR} \to X.$$

Allora esiste ed è unica una funzione

$$F : \mathrm{PROP} \to X$$

tale che

(1) $F(A) = h(A)$ *se A è una variabile proposizionale,*
(2) $F(\neg A) = g(F(A))$,
(3) $F((A \square B)) = f(F(A), F(B))$.

Dimostrazione. Esercizio! □

Diamo alcuni esempi di definizioni per ricorsione.

Esempio 2.5. Definiamo per ricorsione il rango di una proposizione.

$$r(A) = \begin{cases} 0 & \text{se } A \in \mathrm{VAR} \\ r(B) + 1 & \text{se } A = (\neg B) \\ \max(r(B), r(C)) + 1 & \text{se } A = (B \square C) \end{cases}$$

Si può dimostrare che $r(A) = h(A)$, dove h è l'altezza definita sopra.

Esempio 2.6. Definiamo per ricorsione il numero di parentesi di una proposizione.

$$b(A) = \begin{cases} 0 & \text{se } A \in \mathrm{VAR} \\ b(B) + 2 & \text{se } A = (\neg B) \\ b(B) + b(C) + 2 & \text{se } A = (B \square C) \end{cases}$$

Esempio 2.7. Definiamo per ricorsione una funzione che associa ad una proposizione un albero finito con radice i cui nodi sono etichettati da proposizioni.

- $T(A)$ è l'albero consistente di un solo nodo etichettato con A, se A è una variabile proposizionale.
- $T((\neg A))$ è l'albero consistente di un nodo etichettato con $(\neg A)$ il cui unico figlio è l'albero $T(A)$.
- $T((A \square B))$ è l'albero consistente di un nodo etichettato con $(A \square B)$ il cui figlio sinistro è l'albero $T(A)$ e il cui figlio destro è l'albero $T(B)$.

$T(A)$ è detto il *parsing tree* di A.

3. Semantica della Logica Proposizionale

Definizione 3.1 (Assegnamento)**.** Un assegnamento è una funzione di tipo

$$v : \mathrm{VAR} \to \{1, 0\}.$$

I numeri $1, 0$ vengono detti *valori di verità*, e sono intuitivamente da identificarsi come *Vero* e *Falso*.
Vogliamo estendere un qualunque assegnamento $v : \mathrm{VAR} \to \{1, 0\}$ a una funzione

$$v' : \mathrm{PROP} \to \{0, 1\}.$$

Lo facciamo dando delle regole per calcolare ricorsivamente il valore di v' su una proposizione A come funzione dei valori di v' sulle sottoformule immediate di A. Per alleggerire la notazione, a rischio di ambiguità, usiamo v per indicare la funzione di tipo $\mathrm{PROP} \to \{0, 1\}$ ottenuta estendendo v secondo le regole seguenti.

$$v((\neg A)) = \begin{cases} 1 & \text{se } v(A) = 0 \\ 0 & \text{se } v(A) = 1 \end{cases}$$

$$v((A \vee B)) = \begin{cases} 0 & \text{se } v(A) = v(B) = 0 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \wedge B)) = \begin{cases} 1 & \text{se } v(A) = v(B) = 1 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \to B)) = \begin{cases} 0 & \text{se } v(A) = 1 \text{ e } v(B) = 0 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \leftrightarrow B)) = \begin{cases} 1 & \text{se } v(A) = v(B) \\ 0 & \text{altrimenti.} \end{cases}$$

Osserviamo che è possibile presentare i casi della definizione di v qui sopra in modo compatto usando le cosidette Tavole di verità. Per esempio, possiamo riscrivere la definizione di $v((\neg A))$ in forma tabulare come segue.

A	$\neg A$
1	0
0	1

Analogamente possiamo riscrivere la definizione di $v((A \vee B))$ in forma tabulare come segue.

A	B	$(A \vee B)$
1	1	1
1	0	1
0	1	1
0	0	0

Lo stesso possiamo fare per tutti gli altri casi.

Con la definizione data sopra di $v : \text{PROP} \to \{0, 1\}$ abbiamo identificato una proposizione con una funzione booleana. Una proposizione A contenente n variabili proposizionali si può identificare con una funzione booleana di n argomenti, $A : \{0, 1\}^n \to \{0, 1\}$. Chiamiamo funzioni di questo tipo *funzioni di verità*.

Osservazione 3.2. La definizione del valore di verità di una implicazione $A \to B$ data sopra definisce la cosidetta *implicazione materiale*. Secondo questa definizione una implicazione $A \to B$ è vera nei tre casi seguenti.

(1) A e B sono vere,
(2) A è falsa e B è vera,
(3) A è falsa e B è falsa.

La scelta della definizione di $v(A \to B)$ in funzione di $v(A)$ e $v(B)$, e in particolare i punti (2) e (3), possono giustificarsi come segue.

Nel nostro sistema vogliamo che la proposizione $(A \wedge B) \to B$ sia sempre vera, qualunque siano A e B. Vediamo come questa richiesta impone un vincolo alla definizione di $v(A \to B)$.

A	B	$A \wedge B$	$(A \wedge B) \to B$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

Se vogliamo riempire la tavola di verità di $X \to Y$, siamo vincolati dalla tavola precedente alla scelta seguente, leggendo X come $(A \wedge B)$ e Y come B.

X	Y	$X \to Y$
1	1	1
1	0	0
0	1	1
0	0	1

Un'altra giustificazione (parziale) della scelta della definizione della tavola di verità di $\to$ è che vogliamo che valga l'implicazione seguente, che formalizza il ragionamento per contrapposizione:

$$(A \to B) \to (\neg B \to \neg A).$$

Se A e B sono vere la premessa è vera e il conseguente è di tipo $0 \to 0$.

4. Tavole di verità

La possibilità di organizzare in una tabella i valori di verità di una proposizione composta come funzione dei valori di verità delle sue componenti sopra accennato può essere generalizzato a proposizioni qualunque.

Data una proposizione A che contiene le variabili proposizionali $p_1, \ldots, p_n$ distinte e le sottoformule $B_1, \ldots, B_k$, possiamo organizzare la Tavola di verità di A come segue. Nelle prime n colonne scriviamo tutti i possibili valori assunti dalle variabili proposizionali $p_1, \ldots, p_n$. Nelle restanti colonne scriviamo i valori assunti dalle sottoformule di A in ordine crescente di complessità (misurata in termini di rango).

Esempio Sia $A = ((P \vee Q) \to (R \vee (R \to Q)))$.

P	Q	R	$(R \to Q)$	$(R \vee (R \to Q))$	$(P \vee Q)$	A
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	0	1	1	1
1	0	0	1	1	1	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	0	1	0	1
0	0	0	1	1	0	1

Esempio Sia $A = ((\neg P) \wedge Q) \to R)$.

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

Possiamo costruire (meccanicamente) la tavola di verità di una qualunque proposizione A. Se la proposizione contiene n variabili proposizionali, la sua tavola di verità ha 2^n righe. Ogni assegnamento di valori di verità alle variabili proposizionali di A corrisponde ad una riga della tavola di verità di A, e viceversa.

5. soddisfacibilità, conseguenza logica, valitdità logica

Definizione 5.1 (Proposizione Soddisfacibile)**.** Un assegnamento v soddisfa una proposizione A se $v(A) = 1$. Si dice anche che v è un modello di A. A è soddisfacibile se esiste un assegnamento che la soddisfa. Altrimenti A è insoddisfacibile. Indichiamo con Sat l'insieme delle proposizioni soddisfacibili (*satisfiable*) e con UnSat l'insieme delle proposizioni insoddisfacibili.

Definizione 5.2 (Conseguenza Logica)**.** Siano $\mathcal{F} = \{A_1, \ldots, A_n\}$ un insieme di proposizioni e sia A una proposizione. Diciamo che A è conseguenza logica di $\mathcal{F}$ se ogni assegnamento che soddisfa tutti gli elementi di $\mathcal{F}$ soddisfa anche A. Scriviamo in tal caso $A_1, \ldots, A_n \models A$ e diciamo che le premesse $A_1, \ldots, A_n$ implicano logicamente la conclusione A.

Se $\mathcal{F}$ è l'insieme vuoto scriviamo $\models A$ per $\varnothing \models A$. In questo caso la definizione, letta correttamente, dice che A è soddisfatta da tutti gli assegnamenti, i.e., che per ogni assegnamento v, $v(A) = 1$. Infatti per qualunque v è vero a vuoto che v soddisfa tutti gli elementi dell'insieme $\varnothing$.

Definizione 5.3 (Equivalenza Logica)**.** Diciamo che A e B sono logicamente equivalenti se per ogni assegnamento v, $v(A) = v(B)$. In questo caso scriviamo $A \equiv B$.

Definizione 5.4 (Tautologia, verità Logica)**.** Una proposizione A è una verità logica se per ogni assegnamento v, $v(A) = 1$. Si dice anche che A è valida, o è una tautologia. Indichiamo con TAUT l'insieme delle tautologie.

Si osserva che A è una tautologia se e solo se $\models A$. Anche, $A \equiv B$ se e solo se $\models (A \leftrightarrow B)$.
Si osserva che $A \in$ SAT è un concetto *esistenziale*:

$$A \in \text{SAT} \Leftrightarrow \exists v(v(A) = 1),$$

mentre $A \in$ TAUT è un concetto *universale*:

$$A \in \text{TAUT} \Leftrightarrow \forall v(v(A) = 1),$$

Esiste la seguente dualità tra TAUT e UNSAT:

$$A \in \text{TAUT} \Leftrightarrow \neg A \in \text{UNSAT}.$$

D'altra parte è ovvio che esistono proposizioni tali che sia $A \in$ SAT che $\neg A \in$ SAT.

Vale inoltre il seguente Teorema, che riduce il problema della conseguenza logica (valitdità di un argomento) a quello della verità logica e della soddisfacibilità.

Teorema 5.5. *Siano $A_1, \ldots, A_n, A$ proposizioni. Allora i seguenti punti sono equivalenti.*
(1) $A_1, \ldots, A_n \models A$.
(2) $((A_1 \wedge \cdots \wedge A_n) \rightarrow A) \in$ TAUT.
(3) $(A_1 \wedge \cdots \wedge A_n \wedge \neg A) \in$ UNSAT.

Dimostrazione. Esercizio! □

Osservazione 5.6. Il metodo delle tavole di verità permette di calcolare i valori di verità di una funzione arbitrariamente complessa. Data una proposizione A qualunque, possiamo rispondere algoritmicamente alla domanda: $A \in$ TAUT? Basta costruire la tavola di verità di A e controllare se l'ultima colonna contiene solo il valore 1. La tavola di verità di una proposizione in cui appaiono n variabili proposizionali contiene 2^n righe. Per questo motivo il metodo delle tavole di verità è *computazionalmente inefficiente*. Lo stesso vale per la domanda: $A \in$ SAT? Anche in questo caso le tavole di verità danno una risposta, ma in modo inefficiente.

Non si conoscono però algoritmi efficienti (polinomiali) per rispondere a questa domanda. Trovare un tale algoritmo o dimostrare che un tale algoritmo non esiste equivale a risolvere il Problema del Millennio ($\mathbf{P} = \mathbf{NP}$)? (i.e., la classe dei problemi risolvibili in tempo polinomiale da un algoritmo deterministico coincide con la classe dei problemi risolvibili in tempo polinomiale da un algoritmo non-deterministico?). Per questo problema il *Clay Mathematical Institute* offre un premio di un milione di dollari.

In molti casi è possibile decidere se una certa proposizione è in TAUT o no, oppure se una certa conclusione è conseguenza logica di certe altre proposizioni senza costruire la tavola di verità, ma ragionando in modo rigoroso a un più alto livello. Nel seguito vediamo alcuni risultati che permettono di manipolare proposizioni in modo algebrico, preservando la relazione di equivalenza logica.

6. Teoremi di Sostituzione

Vogliamo dimostrare che valgono le seguenti proprietà (intuitivamente corrette).

(1) Se A è una tautologia, se sostituisco in A una variabile proposizionale con una formula qualunque, ottengo ancora una tautologia.
(2) Se A e B sono equivalenti, e sostituisco sia in A che in B una stessa variabile proposizionale con una stessa formula qualunque, ottengo due formule equivalenti.

(3) Se sostituisco in una stessa formula A una variabile proposizionale con due formule equivalenti, ottengo due formule equivalenti.

Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Denotiamo con $A[p_1/B_1 \ldots p_n/B_n]$ il risultato di sostituire simultaneamente nella proposizione A la variabile proposizionale p_i con la formula B_i, per ogni $i \in \{1, \ldots, n\}$. Nota bene: la sostituzione è un'operazione puramente sintattica che trasforma proposizioni in proposizioni, e la sostituzione deve essere simultanea, non sequenziale! La proposizione $A[p_1/B_1 \ldots p_n/B_n]$ può essere definita rigorosamente per ricorsione (Esercizio!).

Otteniamo (1) e (2) come conseguenze del seguente teorema.

Teorema 6.1. *Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Abbreviamo $A[p_1/B_1 \ldots p_n/B_n]$ con A^*. Sia v un assegnamento. Definiamo un nuovo assegnamento $v^* : \mathrm{VAR} \to \{0,1\}$ (in funzione di v, p_i, B_i) come segue.*

$$v^*(Q) = \begin{cases} v(Q) & \text{se } Q \neq P_i \text{ per ogni } i \in \{1, \ldots, n\} \\ v(B_i) & \text{se } Q = P_i \text{ per qualche } i \in \{1, \ldots, n\}. \end{cases}$$

Allora

$$v(A^*) = v^*(A).$$

Dimostrazione. Per induzione strutturale su A.

(Caso Base) A è una variabile proposizionale Q. Distinguiamo due casi.

Se Q è p_i per un $i \in \{1, \ldots, n\}$, allora

$$A^* = Q[p_1/B_1 \ldots p_n/B_n] = p_i[p_1/B_1 \ldots p_n/B_n] = B_i.$$

Dunque

$$v(A^*) = v(B_i) = v^*(p_i) = v^*(A).$$

Se Q è diversa da p_i per ogni $i \in \{1, \ldots, n\}$, allora

$$A^* = Q[p_1/B_1 \ldots p_n/B_n] = Q.$$

Dunque

$$v(A^*) = v(Q) = v^*(Q) = v^*(A).$$

(Caso induttivo 1) Sia A la formula $(\neg C)$.

$$A^* = (\neg C)^* = (\neg C)[p_1/B_1 \ldots p_n/B_n] = (\neg C[p_1/B_1 \ldots p_n/B_n]) = (\neg C^*).$$

Allora

$$v(A^*) = v(\neg C^*) = \begin{cases} 1 & \text{se } v(C^*) = 0 \\ 0 & \text{se } v(C^*) = 1 \end{cases}$$

D'altra parte,

$$v^*(A) = v^*(\neg C) = \begin{cases} 1 & \text{se } v^*(C) = 0 \\ 0 & \text{se } v^*(C) = 1 \end{cases}$$

Per ipotesi induttiva $v^*(C) = v(C^*)$. Dunque $v(A^*) = v^*(A)$.

(Caso induttivo 2) Sia A la formula $(C \wedge D)$.

$$A^* = (C \wedge D)^* = (C[p_1/B_1 \ldots p_n/B_n] \wedge D[p_1/B_1 \ldots p_n/B_n]) = (C^* \wedge D^*).$$

$$v(A^*) = v(C^* \wedge D^*) = \begin{cases} 1 & \text{se } v(C^*) = v(D^*) = 1 \\ 0 & \text{altrimenti} \end{cases}$$

D'altra parte

$$v^*(A) = v^*(C \wedge D) = \begin{cases} 1 & \text{se } v^*(C) = v^*(D) = 1 \\ 0 & \text{altrimenti} \end{cases}$$

Per ipotesi induttiva $v(C^*) = v^*(C)$ e $v(D^*) = v^*(D)$.

I casi degli altri connettivi si trattano analogamente. □

Corollario 6.2 (Sostituzione in tautologie)**.** *Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Se A è una tautologia allora $A[p_1/B_1 \ldots p_n/B_n]$ è una tautologia.*

Dimostrazione. Segue facilmente dal teorema precedente. Esercizio! □

Corollario 6.3 (Sostituzione in formule equivalenti)**.** *Siano $C, D, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Se $\models (C \leftrightarrow D)$ allora*

$$\models (C[p_1/B_1 \ldots p_n/B_n]) \leftrightarrow (D[p_1/B_1 \ldots p_n/B_n]).$$

Dimostrazione. Segue facilmente dal teorema precedente. Esercizio! □

Dimostriamo ora un risultato duale del precedente: l'equivalenza logica è preservata sostituendo all'interno di una formula variabili proposizionali con formule logicamente equivalenti.

Lemma 6.4. *$\models (A \to B)$ se e solo se $v(A) \leq v(B)$, per ogni assegnamento v.*

Dimostrazione. Esercizio! □

Teorema 6.5. *Siano A, B_1, B_2 proposizioni e sia p una variabile proposizionale. Allora*

$$v(B_1 \leftrightarrow B_2) \leq v(A[p/B_1] \leftrightarrow A[p/B_2]).$$

Osserviamo che dal Teorema, usando il Lemma precedente, segue il risultato desiderato, ossia

$$\models (B_1 \leftrightarrow B_2) \to (A[p/B_1] \leftrightarrow A[p/B_2]).$$

Dimostriamo ora il Teorema.

Dimostrazione. Il caso $v(B_1 \leftrightarrow B_2) = 0$ è facile: ovviamente $0 \leq v(A[p/B_1] \leftrightarrow A[p/B_2])$. Consideriamo il caso $v(B_1 \leftrightarrow B_2) = 1$. Procediamo per induzione su A.

(Caso Base) A è una variabile proposizionale. Distinguiamo due sottocasi.

Se A è p, allora

$$A[p/B_1] = p[p/B_1] = B_1$$

e

$$A[p/B_2] = p[p/B_2] = B_2.$$

La tesi è allora che $v(B_1 \leftrightarrow B_2) = 1$, che è vera per ipotesi.

Se A non è p, allora

$$A[p/B_1] = A$$

e

$$A[p/B_1] = A$$

La tesi è allora che $v(A \leftrightarrow A) = 1$, che è ovviamente vero.

(Caso Induttivo 1) Sia A la proposizione $(\neg C)$. Allora

$$A[p/B_1] = (\neg C[p/B_1]),$$

e

$$A[p/B_2] = (\neg C[p/B_2]).$$

Per ipotesi induttiva su C vale che $v(C[p/B_1] \leftrightarrow C[p/B_2]) = 1$. Questo vale se e solo se

$$v(C[p/B_1]) = v(C[p/B_2]).$$

Allora

$$v(A[p/B_1]) = v((\neg C[p/B_1]) = v(\neg C[p/B_2]) = v(A[p/B_2]),$$

perché il valore $v(\neg X)$ dipende soltanto dal valore di verità $v(X)$.

(Caso Induttivo 2) Trattiamo uniformemente il caso dei connettivi binari. Sia A la proposizione $(C \square D)$. Allora

$$A[p/B_1] = (C[p/B_1] \square D[p/B_1]),$$

e

$$A[p/B_2] = (C[p/B_2] \square D[p/B_2]).$$

Per ipotesi induttiva su C vale che $v(C[p/B_1] \leftrightarrow C[p/B_2]) = 1$. Questo vale se e solo se

$$v(C[p/B_1]) = v(C[p/B_2]).$$

Per ipotesi induttiva su D vale che $v(D[p/B_1] \leftrightarrow D[p/B_2]) = 1$. Questo vale se e solo se

$$v(D[p/B_1]) = v(D[p/B_2]).$$

Ma allora

$$v(A[p/B_1]) = v((C[p/B_1] \square D[p/B_1]) = v(C[p/B_2] \square D[p/B_2]) = v(A[p/B_2]),$$

perché $(x, y) \mapsto v(x \square y)$ è una funzione dei valori di verità $v(x)$ e $v(y)$. □

7. Principi generali e verità notevoli

Enunciamo alcune proprietà fondamentali della conseguenza logica e alcune leggi logiche notevoli. Tutte le dimostrazioni sono lasciate per Esercizio.

7.1. **proprietà della conseguenza logica.** La relazione $\models$ di conseguenza logica gode delle seguenti proprietà

(1) $A \models A$
(2) Se $A \models B$ e $B \models C$ allora $A \models C$
(3) $A \models B$ se e solo se $\models (A \to B)$.

La relazione di equivalenza logica (definita come $A \equiv B$ se e solo se $\models (A \leftrightarrow B)$) è invece una relazione di equivalenza sull'insieme delle proposizioni.

(1) $A \equiv A$
(2) Se $A \equiv B$ e $B \equiv C$ allora $A \equiv C$
(3) Se $A \equiv B$ allora $B \equiv A$.

7.2. **Leggi Algebriche.**

(1) associatività
  (a) $(A \vee (B \vee C)) \equiv A \vee (B \vee C)$
  (b) $(A \wedge (B \wedge C)) \equiv A \wedge (B \wedge C)$
(2) Commutatività
  (a) $(A \vee B) \equiv (B \vee A)$
  (b) $(A \wedge B) \equiv (B \wedge A)$
(3) distributività
  (a) $(A \vee (B \wedge C)) \equiv (A \vee B) \wedge (A \vee C)$
  (b) $(A \wedge (B \vee C)) \equiv (A \wedge B) \vee (A \wedge C)$
(4) Leggi di De Morgan
  (a) $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$
  (b) $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$
(5) Doppia Negazione $\neg\neg A \equiv A$
(6) Idempotenza
  (a) $(A \vee A) \equiv A$
  (b) $(A \wedge A) \equiv A$

7.3. **Interdefinibilità dei connettivi.** Questo gruppo di leggi logiche notevoli illustra la possibilità di definire alcuni connettivi in funzione di altri.

(1) $(A \leftrightarrow B) \equiv ((A \to B) \wedge (B \to A))$
(2) $(A \to B) \equiv (\neg A \vee B)$
(3) $(A \vee B) \equiv (\neg A \to B)$
(4) $(A \vee B) \equiv \neg(\neg A \wedge \neg B)$
(5) $(A \wedge B) \equiv \neg(\neg A \vee \neg B)$

Possiamo dimostrare l'equivalenza logica di due formule usando le verità notevoli qui sopra *e i teoremi di sostituzione*, scrivendo una serie di equazioni logiche.

Esempio Dimostriamo che $\models (A \to (B \to C)) \leftrightarrow ((A \wedge B) \to C)$.

$$\begin{aligned} A \to (B \to C) &\equiv \neg A \vee (B \to C) \\ &\equiv \neg A \vee (\neg B \vee C) \\ &\equiv (\neg A \vee \neg B) \vee C \\ &\equiv \neg(A \wedge B) \vee C \\ &\equiv (A \wedge B) \to C \end{aligned}$$

Esempio Dimostriamo che $\models (A \to B) \leftrightarrow (\neg B \to \neg A)$.

$$\begin{aligned} \neg B \to \neg A &\equiv \neg\neg B \vee \neg A \\ &\equiv B \vee \neg A \\ &\equiv \neg A \vee B \\ &\equiv A \to B \end{aligned}$$

7.4. **Altre leggi algebriche.** Se conveniamo di usare — all'interno di proposizioni — la costante 1 al posto di una qualunque tautologia e la costante 0 al posto di una qualunque formula insoddisfacibile, allora possiamo formulare le seguenti leggi algebriche aggiuntive.

(1) Assorbimento
   (a) $(A \vee 0) \equiv A$
   (b) $(A \wedge 1) \equiv A$
(2) Contraddizione, Terzo Escluso
   (a) $(A \vee \neg A) \equiv 1$
   (b) $(A \wedge \neg A) \equiv 0$

8. Principio di dualità tra $\wedge$ e $\vee$

Se osserviamo le leggi logiche notevoli osserviamo una dualità tra $\vee$ e $\wedge$. In questo paragrafo dimostriamo rigorosamente che vale il seguente.

> **Principio di dualità** Ogni enunciato corretto che riguarda i connettivi $\wedge$, $\vee$, e le costanti 0 e 1 si traduce in un enunciato duale corretto invertendo $\wedge$ con $\vee$, 0 con 1.

Naturalmente l'applicazione corretta del Principio prevede che le nozioni che riguardano la verità siano sostituite con le loro duali, per esempio "tautologia" con "insoddisfacibile", etc. così, per esempio, il duale di "$A \vee \neg A \in$ Taut" è "$A \wedge \neg A \in$ UnSat", e il duale di "Se $A \vee B \notin$ Taut allora $A \notin$ Taut" è "Se $A \wedge B \notin$ UnSat allora $A \notin$ UnSat".

Per dirla con Martin Davis,

> Un essere di un altro pianeta che ci osservasse fare logica proposizionale sarebbe in grado di capire che stiamo facendo logica proposizionale. Ma questo essere non avrebbe modo di capire quale valore di verità stiamo rappresentando con 0 e quale con 1, e di conseguenza non sarebbe in grado di dire quale dei due connettivi rappresenti "e" e quale "o".

Dimostriamo il Principio di dualità definendo una mappa d da proposizioni in proposizioni che scambia $\wedge$ con $\vee$ e dimostrando che la mappa preserva l'equivalenza logica. Facciamo un passo intermedio definendo una mappa $*$ da proposizioni in proposizioni che scambia $\wedge$ con $\vee$ e ogni variabile proposizionale con la sua negazione.

Definizione 8.1. Definiamo una mappa * da proposizioni in proposizioni.

$$A^* = \neg A \text{ se } A \text{ è una variabile.}$$

$$(B \wedge C)^* = (B^* \vee C^*)$$

$$(B \vee C)^* = (B^* \wedge C^*)$$

$$(\neg B)^* = \neg B^*$$

Lemma 8.2. *Per ogni assegnamento v,*

$$v(A^*) = v(\neg A).$$

Dimostrazione. Esercizio (induzione). □

Definizione 8.3. Definiamo una mappa ^{d} da proposizioni in proposizioni.

$$A^d = A \text{ se } A \text{ è una variabile.}$$

$$(B \wedge C)^d = (B^d \vee C^d)$$

$$(B \vee C)^d = (B^d \wedge C^d)$$

$$(\neg B)^d = \neg B^d$$

Teorema 8.4. *$A \equiv B$ se e solo se $A^d \equiv B^d$.*

Dimostrazione. Supponiamo $A \equiv B$ e dimostriamo $A^d \equiv B^d$. Osserviamo che

$$A^* = A^d[p_1/\neg p_1, \ldots, p_n/\neg p_n].$$

Allora

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] = A^d[p_1/\neg\neg p_1, \ldots, p_n/\neg\neg p_n].$$

Dato che $\neg\neg p_i \equiv p_i$, abbiamo che

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv A^d,$$

per il Teorema di Sostituzione di equivalenti. Con lo stesso ragionamento, per B, abbiamo che

$$B^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^d,$$

Dal Lemma precedente abbiamo che

$$\neg A \equiv A^*$$

e

$$\neg B \equiv B^*$$

Da $A \equiv B$ (ipotesi) segue $\neg A \equiv \neg B$ e dunque $A^* \equiv B^*$, e dunque anche

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^d,$$

per il Teorema di Sostituzione in equivalenti. Per quanto visto sopra, segue

$$A^d \equiv B^d.$$

L'altra direzione dell'implicazione (se $A^d \equiv B^d$ allora $A \equiv B$) è lasciata per Esercizio. □

9. Espressività della Logica Proposizionale

Vogliamo usare la Logica Proposizionale per giudicare in modo rigoroso (e per quanto possibile automatizzabile) della valitdità di argomenti e della verità di proposizioni. Ma che tipo di argomenti e che tipo di proposizioni possiamo formalizzare nel linguaggio proposizionale?

Diamo tre esempi per farci un'idea.

Esempio 9.1. Semplici argomenti matematici che non riguardano i quantificatori.

(1) Se $a = 0$ o $b = 0$ allora $a \cdot b = 0$.
(2) $a \cdot b \neq 0$.
(3) $a \neq 0$ e $b \neq 0$.

Intuitivamente la terza proposizione è la conclusione di un argomento che ha come premesse le prime due. Come si formalizza? Per prima cosa si individuano le parti atomiche, ossia quelle parti che non possono essere ulteriormente analizzate in termini di connettivi logici booleani e che possono essere vere o false. Nel nostro caso, queste parti atomiche sono $a = 0$, $b = 0$, e $a \cdot b = 0$. Associamo a ciascuna parte atomica una distinta variabile proposizionale: a $a = 0$ associamo p_1, a $b = 0$ associamo p_2, a $a \cdot b = 0$ associamo p_3. Infine sostituiamo i costrutti logici del linguaggio naturale (Se...allora, o, e, non) con i connettivi formali. Otteniamo la seguente formalizzazione.

(i) $(p_1 \vee p_2) \to p_3$.
(ii) $(\neg p_3)$.
(iii) $(\neg p_1 \wedge \neg p_2)$.

La nozione di conseguenza logica dà un criterio rigoroso per giudicare la valitdità dell'argomento che ha per premesse $(p_1 \vee p_2) \to p_3$ e $(\neg p_3)$ e per conclusione $(\neg p_1 \vee \neg p_2)$. In altre parole possiamo rispondere alla domanda: la conclusione segue logicamente dalle premesse? Osserviamo che la valitdità dell'argomento non dipende più dal significato matematico delle parti atomiche ma solo dal loro essere vere o false (dal loro *valore di verità*). Se l'argomento formalizzato è valido, allora sono validi tutti gli argomenti ottenuti sostituendo proposizioni alle variabili proposizionali. Per esempio, se l'argomento di sopra è valido, allora è valido anche il seguente.

(a) Se il padre è alto o la madre è alta allora il figlio è alto.
(b) Il figlio è basso.
(c) Il padre è basso e la madre è bassa.

Ovviamente la prima premessa (a) è empiricamente falsa, mentre la prima premessa (1) è matematicamente vera. Quando diciamo che l'argomento è valido intendiamo dire che *se* le premesse sono vere, allora è vera la conclusione. Ma non diciamo che le premesse sono vere.

La validità degli argomenti di sopra può essere – per il momento – verificata in tre modi:

(1) Verificando se vale $(p_1 \vee p_2) \to p_3, (\neg p_3) \models (\neg p_1 \vee \neg p_2)$, secondo la definizione di $\models$.
(2) Verificando se la formula $(((p_1 \vee p_2) \to p_3) \wedge (\neg p_3)) \to (\neg p_1 \vee \neg p_2)$ è in Taut (usando la tavola di verità).
(3) Verificando se la formula $(((p_1 \vee p_2) \to p_3) \wedge (\neg p_3)) \wedge \neg(\neg p_1 \vee \neg p_2)$ è in UnSat (usando la tavola di verità).

Esempio 9.2. Semplici argomenti verbali. La logica proposizionale si presta bene anche a a formalizzare argomenti verbali.

(1) Se studi e sei intelligente allora superi l'esame.
(2) Se sei intelligente allora studi.
(3) Non superi l'esame.
(4) Sei scemo.

Come si formalizza? Le parti atomiche in questo caso sono (studi), (sei intelligente), (superi l'esame). Possiamo infatti assumere che (sei scemo) equivalga a (non sei intelligente). Associamo p_1 a (studi), p_2 a (sei intelligente), p_3 a (superi l'esame). L'argomento si formalizza così.

(i) $(p_1 \wedge p_2) \to p_3$.
(ii) $p_2 \to p_1$.
(iii) $\neg p_3$.

(iv) $\neg p_2$.

Esempio 9.3. Consideriamo il problema: si può colorare la mappa in figura usando due colori (Rosso e Blu) rispettando il vincolo che due stati adiacenti hanno colori diversi?

Per iniziare, consideriamo il sottoproblema relativo a Italia, Austria e Ungheria. Dichiariamo il seguente linguaggio proposizionale: le variabili proposizionali sono $I_R, I_B, A_R, A_B, U_R, U_B$ e il loro significato intuitivo è I_R = l'Italia è rossa, I_B = l'Italia è blu, etc.

Per esprimere il vincolo che ogni nazione riceve almeno un colore scriviamo:

$$(I_R \vee I_B) \wedge (A_R \vee A_B) \wedge (U_R \vee U_B)$$

Per esprimere il vincolo che ogni nazione riceve al più un colore scriviamo:

$$(I_R \to \neg I_B) \wedge (A_R \to \neg A_B) \wedge (U_R \to \neg U_B).$$

Per esprimere il vincolo che nazioni confinanti hanno colori diversi, scriviamo:

$$(I_R \to \neg A_R) \wedge (I_B \to \neg A_B) \wedge (A_R \to \neg U_R) \wedge (A_B \to \neg U_B).$$

Osserviamo che questa proposizione dipende dall'istanza del problema in questione ossia dai confini presenti nella mappa.

Intuitivamente l'insieme di proposizioni sopra descritte formalizza adeguatamente il problema della 2-colorazione. Tecnicamente questo significa che l'insieme delle proposizioni scritte sopra è in SAT se e soltanto se la mappa di Italia, Austria e Ungheria è 2-colorabile (rispettando il vincolo).

Supponiamo infatti che sia 2-colorabile. Allora esiste un assegnamento di colori Rosso, Blu a Italia, Austria e Ungheria che rispetta il vincolo. Se questa colorazione è Italia Rossa, Austria Blu, Ungheria Rossa, definiamo l'assegnamento proposizionale $v(I_R) = 1$, $v(I_B) = 0$, $v(A_R) = 0$, $v(A_B) = 1$, $v(U_R) = 1$, $v(U_B) = 0$. Si verifica facilmente che questo assegnamento soddisfa tutte le proposizioni usate per formalizzare il problema.

Viceversa, dato un assegnamento v che mette a 1 tutte le proposizioni usate per la formalizzazione del problema, posso estrarre una colorazione: se $v(I_R) = 1$ allora coloro l'Italia di Rosso, se $v(A_B) = 1$ coloro l'Austria di Blu, e così via. Dato che l'assegnamento soddisfa, per es., la formula $I_R \to \neg I_B$, non assegnerò due colori distinti all'Italia. Si verifica facilmente che il fatto che v soddisfa tutte le formule in questione implica che la colorazione ottenuta soddisfai vincoli per essere una soluzione corretta al problema della 2-colorazione.

Esempio 9.4. Consideriamo ancora il problema della 2-colorazione per Slovenia, Austria e Ungheria. Analogamente a quanto fatto sopra usiamo un vocabolario proposizionale composto dalle variabili $A_R, A_B, S_R, S_B, U_R, U_B$ e formalizziamo con le seguenti proposizioni:

$$(S_R \vee S_B) \wedge (A_R \vee A_B) \wedge (U_R \vee U_B).$$

$$(S_R \rightarrow \neg S_B) \wedge (A_R \rightarrow \neg A_B) \wedge (U_R \rightarrow \neg U_B).$$

$$(S_R \rightarrow \neg A_R) \wedge (S_B \rightarrow \neg A_B) \wedge (S_R \rightarrow \neg U_R) \wedge (S_B \rightarrow \neg U_B) \wedge (A_R \rightarrow \neg U_R) \wedge (A_B \rightarrow \neg U_B)$$

Si verifica che l'insieme delle proposizioni qui sopra (o equivalentemente la loro congiunzione) è insoddisfacibile. Invece di usare una tavola di verità si può ragionare, per es. così: Supponiamo che v soddisfi tutte le proposizioni di sopra. Supponiamo che $v(S_R) = 1$. Allora $v(\neg A_R) = 1$ e dunque $v(A_B) = 1$. Ma allora $v(\neg U_B) = 1$ e dunque $v(U_R) = 1$. Ma allora $v(S_R \rightarrow \neg U_R) = 0$. Contraddizione.

La formalizzazione è adeguata perché, come nell'esempio precedente, l'insieme di formule è soddisfacibile se e solo se esiste una soluzione al problema della 2-colorazione della mappa.

Esempio 9.5. Principi combinatori su domini finiti. Questo esempio illustra come formalizzare in logica proposizionale principi matematici in cui appaiono quantificatori (per ogni, esiste) ma solo su un numero finito di oggetti. Consideriamo il famoso Principio dei Cassetti (o dei Piccioni, *Pigeonhole Principle*.

> **Principio dei Cassetti**. Per ogni $n \in \mathbf{N}$, $n \geq 1$, se ho messo $n + 1$ oggetti in n cassetti allora un cassetto contiene più di un oggetto.

Indichiamo questo principio, per ogni $n \geq 1$ fissato, con $PHP(n + 1, n)$. Ovviamente un analogo principio vale se usiamo un qualunque $m \geq n + 1$ al posto di $n + 1$. In termini più matematici, $PHP(n + 1, n)$ si può esprimere come segue.

> **PHP**$(\mathbf{n + 1, n})$. Se f è una funzione suriettiva con dominio $\{1, \ldots, n + 1\}$ e codominio $\{1, \ldots, n\}$, allora esiste un elemento del codominio che ha almeno due preimmagini secondo f.

In altre parole, non esiste una funzione iniettiva e suriettiva con dominio $\{1, \ldots, n+1\}$ e codominio $\{1, \ldots, n\}$. Per ogni scelta di n, facciamo vedere come formalizzare $PHP(n + 1, n)$ nel linguaggio proposizionale.

Fissiamo per semplicità $n = 3$. Vogliamo formalizzare $PHP(4, 3)$, che dice che se f è una funzione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$ allora un elemento del dominio ha almeno due preimmagini secondo f. Spezziamo questo enunciato in tre parti.

(1) f è una associazione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$.
(2) f è una funzione con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$.
(3) f non è iniettiva.

Dobbiamo formalizzare: **Se** f è una funzione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$ **allora** f non è iniettiva. Ossia **Se** ((1) e (2)) allora (3).

Un linguaggio adeguato per formalizzare $PHP(4, 3)$ è il linguaggio che ha come variabili proposizionali i simboli $p_{i,j}$, dove i varia in $\{1, 2, 3, 4\}$ e j varia in $\{1, 2, 3\}$. Dunque le variabili del linguaggio sono 12 in tutto. (N.B.B. I simboli $p_{i,j}$ non fanno parte del linguaggio!! Sono solo un modo comodo per quantificare su $\{1, 2, 3, 4\}$ e $\{1, 2, 3\}$. Le vere variabili sono simboli del tipo $p_{1,1}$, $p_{4,2}$, $p_{4,3}$ etc.). Il significato *intuitivo* delle variabili scelte è il seguente.

$$p_{i,j} \text{ sta per } f(i) = j.$$

Cominciamo a formalizzare (1). f è suriettiva se e solo se ogni elemento del codominio ha una preimmagine nel dominio, i.e., se e solo

$$\forall j \in \{1, 2, 3\} \exists i \in \{1, 2, 3, 4\} (f(i) = j).$$

Anche se stiamo usando delle quantificazioni possiamo formalizzare l'enunciato in logica proposizionale perché stiamo quantificando su insiemi finiti. Possiamo quindi enumerare tutte le possibilità, e usare $\vee$ per tradurre $\exists$ e $\wedge$ per tradurre $\forall$.

Per $j = 1$, dobbiamo tradurre

$$\exists i \in \{1, 2, 3, 4\} (f(i) = 1).$$

$f(i) = 1$ si traduce ovviamente con $p_{i,1}$. La quantificazione esistenziale sull'insieme $\{1, 2, 3, 4\}$ si traduce con una disgiunzione a quattro termini:

$$p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}.$$

Per $j = 2$, dobbiamo tradurre

$$\exists i \in \{1, 2, 3, 4\}(f(i) = 2).$$

Analogamente a quanto visto sopra otteniamo

$$p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}.$$

Per $j = 3$ otteniamo in modo analogo

$$p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}.$$

Dobbiamo ora mettere insieme le tre proposizioni ottenute in modo da esprimere la quantificazione universale $\forall j \in \{1, 2, 3\} \dots$. Basta usare la congiunzione, perché la quantificazione universale in questione sta dicendo che

$$\text{Se } j = 1 \text{ allora } \exists i \in \{1, 2, 3, 4\}(f(i) = 1),$$

e

$$\text{Se } j = 2 \text{ allora } \exists i \in \{1, 2, 3, 4\}(f(i) = 2),$$

e

$$\text{Se } j = 3 \text{ allora } \exists i \in \{1, 2, 3, 4\}(f(i) = 3).$$

Otteniamo quindi la proposizione

$$(p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}) \wedge (p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}) \wedge (p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}).$$

come formalizzazione di (f è una associazione suriettiva da $\{1, 2, 3, 4\}$ su $\{1, 2, 3\}$).

Ora formalizziamo (2). f è una funzione (e non una semplice relazione) se e solo se non esiste un elemento del dominio che ha due immagini distinte. In altre parole, per ogni elemento i del dominio, per ogni scelta di due immagini distinte j, j' nel codominio, dobbiamo dire che non è possibile che $f(i) = j$ e $f(i) = j'$. In altre parole dobbiamo formalizzare la seguente proposizione.

$$\forall i \in \{1, 2, 3, 4\} \forall j \neq j' \in \{1, 2, 3\}(f(i) \neq j \vee f(i) \neq j').$$

Come sopra, consideriamo i possibili valori di i uno per uno.

Per $i = 1$ dobbiamo formalizzare

$$\forall j \neq j' \in \{1, 2, 3\}(f(1) \neq j \vee f(1) \neq j').$$

Per ogni scelta di $j, j' \in \{1, 2, 3\}$ con $j \neq j'$ dobbiamo formalizzare

$$(f(1) \neq j \vee f(1) \neq j').$$

Per questo basta scrivere $\neg(p_{1,j} \wedge p_{1,j'})$. Dato che la quantificazione è universale, dobbiamo congiungere tutte le proposizioni così ottenute. Otteniamo

$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}).$$

Per $i = 2$ dobbiamo formalizzare

$$\forall j \neq j' \in \{1, 2, 3\}(f(2) \neq j \vee f(2) \neq j').$$

Analogamente a sopra ottenitamo

$$\neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}).$$

Per $i = 3$ con lo stesso ragionamento otteniamo

$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}).$$

Per $i = 4$ con lo stesso ragionamento otteniamo

$$\neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3}).$$

Ora possiamo esprimere la quantificazione su i, $\forall i \in \{1, 2, 3, 4\} \dots$ congiungendo le quattro proposizioni ottenute per i singoli valori di i.

$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}) \wedge \neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}) \wedge$$

$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}) \wedge \neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3}).$$

Ora formalizziamo (3). f non è iniettiva se e solo se non esiste un elemento del codominio con due preimmagini distinte secondo f. In altre parole, f non è iniettiva se e solo se per ogni elemento j del codominio, per ogni scelta di due preimmagini distinte i, i' nel dominio, non è vero che $f(i) = j$ e $f(i') = j$. Dobbiamo quindi formalizzare l'enunciato seguente.

$$(\forall j \in \{1,2,3\} \forall i \neq i' \in \{1,2,3,4\} (f(i) \neq j \vee f(i') \neq j).$$

Procediamo come sopra. Consideriamo uno per uno i valori di j.

Per $j = 1$, dobbiamo formalizzare

$$\forall i \neq i' \in \{1,2,3,4\} (f(i) \neq 1 \vee f(i') \neq 1).$$

Per ognuna delle $\binom{4}{2}$ scelte di due elementi distinti $i, i' \in \{1,2,3,4\}$ dobbiamo formalizzare $(f(i) \neq 1 \vee f(i') \neq 1)$. Quest'ultimo enunciato si formalizza ovviamente con $\neg(p_{i,1} \wedge p_{i',1})$ (o equivalentemente con $(\neg p_{i,1} \vee \neg p_{i',1})$). Dato che la quantificazione su i, i' è universale, otteniamo la seguente congiunzione.

$$\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge \neg(p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}).$$

Analogamente, per $j = 2$ otteniamo

$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}).$$

Analogamente, er $j = 3$ otteniamo

$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3}).$$

Infine, per esprimere la quantificazione universale $\forall j \in \{1,2,3\} \ldots$ basta prendere la congiunzione delle tre proposizioni ottenute per i singoli valori di j.

$$\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge \neg(p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}) \wedge$$

$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}) \wedge$$

$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3}).$$

Per concludere, possiamo formalizzare $PHP(4,3)$ formalizzando: Se ((1) e (2)) allora (3). Otteniamo la proposizione seguente.

$$((p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}) \wedge (p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}) \wedge (p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}) \wedge$$

$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}) \wedge \neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}) \wedge$$

$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}) \wedge \neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3})) \rightarrow$$

$$(\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge (p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}) \wedge$$

$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}) \wedge$$

$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3})).$$

Tanta fatica per formalizzare un singolo caso del Principio dei Cassetti? Osserviamo che la formalizzazione svolta sopra è *uniforme* nel senso che se volessimo formalizzare $PHP(101, 100)$ o $PHP(2^9, 2^9 - 1)$ potremmo usare lo stesso procedimento. Avremmo proposizioni più lunghe ma di stessa struttura.

10. Completezza Funzionale

Siamo sicuri che con connettivi che abbiamo scelto siamo capaci di rappresentare il comportamento di qualunque funzione di verità

$$f : \{0,1\}^n \to \{0,1\}$$

a n argomenti, per $n \in \mathbf{N}$?

Teorema 10.1. *Sia $f : \{0,1\}^n \to \{0,1\}$ una funzione di verità. Esiste una proposizione A contenente n variabili proposizionali $\{p_1, \ldots, p_n\}$ e i connettivi logici $\{\neg, \vee, \wedge\}$ e tale che per ogni assegnamento v,*

$$v(A) = f(v(p_1), \ldots, v(p_n)).$$

Dimostrazione. Per induzione su n.

Se $n = 1$ abbiamo solo quattro possibili f.

$$f_1(0) = 0, f_1(1) = 0$$

$$f_2(0) = 1, f_2(1) = 1$$

$$f_3(0) = 0, f_3(1) = 1$$

$$f_4(0) = 1, f_4(1) = 0$$

Alla funzione f_1 corrisponde la formula $(p \wedge \neg p)$, alla funzione f_2 la formula $(p \vee \neg p)$, allora funzione f_3 la formula p, e alla funzione f_4 la formula $(\neg p)$.

Se $n > 1$, scriviamo il grafico di $f : \{0,1\}^n \to \{0,1\}$ in forma di tavola di verità, come segue.

p_1	p_2	$\ldots$	p_n	$f(p_1, \ldots, p_n)$
0	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	$\ldots$	$\ldots$	$\ldots$	$\ldots$

La parte superiore della tabella, senza considerare la prima colonna, definisce una funzione f_0 di $n-1$ argomenti, il cui comportamento è definito dalle prime 2^{n-1} righe. La parte inferiore della tabella, senza considerare la prima colonna, definisce una funzione f_1 di $n-1$ argomenti, il cui comportamento è definito dalle ultime 2^{n-1} righe.

Per ipotesi induttiva sulle funzioni f_0 e f_1, esistono formule B_0 e B_1 con $n-1$ variabili proposizionali (siano senza pregiudizio di generalità $p_2, \ldots, p_n$) e contenenti soltanto i connettivi $\wedge, \vee, \neg$ tali che, per ogni assegnamento v,

$$v(B_0) = f_0(v(p_2), \ldots, v(p_n)),$$

e

$$v(B_1) = f_1(v(p_2), \ldots, v(p_n)).$$

Sia A la formula seguente

$$((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1)).$$

Dimostriamo che A soddisfa la tesi del teorema rispetto alla funzione f. Sia v un assegnamento qualunque. Dimostriamo che

$$v(A) = f(v(p_1), v(p_2), \ldots, v(p_n)).$$

Distinguamo due casi.

Se $v(p_1) = 1$, allora $v(p_1 \vee B_0) = 1$ e vale

$$v(((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1))) = 1 \text{ se e solo se } v(((\neg p_1) \vee B_1)) = 1.$$

Inoltre, $v((\neg p_1)) = 0$, e dunque

$$v((\neg p_1 \vee B_1)) = 1 \text{ se e solo se } v(B_1) = 1.$$

Ma per quanto visto circa B_1, vale

$$v(B_1) = f_1(v(p_2, \ldots, v(p_n))),$$

e in questo caso – dato che $v(p_1) = 1$ – vale

$$f(v(p_1), v(p_2), \ldots, v(p_n)) = f(1, v(p_2), \ldots, v(p_n)) = f_1(v(p_2), \ldots, v(p_n)).$$

Dunque in questo caso

$$v(A) = f(v(p_1), v(p_2), \ldots, v(p_n)).$$

Se $v(p_1) = 0$, allora $v((\neg p_1)) = 1$ e dunque $v(((\neg p_1) \vee B_1))) = 1$. Allora

$$v(((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1))) = 1 \text{ se e solo se } v((p_1 \vee B_0)) = 1.$$

Inoltre, dato che $v(p_1) = 0$,

$$v((p_1 \vee B_0)) = 1 \text{ se e solo se } v(B_0) = 1.$$

Ma per quanto visto circa B_0, vale

$$v(B_0) = f_0(v(p_2, \ldots, v(p_n))),$$

e in questo caso – dato che $v(p_1) = 0$ – vale

$$f(v(p_1), v(p_2), \ldots, v(p_n)) = f(0, v(p_2), \ldots, v(p_n)) = f_0(v(p_2), \ldots, v(p_n)).$$

Dunque in questo caso

$$v(A) = f(v(p_1), v(p_2), \ldots, v(p_n)).$$

□

11. Forme Normali

Chiamiamo "letterale" una variabile proposizionale o una negazione di una variabile proposizionale. Diciamo che A è in Forma Normale Congiuntiva (CNF) se A è una congiunzione di disgiunzioni di letterali, ossia è della forma seguente, dove gli $A_{i,j}$ sono letterali.

$$(A_{1,1} \vee A_{1,2} \vee \cdots \vee A_{1,m_1}) \wedge (A_{2,1} \vee A_{2,2} \vee \cdots \vee A_{2,m_2}) \cdots \wedge (A_{n,1} \vee A_{n,2} \vee \cdots \vee A_{n,m_n})$$

Diciamo che A è in Forma Normale Disgiuntiva (DNF) se A è una disgiunzione di congiunzioni di letterali, ossia è della forma seguente, dove gli $A_{i,j}$ sono letterali.

$$(A_{1,1} \wedge A_{1,2} \wedge \cdots \wedge A_{1,m_1}) \vee (A_{2,1} \wedge A_{2,2} \wedge \cdots \wedge A_{2,m_2}) \cdots \vee (A_{n,1} \wedge A_{n,2} \wedge \cdots \wedge A_{n,m_n}).$$

Usiamo $\bigwedge_{i \leq n} A_i$ come abbreviazione di

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n.$$

e analogamente $\bigvee_{i \leq n} A_i$ come abbreviazione di

$$A_1 \vee A_2 \vee \cdots \vee A_n.$$

Conquesta notazione, A è una CNF se è della forma

$$\bigwedge_{i \leq n} \bigvee_{j \leq m_i} A_{i,j},$$

ed è in DNF se è della forma

$$\bigvee_{i \leq n} \bigwedge_{j \leq m_i} A_{i,j},$$

dove gli $A_{i,j}$ sono letterali.

Diamo due dimostrazioni (una induttiva l'altra più intuitiva) del seguente Teorema di Forma Normale.

Teorema 11.1 (Forme Normali Congiuntive e Disgiuntive)**.** *Per ogni A esiste A^{CNF} e A^{DNF} tali che A^{CNF} è una CNF, A^{DNF} è una DNF, e*

$$\models A \leftrightarrow A^{\mathrm{CNF}},$$
$$\models A \leftrightarrow A^{\mathrm{DNF}},$$

Dimostrazione n.1. Assumiamo che A sia scritta nel linguaggio ristretto ai connettivi $\{\vee, \wedge, \neg\}$. Dimostriamo il Teorema per induzione su A.

Se A è atomica, è ovvio.

Se A è $(B \wedge C)$, allora scegliamo $(B^{\mathrm{CNF}} \wedge C^{\mathrm{CNF}})$ come A^{CNF}. Sia $B^{\mathrm{DNF}} = \bigvee B_i$, e $C^{\mathrm{DNF}} = \bigvee C_j$. Allora

$$A = B \wedge C \equiv \bigvee B_i \wedge \bigvee C_j \equiv \bigvee_{i,j} (B_i \wedge C_j).$$

Poniamo A^{DNF} uguale a $\bigvee_{i,j}(B_i \wedge C_j)$.

Se A è $(B \vee C)$, il ragionamento è duale.

Se A è $(\neg B)$. Sia $B^{\mathrm{DNF}} = \bigvee \bigwedge B_{i,j}$. Allora

$$\neg B \equiv \neg B^{\mathrm{DNF}} \equiv \neg \bigvee \bigwedge B_{i,j} \equiv \bigwedge \bigvee \neg B_{i,j}.$$

Poniamo A^{CNF} uguale a $\bigwedge \bigvee \neg B'_{i,j}$, dove $B'_{i,j}$ è $B_{i,j}$ se $B_{i,j}$ è una variabile negata ed è $\neg B_{i,j}$ altrimenti.

A^{DNF} si definisce in maniera duale partendo da B^{CNF}. □

Dimostrazione n.2. Scriviamo la tavola di verità di A

p_1	p_2	$\dots$	p_n	A
0	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\dots$	$\dots$	$\dots$	$\dots$
1	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	$\dots$	$\dots$	$\dots$	$\dots$

La tavola ha 2^n righe. Per ogni $1 \leq i \leq n$, la riga i determina un assegnamento di valori di verità a $p_1, \dots, p_n, A$, che chiamiamo v_i. La riga i-esima dice che se p_1 ha valore $v_i(p_1)$, e p_2 ha valore $v_i(p_2)$, ..., e p_n ha valore $v_i(p_n)$ allora A ha il valore $v_i(A)$. I casi in cui A è vera sono completamente descritti dalle righe i in cui $v_i(A) = 1$. In altre parole, A è vera se e solo se le variabili proposizionali $p_1, \dots, p_n$ assumono i valori $v_i(p_1), \dots, v_i(p_n)$ per una qualche riga i tale che $v_i(A)$. Dunque, per ogni assegnamento v, $v(A) = 1$ se e solo se v coincide con v_i su $p_1, \dots, p_n$ dove i è una riga in cui A è vera.

Usiamo i letterali per rappresentare all'interno del linguaggio i due casi $v_i(p_{i,j}) = 1$ e $v_i(p_{i,j}) = 0$, per $i \in \{1, \dots, 2^n\}$ e $j \in \{1, \dots, n\}$. Definiamo $p'_{i,j} = p_{i,j}$ se $v_i(p_{i,j}) = 1$ e $p'_{i,j} = \neg p_{i,j}$ se $v_i(p_{i,j}) = 0$. Consideriamo ora l'insieme $I_1 \subseteq \{1, \dots, 2^n\}$ delle righe in cui A ha valore 1. Per $i \in I_1$, alla riga i-esima associamo la congiunzione

$$p'_{i,1} \wedge \dots \wedge p'_{i,n}.$$

Questa congiunzione rappresenta l'assegnamento v_i, nel senso che, per ogni assegnamento v,

$$v(p'_{i,1} \wedge \dots \wedge p'_{i,n}) = 1 \Rightarrow v(A) = 1.$$

Infatti vale che

$$v(p'_{i,1} \wedge \dots \wedge p'_{i,n}) = 1 \Rightarrow v(p'_{i,1}) = v_i(p_{i,1}), \dots, v(p'_{i,n}) = v_i(p_{i,n}).$$

Dato che per ogni v vale $v(A) = 1$ se e solo se per qualche $i \in I_1$, v coincide con v_i sulle variabili $p_1, \dots, p_n$ di A, abbiamo che l'intera tavola di verità di A è rappresentata dalla DNF

$$\bigvee_{i \in I_1} \bigwedge_{j \in \{1,\dots,n\}} p'_{i,j}.$$

Per Esercizio, sviluppare i dettagli di un argomento analogo per ottenere una CNF equivalente a A. □

Proposizione 11.2. *Una CNF è una tautologia se e soltanto se tutti i suoi congiunti sono tautologie.*

Proposizione 11.3. *Una DNF è insoddisfacibile se e soltanto se tutti i suoi disgiunti sono insoddisfacibili.*

Potremmo allora pensare di affrontare il problema di decidere se $A \in$ Taut (o equivalentemente $\neg A \in$ UnSat) scrivendola in CNF e decidendo se i congiunti sono in Taut o scrivendola in DNF e decidendo se i disgiunti sono in UnSat. Purtroppo questo metodo non dà luogo a un algoritmo efficiente (vedi *infra* per un esempio).

12. Altre manipolazioni algebriche

Illustriamo un altro metodo per manipolare le verità logiche basato sulle leggi di distributività. Si procede come segue, data una proposizione A.

(1) Si eliminano i connettivi $\to$ e $\leftrightarrow$, utilizzando le equivalenze $A \to B \equiv \neg A \vee B$ e $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$.
(2) Si spingono le negazioni all'interno, utilizzando le equivalenze $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$ e $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$.
(3) Si sostituisce $\wedge$ con $+$ e $\vee$ con $\cdot$ (o viceversa!)
(4) Si sviluppa usando la legge di distributività.
(5) Se abbiamo sostituito $\wedge$ con $+$ e $\vee$ con $\cdot$ allora sostituiamo le occorrenze di tipo $p + (\neg p)$ con 0 e quelle di tipo $p \cdot (\neg p)$ con 1 (se abbiamo sostituito $\wedge$ con $\cdot$ e $\vee$ con $+$, facciamo il viceversa).
(6) Si sostituisce $+$ con $\wedge$ e $\cdot$ con $\vee$ (o viceversa, a seconda della scelta fatta sopra!).

Questo metodo permette di trasformare una proposizione preservando l'equivalenza logica. In particolare permette di ottenere verità logiche (formule valide) da altre verità logiche. Inoltre, permette di ottenere forme normali CNF o DNF.

Esempio 12.1.

$$(A \to B) \to (\neg B \to \neg A)$$
$$\neg(A \to B) \vee (\neg B \to \neg A)$$
$$\neg(\neg A \vee B) \vee (\neg\neg B \vee \neg A)$$
$$(A \wedge \neg B) \vee (B \vee \neg A)$$
$$(A + \bar{B}) \cdot (B \cdot \bar{A})$$
$$(AB\bar{A}) + (\bar{B}B\bar{A})$$
$$(A \vee B \vee \neg A) \wedge (\neg B \vee B \vee \neg A)$$

In questo modo abbiamo ottenuto una CNF equivalente alla proposizione iniziale. Alternativamente, possiamo continuare la valutazione dalla penultima riga come segue.

$$(AB\bar{A}) + (\bar{B}B\bar{A})$$
$$B1 + \bar{A}1$$
$$(B \vee 1) \wedge (\bar{A} \vee 1)$$
$$1$$

così abbiamo dimostrato che la proposizione iniziale è una verità logica.

Esempio 12.2. Vogliamo verificare la seguente relazione di conseguenza logica

$$(A \to B), (C \vee \neg B), \neg(A \wedge C) \models \neg A$$

Abbiamo due strade.

(1) Verifichiamo che
$$(((A \to B) \wedge (C \vee \neg B) wedge \neg(A \wedge C)) \to \neg A) \in \text{Taut}$$
(2) Verifichiamo che
$$(((A \to B), (C \vee \neg B), \neg(A \wedge C)) \wedge A) \in \text{UnSat}$$

Nel primo caso, trasformiamo in CNF e verifichiamo che ogni congiunto è una tautologia. Nel secondo caso, trasformiamo in DNF e verifichiamo che ogni disgiunto è insoddisfacibile. Sviluppiamo entrambi gli esempi e osserviamo che danno luogo a procedimenti di stessa lunghezza.

Cominciamo con (1), verificando che

$$(((A \to B) \land (C \lor \neg B) \land \neg(A \land C)) \to \neg A) \in \textsc{Taut}$$

Per farlo, trasformiamo in CNF e verifichiamo che ogni congiunto è una tautologia.

$$\neg((A \to B) \land (C \lor \neg B) \land \neg(A \land C)) \lor \neg A$$
$$(\neg(A \to B) \lor \neg(C \lor \neg B) \lor \neg\neg(A \land C)) \lor \neg A$$
$$(\neg(\neg A \lor B) \lor (\neg C \land \neg\neg B) \lor (A \land C)) \lor \neg A$$
$$((A \land \neg B) \lor (\neg C \land B) \lor (A \land C)) \lor \neg A$$

Osserviamo che la formula appena scritta è in DNF, ma non è questa la forma normale che ci serve! Sostituiamo $\land$ con $+$ e $\lor$ con $\cdot$

$$((A + \bar{B}) \cdot (\bar{C} + B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A + \bar{B}) \cdot (\bar{C} + B)) \cdot (A + C)) \cdot \bar{A}$$
$$(((A + \bar{B}) \cdot \bar{C} + (A + \bar{B}) \cdot B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A\bar{C} + \bar{B}\bar{C}) + (AB + \bar{B}B)) \cdot (A + C)) \cdot \bar{A}$$
$$((A\bar{C} + \bar{B}\bar{C}) \cdot (A + C) + (AB + \bar{B}B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A\bar{C} \cdot (A + C) + \bar{B}\bar{C} \cdot (A + C)) + (AB \cdot (A + C) + \bar{B}B \cdot (A + C))) \cdot \bar{A}$$
$$(A\bar{C}A + A\bar{C}C + \bar{B}\bar{C}A + \bar{B}\bar{C}C + ABA + ABC + \bar{B}BA + \bar{B}BC) \cdot \bar{A}$$
$$A\bar{C}A\bar{A} + A\bar{C}C\bar{A} + \bar{B}\bar{C}A\bar{A} + \bar{B}\bar{C}C\bar{A} + ABA\bar{A} + ABC\bar{A} + \bar{B}BA\bar{A} + \bar{B}BC\bar{A}$$

Sostituendo $+$ con $\land$ e $\cdot$ con $\lor$ otteniamo la seguente proposizione

$$(A \lor \neg C \lor A \lor \neg A) \land (A \lor \neg C \lor C \lor \neg A) \land (\neg B \lor \neg C \lor A\neg A) \land (\neg B \lor \neg C \lor C\neg A) \land$$
$$(A \lor B \lor A \lor \neg A) \land (A \lor B \lor C \lor \neg A) \land (\neg B \lor B \lor A\neg A) \land (\neg B \lor B \lor C \lor \neg A)$$

La proposizione è in CNF e tutti i congiunti sono tautologie. Dunque la relazione di conseguenza logica iniziale è verificata.

Procediamo ora con (2), verificando che

$$(((A \to B), (C \lor \neg B), \neg(A \land C)) \land A) \in \textsc{UnSat}$$

Per farlo, trasformiamo in DNF e verifichiamo che ogni disgiunto è insoddisfacibile.

$$(\neg A \lor B) \land (C \lor \neg B) \land (\neg A \lor \neg C) \land A$$

Osserviamo che la formula appena scritta è in CNF, ma non è questa la forma normale che ci serve! Sostituiamo $\land$ con $\cdot$ e $\lor$ con $+$ e otteniamo

$$(\bar{A} + B) \cdot (C + \bar{B}) \cdot (\bar{A} + \bar{C}) \cdot A$$

Osserviamo che l'espressione appena ottenuta è duale a quella ottenuta nell'approccio precedente dopo la sostituzione, se invertiamo $\cdot$ e $+$ e sostituiamo ogni lettera X con la sua negata $\bar{X}$. Procedendo nello sviluppo usando la legge di distributività, otterremo una forma DNF con lo stesso numero di clausole della CNF ottenuta sopra.

Metodi Matematici per l'Informatica - SAT e Risoluzione (a.a. 19/20, I canale)

Docente: Lorenzo Carlucci (carlucci@di.uniroma1.it)*

Risultati strutturali su SAT

Abbiamo osservato che, dato un problema di conseguenza logica, ossia

$$F_1, \ldots, F_n \models^? F$$

possiamo seguire due strade:

Metodo 1: Verificare che $(F_1 \wedge \cdots \wedge F_n) \rightarrow F) \in \mathsf{TAUT}$. In questo caso la risposta è facile se riusciamo a mettere l'intera formula in CNF.

Metodo 2: Verificare che $(F_1 \wedge \cdots \wedge F_n \wedge F) \in \mathsf{UNSAT}$. In questo caso la risposta è facile se riusciamo a mettere l'intera formula in DNF.

Presentiamo ora un metodo, dovuto a Martin Davis e Hilary Putnam per risolvere algoritmicamente il problema $F \in \mathsf{SAT}$? in maniera abbastanza efficiente su un buon numero di istanze.

In vista delle osservazioni qui sopra ci poniamo nel caso in cui abbiamo una formula F in CNF e vogliamo decidere se $F \in \mathsf{SAT}$ o $F \in \mathsf{UNSAT}$ (ossia ci poniamo nel caso più difficile tra i due distinti sopra).

Rappresentazione insiemistica di CNF

Fissiamo una rappresentazione agile e compatta per formule in CNF. Una formula F in CNF ha questa forma:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_n$$

dove ogni C_i (detta clausola) è una disgiunzione di letterali, ossia C_i è di forma

$$\ell_1 \vee \cdots \vee \ell_k$$

per qualche k, per qualche letterale $\ell_1, \ldots, \ell_k$.

Rappresentiamo una clausola $C = \ell_1 \vee \cdots \vee \ell_k$ come l'insieme dei suoi letterali

$$\{\ell_1, \ldots, \ell_k\}$$

e rappresentiamo una formula $F = C_1 \wedge \cdots \wedge C_n$ come l'insieme delle sue clausole

$$\{C_1, \ldots, C_n\}$$

.

Per esempio, la formula

*Il materiale di questa dispensa è tratto principalmente da M.D. Davis, R.Sigal, E.J. Weyuker, *Computability, Complexity and Languages, Fundamentals of Theoretical Computer Science*, 2nd Edition, 1994 Kaufmann

Clausola vuota e formula vuota

Usiamo il simbolo $\square$ per indicare la clausola vuota, ossia senza letterali.

Usiamo il simbolo $\emptyset$ per indicare la formula vuota, ossia senza clausole.

Osserviamo che, secondo le definizioni:

1. $\square$ è in UNSAT: infatti non è vero che esiste un assegnamento v tale che esiste un letterale $\ell \in \square$ tale che $v(\ell) = 1$.
2. $\emptyset$ è in SAT: Infatti esiste un assegnamento v tale che per ogni clausola C, se $C \in \emptyset$ allora $v(C) = 1$ (l'implicazione è vera a vuoto).

Si noti che secondo le definizioni avremmo che $\emptyset$ è anche in TAUT, ma conveniamo di considerarla in SAT.

Si osserva facilmente che se $\square \in F$ allora anche $F \in \mathsf{UNSAT}$, perché un assegnamento che soddisfa F dovrebbe soddisfare tutte le clausole in F ma $\square$ è insoddisfacibile.

Dato che una clausola è in TAUT se e solo contiene un letterale e la sua negazione, si osserva facilmente che se $C \in F$ e $C \in \mathsf{TAUT}$ allora: $F \in \mathsf{SAT}$ sse $F - \{C\} \in \mathsf{SAT}$. Per questo possiamo assumere da ora in poi, senza perdita di generalità, che le nostre formule non contengano clausole tautologiche. Alternativamente possiamo immaginare di partire da una formula contenente anche clausole tautologiche e di cancellare tutte queste clausole. La formula ottenuta è SAT sse lo era la formula di partenza.

Clausole positive e negative, Teorema di Splitting

Definizione 1 *Sia C una clausola e ℓ un letterale.*

1. *C è ℓ-positiva se $\ell \in C$*
2. *C è ℓ-negativa se $\neg\ell \in C$*
3. *C è ℓ-neutra se $\ell \notin C$ e $\neg\ell \notin C$.*

Se F è una formula e ℓ un letterale, denotiamo con F^+_ℓ, F^-_ℓ e F^0_ℓ, rispettivamente, l'insieme delle clausole ℓ-positive, ℓ-negative e ℓ-neutre di F.

Dato che le formule che consideriamo non hanno clausole tautologiche, sappiamo che nessuna clausola può essere contemporaneamente ℓ-positiva e ℓ-negativa per qualche letterale ℓ.

Dunque, data una formula F e un letterale ℓ, abbiamo la seguente partizione di F:

$$F = F^0_\ell \cup F^+_\ell \cup F^-_\ell$$

Definiamo

$$\mathsf{POS}_\ell(F) = F^0_\ell \cup \{C - \{\ell\} \,:\, C \in F^+_\ell\}$$
$$\mathsf{NEG}_\ell(F) = F^0_\ell \cup \{C - \{\neg\ell\} \,:\, C \in F^-_\ell\}$$

Teorema 1 (Splitting) *Sia F in CNF e ℓ un letterale. Allora*

$$F \in \mathsf{SAT} \text{ } \textit{se e solo se} \text{ } \mathsf{POS}_\ell(F) \in \mathsf{SAT} \text{ } \textit{oppure} \text{ } \mathsf{NEG}_\ell(F) \in \mathsf{SAT}.$$

Dimostrazione. Dimostriamo che se $F \in \mathsf{SAT}$ allora $\mathsf{POS}_\ell(F) \in \mathsf{SAT}$ oppure $\mathsf{NEG}_\ell(F) \in \mathsf{SAT}$.

Se $F \in \mathsf{SAT}$ allora esiste un assegnamento v tale che $v(F) = 1$. Dato che F è in CNF, v deve mettere a vero tutte le clausole di F. Dato che queste clausole sono disgiunzioni di letterali, vale che per ogni clausola $C \in F$ esiste un letterale, chiamiamolo ℓ_C, tale che $v(\ell_C) = 1$.

Ragioniamo per casi.

Caso 1. $v(\ell) = 0$

Dimostriamo che v soddisfa $\mathsf{POS}_\ell(F)$. Una clausola in $\mathsf{POS}_\ell(F)$ è o ℓ-neutra oppure è di tipo $C - \{\ell\}$ con C clausola ℓ-positiva. Se C è ℓ-neutra, ovviamente $v(C) = 1$ perché C è anche in F. Se C è ℓ-positiva, allora $v(C - \{\ell\}) = v(C) = 1$. La prima identità vale perché $v(\ell) = 0$. Dunque v soddisfa $\mathsf{POS}_\ell(F)$.

Caso 2. $v(\ell) = 1$.

Dimostriamo che in questo caso v soddisfa $\mathsf{NEG}_\ell(F)$. Questo insieme contiene le clausole ℓ-neutre, per cui $v(C) = 1$ per ipotesi, e le clausole di tipo $C - \{\neg\ell\}$ dove C è ℓ-negativa. Ma se C è ℓ-negativa, C non contiene ℓ, e dato che $v(C) = 1$ per ipotes e $v(\neg\ell) = 0$, abbiamo $v(C - \{\neg\ell\}) = 1$. Dunque v soddisfa $\mathsf{NEG}_\ell(F)$.

Dimostriamo l'altro verso dell'implicazione. Supponiamo che $\mathsf{POS}_\ell(F)$ sia SAT. Esiste un assegnamento v che soddisfa tutte le clausole. Definiamo un assegnamento v^* ponendo $v^*(\ell) = 0$ e $v^*(k) = v(k)$ per ogni letterlae k diverso da ℓ (Es: perché $v*$ è ben definito?). Dimostriamo che v^* soddisfa F. Ricordiamo che

$$F = F_\ell^0 \cup F_\ell^+ \cup F_\ell^-$$

Consideriamo i tre gruppi di clausole separatamente.

Se $C \in F_\ell^0$ allora $v^*(C) = 1$ perché coincide con v su clausole ℓ-neutre.

Se $C \in F_\ell^+$ allora $v^*(C) = v^*(C - \{\ell\})$ perché ho posto $v^*(\ell) = 0$. Dato che $C - \{\ell\}$ non contiene ℓ, ho $v^*(C - \{\ell\}) = v(C - \{\ell\})$ e dunque è $= 1$.

Se $C \in F_\ell^-$ allora dato che $v*(\ell) = 0$ ho che $v^*(\neg\ell) = 1$ e dunque $v^*(C) = 1$ poiché $\neg\ell \in C$.

Supponendo che $\mathsf{NEG}_\ell(F) \in \mathsf{SAT}$ posso ragionare in modo analogo estendendo l'assegnamento ponendo $v^*(\ell) = 1$. (Esercizio: completare i dettagli della dimostrazione). **QED**

Ci sono due casi particolari in cui la conclusione del Teorema precedente ha una forma più semplice.

PURE LITERAL RULE: Supponiamo che F sia tale che $F_\ell^- = \emptyset$, ossia che *non contenga occorrenze negative* del letterale ℓ. Allora per definizione ho che $\mathsf{NEG}_\ell(F) = F_\ell^0$ (ossia coincide con le formula ℓ-neutre) e dunque $\mathsf{NEG}_\ell(F) \subseteq \mathsf{POS}_\ell(F)$. Dunque se un assegnamento soddisfa $\mathsf{POS}_\ell(F)$ allora soddisfa anche $\mathsf{NEG}_\ell(F)$. Per il Teorema abbiamo che:

$$F \in \mathsf{SAT} \text{ sse } \mathsf{NEG}_\ell(F) \in \mathsf{SAT}$$

UNIT RULE: Supponiamo ora che per qualche ℓ valga $\{\ell\} \in F$, ossia che una delle clausole di F sia composta da un singolo letterale. Dato che $\{\ell\} - \{\ell\} = \Box$, abbiamo che $\Box \in \mathsf{POS}_\ell(F)$. Dunque $\mathsf{POS}_\ell(F)$ è in UNSAT. Per il Teorema abbiamo dunque, anche in questo caso, che:

$$F \in \mathsf{SAT} \text{ sse } \mathsf{NEG}_\ell(F) \in \mathsf{SAT}$$

Le proprietà di sopra (Splitting, Pure Literal Rule, Unit Rule) si possono applicare ripetutamente e, in alcuni casi, permettono di verificare se una data formula è SAT o meno.

Esempio: Sia F la seguente formula in CNF:

$$F = \{\{\neg p, \neg q, r\}, \{\neg p, \neg q, s\}, \{\neg p_1, \neg q_1, r_1\}, \{\neg r_1, \neg s, s_1\}, \{p\}, \{q\}, \{q_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{p\}$ abbiamo che $F \in \mathsf{SAT}$ se e solo se $\mathsf{NEG}_p(F) \in \mathsf{SAT}$, dove:

$$\mathsf{NEG}_p(F) = \{\{\neg q, r\}, \{\neg q, s\}, \{\neg p_1, \neg q_1, r_1\}, \{\neg r_1, \neg s, s_1\}, \{q\}, \{q_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{q\}$ abbiamo che $\mathsf{NEG}_p(F) \in \mathsf{SAT}$ sse $\mathsf{NEG}_q(\mathsf{NEG}_p(F))) \in \mathsf{SAT}$, dove

$$\mathsf{NEG}_q(\mathsf{NEG}_p(F))) = \{\{r\}, \{s\}, \{\neg p_1, \neg q_1, r_1\}, \{\neg r_1, \neg s, s_1\}, \{q_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{s\}$ ottengo che la formula precedente è in SAT se e solo se lo è la seguente:

$$\{\{r\}, \{\neg p_1, \neg q_1, r_1\}, \{\neg r_1, s_1\}, \{q_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{q_1\}$ ottengo che la formula precedente è in SAT se e solo se lo è la seguente:

$$\{\{r\}, \{\neg p_1, r_1\}, \{\neg r_1, s_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{p_1\}$ ottengo che la formula precedente è in SAT se e solo se lo è la seguente:

$$\{\{r\}, \{r_1\}, \{\neg r_1, s_1\}, \{\neg s_1\}\}.$$

Applicando la UNIT RULE a $\{\neg s_1\}$ ottengo che la formula precedente è in SAT se e solo se lo è la seguente:

$$\{\{r\}, \{r_1\}, \{\neg r_1\}, \}.$$

Applicando la UNIT RULE a $\{r_1\}$ ottengo che la formula precedente è in SAT se e solo se lo è la seguente:

$$\{\{r\}, \square\}.$$

Quest'ultima formula è UNSAT perché contiene $\square$.

Esempio: Consideriamo la formula F seguente

$$(((p \leftrightarrow q) \rightarrow (r \rightarrow s)) \wedge (q \rightarrow \neg(p \wedge r))$$

che in CNF si scrive:

$$\{\{p, q, \neg r, s\}, \{\neg q, \neg p, \neg r, s\}, \{\neg q, \neg p, \neg r\}\}.$$

Applicando la PURE LITERAL RULE a $\neg r$ ho che $F \in \mathsf{SAT}$ se e solo se $F^0_{\neg r} \in \mathsf{SAT}$. $F^0_{\neg r} = \emptyset$, perché non ci sono clausole $\neg r$-neutre in F. Dato che $\emptyset \in \mathsf{SAT}$ posso concludere che $F \in \mathsf{SAT}$.

Applicandola a s ho che $F \in \mathsf{SAT}$ sse $F^0_s \in \mathsf{SAT}$. $F^0_s = \{\{\neg q, \neg p, \neg r\}\}$ si verifca facilmente essere in SAT (ponendo per esempio tutte le variabili a 0, o applicando un'altra volta la PLR, ottenendo la formula vuota).

Esempio: Consideriamo la formula F seguente

$$\{\{\neg q, p\}, \{r, p\}, \{\neg p, \neg q\}, \{\neg p, s\}, \{q, \neg r\}, \{q, \neg r\}, \{q, \neg s\}\}.$$

Applicando lo SPLITTING al letterale p, consideriamo

$$\mathsf{POS}_p(F) = \{\{\neg q\}, \{r\}, \{q, \neg r\}, \{q, \neg s\}\}$$

$$\mathsf{NEG}_p(F) = \{\{\neg q\}, \{s\}, \{q, \neg r\}, \{q, \neg s\}\}$$

Applicando PURE LITERAL RULE (su $\neg s$) e due volte la UNIT RULE (su r e su q) a $\mathsf{POS}_p(F)$ abbiamo

$$\{\{\neg q\}, \{r\}, \{q, \neg r\}\}; \{\{q\}, \{\neg q\}\}; \{\square\} \in \mathsf{UNSAT}$$

Analogamente da $\mathsf{NEG}_p(F)$:

$$\{\{\neg q\}, \{s\}, \{q, \neg s\}\}; \{\{q\}, \{\neg q\}\}; \{\square\} \in \mathsf{UNSAT}.$$

Concludiamo così che $F \in \mathsf{UNSAT}$.

Risoluzione

Siano C_1 e C_2 due clausole, tali che $\ell \in C_1$ e $\neg\ell \in C_2$. Definiamo

$$\mathsf{res}_\ell(C_1, C_2) = (C_1 - \{\ell\}) \cup (C_2 - \{\neg\ell\}).$$

L'interesse della nozione è che la formula a destra segue logicamente dalle due clausole a sinistra, ossia: sia ℓ un letterale tale che $\ell \in C_1$ e $\neg\ell \in C_2$. Allora

$$\{C_1\}, \{C_2\} \models \{\mathsf{res}_\ell(C_1, C_2)\}.$$

(Per alleggerire la notazione a volte scriveremo $C_1, C_2 \models \mathsf{res}_\ell(C_1, C_2)$). Sia v un assegnamento che mette a 1 le due premesse C_1 e C_2. Se $v(\ell) = 1$ allora $v(C_2 - \{\neg\ell\}) = 1$ e dunque v mette a 1 anche $\mathsf{res}_\ell(C_1, C_2)$.

Se $v(\ell) = 0$ allora $v(C_1 - \{\ell\}) = 1$ e dunque v mette a 1 anche $\mathsf{res}_\ell(C_1, C_2)$.

In entrambi i casi ho che $v(\mathsf{res}_\ell(C_1, C_2)) = 1$.

Estendiamo l'operazione di risoluzione su due clausole a una operazione di risoluzione su una formula: fissato un letterale ℓ, collezioniamo le formule ℓ-positive e tutte le clausole che si possono ottenere per risoluzione accoppiando una clausola ℓ-positiva e una clausola ℓ-negativa di F:

$$\mathsf{RES}_\ell(F) = F^0_\ell \cup \{\mathsf{res}_\ell(C_1, C_2) \ : \ C_1 \in F^+_\ell, C_2 \in F^-_\ell\}.$$

Vale il seguente importante Teorema.

Teorema 2 (Risoluzione) *F in* CNF*, ℓ un letterale.*

$$F \in \mathsf{SAT} \textit{ se e soltanto se } \mathsf{RES}_\ell(F) \in \mathsf{SAT}.$$

Dimostrazione. Supponiamo che $F \in \mathsf{SAT}$ e sia v tale che $v(F) = 1$. Se C è ℓ-neutra, allora $v(C) = 1$ perché $C \in F$. Sia $C = \mathsf{res}_\ell(C_1, C_2)$ con C_1 ℓ-positiva e C_2 ℓ-negativa. Allora $v(C_1) = 1 = v(C_2)$ perché entrambe sono in F e il Teorema precedente implica che $v(C) = 1$. Questo dimostra che ogni clausola in $\mathsf{RES}_\ell(F)$ è messa a 1 da v.

Supponiamo ora che $\mathsf{RES}_\ell(F) \in \mathsf{SAT}$ e sia v tale che $v(\mathsf{RES}_\ell(F)) = 1$. Invocando il Teorema di Splitting sappiamo che $F \in \mathsf{SAT}$ sse $\mathsf{POS}_\ell(F) \in \mathsf{SAT}$ o $\mathsf{NEG}_\ell(F) \in \mathsf{SAT}$. Dimostriamo che che se v mette a 0 la formula $\mathsf{POS}_\ell(F)$ allora mette a 1 la formula $\mathsf{NEG}_\ell(F)$.

Supponiamo che v metta a 0 la formula $\mathsf{POS}_\ell(F)$. Vogliamo dimostrare che v mette a 1 tutte le clausole di $\mathsf{NEG}_\ell(F)$. Queste sono di due tipi: o sono clausole ℓ-neutre, oppure sono di forma $C_2 - \{\neg\ell\}$ per qualche C_2 clausola ℓ-negativa in F.

Dato che tutte le clausole ℓ-neutre sono anche in $\mathsf{RES}_\ell(F)$ e v mette a 1 questa formula, v mette a 1 tutte le clausole ℓ-neutre.

Consideriamo le clausole del secondo tipo, ossia $C_2 - \{\neg\ell\}$ per qualche C_2 in F che contiene $\neg\ell$. Dato che $\mathsf{RES}_\ell(F)$ è messo a 1 da v, abbiamo che, per ogni C_2 di questo tipo, per ogni C_1 in F ℓ-positiva, deve valere che

$$v(\mathsf{res}_\ell(C_1, C_2)) = v((C_1 - \{\ell\}) \cup (C_2 - \{\neg\ell\})) = 1.$$

D'altro canto abbiamo ipotizzato che v mette a 0 la formula $\mathsf{POS}_\ell(F)$, ma che tutte le ℓ-neutre sono a 1. Dunque deve esistere una C_1 clausola ℓ-positiva tale che $v(C_1 - \{\ell\}) = 0$. Ma per questa C_1 e per ogni C_2 clausola ℓ-negativa, deve valere che il risolvente $\mathsf{res}_\ell(C_1, C_2)$ è messo a 1 da v. Dunque deve necessariamente valere che $v(C_2 - \{\neg\ell\}) = 1$. Ricapitolando abbiamo dimostrato che tutte le clausole in $\mathsf{NEG}_\ell(F)$ sono messe a 1 da v. **QED**

Algoritmo per SAT

I risultati visti finora danno luogo a un **algoritmo** per testare se $F \in \mathsf{SAT}$. Iniziamo cercando un letterale cui applicare la Pure Literal Rule o la Unit Rule. Se non ve ne sono, scegliamo ℓ in F e calcoliamo $\mathsf{RES}_\ell(F)$. Procediamo ricorsivamente.

L'agoritmo termina perché il numero dei letterali diminuisce strettamente a ogni iterazione, e si conclude necessariamente in $\{\Box\}$ oppure in $\emptyset$ (ossia in UNSAT oppure in SAT), perché a ogni passo la formula ottenuta ha un letterale in meno della formula immediatamente precedente.

Correttezza e Completezza della Risoluzione

Osserviamo che è possibile decidere la soddisfacibilità applicando iterativamente la sola risoluzione di clausole.

Esempio Consideriamo la formula

$$((p \wedge q) \to (r \wedge s)) \wedge ((p_1 \wedge q_1) \to r_1) \wedge$$
$$((r_1 \wedge s) \to s_1) \wedge p \wedge q \wedge q_1 \wedge p_1 \wedge \neg s_1.$$

In CNF si scrive così:

$$F = \{\{\neg p, \neg q, r\}, \{\neg p, \neg q, s\}, \{\neg p_1, \neg q_1, r_1\}, \{\neg r_1, \neg s, s_1\}, \{p\}, \{q\}, \{q_1\}, \{p_1\}, \{\neg s_1\}\}.$$

Possiamo applicare la risoluzione di clausole partendo dall'insieme di clausole F, scegliendo ogni volta una coppia di clausole a cui è possibile applicare la risoluzione. Otteniamo una sequenza finita di clausole come segue:

$$\{\neg p, \neg q, s\}, \{\neg r_1, \neg s, s_1\}, \{\neg p, \neg q, \neg r_1, s_1\}, \{p\}, \{\neg q, \neg r_1, s_1\}, \{q\}, \{\neg r_1, s_1\}, \{\neg s_\}, \{\neg r_1\},$$
$$\{\neg p_1, \neg q_1, r_1\}, \{\neg p_1, \neg q_1\}, \{q_1\}, \{\neg p_1\}, \{p_1\}, \Box.$$

Dal fatto che l'ultima clausola è la clausola vuota, che è insoddisfacibile, e dalla proprietà sopra dimostrata che il risolvente è conseguenza logica delle due clausole premesse, possiamo concludere che F è insoddisfacibile.

Da quanto già dimostrato segue facilmente che: se esiste una successione ordinata di clausole ottenute partendo dalle clausole in F e applicando la risoluzione di clausole, e che termina con la clausola vuota allora la formula F è insoddisfacibile. Questa proprietà del metodo di Risoluzione si chiama **correttezza**: se applicando iterativamente la risoluzione alle clausole di una formula raggiungo la clausola vuota, allora la formula di partenza è insoddisfacibile.

Consideriamo la domanda opposta: se F è in UNSAT, è vero che posso certificarlo applicando iterativamente la regola di risoluzione di clausole partendo dalle clausole di F e raggiungendo la clausola vuota? Questa proprietà, se vale, è detta **completezza** (del metodo di Risoluzione): il metodo è capace di certificare tutti i casi di $F \in \mathsf{UNSAT}$.

Per dimostrare la completezza della Risoluzione è opportuno introdurre il concetto formale di *derivazione in Risoluzione* di una clausola C da una formula F, che generalizza l'esempio visto prima.

Definizione 2 *Sia $F = \{C_1, \ldots, C_{n-1}\}$ una formula (insieme finito di clausole). La sequenza ordinata*

$$C_1, C_2, \ldots, C_{n-1}, C_n$$

è una derivazione in Risoluzione di C_n se, per ogni $i \in [1, n]$, o $C_i \in F$ oppure esistono $j, k < i$ tali che $C_i = \mathsf{res}_\ell(C_j, C_k)$, per qualche letterale ℓ. In altre parole, ogni clausola C_i ha un certificato per appartendere alla sequenza/derivazione: o è una clausola di F oppure deriva da due clausole precedenti per applicazione di risoluzione.

Se $C_n = \Box$ diciamo che la derivazione è detta una refutazione di F.

Il Teorema seguente formalizza adeguatamente una proprietà già osservata, e permette di dimostrare la correttezza del metodo di Risoluzione: si dimostra che se esiste una derivazione di una clausola C da una formula F allora C è conseguenza logica di F.

Teorema 3 *Sia F in* CNF *e sia C una clausola. Se esiste una derivazione in Risoluzione di C da F allora*

$$F \models C.$$

Dimostrazione. Sia $C_1, \ldots, C_n$, con $C_n = C$ una derivazione in risoluzione di C da F.
Dimostriamo che per ogni $i \in [1, n]$ $v(C_i) = 1$.
Caso 1: $C_i \in F$. Per ipotesi $v(F) = 1$ dunque $v(C_i) = 1$.
Caso 2: C_i deriva da C_j, C_k con $j, k < i$ per risoluzione, i.e. $\mathsf{res}_\ell(C_j, C_k) = C_i$. Per Ipotesi Induttiva $v(C_j) = v(C_k) = 1$. Per il Teorema di sopra segue $v(C_i) = 1$. **QED**

Il risultato seguente dimostra la correttezza del metodo di refutazione con Risoluzione: **se** è possibile refutare in Risoluzione una formula **allora** quella formula è veramente insoddisfacibile.

Corollario 1 (Correttezza) *Se esiste una refutzazione in Risoluzione di F allora*

$$F \in \mathsf{UNSAT}.$$

Dimostrazione. Per definzione, una refutazione di F è una derivazione in Risoluzione di $\Box$ da F. Per il Teorema di sopra, se $v(F) = 1$ allora avremmo $v(\Box) = 1$. Impossibile. **QED**

Il seguente teorema dimostra che il metodo di refutazione in Risoluzione è completo relativamente all'insieme UNSAT: ossia, se una formula è veramente in UNSAT, allora è possibile costruire una sua refutazione in Risoluzione.

Teorema 4 (Completezza) *Se $F \in \mathsf{UNSAT}$ allora esiste una refutazione in Risoluzione di F.*

Dimostrazione. Sia $F \in \mathsf{UNSAT}$. Siano $\ell_1, \ell_2, \ldots, \ell_k$ tutti gli atomi proposizionali che compaiono in F. Definiamo una sequenza di formule come segue:

$$F_0 = F, F_1 = \mathsf{RES}_{\ell_1}(F_0), F_2 = \mathsf{RES}_{\ell_2}(F_1), \ldots, F_k = \mathsf{RES}_{\ell_k}(F_{k-1}).$$

Si osserva che F_0 contiene tutti i letterali di F, F_1 non contiene ℓ_1, F_2 non contiene ℓ_1, ℓ_2, etc. fino a concludere che F_k non contiene $\ell_1, \ell_2, \ldots, \ell_k$; dunque non contiene letterali, e dunque F_k è la formula vuota $\emptyset$ oppure $\{\Box\}$. D'altro canto si osserva facilmente che: $F_0 \in \mathsf{UNSAT}$, per ipotesi. $F_1 \in \mathsf{UNSAT}$, perché è ottenuta risolvendo su ℓ_1 da F_0, e per il Teorema di Risoluzione visto sopra vale

$$F_0 \in \mathsf{SAT} \text{ sse } \mathsf{RES}_{\ell_1}(F_0) \in \mathsf{SAT}.$$

Analogamente $F_2, F_3, \ldots, F_k$ sono tutte in UNSAT. Dunque F_k non può essere $\emptyset$ ma è necessariamente la formula insoddisfacibile $\{\Box\}$.

Dalla successione di formule $F_0, F_1, \ldots, F_k$ così ottenuta definiamo facilmente una successione di clausole

$$C_1, C_2, \ldots, C_m$$

enumerando in ordine le clausole di $F = F_0$, poi quelle di F_1, poi quelle di F_2, etc. fino a quelle di F_k, che sono la sola $\Box$. Si verifica facilmente che la sequenza in questione è una derivazione in Risoluzione, ossia, per ogni clausola C_i, o C_i è una clausola della formula F iniziale, oppure è ottenuta per risoluzione di clausole da due clausole che la precedono nella sequenza (Esercizio). Dunque abbiamo esibito una refutazione in Risoluzione della formula F. **QED**

Complessivamente i risultati di sopra (correttezza e completezza) dimostrano che l'esistenza di una refutazione in Risoluzione di una formula è **equivalente** al fatto che la formula è insoddisfacibile. In altre parole: le refutazioni in Risoluzione sono un metodo affidabile e infallibile per dimostrare se una formula è UNSAT o SAT.

METODI MATEMATICI PER L'INFORMATICA

ANNO ACCADEMICO 2019/2020

SOMMARIO. Limitazioni della Logica Proposizionale e introduzione del linguaggio della Logica Predicativa. Sintassi e semantica della Logica Predicativa. Strutture e modelli. Verità e conseguenza logica.

Nota Qui trovate alcuni appunti sulle cose viste in classe. Il libro di testo contiene una trattazione più ampia in cui si usano anche simboli di funzione.

1. Limitazioni espressive della Logica Proposizionale

In questa sezione cerchiamo di motivare la necessità di estendere la logica proposizionale. Procediamo così: analizziamo alcuni esempi abitualmente usati per illustrare le limitazioni della logica proposizionale. Ne diamo formalizzazioni proposizionali e analizziamo in quali casi e sotto quali aspetti queste formalizzazioni sono carenti. Vediamo in che senso la logica predicativa supplisce a queste carenze. Motiviamo attraverso esempi i costrutti fondamentali della logica predicativa: costanti, variabili, quantificatori, predicati, relazioni, funzioni.

Esempio 1.1. Il seguente è un classico esempio che viene presentato per illustrare le limitazioni della logica proposizionale (vedi e.g., E. Mendelson, *Introduzione alla Logica Matematica*).

Ogni amico di Marco è amico di Pietro.
Claudio non è amico di Pietro.
Dunque Claudio non è amico di Marco.

Proponiamo la seguente formalizzazione in logica proposizionale. È naturale assumere che il dominio di discorso di interesse per questo esempio, ossia l'insieme degli esseri umani, è un dominio finito. Sia U il numero degli essere umani. Usiamo un linguaggio composto da variabili $p_{i,j}$, che intuitivamente stanno per "i è amico di j", dove i, j variano su un insieme finito di indici $\{1, \ldots, U\}$. Assumiamo inoltre che nella numerazione $\{1, \ldots, U\}$ degli esseri umani Marco sia il numero 1, Pietro il numero 2 e Claudio il numero 3. Possiamo allora formalizzare l'argomento precedente come segue, riducendo le quantificazioni universali a congiunzioni.

$$(p_{1,1} \to p_{1,2}) \wedge (p_{2,1} \to p_{2,2}) \wedge \cdots \wedge (p_{U,1} \to p_{U,2})$$
$$\neg p_{3,2}$$
$$\neg p_{3,1}$$

Si verifica facilmente che le prime due proposizioni implicano logicamente la terza.

Perché le formalizzazioni proposte non sono soddisfacenti? Perché gli esempi di sopra ci indicano che dobbiamo estendere la logica proposizionale? Consideriamo due nuove versioni degli esempi fatti.

Esempio 1.1 (Revisited)
Consideriamo la seguente variante dell'Esempio 1.1.

Ogni numero intero inferiore a 5 è inferiore a 10.
20 non è inferiore a 10
Dunque 20 non è inferiore a 5

La struttura dell'argomento è identica a quella dell'Esempio 1. Cosa succede se proviamo a formalizzarlo in logica proposizionale come abbiamo fatto per l'Esempio 1? La differenza fondamentale è che il dominio del discorso in questo caso consiste di un numero infinito di elementi (gli interi). Per formalizzare la prima

Note preparate da Lorenzo Carlucci, carlucci@di.uniroma1.it.

premesse (con quantificazione universale) dovremmo allora usare congiunzioni infinite, o perlomeno usare un insieme infinito di premesse, e.g.,

$$(p_{-100,5} \to p_{-100,10}), (p_{-99,5} \to p_{-99,10}), (p_{-98,5} \to p_{-98,10}) \dots$$

dove usiamo la variabile $p_{i,j}$ con $i, j \in \mathbf{Z}$ per indicare che "$i < j$". Qui osserviamo un primo limite concreto della logica proposizionale. Per esprimere una quantificazione su un dominio infinito abbiamo bisogno di infinite proposizioni.

Esempio 1.2 (Revisited)
Una seconda osservazione riguarda l'Esempio 2. In questo caso il problema è che gli insiemi delle cose viventi, degli uomini e delle cose mortali sono insiemi *dinamici*, ossia variano nel tempo (gli uomini nascono e muoiono). Ma è chiaro che non vogliamo che la validità dell'argomento dell'Esempio 2 dipenda da quali uomini esistono in un determinato momento. La validità dell'Esempio 2 dipende dalla relazione tra i *concetti* di "uomo", "mortale" e "vivente". Se adottassimo la formalizzazione in logica proposizionale proposta sopra dovremmo aggiornare le nostre premesse ogni volta che nasce un nuovo uomo o che muore un nuovo essere mortale. Dovremmo ogni volta aggiornare le nostre numerazioni di questi insiemi finiti. Questo è ovviamente poco desiderabile. Inoltre, le formule usate per descrivere il ragionamento sono molto ingombranti.

Vediamo come la logica predicativa risponde esattamente ai problemi che sono emersi dall'analisi degli esempi prededenti, ossia

(1) Permette di esprimere quantificazioni su dominii infiniti con singole proposizioni finite.
(2) Permette di distinguere le relazioni tra i concetti (proprietà) dalle relazioni tra gli individui.

A livello formale questo si esprime con l'introduzione di **costanti**, **variabili**, **quantificatori** e **predicati**. Le costanti (che denoteremo per il momento con $a, b, c, d, \dots$) vanno lette come nomi propri per individui del dominio di discorso. Le variabili (che denoteremo per il momento con $x, y, z, w, \dots$) e i quantificatori (universale $\forall$ ed esistenziale $\exists$) permettono permettono di esprimere quantificazioni su domini finiti o infiniti. I simboli di predicato, che denoteremo con P, Q, R permettono di rendere esplicita la distinzione tra concetti (proprietà) e individui. I simboli di predicato vengono usati in combinazione con i simboli che denotano individui (variabili e costanti) in espressioni formali di tipo $P(x)$ o $P(c)$, da leggersi come "l'oggetto x ha la proprietà P", o "x è un P" (e analogamente per c).

Torniamo ora ai nostri esempi problematici e formalizziamoli nel nuovo linguaggio.

Formalizzazione predicativa dell'Esempio 1.1, (versione 1). Prima di tutto dobbiamo scegliere un linguaggio opportuno. In particolare scegliere quanti predicati e quante costanti utilizzare. Possiamo analizzare la prima premessa come segue: Se un individuo ha la proprietà "Essere amico di Marco" allora quell'individuo ha la proprietà "Essere amico di Pietro". La seconda premessa di può analizzare come: L'individuo "Claudio" non ha la proprietà "Essere amico di Pietro". La terza premessa si può analizzare come: L'individuo "Claudio" non ha la proprietà "Essere amico di Marco". Questa analisi ci suggerisce che abbiamo bisogno di

(1) Un simbolo di costante c per l'individuo Claudio,
(2) Un simbolo di predicato AM per la proprietà Essere amico di Marco,
(3) Un simbolo di predicato AP per la proprietà Essere amico di Pietro.

Possiamo allora formalizzare l'argomento come segue.

$$\forall x(AM(x) \to AP(x))$$
$$\neg AP(c)$$
$$\neg AM(c)$$

Le regole della logica predicativa che svilupperemo saranno tali da rendere l'argomento logicamente valido (nel nuovo senso, da definire).

Formalizzazione predicativa dell'Esempio 1.1, (versione 2). Consideriamo ora la variante numerica dell'Esempio 1. Scegliamo un linguaggio opportuno. Possiamo analizzare la prima premessa come segue: Se un individuo ha la proprietà "Essere inferiore a 5" allora quell'individuo ha la proprietà "Essere inferiore a 10". La seconda premessa di può analizzare come: L'individuo "20" non ha la proprietà "Essere inferiore a

10". La terza premessa si può analizzare come: L'individuo "20" non ha la proprietà "Essere inferiore a 5". Questa analisi ci suggerisce che abbiamo bisogno di

(1) Un simbolo di costante v per l'individuo 20,
(2) Un simbolo di predicato $Inf5$ per la proprietà Essere inferiore a 5,
(3) Un simbolo di predicato $Inf10$ per la proprietà Essere inferiore a 10.

Possiamo allora formalizzare l'argomento come segue.

$$\forall x(Inf5(x) \to Inf10(x))$$
$$\neg Inf10(v)$$
$$\neg Inf5(v)$$

Abbiamo così ovviato al problema di formalizzare la quantificazione infinita con una proposizione finita. Si osserva facilmente che la versione formale appena proposta è identica alla versione formale dell'Esempio 1 proposta sopra a meno dei nomi dei predicati e delle costanti. I due argomenti sono infatti identici, ossia hanno la stessa forma logica.

Formalizzazione predicativa dell'Esempio 1.1, (versione 3). La formalizzazione dell'Esempio 1 e dell'Esempio 2 proposta qui sopra è corretta ma si può migliorare. Nell'Esempio 1 è chiaro che i predicati "Essere amico di Marco" e "Essere amico di Pietro" hanno qualcosa in comune, e lo stesso vale per i predicati "Essere inferiore a 5" e "Essere inferiore a 10" nell'Esempio 2. È naturale che questa comunanza venga rispecchiata nel nostro linguaggio formale. A questo scopo estendiamo il concetto di predicato a quello di "predicato a più variabili", o "relazione" e introduciamo nel linguaggio simboli per predicati di questo nuovo tipo. Un'espressione di tipo $P(x, y)$ sarà letta come gli oggetti x, y stanno nella relazione P. Il nostro linguaggio può ora contenere simboli di predicato con qualunque numero finito di variabili. Un'espressione di tipo $R(x_1, \ldots, x_n)$ sarà letta come "Gli individui indicati da $x_1, \ldots, x_n$ stanno nella relazione R". Possiamo allora proporre una nuova formalizzazione degli Esempi 1 e 2 usando il seguente linguaggio.

(1) Un simbolo di predicato $P(x, y)$ a due posti,
(2) Tre simboli di costante a, b, c.

Per l'Esempio 1 $P(x, y)$ viene letto come "x è amico di y", a come Marco, b come Pietro e c come Claudio. Per l'Esempio 2 $P(x, y)$ viene letto come "x è inferiore a y", a come 5, b come 10 e c come 20. La versione formalizzata dei due Esempi è la seguente.

$$\forall x(P(x, a) \to P(x, b))$$
$$\neg P(c, b)$$
$$\neg P(c, a)$$

In conclusione, è opportuno includere nel linguaggio della logica predicativa i seguenti tipi di simboli.

(1) Costanti a, b, c, d, etc. (in quantità al più numerabile)
(2) Variabili x, y, z, w, etc., (in quantità numerabile)
(3) Quantificatori $\forall$, $\exists$,
(4) Simboli per predicati a uno o più posti $P(x)$, $R(x, y)$, $Q(x, y, z)$ etc., (in quantità al più numerabile).

Una scelta di simboli di predicato e di un insieme di costanti determina un *linguaggio predicativo relazionale*.

2. Sintassi della Logica Predicativa

Un linguaggio (relazionale) del I ordine è una collezione (finita o infinita) $\mathcal{L}$ di simboli. I simboli sono di due tipi.

- Simboli di relazioni, ciascuno con la sua molteplicità.
- Costanti.

Inoltre assumiamo sempre un insieme numerabile di variabili $v_1, v_2, \ldots$. Queste sono le variabili ufficiali del linguaggio. Useremo x, y, z, w, v (con pedici) come variabili su variabili (dette anche metavariabili, perché sono usate come variabili per variabili individuali). Costanti e simboli di funzione si possono combinare per costruire nomi più complessi per elementi del dominio.

Definizione 2.1 (Termini)**.** I termini (in un linguaggio relazionale) sono le variabili e le costanti.

Per formulare proposizioni nel linguaggio $\mathcal{L}$ usiamo i simboli logici seguenti

- Connettivi $\wedge$, $\vee$, $\rightarrow$, $\neg$.
- Quantificatori $\exists$, $\forall$.

In logica proposizionale le variabili proposizionali erano la minima unità dotata di un valore di verità (0,1). In logica predicativa il loro posto viene preso da espressioni più complesse, dette formule atomiche.

Definizione 2.2 (Formule Atomiche)**.** Una formula atomica è una stringa del tipo $R(t_1, \ldots, t_k)$ dove R è un simbolo di relazione a k posti e $t_1, \ldots, t_k$ sono termini.

Esempio 2.3. In un linguaggio composto da due costanti c_0 e c_1 e da due simboli di predicato P (a un posto) e R (a due posti), le sole formule atomiche sono del tipo $P(c_0)$, $P(c_1)$, $P(x)$, $R(x, c_1)$, $R(c_0, c_1)$, etc. Le sole formule atomiche *senza variabli* sono $P(c_0)$, $P(c_1)$, $R(c_0, c_1)$, $R(c_1, c_0)$, $R(c_0, c_0)$, $R(c_1, c_1)$.

Definizione 2.4 (Formule)**.** Le formule sono ottenute partendo dalle formule atomiche e chiudendo sotto connettivi proposizionali e quantificatori universali ed esistenziali. Le formule (non atomiche) sono dunque del tipo

$$(F \wedge G), (F \vee G), (\neg F), (F \rightarrow G), ((\forall v)F), ((\exists v)F),$$

dove F e G sono formule (atomiche o non atomiche) e v è una variabile.

Nelle formule $((\forall v)F)$ e $((\exists v)F)$, F è detto il *dominio* (o *scope*, in inglese) del quantificatore e v la variabile quantificata. Se v non occorre in F possiamo identificare le due formule quantificate con F. Una distinzione fondamentale è quella tra variabili quantificate (dette vincolate o legate) e variabili non quantificate (dette libere).

Definizione 2.5 (Variabili libere e legate)**.** Una occorrenza di una variabile x in una formula F è vincolata se e solo se (i) l'occorrenza di x è la variabile quantificata di un quantificatore, oppure (ii) l'occorrenza di x è nel dominio di un quantificatore con variabile quantificata x. Tutte le altre occrrenze di x in F sono dette libere.

Ad ogni formula F possiamo associare in modo ovvio l'insieme delle sue variabili libere (le variabili che hanno almeno un'occorrenza libera in F) e l'insieme delle sue variabili legate (le variabili che hanno almeno un'occorrenza vincolata in F). Ovviamente i due insiemi non sono necessariamente disgiunti.

Esempio 2.6. Le variabili quantificate funzionano in modo simili alle variabili locali in un linguaggio di programmazione. Nella formula

$$(\forall x R(x, y)) \wedge (\exists y S(x, y, z))$$

la prima occorrenza di x (quella in $R(x, y)$ è legata (dal quantificatore $\forall x$, la prima occorrenza di y è libera, la seconda occorrenza di y è legata (dal quantificatore $\exists y$) e la seconda occorrenza di x è libera. La variabile z ha una sola occorrenza ed è libera.

Un *enunciato* è una formula senza variabili libere.

Se F è una formula e $x_1, \ldots, x_n$ sono variabili *distinte*, indichiamo con $F(x_1, \ldots, x_n)$ il fatto che le variabili libere di F sono *contenute* nell'insieme $\{x_1, \ldots, x_n\}$. Analogamente per un termine.

3. Semantica della Logica Predicativa

Il nostro scopo è di definire la nozione di *verità logica* per la logica dei predicati. Questa nozione è analoga a quella di tautologia per la logica proposizionale, ossia indica una formula sempre vera, qualunque sia l'assegnamento di un significato ai simboli che la compongono. A tale scopo dobbiamo definire la nozione di verità di una formula della logica predicativa. Nel caso della logica proposizionale la verità di una formula è fissata una volta che è fissato un assegnamento di valori di verità alle variabili proposizionali. Nel caso della logica predicativa la verità di una proposizione dipende dalla scelta dell'ambiente in cui decidiamo di interpretare i simboli del linguaggio. Un tale ambiente è detto *struttura*.

Si tratta di astrarre dalla normale pratica matematica. In Algebra è abituale definire un gruppo come un insieme G su cui è definita una operazione $\cdot$ associativa e tale che esiste un elemento e di G che è neutro rispetto a $\cdot$ e commuta con tutti gli elementi di G. In Teoria dei Grafi è abituale definire un grafo (semplice)

G come una coppia (V, E), dove V è un insieme (detto insieme dei vertici) e E è una relazione binaria non riflessiva e simmetrica (i.e., gli archi non hanno orientazione). Gruppi e grafi sono esempi di *strutture*, ossia insiemi su cui sono definite operazioni, relazioni e costanti.

In Algebra ci si può interessare alle proprietà di *singoli gruppi* di particolare interesse, o alle proprietà di *classi di gruppi* di particolare interesse (per esempio i gruppi abeliani, i gruppi ciclici, i gruppi di permutazioni, etc.), o alle proprietà di *tuttti i gruppi*. In Teoria dei Grafi ci si può interessare alle verità che valgono in singoli grafi di particolare interesse, o alle verità che valgono di classi di grafi di particolare interesse (bipartiti, completi, Euleriani, etc.), o infine alle verità che valgono per tutti i grafi. In Logica Matematica facciamo un passo di generalizzazione ulteriore e ci interessiamo alla verità *in tutte le strutture*. Per questo motivo diamo le seguenti definizioni in forma molto generale.

Definizione 3.1. Fissiamo un linguaggio $\mathcal{L} = \{R_i, f_j, c_k \,:\, i \in I, j \in J, k \in K\}$ dove I, J, K sono insiemi (di indici). Una struttura (o interpretazione) $\mathcal{A}$ per il linguaggio $\mathcal{L}$ consiste di

- Un insieme A non vuoto, detto *dominio*.
- Per ogni simbolo R_i a k posti, una relazione k-aria su A, che denotiamo con $R_i^{\mathcal{A}}$.
- Per ogni $k \in K$, un elemento di A, che denotiamo con $c_k^{\mathcal{A}}$.

Si ricorda che una relazione k-aria su un insieme A è un insieme di sequenze ordinate di lunghezza k di elementi di A, ossia un sottinsieme del prodotto cartesiano A^k (l'insieme di tutte le k-ple ordinate di elementi di A). Nel caso in cui $k = 1$ il simbolo a k-posti R_i viene interpretato con un sottinsieme del dominio A (che coincide con una relazione a 1 posto...).

Esempio 3.2. Se il linguaggio contiene soltanto le costanti c_0, c_1 e i simboli P (a un posto) e R (a due posti), una struttura per il linguaggio è determinata da:

(1) Un insieme non vuoto, A.
(2) Un elemento di A per interpretare c_0, che denotiamo con $c_0^{\mathcal{A}}$, e un elemento di A per interpretare c_1, che denotiamo con $c_1^{\mathcal{A}}$.
(3) Un sottinsieme di A per interpretare P; che denotiamo con $P^{\mathcal{A}}$.
(4) Una relazione binaria su A, ossia un sottinsieme di $A \times A$; che denotiamo con $R^{\mathcal{A}}$.

Per esempio, una struttura possibile $\mathcal{A}$ si ottiene scegliendo come dominio $\mathbf{N}$, come $c_0^{\mathcal{A}}$, $c_1^{\mathcal{A}}$, $R^{\mathcal{A}} =<$, e $P^{\mathcal{A}} =$ i numeri pari. Un'altra si ottiene scegliendo come dominio gli interi, come interpretazione di c_0 il numero 0, come interpretazone di c_1 il numero -1, come interpretazione di R la relazione $\geq$ sugli interi.

Definiamo la relazione di *validità di una formula F in una struttura $\mathcal{A}$*, che denotiamo con $\mathcal{A} \models F$.
Un *assegnamento* α in $\mathcal{A}$ è una mappa che associa ad ogni variabile un elemento di A, i.e.,

$$\alpha : \{v_n \,:\, n \in \mathbf{N}\} \longrightarrow A$$

Un assegnamento si estende in modo univoco ai termini ponendo $\alpha(c)$ uguale a $c^{\mathcal{A}}$ (ossia: l'interpretazione di una costante in una struttura è, per l'appunto, costante). Indichiamo con $\alpha\binom{x}{a}$ l'assegnamento che differisce da α solo perché associa l'elemento a alla variabile x.

Definiamo la relazione $\mathcal{A} \models F[\alpha]$, che intuitivamente significa: la formula F è soddisfatta nella struttura $\mathcal{A}$ relativamente all'assegnamento α.

Definizione 3.3 (Soddisfazione)**.** Definiamo la relazione $\mathcal{A} \models F[\alpha]$ come segue, per induzione sulla complessità di F.
$\mathcal{A} \models R(t_1, \ldots, t_k)[\alpha]$ se e solo se $(\alpha(t_1), \ldots, \alpha(t_k)) \in R^{\mathcal{A}}$.
$\mathcal{A} \models \neg G[\alpha]$ se e solo se non vale $\mathcal{A} \models G[\alpha]$.
$\mathcal{A} \models (G \wedge H)[\alpha]$ se e solo se $\mathcal{A} \models G[\alpha]$ e $\mathcal{A} \models H[\alpha]$.
$\mathcal{A} \models (G \vee H)[\alpha]$ se e solo se $\mathcal{A} \models G[\alpha]$ o $\mathcal{A} \models H[\alpha]$.
$\mathcal{A} \models (G \to H)[\alpha]$ se e solo se: se $\mathcal{A} \models G[\alpha]$ allora $\mathcal{A} \models H[\alpha]$.
$\mathcal{A} \models (\exists v G)[\alpha]$ se e solo se esiste $a \in A$ tale che $\mathcal{A} \models G[\alpha\binom{v}{a}]$.
$\mathcal{A} \models (\forall v G)[\alpha]$ se e solo se per ogni $a \in A$ vale $\mathcal{A} \models G[\alpha\binom{v}{a}]$.

Esempio 3.4. Sia $\mathcal{L} = \{c_0, c_1, P, R\}$ con P a un posto e R a due posti. Sia $F(x)$ la formula $\exists y(R(x, y)$. Consideriamo la struttura $\mathcal{N}$ con dominio $\mathbf{N}$ che interpreta la costante c_0 nel numero 0 la costante c_1 nel numero 1, il simbolo P con l'insieme dei numeri pari, il simbolo R con la relazione $<$ (la normale relazione d'ordine stretto sui numeri naturali). Svolgendo la definizione abbiamo: $\mathcal{N} \models F(x)[\alpha]$ se e solo se esiste $n \in \mathbf{N}$ tale che $\mathcal{N} \models R(x, y)[\alpha\binom{y}{n}]$ se e solo se $\alpha(x)$ è minore stretto di n. Dunque $\mathcal{N} \models F(x)[\alpha]$ se e solo se $\alpha(x)$ è maggiore di 0.

Osservazione 3.5. Il fatto che valga $\mathcal{A} \models F[\alpha]$ o no dipende soltanto dai valori di α sulle variabili libere che appaiono in F. In altre parole, se le variabili libere di F sono contenute in $\{x_1, \ldots, x_n\}$ e α e β sono due assegnamenti che coincidono sui valori assegnati alle variabili $x_1, \ldots, x_n$, allora $\mathcal{A} \models F[\alpha]$ se e solo se $\mathcal{A} \models F[\beta]$. Pertanto possiamo scrivere $\mathcal{A} \models F[\alpha(x_1), \ldots, \alpha(x_n)]$ indicando esplicitamente gli elementi assegnati alle variabili che contano. Da questa osservazione segue anche che se F è un enunciato, allora $\mathcal{A} \models F[\alpha]$ vale per tutti gli assegnamenti o per nessuno!

Esempio 3.6. Sia $\mathcal{L} = \{c, R\}$ dove R un simbolo di relazione binaria. Sia F l'enunciato $\forall x \forall y(R(x, y) \to \exists z(R(x, z) \wedge R(z, y)))$. Sia $\mathcal{A}$ la struttura con dominio $\mathbb{Z}$, che interpreta c in 0 e R nella relazione d'ordine $<$. $\mathcal{A} \models F[\alpha]$ se e solo se per ogni intero a se $R(\alpha(x), a)$ allora per esiste un intero b tale che $a < b$ e $b < a$. L'enunciato risulta dunque falso in $\mathbb{Z}$, ossia non vale $\mathbb{Z} \models F$. Se cambiamo struttura e consideriamo quella con dominio $\mathbf{Q}$ (i razionali), l'enunciato risulta vero (corrisponde al fatto che i razionali sono ordinati in modo denso).

Definizione 3.7 (Soddisfacibilità, Validità in una struttura)**.** Se $\mathcal{A} \models F[\alpha]$ per qualche assegnamento α, diciamo che α *soddisfa* l'enunciato F in $\mathcal{A}$, e in tal caso F è detta *soddisfacibile in* $\mathcal{A}$. Diciamo che una formula F è *vera in una struttura* se è soddisfatta da tutti gli assegnamenti su quella struttura. In questo caso scriviamo $\mathcal{A} \models F$.

Osservazione 3.8. Una formula F è vera in una struttura se e solo se l'enunciato

$$\forall x_1 \ldots \forall x_n F(x_1, \ldots, x_n),$$

è vero nella struttura, dove $x_1, \ldots, x_n$ sono tutte e sole le variabili libere di F

Di fatto ci basta ragionare sulla validità di enunciati (ossia formule senza variabili libere). In ogni struttura data, un enunciato è soddisfatto da tutti gli assegnamenti o da nessuno.

Definizione 3.9 (Validità)**.** Un enunciato E è *valido* se è vero in tutte le strutture, ossia

$$\text{per ogni } \mathcal{A} \text{ vale } \mathcal{A} \models E$$

Diciamo anche che è una *verità logica* e scriviamo $\models E$. Dualmente un enunciato E è insoddisfacibile se non esiste nessuna strtuttura in cui è vero, ossia

$$\text{per ogni } \mathcal{A} \text{ non vale } \mathcal{A} \models E.$$

Occasionalmente parleremo di validità di una formula (non di un enunciato) intendendo che la formula è vera in ogni struttura rispetto a ogni assegnamento.

Osservazione 3.10. Si osserva che un enunciato F è valido se e solo se $\neg F$ non è soddisfacibile. Dalla definizione di $\models$ segue che, per un enunciato E, $\mathcal{A} \models E$ non vale se e solo se $\mathcal{A} \models \neg E$.

Definizione 3.11 (Conseguenza logica, Equivalenza logica)**.** Siano $F_1, \ldots, F_n, F$ enunciati. Diciamo che F è una *conseguenza (logica)* di $F_1, \ldots, F_n$ se per ogni struttura $\mathcal{A}$, tale che

$$\mathcal{A} \models F_1;\ \mathcal{A} \models F_2, \ldots, \mathcal{A} \models F_n$$

vale anche

$$\mathcal{A} \models F.$$

In tal caso scriviamo $F_1, \ldots, F_n \models F$. Due formule F, G sono *logicamente equivalenti* se $F \models G$ e $G \models F$. In tal caso scriviamo $F \equiv G$.

Vale in logica predicativa un teorema analogo a quello visto per la logica proposizionale:

Teorema 3.12. *Siano $F_1, \ldots, F_n, F$ enunciati in un linguaggio predicativo. I tre punti seguenti sono equivalenti:*

(1) $F_1, \ldots, F_n \models F$
(2) $(F_1 \wedge \cdots \wedge F_n) \to F$ *è valida*
(3) $(F_1 \wedge \cdots \wedge F_n \wedge \neg F)$ *non è soddisfacibile.*

All'inizio della storia della logica matematica la domanda fondamentale era: esiste un algoritmo per risolvere i problemi di conseguenza logica (o validità o insoddisfacibilità) qui sopra formulati, per arbitrari linguaggi predicativi? Questo problema, posto dal matematico David Hilbert come problema del secolo per il secolo XX e noto come Problema della Decisione, motivò Alan Turing a sviluppare il modello astratto di calcolatore universale noto come macchina di Turing.

Mentre nel caso proposizionale il problema può essere risolto da una macchina ma non è noto se possa essere risolto da una macchina in modo efficiente (problema $\mathbf{P} = \mathbf{NP}$, problema del Millennio per XXI secolo), nel caso della logica predicativa la situazione è più complessa: Alan Turing ha infatti dimostrato (nel 1936) che non esiste un algoritmo che risolve il Problema della Decisione. Per ottenere questa risposta negativa Turing ha posto le basi dell'informatica moderna, proponendo con le macchine di Turing il primo modello matematico rigoroso e soddisfacente della nozione di *algoritmo*. Numerosi casi particolari del Problema della Decisione (ristretti a classi di formule particolarmente semplici o a linguaggi particolarmente semplici) ammettono soluzioni algoritmiche che sono alla base di numerosi software di ragionamento automatico o verifica automatica di sistemi usati in numerose aree dell'Informatica.

4. Proprietà fondamentali dei quantificatori

Analogamente a quanto visto in logica proposizionale possiamo stabilire che due enunciati sono equivalenti se e solo se sono soddisfatti esattamente dalle stesse strutture: $E \equiv G$ se e solo se per ogni struttura $\mathcal{A}$, se $\mathcal{A} \models E$ allora $\mathcal{A} \models G$ e viceversa. Il che equivale a dire che $E \equiv G$ se e solo se $E \leftrightarrow G$ è valida. Possiamo estendere la notazione a formule, intendendo che $E \equiv G$.

Dimostriamo le seguenti equivalenze logiche fondamentali riguardanti i quantificatori.

$$\begin{gathered}
\exists x(F \vee G) \equiv \exists x F \vee \exists x G \\
\forall x(F \wedge G) \equiv \forall x F \wedge \exists x G \\
\neg\exists x \neg F \equiv \forall x F \\
\neg\forall x \neg F \equiv \exists x F \\
\neg\exists x F \equiv \forall x \neg F \\
\neg\forall x F \equiv \exists x \neg F \\
\exists x \exists y F \equiv \exists y \exists x F \\
\forall x \forall y F \equiv \forall y \forall x F
\end{gathered}$$

Se x non appare in F,

$$\begin{gathered}
F \vee \exists x G \equiv \exists x(F \vee G), \quad F \wedge \exists x G \equiv \exists x(F \wedge G) \\
F \wedge \forall x G \equiv \forall x(F \wedge G), \quad F \vee \forall x G \equiv \forall x(F \vee G)
\end{gathered}$$

Dimostriamo la prima equivalenza. Cominciamo col dimostrare il primo verso, ossia

$$\models \exists x(F \vee G) \to \exists x F \vee \exists x G$$

Dobbiamo dimostrare che, per ogni struttura $\mathcal{A}$, per ogni assegnamento α in A, se $\mathcal{A} \models \exists x(F \vee G)[\alpha]$ allora allora $\mathcal{A} \models (\exists x F \vee \exists x G)[\alpha]$. Sia α un assegnamento tale che $\mathcal{A} \models \exists x \exists x(F \vee G)[\alpha]$. Per definizione esiste $a \in A$ tale che $\mathcal{A} \models (F \vee G)[\alpha\binom{x}{a}]$. Per definizione $\mathcal{A} \models (F \vee G)[\alpha\binom{x}{a}]$ è vero se e solo se $\mathcal{A} \models F[\alpha\binom{x}{a}]$ oppure $\mathcal{A} \models G[\alpha\binom{x}{a}]$. Ma allora esiste un $a \in A$ tale che $\mathcal{A} \models F[\alpha\binom{x}{a}]$ oppure esiste un $a \in A$ tale che $\mathcal{A} \models G[\alpha\binom{x}{a}]$. Dunque per definizione $\mathcal{A} \models (\exists x F)[\alpha]$ oppure $\mathcal{A} \models (\exists x G)[\alpha]$. Dunque $\mathcal{A} \models (\exists x F \vee \exists x G)[\alpha]$

Dimostriamo ora il secondo verso, ossia

$$\models \exists x(F \vee G) \to \exists x F \vee \exists x G.$$

Dobbiamo dimostrare che, per ogni struttura $\mathcal{A}$, per ogni assegnamento α, se $\mathcal{A} \models (\exists x F \vee \exists x G)[\alpha]$ allora vale $\mathcal{A} \models \exists x(F \vee G)[\alpha]$. Supponiamo l'antecedente e dimostriamo il conseguente. Sia α un assegnamento tale che $\mathcal{A} \models (\exists x F \vee \exists x G)[\alpha]$. Per definizione questo significa che $\mathcal{A} \models (\exists x F)[\alpha]$ oppure $\mathcal{A} \models (\exists x G)[\alpha]$. Dunque o esiste $a \in A$ tale che $\mathcal{A} \models F[\alpha\binom{x}{a}]$ oppure esiste $a \in A$ tale che $\mathcal{A} \models G[\alpha\binom{x}{a}]$. Dunque in ogni caso esiste un $a \in A$ tale che $\mathcal{A} \models (F \vee G)[\alpha\binom{x}{a}]$. Per definizione questo significa che $\mathcal{A} \models (\exists x)(F \vee G)[\alpha]$.

Tutte le altre equivalenze si dimostrano in modo analogo applicando la definizione di soddisfacibilità.

Come dimostrare che una certa formula non è una verità logica? Occorre esibire una struttura e un assegnamento che non la soddisfa. Facciamo un esempio. Dimostriamo che il seguente enunciato non è una verità logica.

$$\forall x \exists y R(x, y) \to \exists y \forall x R(x, y)$$

Esibiamo una struttura che soddisfa l'antecedente ma non il conseguente. Consideriamo la struttura $\mathcal{N}$ con dominio $\mathbf{N}$ in cui il simbolo R è interpretato come la relazione d'ordine tra i naturali, $<$.

$$\mathcal{N} \models \forall x \exists y R(x, y)$$

perché per ogni $n \in \mathbf{N}$ esiste $m \in \mathbf{N}$ tale che $\mathcal{N} \models R(x, y)[\binom{x}{n}\binom{y}{m}]$, ossia per ogni $n \in \mathbf{N}$ esiste $m \in \mathbf{N}$ tale che $n < m$. D'altra parte però $\mathcal{N}$ non soddisfa il conseguente, perché è falso che per esiste $n \in \mathbf{N}$ tale che per ogni $m \in \mathbf{N}$ vale $n > m$.

A volte per dimostrare che un enunciato è una verità logica è comodo ragionare per assurdo e ragionare su una struttura che verifica la negazione dell'enunciato. Facciamo un esempio. Dimostriamo che

$$\models \neg \exists x \forall y (S(x, y) \leftrightarrow \neg S(y, y))$$

Supponiamo per assurdo che l'enunciato non è una verità logica. Allora esiste una struttura $\mathcal{A}$ in cui l'enunciato è vero. La struttura $\mathcal{A}$ avrà un certo dominio $A \neq \emptyset$ e una relazione binaria $S^{\mathcal{A}} \subseteq A \times A$ per interpretare il simbolo S, e stiamo supponendo che

$$\mathcal{A} \models \exists x \forall y (S(x, y) \leftrightarrow \neg S(y, y)).$$

Questo è vero se e solo se esiste $a \in A$ tale che per ogni $b \in A$ $(a, b) \in S^{\mathcal{A}}$ (i.e., a e b stanno nella relazione con cui $\mathcal{A}$ interpreta il simbolo S) se e solo se $(b, b) \notin S^{\mathcal{A}}$. Sia a_0 un tale $a \in A$. Allora

$$\text{per ogni } b \in A \text{ vale che } (a_0, b) \in S^{\mathcal{A}} \text{ se e solo se } (b, b) \notin S^{\mathcal{A}}.$$

Chiediamoci se, in particolare, valga $(a_0, a_0) \in S^{\mathcal{A}}$ o meno (dopotutto a_0 è uno dei possibili b). Se $(a_0, a_0) \in S^{\mathcal{A}}$ allora $(a_0, a_0) \notin S^{\mathcal{A}}$ (perché l'implicazione vale per ogni $b \in A$, incluso a_0). Se invece $(a_0, a_0) \notin S^{\mathcal{A}}$, allora $(a_0, a_0) \in S^{\mathcal{A}}$. L'esistenza di a_0 è dunque contraddittoria. Concludiamo che l'enunciato di partenza è una verità logica.