Metodi matematici per l'informatica

Leonardo Ganzaroli

Indice

Introduzione

Questi appunti sono derivanti principalmente dalle dispense del corso di *Metodi matematici per l'informatica* che ho seguito durante la laurea Triennale di informatica all'università "La Sapienza".

1 Richiami sugli insiemi

1. Un insieme è una collezione di elementi
2. Un insieme può essere definito in 2 modi:
   - Per elencazione
     $X = \{1, 3, x, @\}$
   - Per proprietà caratteristica
     $Y = \{x \mid x \text{ è una casa}\}$
3. La cardinalità di un insieme è il numero di elementi che esso contiene
4. Se un insieme ha cardinalità finita allora è detto "finito"
5. L'insieme vuoto si indica con $\emptyset$
6. L'insieme potenza di un certo insieme è l'insieme dei suoi sottoinsiemi
7. Il prodotto cartesiano di 2 insiemi è l'insieme delle coppie ordinate (x, y) con x appartenente al primo insieme e y al secondo

Le operazioni tra insiemi (dati A e B):

- **Unione** $(A \cup B)$ = L'insieme contenente tutti gli elementi di A e di B
- **Intersezione** $(A \cap B)$= L'insieme contenente gli elementi comuni di A e di B
- **Differenza** $(A \setminus B)$ = L'insieme contenente gli elementi di A che non appartengono a B

Le relazioni tra insiemi (dati A e B):

- **Inclusione** $(A \subseteq B)$ = A è un sottoinsieme di B, ossia B contiene tutti gli elementi di A
- **Inclusione propria** $(A \subset B)$ = Come sopra ma B contiene elementi aggiuntivi non presenti in A
- 2 insiemi si dicono **Coincidenti** ($A \subseteq B$ e $B \subseteq A$) se sono lo stesso insieme, ossia hanno gli stessi elementi
- 2 insiemi si dicono **Disgiunti** $(A \cap B = \emptyset)$ se non hanno nessun elemento in comune

2 Combinatoria

Per combinatoria si intende lo studio del contare gli insiemi finiti, risponde a domande del tipo:

- Quanti numeri primi esistono tra 1 e 1 milione?
- Quante targhe è possibile formare nel sistema attualmente in uso in Italia?
- Quanti sono gli esiti del lancio di 2 dadi a 6 facce?
- ...

2.1 Principio moltiplicativo

Definizione Se scelgo un primo oggetto tra a disponibili, un secondo tra b, un terzo tra c, ..., un ultimo tra z allora ho:

$$a \times b \times c \times \ldots \times z \quad \text{possibili scelte}$$

Esempio:

A una gara di corsa partecipano 8 atleti. Quanti sono i possibili ordini di arrivo, assumendo che tutti arrivino al traguardo e che non vi siano arrivi simultanei?

Applicando il principio ottengo $8 * 7 * 6 * 5 * 4 * 3 * 2 * 1 = 40320$

2.2 Principio additivo

Definizione Per contare gli oggetti che soddisfano un certo vincolo posso:

1. Trovare delle categorie non sovrapposte che descrivano la totalità degli oggetti con quel vincolo
2. Dividere gli oggetti nelle categorie
3. Sommare il numero di oggetti in ciascuna categoria

Si può riformulare anche dal punto di vista insiemistico.

Definizione Sia A un insieme e $T_1, T_2, \ldots, T_k$ una partizione di A, si ha:

$$\#A = \#T_1 + \#T_2 + \ldots + \#T_k$$

Esempio:

In una gara di 8 atleti di cui 2 italiani, 3 francesi e 3 spagnoli, quanti sono gli ordini di arrivo in cui i primi tre atleti hanno nazionalità diverse?

Trovo i possibili casi esclusivi:

1. **IFS** = {ordini di arrivo con un Italiano primo, un Francese secondo e uno Spagnolo terzo}
2. **ISF** = {ordini di arrivo con un Italiano primo, uno Spagnolo secondo e un Francese terzo}
3. **FIS** = {ordini di arrivo con un Francese primo, un Italiano secondo e uno Spagnolo terzo}
4. **FSI** = ...
5. **SIF** = ...
6. **SFI** = ...

Posso adesso calcolare il risultato sommando le cardinalità degli insiemi.

2.3 Figure

Avendo visto i 2 principi base possiamo adesso passare alle *figure* ricorrenti della combinatoria.

2.3.1 Disposizioni con ripetizione

Definizione Una disposizione con ripetizione di ordine k di n oggetti è una sequenza ordinata di k oggetti scelti tra gli n totali.

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

Esempio: Le possibili parole di lunghezza 5 dell'insieme {a,b,c} sono $D'_{3,5} = 3^5$

2.3.2 Disposizioni semplici

Definizione Dato $1 \leq k \leq n$. Una disposizione semplice di ordine k di n oggetti è una sequenza ordinata di k oggetti distinti scelti tra gli n totali.

$$D_{n,k} = n \times (n-1) \times (n-2) \times \ldots \times (n-(k-1)) = \frac{n!}{(n-k)!}$$

Esempio:

Se ad un torneo partecipano 8 squadre scelte tra 15 e l'ordine di partenza è a sorte, quanti sono i possibili schieramenti di partenza?

Soluzione $= D_{15,8} = \frac{15!}{(15-8)!} = \frac{15!}{7!}$

2.3.3 Permutazioni

Se una disposizione semplice ha $n = k$ si parla di permutazione: $P_n = D_{n,n} = n!$

2.3.4 Anagrammi

Gli anagrammi sono un caso particolare di disposizione in cui ci sono dei "gruppi" di lettere ripetute.

$$\#A = \frac{n!}{n_1!n_2!n_3!\dots}$$

Esempio: Gli anagrammi della parola MISSISSIPPI sono $\frac{11!}{4!4!2!}$

2.3.5 Combinazioni semplici

Definizione Le combinazioni semplici di ordine k su n sono i sottoinsiemi di k elementi scelti in un insieme di n elementi.

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

Esempio:

Dato $A = \{a, b, c, d\}$ calcolare il numero di sottoinsiemi di 3 elementi.

Soluzione $= \binom{4}{3} = 4$

Un caso specifico è quello in cui ci si trova con la formula $\binom{n}{m} \times m$, infatti essa risulta equivalente alla formula $n \times \binom{n-1}{m-1}$.

Data la sua definizione si può trovare la seguente correlazione tra l'insieme potenza e le possibili combinazioni dello stesso insieme:

$$\text{Dato A insieme e } n = \#A \text{ si ha } \sum_{x=0}^{n} \binom{n}{x} = \#P(A)$$

2.3.6 Combinazioni con ripetizioni

Definizione Le combinazioni con ripetizione di ordine k di n oggetti sono un raggruppamento di k oggetti scelti tra n elementi con possibili ripetizioni.

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

2.3.7 Principio di inclusione-esclusione

Si possono presentare dei casi in cui sia necessario usare il principio additivo ma non è possibile creare dei tipi mutualmente esclusivi, in questo caso si andrebbero a contare degli elementi più di una volta portando ad un risultato sbagliato.

Per ovviare al problema vanno rimossi gli elementi comuni per non contarli più volte:

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

Nel caso siano 3 insiemi va reinserita la parte comune a tutti e 3, altrimenti resterà fuori dalla somma:

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

Più in generale vanno aggiunte le operazioni con numero di elementi dispari e tolte quelle con numero di elementi pari.

3 Relazioni

Definizione Siano A e B due insiemi. Una relazione R tra A e B è un sottoinsieme del prodotto cartesiano $A \times B$.

Per indicare che 2 elementi sono in relazione tra loro si può scrivere $R(a, b)$ oppure aRb.

3.1 Rappresentazione

Per rappresentare graficamente una relazione ho 2 alternative:

1. **Matrice**

   Si utilizza una matrice in cui il valore di una singola cella è descritto da:

$$m_{ij} = \begin{cases} 1 & \text{se } (a_i, b_j) \in R \\ 0 & \text{se } (a_i, b_j) \notin R \end{cases}$$

Esempio:

Siano $A = \{1, 2, 3, 4\}$ e $R = \{(1, 2), (2, 4), (3, 2), (4, 2), (4, 4)\}$.

$$M_R = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

---

2. **Grafo diretto**

   A SX gli elementi del primo insieme, a DX quelli del secondo, disegno una freccia da SX a DX solo se quella coppia è nella relazione.

Esempio:

Siano $A = \{a, b, c, d, e\}$, $B = \{1, 2, 3, 4, 5\}$ e $R = \{(a, 2), (b, 4), (c, 2), (e, 1), (e, 4)\}$.

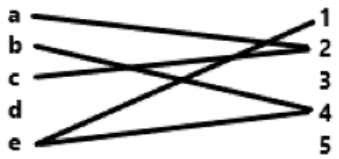

Figura 1: Grafo diretto

3.2 Inversa

Definizione Data una relazione $R \subseteq A \times B$. Si definisce R^{-1} (inversa di R) il sottoinsieme di $B \times A$ tale che:

$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

3.3 Composizione

Definizione Date $R \subseteq A \times B$ e $S \subseteq B \times C$. Si definisce composizione di R ed S $(S \circ R)$ la relazione tra A e C in cui:

$$(a, c) \in (S \circ R) \text{ con } a \in A,\ c \in C \iff \exists b \in B \mid aRb \text{ e } bSc$$

3.4 Rel. transitive

Definizione Una relazione $R \subseteq A \times A$ è transitiva se:

$$\forall\ a, b, c \in A \quad aRb \text{ e } bRc \ \Rightarrow\ aRc$$

3.4.1 Chiusura transitiva

Definizione La chiusura transitiva di una relazione R è la più piccola relazione transitiva che estende R (definita R^T) tale che:

1. $R \subseteq R^T$
2. R^T è transitiva
3. Se S estende R ed è transitiva allora $R^T \subseteq S$

Estendendo il discorso si può definire una relazione di raggiungibilità definita come:

$$R^C = \{(a, b) \in A \times A \mid \exists \text{ un cammino di lunghezza} \geq 1 \text{ da } a \text{ verso } b\}$$

3.5 Rel. di equivalenza

Definizione Una relazione $R \subseteq A \times A$ è detta di equivalenza se gode di queste proprietà:

- **Riflessività** $\forall\ a \in A \quad aRa$
- **Simmetria** $\forall\ a, b \in A \quad aRb \ \Rightarrow\ bRa$
- **Transitività** (Vista prima)

Definizione La classe di equivalenza di un elemento di A è definita come:

$$[a]_R = \{b \in A \mid aRb\}$$

Inoltre:

- $\forall\ a \in A \quad [a]_r \neq \emptyset$
- $\forall\ a, b \in A \quad [a]_r \ \cap\ [b]_r = \emptyset$ oppure $[a]_r = [b]_r$

Questo dimostra che ogni relazione di equivalenza su un insieme crea una partizione di quell'insieme.

Posso formulare la partizione come:

$$\{C_i \mid i \in I\} \text{ con } I = \text{insieme di indici qualunque, } C_i \neq \emptyset \text{ e } C_i \subseteq A$$

Valgono:

1. $\forall\ a \in A\ \ \exists i \in I \mid a \in C_i$
2. $\forall\ i, j \in I\ \ i \neq j\ \Rightarrow\ C_i\ \cap\ C_j = \emptyset$

3.6 Rel. d'ordine

Definizione Una relazione $R \subseteq A \times A$ è detta di ordine parziale se gode di queste proprietà:

- **Riflessività** (Vista prima)
- **Antisimmetria** $\forall\ a, b \in A\ \ aRb$ e $bRa\ \Rightarrow\ a = b$
- **Transitività** (Vista prima)
- **Totalità** (Se vale questa proprietà la relazione è d'ordine totale)
  $\forall\ a, b \in A\ \ a \leq b$ oppure $b \leq a$

In caso di ordini parziali finiti posso rappresentare graficamente la relazione con il diagramma di Hasse.

Esempio:

Diagramma della relazione d'ordine "$\leq$" nell'insieme dei divisori del 60.

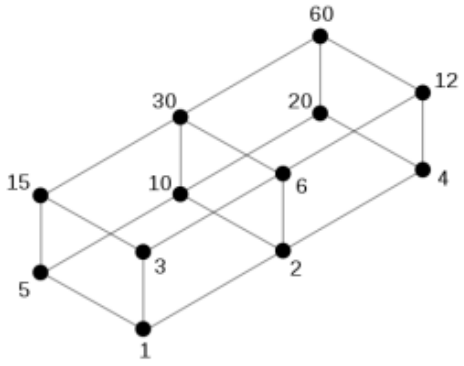

Figura 2: Diagramma di Hasse

Partendo da una relazione parziale R è possibile trovare una relazione totale R^* che va ad estenderla, basta che siano presenti nella nuova relazione:

- Le coppie (a, b) incomparabili di R
- Tutte le coppie (x, y) tali che xRa o bRy

4 Funzioni

Definizione Una funzione è una relazione tra due insiemi che associa ad ogni elemento del dominio (il primo insieme) un solo elemento del codominio (il secondo insieme):

$$f \colon A \to B$$

Dato un elemento x del dominio che la funzione associa all'elemento y del codominio si dice che:

- y è l'immagine di x via f
- x è la pre-immagine di y via f

4.1 Tipi

- **Iniettiva**

  Una funzione è iniettiva se $\forall\ x, y \in$ Dominio $\ f(x) = f(y) \ \Rightarrow \ x = y$

- **Suriettiva**

  Una funzione è suriettiva se $\forall\ y \in$ Codominio $\ \exists x \in$ Dominio $\mid f(x) = y$

- **Biunivoca**

  Una funzione è biunivoca se è sia iniettiva che suriettiva

4.2 Composizione

Definizione Siano $f : X \to Y$ e $g : Y \to Z$. La funzione composta di f e g $(g \circ f)$ è definita come:

$$h : X \to Z,\ h(x) = g(f(x))$$

N.B. Questa operazione non è commutativa.

4.3 Identità

Definizione La funzione identità è quella che associa ad ogni elemento l'elemento stesso (ovviamente dominio e codominio sono uguali).

Si indica con $\mathrm{id}_{NOME\_INSIEME}$.

4.4 Inversa

Definizione Sia $f: X \to Y$ una funzione. Un'altra funzione $g: Y \to X$ si dice inversa di f se:

1. $(g \circ f)$ è l'identità su X
2. $(f \circ g)$ è l'identità su Y

La funzione inversa di f si denota con f^{-1}.

Una funzione è invertibile solo se è biunivoca.

5 Cardinalità degli insiemi

Si possono adesso legare le cardinalità degli insiemi alle funzioni tra di essi, dati A e B:

- Se esiste una funzione iniettiva tra i due allora $\#A \leq \#B$
- Se esiste una funzione iniettiva tra i due allora $\#A \geq \#B$
- Se esiste una funzione biunivoca tra i due allora $\#A = \#B$

5.1 Insiemi numerabili

Viene definito numerabile un insieme finito oppure per cui esiste una funzione biunivoca con $\mathbb{N}$ (in questo caso si dice infinito numerabile).

5.2 Insiemi non numerabili

Rientrano in questa categoria tutti gli insiemi per cui non esiste una funzione biunivoca con $\mathbb{N}$.

6 Induzione

Il principio d'induzione serve a dimostrare che se una proprietà vale per il numero 0/1 allora vale per ogni numero n.

Il procedimento è composto da 2 passi:

1. **Base**

   Verificare che la proprietà valga per 0/1

2. **Passo induttivo**

   Assumendo che la proprietà sia valida per un numero n dimostrare che è valida anche per $n + 1$

Esempio:

Dimostrare che $\sum_{x=0}^{n} x = \frac{n(n+1)}{2}$.

1. **Base**

   Se $n = 1$ risulta $\frac{1(1+1)}{2} = 1$, quindi è vero

2. **Passo induttivo**

   Dando per buona la formula per n devo dimostrare che $1 + 2 + \ldots + n + n + 1 = \frac{(n+1)(n+2)}{2}$.

   Si può notare che la somma fino ad n si può trasformare in $\frac{n(n+1)}{2}$, che sappiamo essere corretta.

   Si ottiene quindi $\frac{n(n+1)}{2}+n+1$ che con qualche passaggio diventa $\frac{(n+1)(n+2)}{2}$.

   Questa proprietà risulta quindi vera.

Si puo anche generalizzare e dimostrare che una proprietà valga dal numero k in poi:

1. **Base**

   Verificare che la proprietà valga per k

2. **Passo induttivo**

   Assumendo che la proprietà sia valida per un numero $n \geq k$ dimostrare che è valida anche per $n + 1$

6.1 Induzione forte

Una variante del principio d'induzione in cui si lavora con gli insiemi, se un insieme X ha queste caratteristiche:

1. Contiene 1/0
2. Se contiene tutti i numeri minori di un certo $n \geq 1$ allora contiene anche $n + 1$

Si può concludere che $X = \mathbb{N}$

6.2 Principio del minimo intero

Definizione Ogni sottoinsieme non vuoto dei numeri naturali ha un minimo.

Questo principio è essenzialmente una formulazione alternativa di quello d'induzione.

7 Logica proposizionale

La logica proposizionale si occupa delle proprietà dei costrutti logici usati nei linguaggi formali, tra questi ci sono quello naturale e quelli usati nelle scienze e nella matematica.

Nel nostro caso i costrutti logici sono:

- Il **non**
- L'**oppure**
- L'**e**
- Il **se . . . allora**
- Il **se e solo se**

7.1 Alfabeto e proposizioni

L'alfabeto della logica è formato da:

- Un insieme numerabile di simboli di proposizione ($\mathrm{VAR}_{\mathcal{L}}$)
- Le parentesi tonde
- I connettivi logici $\iff, \Rightarrow, \neg, \vee, \wedge$

Le **f**ormule **b**en **f**ormulate (o sintatticamente corrette) sono definite ricorsivamente nel seguente modo:

1. Un simbolo di proposizione è una *fbf*
2. Se A è una *fbf* lo è anche $\neg(A)$
3. Se A e B sono *fbf* lo sono anche $(A \wedge B), (A \vee B), (A \Rightarrow B), (A \iff B)$

7.2 Semantica

Un assegnamento è una funzione definita come:

$$v : \mathrm{VAR}_{\mathcal{L}} \to \{1, 0\}, \quad \text{con } \{1, 0\} \text{ detti valori di verità}$$

Il discorso si può estendere a tutte le *fbf* creando delle regole che permettono di calcolare il valore in maniera ricorsiva (chiamo questa funzione v'):

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

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

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

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

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

7.3 Tavole di verità

Le tavole di verità permettono di organizzare i possibili valori di una proposizione sottoforma di tabella.

Esempio:

$((P \vee Q) \Rightarrow (R \vee (R \Rightarrow Q)))$

P	Q	R	$R \Rightarrow Q$	$R \vee (R \Rightarrow Q)$	$P \vee Q$	Valore completo
0	0	0	1	1	0	1
0	0	1	0	1	0	1
0	1	0	1	1	1	1
0	1	1	1	1	1	1
1	0	0	1	1	1	1
1	0	1	0	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

Tabella 1: Tavola di verità

7.4 Definizioni varie

Definizione Una proposizione A è soddisfacibile se esiste un assegnamento tale che $v(A) = 1$.

Definizione Siano F un insieme di proposizioni ed $A \in F$. A è conseguenza logica di F se ogni assegnamento che soddisfa tutti gli altri elementi di F soddisfa anche A.

In questo caso si scrive $A1, \ldots, An \models A$.

Definizione Una proposizione A è detta tautologia se per ogni assegnamento $v(A) = 1$.

7.5 Espressività

Per verificare la validità di un/una argomento/proposizione si può sfruttare la conseguenza logica, in particolare ci sono 3 modi:

1. Verificare se un assegnamento soddisfa la conseguenza logica
2. Verificare che $(A_1 \wedge \ldots \wedge A_n) \Rightarrow A$ sia una tautologia
3. Verificare che $A_1 \wedge \ldots \wedge A_n \wedge \neg(A)$ sia insoddisfacibile

7.6 Equivalenza logica

Definizione Due formule A, B sono logicamente equivalenti se per ogni assegnamento α $\alpha(A) = \alpha(B)$, si scrive $A \equiv B$.

Si possono adesso enunciare alcune formule rapide:

Nome	Teorema	Duale
Identità	$B \wedge 1 = B$	$B \vee 0 = B$
Elemento nullo	$B \wedge 0 = 0$	$B \vee 1 = 1$
Idempotenza	$B \wedge B = B$	$B \vee B = B$
Involuzione	$B = \neg(\neg(B))$	
Complemento	$B \wedge \neg(B) = 0$	$B \vee \neg(B) = 1$
Commutatività	$B \wedge C = C \wedge B$	$B \vee C = C \vee B$
Associatività	$B \wedge (C \wedge D) = (B \wedge C) \wedge D$	$B \vee (C \vee D) = (B \vee C) \vee D$
Distributività	$B \wedge (C \vee D) = (B \wedge C) \vee (B \wedge D)$	$B \vee (C \wedge D) = (B \vee C) \wedge (B \vee D)$
Assorbimento	$B \wedge (B \vee C) = B$	$B \vee (B \wedge C) = B$
Combinazione	$(B \wedge C) \vee (B \wedge \neg(C)) = B$	$(B \vee C) \wedge (B \vee \neg(C)) = B$
Consenso	$(B \wedge C) \vee (\neg(B) \wedge D) \vee (C \wedge D) = (B \wedge C) \vee (\neg(B) \wedge D)$	$(B \vee C) \wedge (\neg(B) \vee D) \wedge (C \vee D) = (B \vee C) \wedge (\neg(B) \vee D)$
De Morgan	$\neg(ABC\ldots) = \neg(A) \vee \neg(B) \vee \neg(C) \vee \ldots$	$\neg(A \vee B \vee C)\ldots = \neg(A)\neg(B)\neg(C)\ldots$

Tabella 2: Verità notevoli

7.7 Forma normale congiuntiva

Definizione Un letterale è un variabile proposizionale o una sua negazione.

Definizione Una formula è in forma normale congiuntiva se è una congiunzione di disgiunzioni di letterali:

$$\bigwedge_{i \leq n} \bigvee_{j \leq m} L_{i,j} = (L_{1,1} \vee L_{1,2} \vee \cdots \vee L_{1,m_1}) \wedge \cdots \wedge (L_{n,1} \vee L_{n,2} \vee \cdots \vee L_{n,m_n})$$

Una formula CNF si può scrivere come $C_1 \wedge C_2 \wedge \ldots$ con C_i detta **Clausola**, essa rappresenta una disgiunzione di letterali.

7.8 Risoluzione

Se ho un letterale l e 2 clausole C_1, C_2 tali che $l \in C_1$ e $\neg(l) \in C_2$ allora:

$$C_1, C_2 \models \text{Res}_l(C_1, C_2) = (C_1 - l) \cup (C_2 - \neg(l)) \text{ con Res() detto risolvente}$$

Se applico questo concetto ad una formula in CNF un numero finito di volte e alla fine ottengo la clausola vuota allora la formula è insoddisfacibile.

Esempio:

Data $\{\{\neg q, p\}, \{r, p\}, \{\neg p, \neg q\}, \{\neg p, s\}, \{q, \neg r\}, \{q, \neg r\}, \{q, \neg s\}\}$

$$\{\neg q, p\} \text{ e } \{\neg p, \neg q\} \rightarrow \{\neg q\}$$
$$\{\neg q\} \text{ e } \{q, \neg r\} \rightarrow \{\neg r\}$$
$$\{\neg r\} \text{ e } \{r, p\} \rightarrow \{p\}$$
$$\{p\} \text{ e } \{\neg p, s\} \rightarrow \{s\}$$
$$\{s\} \text{ e } \{q, \neg s\} \rightarrow \{q\}$$
$$\{q\} \text{ e } \{\neg q\} \rightarrow \text{ Niente}$$

La formula è insoddisfacibile.

7.9 Derivazione

Definizione Data F formula. Una sequenza ordinata $D_1, D_2, \ldots, D_{k-1}, D_k$ è una derivazione in Risoluzione di D_k se:

$$\forall\, i \in [1, k] \quad D_i \in F \text{ oppure } \exists j, h < i \mid D_i = \text{Res}_l(D_j, D_h) \text{ per qualche } l$$

Se esiste una derivazione della clausola C di F si scrive $F \vdash_{RES} C$, nel caso $D_n = \textit{Niente}$ la derivazione è una refutazione di F.

7.10 Algoritmo di decisione

Un algoritmo per decidere se una CNF è insoddisfacibile è il seguente:

Algorithm 1 $F \in$ UNSAT

while $\exists C_i, C_j \in F \mid Res_l(C_i, C_j) \notin F$ **do**
  $F = F \cup \{Res_l(C_i, C_j\}$
end while