Università degli Studi di Milano

Laurea in Sicurezza dei sistemi e delle reti informatiche

Note di Matematica

STEFANO FERRARI

Fondamenti di informatica per la sicurezza

Indice

1. Insiemistica

Un *insieme* è una collezione *arbitraria* di *elementi* reali o immaginari.
Esempi:

- $\{1, 2, 4, 7\}$ descrizione *intensionale*
- $\{x \mid x \leq 5\}$ descrizione *estensionale*

2. Varie

2.1 Alfabeto greco

alfa	beta	gamma	delta	epsilon	zeta	eta	theta	jota	kappa	lambda	mu (o mi)
α	β	γ	δ	ϵ (o ε)	ζ	η	θ (o ϑ)	ι	κ	λ	μ
A	B	Γ	Δ	E	Z	H	Θ	I	K	Λ	M

nu (o ni)	xi	omicron	pi	rho	sigma	tau	upsilon	phi	chi	psi	omega
ν	ξ	o	π	ρ	σ (o ς)	τ	υ	ϕ (o φ)	χ	ψ	ω
N	Ξ	O	Π	P	Σ	T	Y (o Υ)	Φ	X	Ψ	Ω

2.2 Quantificatori

Il simbolo $\forall$ (chiamato *quantificatore universale*) significa "per ogni". Viene usato per indicare tutti gli elementi di un insieme dato (o sottinteso dal contesto).

Il simbolo $\exists$ (chiamato *quantificatore esistenziale*) significa "esiste". Viene usato per affermare l'esistenza di almeno un elemento con una data proprietà. Talvolta il quantificatore esistenziale viene rafforzato dal simbolo ! ($\exists!$) per indicare che l'elemento esiste ed è unico.

Questi segni si premettono alle formule con variabili per segnalare che, nel raggio d'azione dei quantificatori, determinato dalle parentesi, le variabili stesse devono essere intese limitate dai quantificatori.

Per esempio, la formula $\forall x(x = 2k) \rightarrow \exists! y(y = 2k + 1)$ va letta: per ogni x pari a $2k$, esiste un unico y pari a $2k + 1$.

2.3 Arrotondamento

L'operatore $\lceil \cdot \rceil$ indica l'*arrotondamento per eccesso*. Con $\lceil x \rceil$ si indica il più piccolo intero maggiore o uguale a x.
Esempi:

- $\lceil 3.2 \rceil = 4$
- $\lceil 3 \rceil = 3$
- $\lceil -3.2 \rceil = -3$

L'operatore $\lfloor \cdot \rfloor$ indica l'*arrotondamento per difetto*. Con $\lfloor x \rfloor$ si indica il più grande intero minore o uguale a x.

Esempi:

- $\lfloor 3.2 \rfloor = 3$
- $\lfloor 3 \rfloor = 3$
- $\lfloor -3.2 \rfloor = -4$

2.4 Principio di induzione

La *dimostrazione per induzione* serve per dimostrare un teorema riferito ad una caratteristica enumerabile. Si dimostra prima la validità nel caso base (l'istanza del teorema che coinvolge il minimo numero di elementi), poi, ipotizzando che il teorema sia valido per il caso $n-1$, lo si dimostra valido per il caso n.

2.5 Sommatoria e produttoria

La somma o il prodotto di una sequenza di valori (i quali abbiano una formalizzazione comune) può essere indicata in modo sintetico tramite l'utilizzo degli operatori di sommatoria, $\sum$, e produttoria, $\prod$.
Per esempio, la somma dei primi 7 numeri pari si può indicare come:

$$\sum_{i=1}^{7} 2 \cdot i$$

Analogamente, il prodotto dei primi 9 numeri dispari si può indicare come:

$$\prod_{i=1}^{9} 2 \cdot i + 1$$

2.6 Fattoriale

L'operatore indicato con il simbolo ! si chiama *fattoriale* e assume la seguente forma:

$$n! = \begin{cases} 1 & n = 0 \\ 1 \cdot 2 \cdot \ \ldots \ \cdot (n-1) \cdot n = \prod_{i=1}^{n} i & n \geq 1 \end{cases} \tag{1}$$

2.7 Coefficiente binomiale

Il coefficiente binomiale $\binom{n}{k}$ è:

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!} \tag{2}$$

Il coefficiente binomiale deve il suo nome al fatto che trova impiego nella formula delle potenze del binomio:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \tag{3}$$

I valori del coefficiente binomiale si possono organizzare nel *Triangolo di Tartaglia* (o *di Pascal*):

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$
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

Esso può essere costruito sfruttando la proprietà descritta dalla equazione (7) nel seguito riportata.

Proprietà del coefficiente binomiale

$$\binom{n}{1} = n \tag{4}$$

$$\binom{n}{n} = 1 \tag{5}$$

$$\binom{n}{n-k} = \binom{n}{k} \tag{6}$$

$$\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1} \tag{7}$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{n-k} \tag{8}$$

$$\binom{n}{k+1} = \binom{n}{k} + \frac{n-k}{k+1} \tag{9}$$

3. Calcolo combinatorio

3.1 Permutazioni

Si chiamano *permutazioni* di n elementi distinti, tutti i raggruppamenti diversi che si possono formare con gli elementi dati, rispettando le seguenti proprietà:

1. ciascun raggruppamento contiene n elementi;
2. uno stesso elemento non può figurare più volte in un raggruppamento;
3. due raggruppamenti sono tra loro distinti se differiscono per l'ordine con cui sono disposti gli elementi.

n elementi danno luogo a $n!$ permutazioni:

$$P(n) = n!. \tag{10}$$

3.2 Disposizioni

Si dice *disposizione semplice* di n elementi distinti su k posizioni ($n, k \in \mathbb{N}, 0 < k \leq n$) una collezione di k degli n elementi che rispetti le seguenti proprietà:

1. ciascun raggruppamento contiene k elementi;
2. uno stesso elemento può figurare al più una volta in un raggruppamento;
3. due raggruppamenti sono da considerarsi distinti quando essi differiscono per almeno un elemento, o per l'ordine degli elementi.

Le disposizioni semplici di n elementi presi k per volta sono in totale $\frac{n!}{(n-k)!}$:

$$D(n,k) = \frac{n!}{(n-k)!} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1). \tag{11}$$

3.3 Disposizioni con ripetizione

Si dice *disposizione con ripetizione* (o *reimmissione*) di n elementi distinti su k (intero positivo) posizioni una collezione di k degli n elementi che rispetti le seguenti proprietà:

1. ciascun raggruppamento contiene k elementi;
2. due qualsiasi raggruppamenti sono da considerarsi distinti quando essi differiscono per almeno un elemento, o per l'ordine degli elementi.

Rispetto ad una disposizione semplice, quindi, in una disposizione con ripetizione ogni elemento può essere ripetuto.
Le disposizioni con ripetizione di n su k saranno:

$$D_r(n,k) = n^k. \tag{12}$$

3.4 Combinazioni

Si dice *combinazione semplice* di n elementi distinti su k posizioni ($n, k \in \mathbb{N}, 0 < k \leq n$) una collezione di k degli n elementi che rispetti le seguenti proprietà:

1. ciascun raggruppamento contiene k elementi;
2. uno stesso elemento può figurare al più una volta in un raggruppamento;
3. due raggruppamenti sono da considerarsi diversi soltanto quando differiscono tra loro almeno per un elemento.

L'ordine degli elementi non ha importanza in una combinazione.
Le combinazioni semplici di n elementi su k posti sono:

$$C(n,k) = \frac{D(n,k)}{P(k)} = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-k+1)}{k!}. \tag{13}$$

La quantità $\frac{n!}{(n-k)!\,k!}$ è il coefficiente binomiale di n *su* k, e viene indicato con:

$$\binom{n}{k}. \tag{14}$$

3.5 Combinazioni con ripetizione

Si dice *combinazione con ripetizione* (o con *reimmissione*) di n elementi distinti su k (intero positivo) posizioniuna collezione di k degli n elementi che rispetti le seguenti proprietà:

1. ciascun raggruppamento contiene k elementi;
2. due raggruppamenti sono da considerarsi diversi soltanto quando differiscono tra loro almeno per un elemento.

Uno stesso elemento può quindi comparire più di una volta.
Le combinazioni con ripetizione di n elementi su k posti sono:

$$C_r(n,k) = C(n+k-1,k) = \binom{n+k-1}{k}. \tag{15}$$

4. Logaritmi

Il logaritmo in base a di b, indicato con $\log_a b$, è quel numero x tale per cui $a^x = b$:

$$a^{\log_a b} = b \tag{16}$$

Proprietà

$$\log_a a^x = x \tag{17}$$

$$\log_a bc = \log_a b + \log_a c \tag{18}$$

$$\log_a \frac{b}{c} = \log_a b - \log_a c \tag{19}$$

$$\log_a b^c = c \log_a b \tag{20}$$

$$\log_a b = \frac{\log_c b}{\log_c a} \tag{21}$$