Teoremi di Fondamenti Matematici per l'Informatica

Carlo Ramponi

June 4, 2019

Contents

1 L'ordinamento dei numeri naturali è un buon ordinamento

Enunciato

L'ordinamento dei numeri naturali è un buon ordinamento

Dimostrazione

Supponiamo che l'insieme $A \subseteq \mathbb{N}$ non abbia minimo e proviamo che allora $A = \emptyset$. Chiamiamo B il suo complementare ($B = \mathbb{N} \setminus A$) e dimostriamo per induzione che

$$\forall n \in \mathbb{N} \quad \{0, 1, ..., n\} \subseteq B$$

- $0 \notin A$, altrimenti ne sarebbe il minimo, quindi $0 \in B$ e pertanto $\{0\} \subseteq B$.
- Supponiamo che $\{0, 1, ..., n\} \subseteq B$, allora $0, 1, ..., n \notin A$ e quindi $n + 1 \notin A$, altrimenti ne sarebbe il minimo, ma allora $n + 1 \in B$ e pertanto $\{0, 1, ..., n, n + 1\} \subseteq B$.

Per il principio di induzione di prima forma un insieme con queste proprietà coincide con quello dei numeri naturali ($B = \mathbb{N}$) e quindi $A = \emptyset$

2 Il principio di induzione (seconda forma)

Enunciato

Sia $P(n)$ una famiglia di proposizioni indicate su $\mathbb{N}$ e si supponga che

1. $P(0)$ sia vera
2. $\forall n > 0 (P(k) vera \forall k < n) \Rightarrow P(n) vera$

allora $P(n)$ è vera $\forall n \in \mathbb{N}$

Dimostrazione

Sia $A = \{n \in \mathbb{N} | P(n)$ non è vera $\}$, e supponiamo per assurdo che $A \neq \emptyset$.
Allora per la proprietà di buon ordinamento A ha minimo n.
Chiaramente $n \neq 0$ in quanto $P(0)$ è vera per ipotesi.
Inoltre se $k < n$ allora $k \notin A$ in quanto $n = \min A$, ma allora dalla (2) segue che $P(n)$ è vera e quindi $n \notin A$, contraddicendo il fatto che $n \in A$.

3 La divisione euclidea (esistenza e unicità)

Enunciato

Siano $n, m \in \mathbb{Z}$ con $m \neq 0$, allora esistono unici $q, r \in \mathbb{Z}$ tali che

$$\begin{cases} n = mq + r \\ 0 \leq r < |m| \end{cases}$$

Dimostrazione

- **Esistenza** Supponiamo dapprima che $n, m \in \mathbb{N}$, ed usiamo il principio di induzione della seconda forma su n.

  - Se $n = 0$ basta prendere $q = 0$ e $r = 0$.
  - Supponiamo $n > 0$ e che la tesi sia vera $\forall k < n$. Se $n < m$ basta prendere $q = 0$ e $r = n$, altrimenti sia $k = n - m$, dato che $m \neq 0$, $0 < k < n$, quindi per ipotesi di induzione esistono $q, r \in \mathbb{N}$ tali che
  $$\begin{cases} k = mq + r \\ 0 \leq r < |m| \end{cases}$$

  ma allora $n = k + m = mq + r + m = (q + 1)m + r$.
  Supponiamo ora $n < 0$ e $m > 0$. Allora $-n > 0$ e quindi per il caso precedente si ha che esistono $q, r \in \mathbb{Z}$ tali che $-n = mq + r$ e $0 \leq r < m = |m|$. E quindi $n = m(-q) - r$. Se $r = 0$ abbiamo finito, se invece $0 < r < m$ allora $0 < m - r < m = |m|$ e $n = m(-q) - r = m(-q) - m + m - r = m(-1 - q) + (m - r)$.
  Sia infine $m < 0$ allora $-m > 0$, quindi per i due casi precedenti $\exists q, r \in \mathbb{Z}$ tali che $n = (-m)q + r = m(-q) + r$ con $0 \leq r < -m = |m|$

- **Unicità** Supponiamo che $n = mq + r$ e $n = mq' + r'$ con $0 \leq r, r' < m$. Supponiamo che $r' \geq r$, allora $m(q - q') = r' - r$ e quindi passando ai moduli si ha $|m||q - q'| = |r' - r| = r' - r < |m|$, da cui $0 \leq |q - q'| < 1$ e quindi $|q - q'| = 0$ ovvero $q = q'$.
  Ma allora da $mq + r = mq' + r'$ segue che anche $r = r'$.

4 Codifica dei natuali in base maggiore o uguale a 2

Enunciato

Definizione Sia $b \in \mathbb{N}$, diremo che $n \in \mathbb{N}$ è rappresentabile in base b se esistono numeri $\epsilon_0, \epsilon_1, ..., \epsilon_k \in I_b = \{0, 1, ..., b-1\}$ tali che $n = \epsilon_0 + \epsilon_1 b + \epsilon_2 b^2 + ... + \epsilon_k b^k$.

Sia $b \in \mathbb{N}, b \geq 2$. Allora ogni $n \in \mathbb{N}$ è rappresentabile in modo unico in base b. Ossia esiste una successione $\{\epsilon_i\}_{i \in \mathbb{N}}$ tale che:

1. $\{\epsilon_i$ è definitivamente nulla ($\exists i_0 \in \mathbb{N} : \epsilon_i = 0 \quad \forall i > i_0$)
2. $\epsilon_i \in I_b$ (ossia $0 \leq \epsilon_i < b$) per ogni $i \in \mathbb{N}$
3. $n = \sum_{i=0}^{\infty} \epsilon_i b^i$

e se $\{\epsilon'_i\}_{i \in \mathbb{N}}$ è un'altra tale successione, allora $\epsilon_i = \epsilon'_i \quad \forall i \in \mathbb{N}$

Dimostrazione

Esistenza per induzione su n.

1. Se $n = 0$ basta prendere $\epsilon_i = 0 \quad \forall i \in \mathbb{N}$.
2. Supponiamo ora $n > 0$ e che la tesi sia vera per ogni $k < n$.
   Siano q, r tali che $n = bq + r$ con $0 \leq r < b$. Dato che $b \geq 2$ si ha che $0 \leq q < bq \leq bq + r = n$ e quindi per l'ipotesi di induzione esiste una successione definitivamente nulla $\{\delta_i\}_{i \in \mathbb{N}}$, costituita da interi tali che $0 \leq \delta_i < b \quad \forall i \in \mathbb{N}$ e tale che $q = \sum_{i=0}^{\infty} \delta_i b^i$. Ma allora
   $$n = bq + r = b \sum_{i=0}^{\infty} \delta_i b^i + r = \sum_{i=0}^{\infty} \delta_i b^{i+1} + r = \sum_{i=1}^{\infty} \delta_{i-1} b^i + r = \sum_{i=0}^{\infty} \epsilon_i b^i$$
   dove si è posto $\epsilon_0 = r$ e $\epsilon_i = \delta_{i-1} \quad \forall i > 0$.
   La successione $\{\epsilon_i\}$ è definitivamente nulla, dato che lo è $\{\delta_i\}$ ed inoltre $0 \leq \epsilon_i = \delta_{i-1} < b \quad \forall i > 0$ e $0 \leq \epsilon_0 = r < b$.

Unicità per induzione su n.

1. Se $n = 0 = \sum_i \epsilon_i b^i$ allora ogni addendo della somma, essendo non negativo, deve essere nullo e quindi $\epsilon_i = 0 \quad \forall i \in \mathbb{N}$

2. Supponiamo ora $n > 0$ e che l'espressione in base b sia unica per tutti i numeri $k < n$. Sia n tale che $n = \sum_{i=0}^{\infty} \epsilon_i b^i = \sum_{i=0}^{\infty} \epsilon'_i b^i$, allora possiamo scrivere

$$n = b \sum_{i=1}^{\infty} \epsilon_i b^{i-1} + \epsilon_0 = b \sum_{i=1}^{\infty} \epsilon'_i b^{i-1} + \epsilon'_0$$

ma per l'unicità della divisione euclidea si ha che $\epsilon_0 = \epsilon'_0$ e $q = \sum_{i=1}^{\infty} \epsilon_i b^{i-1} = \sum_{i=1}^{\infty} \epsilon'_i b^{i-1}$. Come prima $q < n$ e quindi per ipotesi induttiva si ha anche che $\epsilon_i = \epsilon'_i \quad \forall i \geq 1$

5 Il massimo comun divisore

Enunciato

Definizione Dati due interi $n, m \in \mathbb{Z}$ non entrambi nulli, si dice che d è un *massimo comun divisore tra n e m* se:

1. $d|n$ e $d|m$ (è un divisore)
2. Se $c|n$ e $c|m$ allora $c|d$ (è il massimo)

Proposizione Se d e d' sono due *massimi comun divisori tra n ed m* allora $d' = \pm d$.
Dimostrazione d è un divisore comune di n e m, quindi poichè d' è un massimo comun divisore di ha che $d|d'$. Scambiando i ruoli di d e d' si ha allora che anche $d'|d$ e quindi si ha che $d' = \pm d$.
Definizione Diremo che d è il massimo comun divisore di n e m se è un massimo comun divisore positivo. La proposizione precedente ci garantisce che se esiste un massimo comun divisore esso è unico.

Dati due numeri $n, m \in \mathbb{Z}$ non entrambi nulli, allora esiste il *massimo comun divisore tra n ed m.*

Dimostrazione

Esistenza Si consideri l'insieme

$$S = \{s \in \mathbb{Z} | s > 0, \exists x, y \in \mathbb{Z} : s = nx + my\}$$

$S \neq \emptyset$ dato che $nn + mm > 0$ (visto che n ed m non sono entrambi nulli).
Sia ora

$$d = nx + my = \min S$$

dimostriamo che d è il massimo comun divisore:
Se $c|n$ e $c|m$ allora $n = ck$ e $m = ch$, quindi $d = nx + my = ckx + chy = c(kx + hy)$, ossia $c|d$.
Dimostriamo ora che $d|n$:
consideriamo la divisione euclidea tra n e d, ossia $n = dq + r$ con $0 \leq r < d$, se $r > 0$, allora $r = n - dq = n - (nx + my)q = n(1 - qx) + (-m)y \in S$. Ciò è assurdo perchè $r < d$ e $d = \min S$. Quindi $r = 0$ ossia $d|n$. In modo del tutto analogo si prova che $d|m$.

6 Il minimo comune multiplo

Enunciato

Definizione Dati due interi $n, m \in \mathbb{Z}$ si dice che M è un *minimo comune multiplo di n ed m* se:

1. $n|M$ e $m|M$ (è un multiplo)
2. se $n|c$ e $m|c$ allora $M|c$ (è il minimo)

Come nel caso del massimo comun divisore di dimostra che due minimi comuni multipli sono uguali a meno del segno e quindi si chiama *il minimo comune multiplo* quello positivo (è quindi unico)

Siano $n, m \in \mathbb{Z}$ non entrambi nulli, allora esiste il *minimo comune multiplo tra n e m.*

Dimostrazione

Esistenza Sia

$$M = \frac{nm}{(n,m)} = n'm'(n,m)$$

dove si è posto

$$\begin{cases} n = n'(n,m) \\ m = m'(n,m) \end{cases}$$

Chiaramente allora $M = nm' = n'm$ e quindi $n|M$ e $m|M$.
Se $n|c$ e $m|c$ allora $(n,m)|c$ e quindi posto $c = c'(n,m)$ si ha che $n'|c'$ e $m'|c'$.
Dato che $(n',m') = 1$, si ha che $n'm'|c'$ e quindi che $M = n'm'(n,m)|c'(n,m) = c$.

7 Teorema fondamentale dell'aritmetica

Enunciato

Per ogni $n \in \mathbb{Z}, n \geq 2$ esistono numeri primi $p_1, p_2, ..., p_k > 0$ tali che $n = p_1 p_2 ... p_k$
Se anche $q_1, q_2, ..., q_h$ sono numeri primi positivi tali che $n = q_1 q_2 ... q_h$, allora esiste una bigezione $\sigma : \{1, 2, ..., h\} \to \{1, 2, ..., k\}$ tale che $q_i = p_{\sigma(i)}$.
In altre parole, ogni intero maggiore di 1 si scrive **in modo unico**, a meno dell'ordine, come **prodotto di numeri primi positivi**.

Dimostrazione

Esistenza. Procediamo per induzione su n:

1. Se $n = 2$ non c'è nulla da dimostrare in quanto 2 è primo.
2. Supponiamo $n > 2$ e che la tesi sia vera per ogni $k < n$:
   Se n è primo non c'è nulla da dimostrare,
   se n non è primo allora esistono due numeri d_1, d_2 con $1 < d_1, d_2 < n$ tali che $n = d_1 d_2$.
   Per ipotesi di induzione esistono dei numeri primi positivi tali che $d_1 = p_1 p_2 ... p_{k_1}$ e $d_2 = q_1 q_2 ... q_{k_2}$,
   ma allora $n = p_1 p_2 ... p_{k_1} q_1 q_2 ... q_{k_2}$ è prodotto di numeri primi positivi.

Unicità. Sia $n = p_1 ... p_k = q_1 ... q_h$ con p_i e q_j numeri primi positivi e $k \leq h$. Procediamo per induzione su k:

1. Se $k = 1$ allora $n = p_1 = q_1 ... q_h$, quindi $q_j | p_1 \quad \forall j$, e dato che p_1 è primo $q_j = p_1 \quad \forall j$. Se fosse $h > 1$ si avrebbe $n = q_1 ... q_h \geq q_1 q_2 = p_1^2 > p_1 = n$ e questo è assurdo, e quindi $h = 1$ e $q_1 = p_1$.
2. Sia $k > 1$, allora $p_k | n = q_1 ... q_h$, quindi esiste un j tale che $p_k | q_j$.
   Dato che sia p_k che q_j sono primi positivi, allora $p_k = q_j$. Ma allora $p_1 ... p_{k-1} = q_1 ... q_{j-1} q_{j+1} ... q_h$, per ipotesi di induzione possiamo allora dire che le due fattorizzazioni hanno lo stesso numero di elementi, ossia $k - 1 = h - 1$, e che esiste una bugezione $\delta : \{1, ..., j-1, j+1, ..., k\} \to \{1, ..., k-1\}$ tale che $q_i = p_{\delta(i)} \quad \forall i$. Definendo allora $\sigma : \{1, 2, ..., k\} \to \{1, 2, ..., k\}$ tale che
   $$\sigma(i) = \begin{cases} k & \text{se } i = j \\ \delta(i) & \text{se } i \neq j \end{cases}$$
   si ottiene una bigezione tale che $q_i = p_{\sigma(i)} \quad \forall i$.

8 Il Teorema Cinese del resto

Enunciato

Il sistema di congruenze:

$$\begin{cases} x \equiv a & \mod n \\ x \equiv b & \mod m \end{cases}$$

ha soluzione se e solo se $(n,m)|b-a$.
Se c è una soluzione del sistema, allora gli elementi di $[c]_{[n,m]}$ sono **tutte** e **sole** le soluzioni del sistema. (i.e. le soluzioni del sistema sono tutte e sole della forma $c+k[n,m]$ al variare di $k \in \mathbb{Z}$).

Dimostrazione

Sia c una soluzione del sistema, allora $\exists h,k \in \mathbb{Z}$ tali che $c = a+hn = b+km$ e quindi $a-b = km-hn$.
Ma allora dal fatto che $(n,m)|n$ e $(n,m)|m$ si ha che $(n,m)|a-b$.
Viceversa, supponiamo che $(n,m)|a-b$, allora, per quanto visto in precedenza, $\exists h,k \in \mathbb{Z}$ tali che $a-b = hn+km$. Ma allora $a-hn = b+kn$, detto quindi $c = a-hn = b+km$, si ha evidentemente che c risolve entrambe le congruenze.
Sia $S = \{x \in \mathbb{Z} \mid x \text{ risolve il sistema}\}$. Dobbiamo provare che se c è una soluzione del sistema allora $S = [c]_{[n,m]}$.

- $\mathbf{S \subseteq [c]_{[n,m]}}$. Sia c' un'altra soluzione del sistema, allora $c = a+hn = b+km$ e $c' = a+h'n = b+k'm$ e quindi sottraendo si ha:

  $$\begin{array}{rcl} c-c' & = & a+hn-a-h'n = (h-h')n \quad \Rightarrow \quad n \mid (c-c') \\ c-c' & = & a+km-a-k'm = (k-k')m \quad \Rightarrow \quad m \mid (c-c') \end{array}$$

  Ma allora $[n,m] \mid c-c'$, ossia $c' \equiv c \mod [n,m]$ ovvero $c' \in [c]_{[n,m]}$.

- $\mathbf{[c]_{[n,m]} \subseteq S}$. Sia $c' \in [c]_{[n,m]}]$, ovvero $c' = c+h[n,m]$. Dal fatto che $c \equiv a \mod n$ e che $h[n,m] =\equiv 0 \mod n$ segue che $c' = c+h[n,m] \equiv a \mod n$. In modo analogo si ha che $c' \equiv b \mod m$ e quindi che $c' \in S$.

9 Teorema di Fermat-Eulero

Enunciato

Sia $u \in \mathbb{Z}/n\mathbb{Z}^*$ allora $u^{\Phi(n)} = 1$ (in $\mathbb{Z}/n\mathbb{Z}$).

Dimostrazione

Sia $L_u : \mathbb{Z}/n\mathbb{Z}^* \to \mathbb{Z}/n\mathbb{Z}^*$ tale che $L_u(v) = uv$, osserviamo che la funzione risulta iniettiva, infatti $L_u(v_1) = L_u(v_2) \Leftrightarrow uv_1 = uv_2$ e dato che u è invertibile $\Leftrightarrow v_1 = v_2$. Visto che l'insieme $\mathbb{Z}/n\mathbb{Z}^*$ è finito L_u risulta essere bigettiva.
Sia $k = \Phi(n)$, e siano $x_1, ..., x_k$ tutti gli elementi di $\mathbb{Z}/n\mathbb{Z}^*$, dato che l'applicazione L_u è bigettiva, allora $L_u(x_1), ..., L_u(x_k)$ sono ancora tutti elementi di $\mathbb{Z}/n\mathbb{Z}^*$, ma allora, per la commutatività del prodotto

$$x_1 x_2 ... x_k = L_u(x_1) L_u(x_2) ... L_u(x_k)$$

e quindi:

$$x_1 x_2 ... x_k = u x_1 u x_2 ... u x_k = u^k (x_1 x_2 ... x_k)$$

Dato che $x_1 x_2 ... x_k$ è invertibile ne segue che

$$u^k = 1 \quad (\text{in } \mathbb{Z}/n\mathbb{Z})$$

10 Crittografia RSA

Enunciato

Sia c coprimo con $\Phi(n)$ allora l'applicazione

$$C : \mathbb{Z}/n\mathbb{Z}^* \to \mathbb{Z}/n\mathbb{Z}^* \text{ definita da } x \mapsto x^c$$

è invertibile e la sua inversa è data da

$$D(x) = x^d \text{ con } cd \equiv 1 \mod \Phi(n)$$

Dimostrazione

Se c è coprimo con $\Phi(n)$, allora esiste un d cone nell'enunciato, ossia tale che $cd \equiv 1 \mod \Phi(n)$, ma allora $cd = k\Phi(n) + 1$ e quindi, $\forall x \in \mathbb{Z}/n\mathbb{Z}^*$ si ha:

$$D(C(x)) = (x^c)^d = x^{cd} = x^{k\Phi(n)+1} = x(x^{\Phi(n)})^k = x \cdot 1^k = x$$

Del tutto analoga è la prova che anche $C(D(x)) = x \ \forall x \in \mathbb{Z}/n\mathbb{Z}^*$, da cui la tesi.

11 Equivalenza tra congiungibilità con cammini e congiungibilità con passeggiate

Enunciato

Definizione. Sia $G = (V, E)$ e siano $v, w, \in V$. Diremo che v e w sono *congiungibili* con un cammino [rispettivamente con una passeggiata] se esiste un cappino [risp. una passeggiata] $(v_0, v_1, ..., v_n)$ tale che $v_0 = v$ e $v_n = w$
Due vertici sono congiungibili mediante un cammino se e solo se lo sono tramite una passeggiata.

Dimostrazione

- (cammino $\Leftarrow$ passeggiata): Banale, in quanto un cammino è anche una passeggiata.
- (cammino $\Rightarrow$ passeggiata):
  Supponiamo quindi che $\exists$ una passeggiata $P = (v_0, ..., v_k)$ in G tale che $v_0 = v$ e $v_k = w$.
  Indichiamo con $\mathbb{P}$ l'insieme di tutte le passeggiate Q in G che partono da v e arrivano in w.
  Per ipotesi $P \in \mathbb{P}$, quindi $\mathbb{P} \neq \emptyset$.
  Dunque $\mathbb{A} = \{lunghezza(Q) \in \mathbb{N} \mid Q \in \mathbb{P}\} \neq \emptyset$.
  Poichè $(\mathbb{N}, \leq)$ è **ben** ordinato, $\exists \min \mathbb{A}$.
  Dunque $\exists P_0 \in \mathbb{P}$ tale che:

  - P_0 è una passeggiata in G che parte da v e arriva in w
  - $lunghezza(P_0) \leq lunghezza(Q) \qquad \forall Q \in \mathbb{P}$

  Proviamo quindi che P_0 è un cammino. Sia:

  $$P_0 = (y_0, y_1, ..., y_h) \text{ dove } y_0 = v \text{ e } y_h = w$$

  Se P_0 non fosse un cammino esisterebbero $i, j \in \{0, 1, ..., h\}$ tali che $i \neq j$ e $y_i = y_j$ (Supp. $i < j$). Possiamo definire:

  $$P_1 = (y_0, y_1, ..., y_i, \cancel{y_{i+1}, ..., y_j}, y_{j+1}, ..., y_h) \in \mathbb{P}$$

  Vale che $lung(P_1) = lung(P_0) - (j - i) \Rightarrow lung(P_1) < lung(P_0)$, ma questo è assurdo perchè P_0 ha lunghezza minima.
  $\Rightarrow P_0$ è un cammino in G.

12 La relazione di congiungibilità

Enunciato

La relazione di congiungibilità è una relazione di equivalenza sui vertici di un grafo finito.

Dimostrazione

Indichiamo con $\sim$ la relazione di congiungibilità.
Dobbiamo provare che la relazione di essere congiungibili $\sim$ è riflessiva, simmetrica e transitiva.

1. $\sim$ **è riflessiva.** Infatti $\forall v \in V(G), (v)$ è un cammino che congiunge v con se stesso, quindi $\forall v \in V(G), v \sim v$.

2. $\sim$ **è simmetrica.** Se $u \sum v$ allora esiste una passeggiata $P = (v_0, ..., v_n)$ tale che $u = v_0$ e $v = v_n$. Ma allora $P' = (v_n, v_{n-1}, ..., v_0)$ è una passeggiata (perchè due vertici consecutivi in P' sono adiacenti dato che lo sono, anche se scambiati, in P) il cui primo vertice è $v_n = v$ e l'ultimo è $v_0 = u$, ovvero $v \sim u$.

3. $\sim$ **è transitiva.** Se $u \sim v$ e $v \sim w$ allora esistono due passeggiate $P_1 = (v_0, ..., v_n)$ e $P_2 = (u_0, ..., u_m)$ tali che $u = v_0, v = v_n = u_0$ e $w = u_m$. Sia $Q = (v_0, ..., v_n, u_1, ..., u_m)$, Q è una passeggiata dato che vertici consecutivi in Q sono consecutivi in P_1 o in P_2 (si osservi che essendo $v_n = u_0$ si ha che v_n e u_1 sono consecutivi in P_2), d'altra parte il primo e l'ultimo vertice di Q sono u e w, quindi $u \sim w$.

13 Relazione fondamentale dei grafi finiti

Enunciato

Se $G = (V, E)$ è un grafo finito, allora:

$$\sum_{v \in V} \deg_G(v) = 2|E|$$

Dimostrazione

Siano $v_1, \ldots, v_n$ i vertici di G e $e_1, \ldots, e_k$ i suoi lati.
Per ogni $i = 1, \ldots, n$ e $j = 1, \ldots, k$ consideriamo il numero

$$m_{i,j} = \begin{cases} 1 & \text{se } v_i \in e_j \\ 0 & \text{se } v_i \notin e_j \end{cases}$$

Dalle proprietà associativa e commutativa della somma si ha evidentemente che

$$\sum_{i=1}^{n}(\sum_{j=1}^{k} m_{i,j}) = \sum_{j=1}^{k}(\sum_{i=1}^{n} m_{i,j})$$

Ma fissato i, il numero $\sum_{j=1}^{k}$ è uguale alla cardinalità dell'insieme

$$\{j \mid m_{i,j} = 1\} = \{j \mid v_i \in e_j\}$$

che è uguale al numero di lati che contengono v_i, ossia $\sum_{j=1}^{k} m_{i,j} = \deg_G(v_i)$.
Pertanto il lato sinistro dell'uguaglianza è pari a $\sum_{i=1}^{n} \deg_g(v_i)$ ossia la somma dei gradi di tutti i vertici.
Invece fissato j, il numero $\sum_{i=1}^{n} m_{i,j}$ è uguale alla cardinalità dell'insieme

$$\{i \mid v_i \in e_j\}$$

che è uguale a 2, dato che ogni lato contiene esattamente due vertici. Ne consegue che il lato destro dell'equazione è uguale a $2k = 2|E|$

Lemma (delle strette di mano)
In un grafo il numero di vertici di grado dispari è pari.

Dimostrazione
Segue banalmente dal fatto che la somma dei gradi (essendo il doppio del numero dei lati) è un numero pari, quindi, dal fatto che sommando un qualsiasi numero di numeri pari si ottiene sempre un numero pari e sommando un numero pari di numeri dispari si ottiene sempre un numero pari, segue che il numero di gradi dispari deve essere pari.

14 Caratterizzazione degli alberi finiti

Enunciato

Sia $T = (V, E)$ un grafo finito. Sono fatti equivalenti:

1. T è un albero
2. T è connesso e $|V| - 1 = |E|$

Dimostrazione

1 ⇒ 2 Procediamo per induzione su $|V(T)|$.

- Se $|V(T)| = 1$ la tesi è vera, infatti in quel caso $|E(T)| = 0$.
- Supponiamo che $|V(T)| \geq 2$ e che la tesi sia vero per ogni albero T' con $|V(T')| = |V(T)| - 1$.
  Sia $v \in V(T)$ una sua foglia (abbiamo dimostrato che ogni albero ha almeno 2 foglie), ora $T-v$ è un albero ed inoltre $|V(T-v)| = |V(T)|-1$. Per ipotesi di induzione abbiamo quindi che

  $$|V(T)| - 1 - 1 = |V(T - v)| - 1 = |E(T - v)|$$

  Ma dato che $\deg_T(v) = 1$, $|E(T - v)| = |E(T)| - 1$ e quindi la tesi.

2 ⇒ 1. Sia dunque T un grafo connesso che rispetta la formula di eulero. Dobbiamo provare che T non ha cicli. Procediamo ancora per induzione su $|V(T)|$.

- Se $|V(T)| = 1$ la tesi è vera, poichè un grafo composto da un solo vertice non può avere cicli.
- Supponiamo ora $|V(T)| \geq 2$. Proviamo innanzitutto che T ha una foglia. Dalla relazione tra numero di vertici e numero di lati, e dalla relazione che lega il numero di lati con il grado dei vertici si ottiene:

  $$2|V(T)| - 2 = 2|E(T)| = \sum_{v \in V(T)} \deg_T(v)$$

  Se non esistessero foglie, ogni $v \in V(T)$ dovrebbe avere $\deg_T(v) \geq 2$. Stimiamo quindi dal basso la somma dei gradi con $2|V(T)|$. Si ottiene subito un assurdo:

  $$\sum_{v \in V(T)} \deg_T(v) = 2|V(T)| - 2 \geq 2|V(T)|$$

Pertanto almeno un vertice deve avere grado 1.
Sia dunque v una foglia di T e si consideri il grafo $T - v$.
Dato che T è connesso e $\deg_T(v) = 1$, anche $T - v$ è connesso.
Inoltre, poichè $|V(T - v)| = |V(T)| - 1$ e $|E(T - v)| = |E(T)| - 1$, si ha che $|V(T - v)| - 1 = |E(T - v)|$. Per ipotesi di induzione si ha che $T - v$ è un albero.
Ma allora T non ha cicli, in quanto i vertici di un ciclo hanno tutti grado almeno 2 e quindi un ciclo in T non potrebbe passare per v, ossia sarebbe contenuto in $T - v$ contraddicendo il fatto che $T - v$ è un albero.

15 Esistenza dell'albero di copertura per grafi connessi finiti

Enunciato

Sia G un grafo connesso finito, allora G ha un albero di copertura, ossia un sottografo T di G tale che T sia una albero e che $V(T) = V(G)$.

Dimostrazione

Si consideri l'insieme

$$\mathcal{T} = \{T \mid T \text{ è sottografo di } G \text{ e } T \text{ è un albero } \}$$

$\mathcal{T} \neq \emptyset$, infatti se $v \in V(G)$ allora $(\{v\}, \emptyset) \in \mathcal{T}$ (è un sottografo di G ed è un albero).
Dato che G è finito, esiste $\overline{T} \in \mathcal{T}$ con massimo numero di vertici, ossia tale che

$$|V(T)| \leq |V(\overline{T})| \quad \forall T \in \mathcal{T}$$

Se proviamo che $V(\overline{T}) = V(G)$ avremo trovato un albero di copertura.
Supponiamo che esista $v \in V(G) \setminus V(\overline{T})$, allora, per la connesione di G, esiste un vertice $w \in V(G) \setminus V(\overline{T})$ ed un vertice $u \in V(\overline{T})$ tali che $\{u, w\} \in E(G)$ (ossia si congiunge v ad un vertice di $\overline{T}$ e si prendono il primo vertice del cammino che arriva in $\overline{T}$ ed il suo predecessore). Ma allora $T' = (V(\overline{T}) \cup \{w\}, E(\overline{T}) \cup \{\{u, w\}\})$ è evidentemente un sottografo di G ed è un albero.
A questo punto $T' \in \mathcal{T}$ e $|V(T')| = |V(\overline{T})| + 1$ e questo è in contraddizione con la massimalità di $\overline{T}$.
Dunque $V(G) \setminus V(\overline{T}) = \emptyset$, quindi $V(G) = V(\overline{T})$.
Esiste quindi un albero di copertura per G (ossia $\overline{T}$).