GRAFI PARTICOLARI

tratta da: "Combinatorial Matrix Theory"
autori: R.Brualdi, H. Ryser
ed. Cambridge University Press.

Relazione a cura di Massimiliano Vassallo
relativa al corso di Matematica discreta, A.A. 2003.

1 GRAFI REGOLARI

Lo studio inizia con due lemmi sulle matrici *nonnegative.* Notazione: e_n indica un vettore di elementi uguali ad uno di cardinalità n.

Si ricorda che una matrice $A \in \mathbb{C}^{nxn}$ è *riducibile* se esiste una matrice di permutazione P tale che la matrice $P^T AP$ sia della forma:

$$B = P^T AP = \begin{bmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{bmatrix}$$

con blocchi diagonali quadrati. Una matrice che non sia riducibile è detta *irriducibile.*

Lemma 5.1.1

Sia A una matrice nonnegativa reale di ordine n, e sia pari a k la somma di tutte le linee di A. Allora k è un autovalore di A corrispondente all'autovettore e_n, e il modulo di ogni altro autovalore di A non supera k. Inoltre, se $n > 1$, l'autovalore k ha molteplicità uno se e solo se A è irriducibile.

Dim:

L'equazione $Ae_n = ke_n$, che descrive l'ipotesi fatta relativamente a k, implica di per sè che k sia un autovalore di A e che l'autovettore corrispondente a questo sia e_n. E' dimostrato che questo è l'autovalore di modulo massimo massimo.

Se A è *riducibile*, allora anche la somma di tutte le linee di ogni componente irriducibile di A è uguale a k, e quindi k ha molteplicità almeno pari a due. Se A è *irriducibile*, allora dalla teoria di Perron Frobenius per le matrici nonnegative segue che la molteplicità di k come autovalore di A vale esattamente uno. C.V.D.

Lemma 5.1.2

Sia A una matrice nonnegativa reale di ordine n. Allora esiste un polinomio $p(x)$ tale che:

$$J = p(A) \tag{1}$$

se e solo se A è irriducibile e sono uguali le somme di tutte le righe di A.

Dim:

Si supponga valida la 1. Allora $AJ = JA$, e di conseguenza le somme delle linee di A sono uguali. Se A è *riducibile*, tutte le potenze integrali positive di A hanno alcune posizioni fisse occupate da zeri, cosa che va a contraddire la 1. Si supponga ora che A sia irriducibile e che le somme di tutte le linee di A siano uguali a k. Allora per il Lemma 5.1.1 si può affermare che k è un autovalore semplice di A. Il polinomio minimo di A può essere scritto nella forma:

$$m(\lambda) = (\lambda - k)\, q(\lambda)$$

e questo implica che

$$Aq(A) = kq(A).$$

Pertanto, ogni colonna non nulla di $q(A)$ è un autovettore di A corrispondente all'autovalore k. Ma l'autospazio associato all'autovalore k ha dimensione uno (k ha molteplicità uno, per il lemma 5.1.1): ne segue che ogni colonna di $q(A)$ è un multiplo di e_n. Si possono riutilizzare le stesse argomentazioni relativamente alla situazione trasposta:

$$A^T q(A)^T = kq(A)^T,$$

e si può concludere che anche ogni colonna di $q(A)^T$ è un multiplo di e_n. Quindi, ogni riga di $q(A)$ è un multiplo di e_n. Ma questo signifca che $q(A)$ è un multiplo di J. Non può essere $q(A) = 0$ perchè $m(\lambda)$ è il polinomio minimo di A. Di conseguenza, J è un polinomio in A, e precisamente descrivibile come $q(A)$ per una costante moltiplicativa. C.V.D.

Possiamo ora applicare il lemma precedente direttamente alla matrice di adiacenza, ed ottenere il teorema di Hoffman[1963].

Teorema 5.1.3

Sia A la matrice di adiacenza di un grafo G di ordine $n > 1$. Esiste un polinomio $p(x)$ tale che:

$$J = p(A) \tag{2}$$

se e solo se G è un grafo connesso regolare.

Corollario 5.1.4

Sia G un grafo connesso regolare di ordine $n > 1$ e siano indicati con $k > \lambda_1 > ... > \lambda_{t-1}$ gli autovalori distinti di G. Allora, se:

$$q(\lambda) = \prod_{i=1}^{t-1} (\lambda - \lambda_i),$$

risulta:

$$J = \left(\frac{n}{q(k)}\right) q(A).$$

Il polinomio

$$p(\lambda) = \left(\frac{n}{q(k)}\right) q(\lambda)$$

è l'unico polinomio di grado minimo tale per cui $p(A) = J$.

Dim:

A è simmetrica, quindi le radici del polinomio minimo di A sono *distinte*.

Dalla dimostrazione del Lemma 5.1.2 si ricava che $q(A) = cJ$ per una qualche costante c non nulla, essendo righe e colonne di $q(A)$ multipli di e_n. Gli autovalori della matrice $q(A)$, per linearità, sono $q(k)$ e $q(\lambda_i)$ $(i = 1, 2, ..., t-1)$, e sono tutti nulli ad eccezione di $q(k)$, essendo cJ una matrice avente tutti gli elementi pari a c. Siccome l'unico autovalore non nullo di cJ è cn, risulta $q(k) = cn$ e quindi $c = \frac{q(k)}{n}$.

Sia $p(\lambda)$ un polinomio tale che $p(A) = J$. Gli autovalori di $p(A)$ sono $p(k)$ e $p(\lambda_i)$ $(i = 1, 2, ..., t-1)$. Dal momento che e_n è un autovettore di $p(A)$ e di J corrispondente agli autovalori $p(k)$ e n, rispettivamente, risulta $p(\lambda_i) = 0$ per $i = 1, 2, ..., t-1$. C.V.D.

Il polinomio

$$p(\lambda) = \left(\frac{n}{q(k)}\right) q(\lambda)$$

nel corollario 5.1.4 è chiamato *polinomio di Hoffman* del grafo regolare connesso G.

Illustriamo la precedente discussione mostrando che l'unico grafo connesso di ordine n avente esattamente due autovalori distinti è il grafo completo K_n. Sia A la matrice di adiacenza di tale grafo con autovalori $\lambda_1 > \lambda_2$. Allora

$$A^2 - (\lambda_1 + \lambda_2) A + \lambda_1 \lambda_2 I = 0.$$

A è simmetrica e ha traccia nulla: ne segue che G è regolare di grado $-\lambda_1\lambda_2$. Quindi, il polinomio di Hoffman di G è di grado 1 e questo implica $J = A + I$.

Nelle sezioni successive si studieranno i grafi regolari connessi aventi esattamente tre autovalori distinti, ovvero grafi il cui polinomio di Hoffman è di grado 2.

2 GRAFI FORTEMENTE REGOLARI

In questa sezione G rappresenta un grafo di ordine n, $(n \geq 3)$, con vertici a_1, a_2, ..., a_n, mentre A indica la matrice di adiacenza di G.

Un *grafo fortemente regolare* di parametri (n, k, λ, μ) è un grafo G di ordine n, $(n \geq 3)$, regolare di grado k, che soddisfa i seguenti requisiti:

- Se a e b sono due vertici distinti di G collegati da un lato, allora ci sono esattamente λ ulteriori vertici di G che sono collegati ad entrambi a e b.
- Se a e b sono due vertici distinti di G non collegati da un lato, allora ci sono esattamente μ ulteriori vertici di G che sono collegati ad entrambi a e b.

Si escludono dalla trattazione il grafo completo K_n ed il suo complemento, il grafo vuoto, che renderebbero senza senso le due proprietà sopra esposte.

Si considerano dapprima alcuni semplici esempi di grafi fortemete regolari.

Il 4-ciclo ed il 5-ciclo sono grafi fortemente regolari di parametri, rispettivamente,

$$(4, 2, 0, 2) \quad \text{e} \quad (5, 2, 0, 1).$$

Nessun altro n-ciclo rappresenta un grafo fortemente regolare.

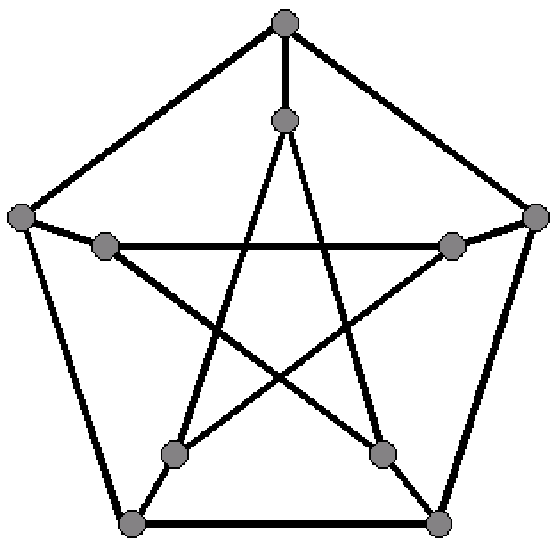

Figure 1: Grafo di Petersen

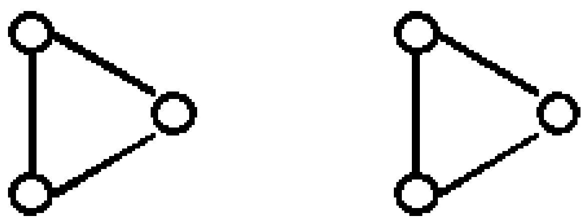

Figure 2: Grafo fortemente regolare di parametri: $(6, 2, 1, 0)$.

Il *grafo di Petersen*, mostrato in figura 1, e un grafo fortemente regolare di parametri

$$(10, 3, 0, 1).$$

Il grafo avente due componenti connesse ognuna delle quali è un 3-ciclo (figura 2) è un grafo fortemente regolare di parametri

$$(6, 2, 1, 0).$$

Il grafo completo bipartito $K_{m,m}$, $(m \geq 2)$ (figura 3), è un grafo fortemente regolare di parametri

$$(2m, m, 0, m).$$

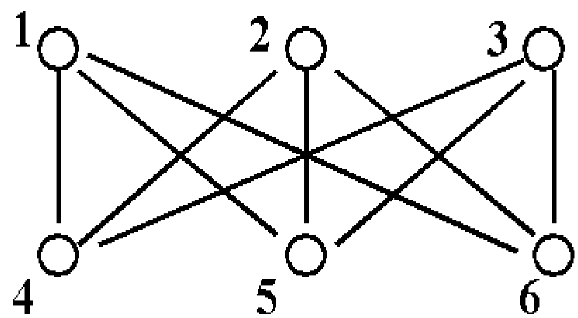

Figure 3: Grafo completo bipartito, $K_{3,3}$.

Sia G un grafo fortemente regolare di parametri (n, k, λ, μ) e sia A la sua matrice di adiacenza. E' noto che il valore alla posizione (i, j) di A^2 è uguale al numero di cammini di lunghezza due tra i vertici a_i ed a_j. Questo numero è pari a k, λ o μ a seconda che questi vertici siano coincidenti, adiacenti o non adiacenti. Pertanto risulta:

$$A^2 = kI + \lambda A + \mu (J - I - A) \tag{3}$$

o, equivalentemente,

$$A^2 - (\lambda - \mu) A - (k - \mu) I = \mu J. \tag{4}$$

Si definisce un nuovo parametro:

$$l = n - k - 1. \tag{5}$$

L'intero l è il grado del complemento $\overline{G}$ di G, mentre $(J - I - A)$ ne è la matrice di adiacenza. Attraverso un semplice calcolo, dalla 3 si ricava:

$$(J - I - A)^2 = lI + (l - k + \mu - 1)(J - I - A) + (l - k + \lambda + 1) A.$$

Quindi, ne segue che se G è un grafo fortemente regolare, anche il suo complemento $\overline{G}$ è fortemente regolare, ed ha paramentri:

$$\left(\overline{n} = n, \overline{k} = l, \overline{\lambda} = l - k + \mu - 1, \overline{\mu} = l - k + \lambda + 1\right).$$

Moltiplicando l'equazione 3 per il vettore colonna e_n si ottiene

$$k^2 = k + \lambda k + \mu (n - 1 + k),$$

e questa relazione può scriversi come

$$l\mu = k (k - \lambda - 1). \tag{6}$$

Nel caso sia $\mu = 0$, allora dalla 6 risulta $\lambda = k - 1$. Questo significa che ogni vertice di G appartiene ad un grafo completo K_{k+1}, e quindi G è un grafo disconnesso le cui componenti connesse sono tutte della forma K_{k+1}. Il requisito $\mu \geq 1$ è equivalente all'asserzione che il grafo fortemente regolare G sia connesso. Per questa regione spesso è richiesto che i grafi fortemente regolari abbiano $\mu \geq 1$.

Il seguente teorema afferma che i grafi fortemente regolari hanno **esattamente 3 autovalori distinti**, e fornisce la regola per il calcolo dei due autovalori più piccoli in valore assoluto e della loro molteplicità (si ricordi che l'autovalore maggiore vale k, ed ha molteplicità 1).

Teorema 5.2.1

Sia G un grafo connesso fortemente regolare di parametri (n, k, λ, μ). Siano poi definiti i parametri d e δ come:

$$d = (\lambda - \mu)^2 + 4\,(k - \mu)\,, \qquad \delta = (k + l)\,(\lambda - \mu) + 2k. \tag{7}$$

Allora, la matrice di adiacenza A di G ha l'autovalore massimo, k, di molteplicità 1, ed esattamente due altri autovalori

$$\rho = \frac{1}{2}\left(\lambda - \mu + \sqrt{d}\right) \geq 0, \qquad \sigma = \frac{1}{2}\left(\lambda - \mu - \sqrt{d}\right) \leq -1 \tag{8}$$

di molteplicità, rispettivamente,

$$r = \frac{1}{2}\left(k + l - \frac{\delta}{\sqrt{d}}\right), \qquad s = \frac{1}{2}\left(k + l + \frac{\delta}{\sqrt{d}}\right). \tag{9}$$

Dim:

Dal momento che G è un grafo connesso e non è completo, A ha almeno tre distinti autovalori. La prima asserzione del teorema deriva dal Lemma 5.1.1: si moltiplica l'equazione 4 per $A - kI$: quindi, siccome per il lemma 5.1.1 $AJ = kJ$, risulta:

$$(A - kI)\left(A^2 - (\lambda - \mu)\,A - (k - \mu)\,I\right) = 0.$$

Osservando che la 4 afferma implicitamente $\left(A^2 - (\lambda - \mu)\,A - (k - \mu)\,I\right)$ è proporzionale a $q\,(A)$, si può concluderre che le quantità ρ e σ mostrate nella 8, radici del polinomio $\left(A^2 - (\lambda - \mu)\,A - (k - \mu)\,I\right)$, sono autovalori di A.

Se $d = 0$ allora $\lambda = \mu = k$. Ma dal momento che G è regolare di grado k deve valere $\lambda \leq k - 1$, e quindi $d \neq 0$ e $\rho > \sigma$. Si noti che i parametri λ e μ sono esprimibili in funzione delle quantità $k > \rho > \sigma$:

$$\lambda = k + \rho + \sigma + \rho\sigma, \qquad \mu = k + \rho\sigma.$$

E' noto che $\mu \leq k$ e che $\rho \geq 0$ e $\sigma \leq 0$. Ma $\sigma = 0$ implicherebbe $\lambda = k + \rho$ e questo andrebbe a contraddire la condizione $\lambda \leq k - 1$. Quindi, si ha $\rho \geq 0$ e $\sigma < 0$.

Si consideri ora il complemento $\overline{G}$ di G. Un semplice calcolo consente di affermare che, per $\overline{G}$, si ha

$$\overline{d} = d, \quad \overline{\rho} = -\sigma - 1, \quad \overline{\sigma} = -\rho - 1.$$

Ma ancora, per $\overline{G}$, si ha $\overline{\rho} \geq 0$ e quindi si può concludere che $\rho \geq 0$ e $\sigma \leq -1$ come richiesto.

Siano ora r e s le molteplicità di ρ e σ, rispettivamente, come autovalori di A. Quindi risulta

$$r + s = n - 1,$$

e siccome A ha traccia nulla,

$$k + r\rho + s\sigma = 0.$$

Risolvendo questa equazione per r e s si ritrova la 9. C.V.D.

Le molteplicità r e s degli autovalori sono interi non negativi, e questo fatto, con la 9, induce severe restrizioni sull'insieme dei parametri per grafi fortemente connessi.

Teorema 5.2.2

Sia G un grafo connesso fortemente regolare di parametri (n, k, λ, μ).

- *Se $\delta = 0$, allora*

$$\lambda = \mu - 1, \quad k = l = 2\mu = r = s = \frac{n-1}{2}$$

- *Se $\delta \neq 0$, allora $\sqrt{d}$ è un intero ed anche ali autovalori ρ e σ sono interi. Inoltre, se n è pari, allora $\sqrt{d} \mid \delta$ siccome $2\sqrt{d} \nmid \delta$. e se n è dispari, allora $2\sqrt{d} \mid \delta$.*

Dim

Se $\delta = 0$, allora $k + l = \frac{2k}{(\mu - \lambda)} > k$ e quindi $0 < \mu - \lambda < 2$. Quindi risulta $\lambda = \mu - 1$. La restante equazione della prima conclusione del teorema segue direttamente dalle 6 e 9.

Se $\delta \neq 0$, allora la seconda conclusione del teorema segue direttamente dalle 6 e 9. C.V.D.

I grafi fortemente regolari della forma espressa dalla prima condizione del teroema 5.2.2 sono detti *grafi di conferenza*. Questi hanno gli stessi parametri dei loro complementi e sono stati generati per ordini n uguali ad una potenza di un primo congruente ad 1 (modulo4) (cioè: $n = 4m + 1$). Sia F un campo finito di n elementi, con n potenza di un primo congruente ad 1 (modulo4): si potrebbe costruire un grafo G di ordine n i cui vertici siano gli elementi di F. Due vertici a e b sono adiacenti in G se e solo se la differenza $a - b$ è il quadrato di un elemento non nullo in F. Si noti che -1 è un quadrato in F e quindi G è non direzionale. Il grafo risultante è fortemente regolare di parametri

$$\left(n, k = \frac{n-1}{2}, \lambda = \frac{n-5}{4}, \mu = \frac{n-1}{4}\right).$$

Questi grafi particolari sono detti *grafi di Paley*.

Teorema dell'amicizia: in una società finita in cui ogni coppia di individui ha esattamente un amico in comune, c'è qualcuno che è amico di tutti gli altri. Questo teorema è stato enunciato nel 1966 da Erdos, Rényi e Sos.

Teorema 5.2.3

Sia G un grafo di ordine n e si supponga che per ogni coppia di vertici distinti a e b ci sia un unico vertice c che sia collegato ad entrambi a e b. Allora n è dispari e G consiste in un insieme di triangoli aventi un vertice comune.

Dim:

Sia G un grafo che soddisfi le ipotesi del teorema. Siano a e b vertici non adiacenti di G. Allora esiste un unico vertice c adiacente ad entrambi a e b. Per le ipotesi fatte esistono anche vertici d ed e, unici, tali che $d \neq b$ sia adiacente sia ad a che a c ed $e \neq a$ sia adiacente sia a b che a c. Sia ora x un vertice diverso da c e da d ma adiacente ad a: allora esiste un unico vertice y, diverso da c e da e, che è adiacente sia ad x che a b. Lo stesso ragionamento vale con a e b scambiate. Di conseguenza, il grado di a e b è lo stesso.

Si supponga ora che G sia un grafo non regolare: siano a e b vertici di ordine diverso, e c l'unico vertice che sia collegato ad entrambi. Il paragrafo precedente implica che a e b siano adiacenti. (Infatti, se per ogni x adiacente ad a esistesse una y diversa da a ed adiacente a b, a e b avrebbero lo stesso grado, quindi almeno una y deve coincidere con a, che risulta pertanto adiacente a b).

Si può supporre, eventualmente scambiando a e b che il grado di a sia diverso da quello di c. Sia d un qualsiasi altro vertice: d è adiacente ad almeno un vertice tra a e b, essendo questi di gradi diversi. Allo stesso modo, d è adiacente ad almeno un vertice tra a e c. Ma d non può essere adiacente sia a c che a b in quanto già a soddisfa questa condizione: pertanto, d deve essere per forza adiacente ad a. Ne segue che G è consituito da triangoli aventi vertice comune in a.

Si può ora considerare il caso in cui G sia un grafo regolare di grado k. Sulla base delle ipotesi del teorema, G è fortemente regeolare con $\lambda = \mu = 1$. Dal teorema 5.2.1 segue che $s - r = \frac{\delta}{\sqrt{d}}$ è un intero. Ma allora $(k-1) \mid k^2$ e si ricava facilemnte che le uniche possibilità affinche valga questo risultato sono $k = 0$ e $k = 2$. Questi generano i casi di un vertice singolo e di un triangolo. C.V.D.

Si concentrerà ora l'attenzione su alcuni ulteriori esempi di grafi fortemente regolari.

Il *grafo triangolare* $T(m)$ è definito come il grafo commutato del grafo completo K_m, $(m \geq 4)$. Quindi i vertici di $T(m)$ sono identificati come i 2-sottoinsiemi di $\{1, 2, ..., m\}$, e sono adiacenti tra loro quando i corrispondenti 2-sottoiniemi hanno intersezione non nulla. Lo studio della struttura di $T(m)$ rivela che $T(m)$ è un grafo fortemente regolare di parametri

$$\left(n = \frac{m\,(m-1)}{2}, k = 2\,(m-2)\,, \lambda = m-2, \mu = 4\right).$$

Teorema 5.2.4

Sia G un grafo fortemente regolare di parametri $\left(\frac{m(m-1)}{2}, 2\,(m-2)\,, m-2, 4\right)$, $(m \geq 4)$. Se $m \neq 8$, allora G è isomorfo al grafo triangolare $T(m)$. Se $m = 8$, allora G è isomorfo ad uno di quattro grafi, uno dei quali è $T(8)$.

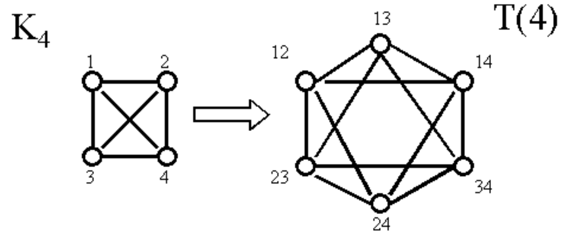

Figure 4: Grafo completo K_4 e relativo grafo triangolare $T\left(4\right)$.

Il *grafo reticolo* $L_2\left(m\right)$ è definito come il grafo commutato del grafo completo bipartito $K_{m,m}$, $(m \geq 2)$. E' fortemente regolare di parametri

$$\left(n = m^2, k = 2\left(m-2\right), \lambda = m-2, \mu = 2\right).$$

Teorema 5.2.5

Sia G un grafo fortemente regolare di parametri $\left(m^2, 2\left(m-2\right), m-2, 2\right)$, $(m \geq 2)$. Se $m \neq 4$, allora G è isomorfo al grafo reticolo $L_2(m)$. Se $m = 4$, allora G è isomorfo a $L_2(4)$ o al grafo in figura 5.2 del testo di riferimento.

Il *grafo di Moore* (di diametro 2) è un grafo fortemente regolare con $\lambda = 0$ e $\mu = 1$. I grafi di questa famiglia non contengono triangoli e, per ogni coppia di vertici non adiacenti, c'è un unico vertice adiacente ad entrambi. Hoffman e Singleton hanno dimostrato che l'insieme dei parametri per i grafi di Moore ha condizioni molto restrittive.

Teorema 5.2.6

I soli insiemi di parametri (n, k, λ, μ) possibili per un grafo di Moore sono i seguenti:

$$(5, 2, 01), \ (10, 3, 0, 1), \ (50, 7, 0, 1) \ \text{e} \ (3250, 57, 0, 1).$$

Dim:

La prima condizione del teorema 5.2.2 è verficata riguardo ai paramentri $(5, 2, 01)$. Applicando la seconda condizione, si trova che $d = 4k - 3$ è un quadrato perfetto. L'equazione 6 afferma che $k + l = k^2$ e quindi $\delta = k\left(2-k\right)$. Pertanto risulta $k\left(2-k\right) \equiv 0 \left(\bmod \sqrt{d}\right)$. Risulta inoltre $4k - 3 \equiv 0 \left(\bmod \sqrt{d}\right)$. Moltiplicando la prima delle due congruenze per 4 e la seconda per k, e sommandole, si ottiene $5k \equiv 0 \left(\bmod \sqrt{d}\right)$. Questo risultato, con la condizione $4k - 3 \equiv 0 \left(\bmod \sqrt{d}\right)$, implica che $15 \equiv 0 \left(\bmod \sqrt{d}\right)$. Pertanto, gli unici valori possibili per $\sqrt{d}$ risultano essere 1, 3, 5, e 15. Il primo caso rappresenta una degenerazione ed è da escludersi, gli altri tre valori conducono invece agli ultimi tre insiemi di parametri enunciati nel teorema. C.V.D.

Il primo degli insiemi di parametri espressi nel teorema 5.2.6 è soddisfatto dal pentagono, il secondo dal grafo di Petersen (figura 1), il terzo dal grafo di Hoffman-Sigleton. Questi sono gli unici grafi fortemente regolari che rispettano quei parametri. L'esistenza di un grafo fortemente regolare che soddisfi l'ultimo set di parametri espresso nel teorema è al momento sconosciuta.

Un *grafo di Moore generalizzato* è un grafo fortemente regolare avente $\mu = 1$. Il parametro λ può assumere qualsiasi valore in un grafo di questa famiglia, ma non è ancora stato proposto nessun grafo avente $\lambda \geq 1$.

3 DIGRAFI POLINOMIALI

Un *digrafo* è una coppia di insiemi (V, A), ove V è l'insieme dei vertici ed A è l'insieme dei lati, descritti da copie **ordinate** di elementidi V: un digrafo è quindi un grafo orientato. Un digrafo è *fortemente connesso* se due punti qualsiasi sono mutualmente raggiungibili; è *regolare* se tutti i suoi vertici hanno lo stesso grado. Generalizzando le dimostrazioni del teorema 5.1.3 e del corollario 5.1.4 si ottiene il teorema di Hoffman e McAndrew.

Teorema 5.3.1

Sia A la matrice di adiacenza di un digrafo D di ordine $n > 1$. Esiste un polinomio $p(x)$ tale che

$$J = p(A) \tag{10}$$

se e solo se D è un digrafo regolare fortemente connesso. Sia D un digrafo fortemente connesso regolare di grado k e sia $m(\lambda)$ il polinomio minimo di A. Se

$$q(\lambda) = \frac{m(\lambda)}{\lambda - k}$$

allora il polinomio

$$p(\lambda) = \left(\frac{n}{q(k)}\right) q(\lambda)$$

è l'unico polinomio di grado minimo tale per cui risulta $p(A) = J$.

Dal Lemma 5.1.1 il modulo di ogni autovalore di A è minore o uguale a k. Le radici di $p(\lambda)$ sono autovalori di A e di conseguenza $|p(\lambda)|$ è una funzione monotona crescente se λ è reale e $\lambda \geq k$. Si ha che $p(k) = n$ e si può affermare che il grado k di regolarità di D è uguale alla radice reale maggiore di $p(\lambda) = n$. Estendendo ai digrafi la definizione data nella prima sezione, il polinomio $p(\lambda)$ definito nel teorema 5.3.1 si dice polinomio di Hoffman del digrafo regolare fortemente connesso D.

Sia ora A la matrice di adiacenza di un digrafo D. Se D è regolare di grado k, anche A è regolare di grado k. Similmente, due matrici di adiacenza sono dette *isomorfe* se i loro corrispondenti grafi sono isomorfi.

Si considerano ora i polinomi particolari $p(\lambda) = \frac{(\lambda^m + d)}{c}$ dove c è un intero positivo e d è un intero non negativo.

Teorema 5.3.2

Siano m e c interi positivi, e sia d un intero non negativo. Sia poi A una matrice $(0,1)$ che soddisfi la seguente equazione:

$$A^m = -dI + cJ. \tag{11}$$

Allora esiste un intero positivo k tale che A sia regolare di grado k e $k^m = -d + cn$. Se $d = 0$ allora anche la traccia di A è uguale a k.

Dim:

La regolarità di A è conseguenza del teorema 5.3.1. Moltiplicando poi la 11 per J si ricava che $k^m = -d + cn$. Si consideri ora $d = 0$. Le radici del polinomio caratteristico di A siano $\lambda_1, \lambda_2, \ ..., \lambda_n$. Le radici caratteristiche di cJ sono cn di molteplicità uno e 0 di molteplicità $n-1$. Quindi si può affermare che $\lambda_1 = k, \lambda_2 = 0, \ ..., \lambda_n = 0$. C.V.D.

Si osserva che se $d = 0$ nel terorema 5.3.2 è essenziale che il digrafo D associato ad A abbia lacci in quanto, altrimenti, la sua configurazione sarebbe impossibile. Rispetto a D l'equazione 11 afferma che per ogni coppia di vertici distinti a e b di D ci sono esattamente c cammini di lunghezza m da a a b, e che ogni vertice sta su esattamente $c - d$ cammini chiusi di lunghezza m. Se $c = 1$ e $d = 0$ una matrice $(0, 1)$, A, che soddisfa la condizione $A^m = J$ è una matrice primitiva di esponente m, e il polinomio $p(\lambda) = \lambda^m$ è il polinomio di Hoffman di D.

Si vorrà ora dimostrare che, se $d = 0$, la condizione $k^m = cn$ nel teorema 5.3.2 è **sufficiente** per affermare che esista una matrice $(0, 1)$, A, di ordine n che soddisfa $A^m = cJ$. Una *matrice g-circolante* è una matrice di ordine n in cui ogni riga che non sia la prima è ottenuta dalla riga precedente traslando ciclicamente gli elementi di g posizioni verso destra. Sia $A = [a_{ij}]$, $(i, j = 1, 2, ..., n)$, una matrice g-circolante: allora

$$a_{ij} = a_{i+1,j+g}$$

dove gli indici sono calcolati modulo n. Una matrice 1-circolante è comunemente detta matrice circolante.

Detti $a_0, a_1, \ ..., a_{n-1}$, gli elementi della prima riga di una matrice A g-circolante di ordine n, il *polinomio di Hall* di A è definito come:

$$\theta_A(x) = \sum_{i=0}^{n-1} a_i x^i.$$

Il lemma seguente è diretta conseguenza delle definizioni date.

Lemma 5.3.3

Sia A una matrice g-circolante di ordine n, e B una matrice h-circolante di ordine n. Allora il prodotto AB è una matrice gh-circolante di ordine n e risulta:

$$\theta_{AB}(x) = \theta_A\left(x^h\right)\theta_B(x) \pmod{x^n - 1}.$$

Corollario 5.3.4

Sia A una matrice g-circolante di ordine n. Allora per ogni intero positivo m, A^m è una matrice g^m-circolante e risulta

$$\theta_{A^m}(x) = \theta_A(x)\,\theta_A(x^g)\,...\theta_A\left(x^{g^{m-1}}\right) \pmod{x^n - 1}. \tag{12}$$

Dim:

Basta applicare il lemma 5.3.3. ed usare l'induzione su M. C.V.D.

Le soluzioni g-circolanti dell'equazione $A^m = -dI + cJ$ sono caratterizzate dai loro polinomi di Hall secondo il seguente risultato di Lam [1977].

Lemma 5.3.5

Sia A una matrice g-circolante. Allora $A^m = cJ$ se e solo se

$$\theta_A(x)\,\theta_A(x^g)\ldots\theta_A\left(x^{g^{m-1}}\right) \equiv c\left(1 + x + \ldots + x^{n-1}\right) \pmod{x^n - 1}. \quad (13)$$

Se $d \neq 0$, allora $A^m = dI + cJ$ se e solo se

$$\theta_A(x)\,\theta_A(x^g)\ldots\theta_A\left(x^{g^{m-1}}\right) \equiv d + c\left(1 + x + \ldots + x^{n-1}\right) \pmod{x^n - 1} \quad (14)$$

e

$$g^m \equiv 1 \pmod{n}. \quad (15)$$

Dim:

Dal corollario 5.3.4 risulta che A^m è una matrice g^m-circolante ed il suo polinomio di Hall è dato dalla 12. Se $A^m = cJ$, allora la prima riga di A^m è $(c, c, \ldots, c)$ e questo implica la 13. Viceversa, se è soddisfatta la 13 allora la prima riga di A^m è $(c, c, \ldots, c)$, ed essendo A^m circolante risulta $A^m = cJ$.

Si supponga ora $d \neq 0$ e $A^m = dI + cJ$. Allo stesso modo di quanto detto sopra si può affermare che la 14 è valida. Inoltre, siccome $dI + cJ$ è circolante, si ha $g^m \equiv 1 \pmod{n}$. Se d'altra parte $d \neq 0$ e sono soddisfatte la 14 e la 15, allora la prima riga di A^m è uguale a $(d + c, c, \ldots, c)$. Allora, per la 15 A^m è 1-circolante e quindi si ha $A^m = dI + cJ$. C.V.D.

Segue il teorema di Lam.

Teorema 5.3.6

Si supponga $k^m = cn$. Allora la matrice k-circolante A di ordine n, la cui prima riga consiste in k uni seguiti da $n-k$ zeri, soddisfa la seguente relazione:

$$A^m = cJ.$$

Dim:

Il polinomio di Hall della matrice A soddisfa

$$\theta_A(x) = 1 + x + \ldots + x^{k-1}.$$

Segue quindi che

$$\theta_A(x)\,\theta_A\left(x^k\right)\ldots\theta_A\left(x^{k^{m-1}}\right) = 1 + x + x^2 \ldots + x^{k^m - 1}.$$

Dal momento che $k^m = cn$, risulta

$$\begin{aligned} \theta_A(x)\,\theta_A\left(x^k\right)\ldots\theta_A\left(x^{k^{m-1}}\right) &= 1 + x + x^2 \ldots + x^{cn-1} \\ &\equiv c\left(1 + x + \ldots + x^{n-1}\right) \pmod{x^n - 1}. \end{aligned}$$

Applicando il lemma 5.3.5 si ottine la conclusione desiderata. C.V.D.

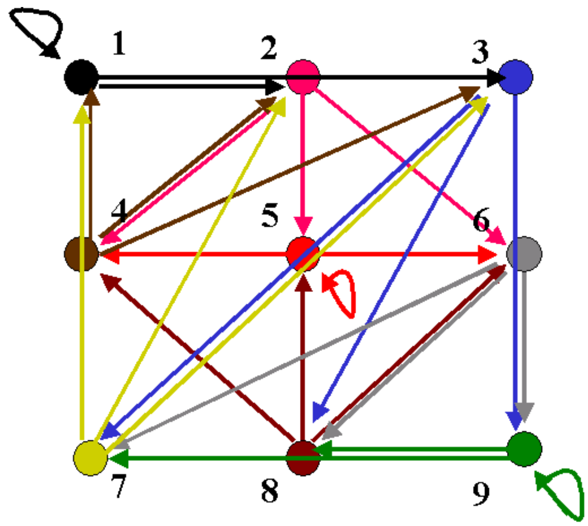

Figure 5: Esempio per teorema di Lam: $k = 3$, $c = 3$, $n = 9$.

La figura 5 mostra un grafo ($n = 3$, $k = 3$) che rispetta le ipotesi del teorema di Lam nel caso i parametri m e c valgano: $c = 3$, $m = 3$. La matrice di adiacenza A vale:

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

e, con $m = 3$ e $c = 3$, la condizione $k^m = cn$ è verificata: risulta pertanto $A^3 = 3J$.

Se $d \neq 0$, allora la condizione $k^m = -d + cn$ non è generalmente in grado di garantire l'esistenza di una matrice $(0, 1)$ A di ordine n che soddisfi la condizione $A^m = -dI + cJ$. Sia $d = -1$. Se $k^m = 1 + cn$, allora il lemma 5.3.5 implica anche che la matrice k-circolante A costruita nel teroema 5.3.6 soddisfi la condizione $A^m = I + cJ$.

Il teorema di Lam e van Lint affronta il caso in cui $c = d = 1$.

Teorema 5.3.7

Sia m un intero positivo. Esiste una matrice $(0, 1)$ A *di ordine* n *che soddisfa l'equazione:*

$$A^m = -I + J$$

se e solo se m *è dispari e* $n = k^m + 1$ *per qualche* k *intero positivo.*

Dim:

Si supponga che A sia una matrice $(0, 1)$ di ordine n che soddisfi $A^m = -I+J$. Allora la traccia di A è nulla e, per il teorema 5.3.2, A è regolare di grado k con $n = k^m + 1$. Si assuma dapprima $m = 2$. Gli autovalori di $-I + J$ sono $n - 1 = k^2$ di molteplicità 1, e -1 di molteplicità $n - 1$.Quindi gli autovalori di A sono k con molteplicità 1 e $\pm i$ con molteplicità uguali. Questo contraddice il fatto che A abbia traccia nulla. Se m è pari, $\left(A^{\frac{m}{2}}\right)^2 = -I + J$ dove $A^{\frac{m}{2}}$ è ancora una matrice $(0, 1)$. Se ne conclude che m deve essere dispari.

Si supponga invece ora che m sia un intero dispari e $n = k^m + 1$. Sia $g = -k$ e sia A la matrice g-circolante di ordine n la cui prima riga consista in 0, seguito da k uni, seguiti a loro volta da $(n - k - 1)$ zeri. Il polinomio di Hall di A soddisfa la seguente equazione:

$$\theta_A(x) = x + x^2 + ... + x^k.$$

Si ha

$$\theta_A(x)\,\theta_A(x^g)\,...\theta_A\left(x^{g^{m-1}}\right) \equiv -1 + \left(1 + x + ... + x^{n-1}\right) \pmod{x^n - 1},$$

e

$$g^m = (-k)^m = -n + 1 \equiv 1 \pmod{n}.$$

Dal lemma 5.3.5 si ricava che $A^m = -I + J$. C.V.D.

Sebbene la matrice $A^m = -dI + cJ$ abbia una forma semplice, esistono alcune questioni di difficile soluzione. Una caratterizzazione completa di quegli interi m, d, e c, per i quali esiste una matrice $(0, 1)$ che sia una soluzione è per lo più sconosciuta. Nelle istanze in cui è risaputo esistere una soluzione, non si conosce virtualmente nulla a proposito del numero di soluzioni non isomorfe per n generico. Se $n = k^2$ il numero di matrici $(0, 1)$ regolari di ordine n che soddisfano $A^2 = J$ è ignoto.

Non concentrandosi sui termini c e d dell'equazione $A^m = -dI + cJ$ si possono effettuare alcune osservazoni: si vogliono ora cercare quelle matrici $(0, 1)$, A, di ordine n talli che A^m abbia tutti gli elementi sulla diagonale uguali tra loro, e tutti quelli al di fuori della diagonale ancora uguali tra loro. Una soluzione banale è la matrice $A = J$, caso che comporterebbe $d = 0$ e $c = n^{m-1}$. Sono state però studiate anche le soluzioni non banali associate a $d = 0$.

Teorema 5.3.8

Siano $m > 2$ e $n \geq 2$ interi. Esiste una matrice $(0, 1)$ A di ordine n, che sia $A \neq J$, e tale che A^m abbia tutti gli elementi uguali tra loro, se e solo se n è divisibile per il quadrato di qualche numero primo. Sia g il prodotto dei divisori primi distinti di n. Se n è divisibile per il quadrato di qualche numero primo, allora esiste una matrice g-circolante $A \neq J$ tale per cui tutti gli elementi di A^m siano uguali.

Sia A una matrice $(0, 1)$ di ordine n. Si consideri l'equazione generica

$$A^2 = E + cJ, \tag{16}$$

dove E è una matrice diagonale, e c è un intero positivo. Questa descrive un digrafo D di ordine n con esattamente c cammini di lunghezza 2 tra ogni coppia di vertici *distinti.*

E' evidente che una matrice A che rispetta la 16 non deve necessariamente essere regolare. Controesempi sono dati dalle seguenti matrici per le quali $c = 1$:

$$\begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & O & \\ 1 & & & \end{bmatrix} \quad (n \geq 2)\,, \tag{17}$$

dove O è una matrice di zeri di ordine $n-1$, e

$$\begin{bmatrix} 0 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{bmatrix} \quad (n \geq 4)\,, \tag{18}$$

dove Q è una matrice simmetrica di permutazione di ordine $n-1$.

Teorema 5.3.9

Sia A una matrice $(0,1)$ di ordine $n > 1$ che soddisfi l'equazione matriciale

$$A^2 = E + cJ,$$

dove E è una matrice diagonale, e c è un intero positivo. Allora esiste un intero k tale che A è regolare di ordine k, ad eccezione delle matrici $(0,1)$ di ordine n con $c = 1$ isomorfe alla 17 o alla 18 e della matrice $(0,1)$ di ordine 5 con $c = 2$ isomorfa a

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Inoltre, se A è regolare di ordine k, allora

$$A^2 = dI + cJ,$$

dove

$$k^2 = d + cn$$

e

$$-c < d \leq k - c.$$

Questo risultato è stato esteso e sono state ricavate tutte le soluzioni non-regolari di

$$A^2 - aA = E + cJ.$$

Inoltre, è stata completamente esplorata la questione della regolarità della forma $A^r = E + cJ$.

Teorema 5.3.10

Sia A una matrice $(0,1)$ di ordine n che soddisfi l'equazione matriciale

$$A^r = E + cJ,$$

dove E è una matrice diagonale, e r e c interi positivi. Allora A è regolare purchè siano $n > 3$ e $r > 3$.