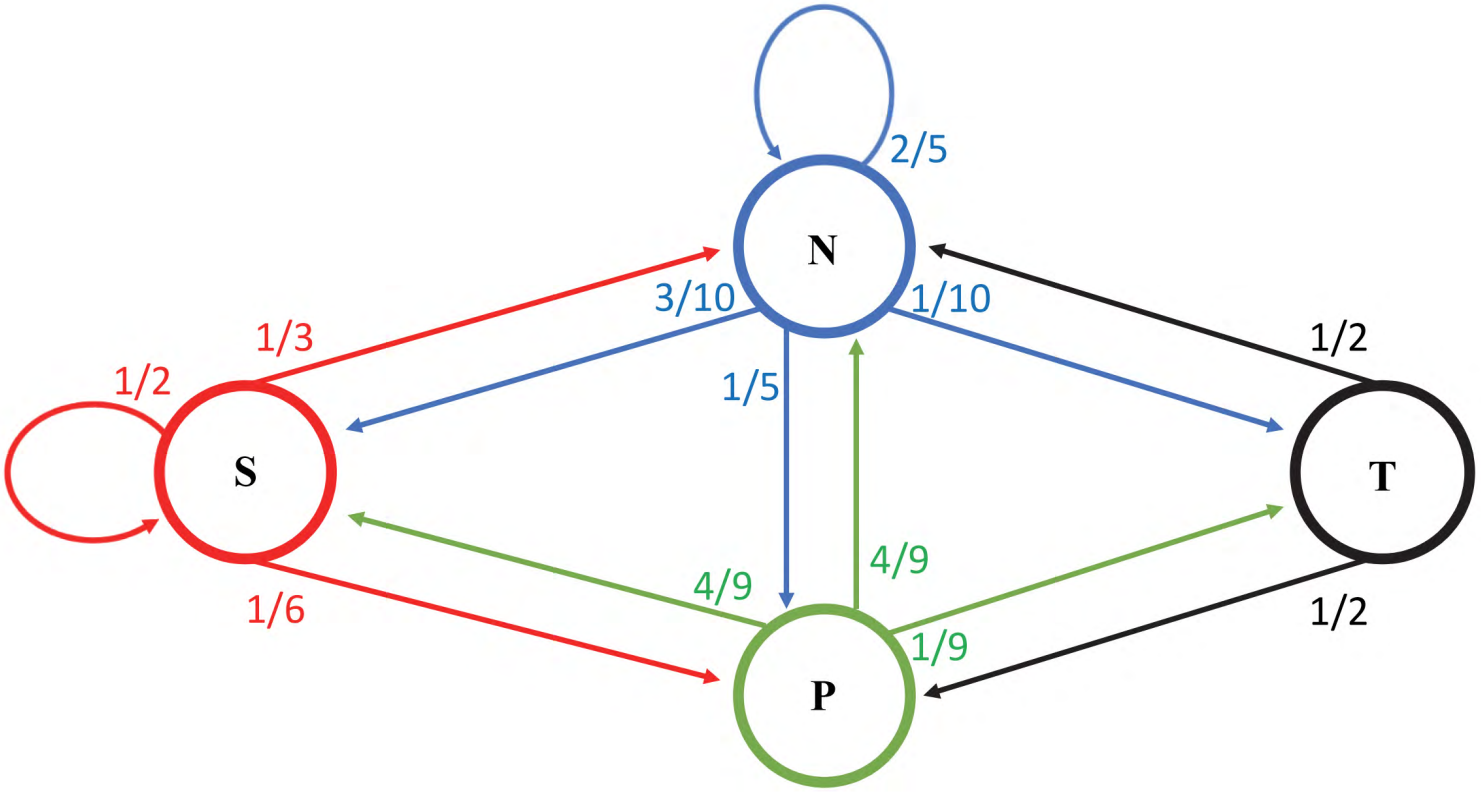
Catene di Markov e applicazioni algoritmiche



Massimiliano Goldwurm

Milano University Press

Massimiliano Goldwurm

Catene di Markov e applicazioni algoritmiche

Milano University Press

Catene di Markov e applicazioni algoritmiche / Massimiliano Goldwurm. Milano: Milano University Press, 2024.

ISBN 979-12-5510-099-7 (print)

ISBN 979-12-5510-100-0 (PDF)

ISBN 979-12-5510-101-7 (EPUB)

DOI 10.54103/milanoup.158

Pubblicato da:
Milano University Press
Via Festa del Perdono 7 – 20122 Milano
Sito web: https://milanoup.unimi.it
e-mail: redazione.milanoup@unimi.it

L'edizione cartacea del volume può essere ordinata in tutte le librerie fisiche e online ed è distribuita da Ledizioni (https://www.ledizioni.it/)

Premessa

Questo lavoro si rivolge principalmente (ma non solo) agli studenti dei corsi di laurea magistrale a indirizzo scientifico, in particolare a quelli di informatica, di matematica e di fisica. Esso contiene gran parte del materiale didattico utilizzato da più di 15 anni in vari insegnamenti, tenuti dall'autore presso l'Università degli Studi di Milano, dedicati agli algoritmi probabilistici e all'uso in un ambito informatico di metodi e tecniche proprie della teoria della probabilità. Il tema centrale che qui viene affrontato è quello delle catene di Markov e delle loro applicazioni algoritmiche.

Le catene di Markov rappresentano un argomento di studio classico che ha avuto origine in ambito probabilistico ma che ha trovato un grande numero di applicazioni in varie discipline, dall'informatica alla fisica, dalla biologia alle scienze naturali, dalla sociologia all'economia e in molti altri contesti. I modelli Markoviani sono stati utilizzati in diversi ambiti di ricerca di notevole interesse e attualità, come per esempio nell'analisi e nell'interpretazione di sequenze di DNA, nel riconoscimento di segnali vocali, nel disegno di procedure di esplorazione della rete web, solo per citarne alcuni.

Il materiale presentato in questo lavoro può essere sostanzialmente suddiviso in due parti. Nella prima (capitoli 1-4) vengono introdotte le catene di Markov come nozione probabilistica, con uno spirito tipicamente matematico, e se ne presentano le proprietà classiche. L'obiettivo principale di questa parte è quello di studiare le catene ergodiche, cioè quelle nelle quali la probabilità di trovarsi in un dato stato, al crescere del numero di passi, converge a una distribuzione fissata, che non dipende dallo stato di partenza.

La seconda parte (capitoli 5-8) è invece dedicata ai metodi Markov Chain Monte Carlo (MCMC) e in generale all'uso delle catene di Markov per la definizione di algoritmi efficienti. Si presentano le caratteristiche generali di questi metodi, in generale basati su catene di Markov ergodiche, e si illustrano alcuni esempi rilevanti. In particolare vengono descritte procedure classiche come l'algoritmo di Metropolis, o quelle per la generazione casuale di indipendent set e di colorazione di grafi, o ancora quelle per risolvere i relativi problemi di conteggio in modo approssimato. Particolare attenzione è dedicata alla velocità di convergenza di queste procedure, cioè al numero complessivo di passi eseguiti sulla catena, necessari per garantire che l'ultimo stato sia raggiunto con una probabilità sufficientemente vicina a quella desiderata.

In questa sede si è cercato di mantenere per quanto possibile autoconsistente la presentazione del materiale. A questo scopo è presente un'appendice dedicata ad argomenti di base di teoria della probabilità e di algebra lineare, che dovrebbero comunque essere noti agli studenti di un corso di laurea magistrale a indirizzo scientifico. Tuttavia, nonostante questo sforzo, la trattazione presuppone una buona maturità scientifica e il lavoro si rivolge a un lettore che abbia dimestichezza con gli argomenti di studio presentati nei tradizionali insegnamenti di matematica e informatica, e in particolare di calcolo delle probabilità e statistica, solitamente

impartiti nei primi anni di un corso di laurea triennale di carattere scientifico.

Segnaliamo infine che lo scopo del presente lavoro è essenzialmente didattico e divulgativo. Desideriamo fissare una base di conoscenze adeguata che permetta allo studente di comprendere i fondamenti delle catene di Markov e delle loro applicazioni, di sviluppare un interesse culturale e scientifico per l'argomento, consentendo facilmente eventuali approfondimenti ed estensioni ulteriori in altre sedi. Gli argomenti specifici qui trattati non esauriscono certamente lo studio delle catene di Markov e delle loro applicazioni, ma sono quelli che si possono ragionevolmente presentare su questi temi, in un insegnamento di 6-9 crediti, tenuto presso un corso di laurea magistrale nelle nostre università. Si possono comunque trovare nei numerosi testi citati nel corso della presentazione e nelle corrispondenti bibliografie, trattazioni più estese e approfondite di questi argomenti.

Milano, dicembre 2023

Indice

Capitolo 1

Introduzione

La nozione di catena di Markov è un concetto relativamente facile da comprendere e assimilare, in particolare per chiunque abbia conseguito una laurea triennale a indirizzo scientifico, sopratutto di carattere informatico o matematico. Intuitivamente si tratta infatti di un automa a stati finiti, privo di nastro di ingresso, nel quale ogni transizione da uno stato a un altro è dotata di una probabilità fissata, in modo tale che la somma delle probabilità delle transizioni uscenti da ciascuno stato sia sempre uguale a 1. Questo modello di calcolo non può quindi essere usato, come negli automi tradizionali, per riconoscere una stringa di ingresso (e quindi per rappresentare un linguaggio). Esso viene invece utilizzato per valutare la probabilità di tutti quegli eventi che si possono definire mediante transizioni tra stati; per esempio, per calcolare la probabilità di trovarsi in un certo stato dopo un certo numero di passi, oppure per determinare i tempi di attesa necessari per entrare in dato stato, o ancora per stimare la frequenza di un dato stato in una passeggiata a caso eseguita a partire da uno stato iniziale. Una catena di Markov può quindi essere rappresentata da un grafo orientato nel quale gli archi sono pesati da probabilità, in modo tale che l'insieme delle probabilità dei lati uscenti da ciascun nodo formi a sua volta una distribuzione sulla stessa famiglia dei vertici.

In alternativa, un modo diverso per definire una catena di Markov è quello di considerare una famiglia S di k stati, ciascuno dei quali dotato di una distribuzione di probabilità sullo stesso insieme S. Tali distribuzioni possono essere rappresentate in modo conveniente mediante una matrice stocastica, cioè una matrice di dimensione $k \times k$ nella quale tutti i coefficienti sono probabilità e su ogni riga la somma dei coefficienti è sempre uguale a 1. Ecco quindi che grafi e matrici, concetti solitamente ben familiari agli studenti dei corsi di laurea magistrale a indirzzo scientifico, sono gli strumenti naturali mediante i quali possiamo introdurre le catene di Markov. Questo è il motivo didattico per il quale, nel presente lavoro, il capitolo successivo è dedicato proprio ai grafi e alle matrici.

Le catene di Markov sono state studiate per la prima volta agli inizi del '900 come modello per l'analisi dei fenomeni di dipendenza tra variabili aleatorie e, proprio per la grande varietà di applicazioni, sono diventate uno dei settori della teoria della probabilità con il maggior numero di pubblicazioni (vedi ad esempio la bibliografia in [9]). In un ambito informatico, e principalmente algoritmico, esse hanno dato origine ai noti metodi Markov Chain Monte Carlo (MCMC), formalizzati negli anni '90 del secolo scorso [13, 12], ma di fatto già utilizzati nei decenni precedenti, per diversi scopi computazionali e scientifici, in contesti anche diversi da quello informatico (basti pensare al famoso algoritmo di Annealing Simulato). I metodi MCMC sono di fatto procedure per la generazione casuale di elementi in un insieme finito,

da utilizzare quando la distribuzione di probabilità fissata non è nota o i suoi elementi sono difficili da calcolare. Questi metodi intuitivamente determinano l'elemento casuale desiderato mediante una passeggiata in una opportuna catena di Markov, nella quale da uno stato corrente si passa al successivo scegliendo quest'ultimo con probabilità data dalla corrispondente transizione. In tale catena gli stati rappresentano l'insieme di oggetti dal quale estrarre il valore cercato e le probabilità di transizione sono determinate in modo tale da garantire che, al crescere del numero di passi, la probabilità di giungere in un qualunque stato si avvicini a quella desiderata. L'importanza dei metodi MCMC è dovuta al fatto che in linea di principio essi possono essere usati come sottoprocedure in ogni algoritmo probabilistico; infatti ogni algoritmo di questo genere è per forza basato sulla generazione casuale di elementi in un dato insieme secondo una distribuzione di probabilità fissata.

Capitolo 2

Matrici non negative

In questo capitolo introduciamo le proprietà principali delle matrici a coefficienti reali non negativi. L'obiettivo principale è quello di presentare il teorema di Perron-Frobenius sull'autovalore principale delle matrici primitive e alcune sue conseguenze riguardanti l'espressione asintotica delle potenze di tali matrici. Questi risultati sono legati allo studio delle proprietà ergodiche delle catene di Markov e saranno riconsiderati nei capitoli successivi. Ogni matrice non negativa può essere associata in modo del tutto naturale a un grafo orientato nel quale i lati sono pesati con valori positivi. Questa associazione permette di visualizzare in maniera semplice e diretta le proprietà di periodicità che in realtà dipendono direttamente dai cammini del grafo considerato. Per questo motivo iniziamo questo studio partendo proprio dai grafi orientati.

2.1 Grafi orientati

Ricordiamo che un *grafo orientato* è una coppia (V, E), dove V è un insieme finito di elementi detti nodi o vertici ed E un insieme di coppie ordinate di nodi, che chiamiamo lati o archi. In questa sede rappresenteremo sempre i nodi mediante interi positivi, quindi $V = \{1, 2, \ldots, k\}$ per un qualche $k \in \mathbb{N}$; di conseguenza un lato è una coppia (i, j), dove $i, j \in \{1, 2, \ldots, k\}$.

Come al solito rappresentiamo un grafo orientato mediante un diagramma nel quale i nodi sono punti o cerchi e i lati sono frecce che connettono tali punti. La figura 2.1 definisce un grafo orientato di 12 nodi.

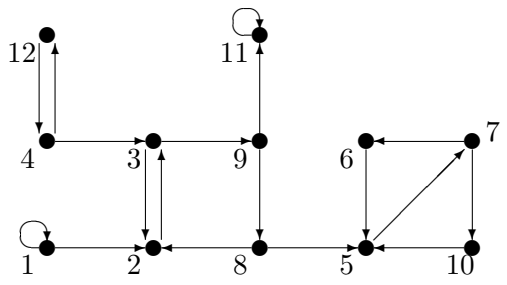


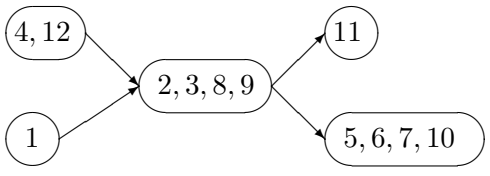
Figura 2.1: Esempio di grafo orientato

In un grafo orientato G, un *cammino* è una sequenza di nodi $C = (i_0, i_1, \ldots, i_n)$, non necessariamente distinti, tale che (i_{t-1}, i_t) è un lato di G per ogni $t = 1, 2, \ldots, n$. Diciamo inoltre che C è un cammino dal primo nodo i_0 all'ultimo nodo i_n e che la sua lunghezza è n (ovvero il numero dei suoi lati). I cammini di lunghezza 0 sono quelli formati da un solo nodo, della forma $C = (i_0)$, mentre quelli di lunghezza 1 coincidono con i lati. Il cammino C inoltre si dice *semplice* se tutti i suoi nodi sono distinti tranne al più il primo e l'ultimo. Un *ciclo* è un cammino (non necessariamente semplice) di lunghezza non nulla nel quale il primo e l'ultimo nodo coincidono. I cicli di lunghezza 1 sono anche detti *cappi*. Nel grafo della figura 2.1 ci sono due cappi, rispettivamente sui nodi 1 e 11, due cicli semplici di lunghezza 2, un ciclo semplice di lunghezza 4 e due di lunghezza 3. Nota che se per un nodo passa un ciclo C allora ne passano infiniti, tutti quelli che si ottengono ripetendo C un numero arbitrario di volte.

Dato un grafo orientato $G = (V, E)$ possiamo definire tra i suoi nodi la relazione di comunicazione $\to$, quella di comunicazione in n passi $\xrightarrow{n}$ e quella di connessione $\leftrightarrow$. Per ogni $i, j \in V$, poniamo $i \to j$ se esiste un cammino da i a j in G. Vale inoltre $i \xrightarrow{n} j$, per $n \in \mathbb{N}$, se esiste in G un cammino di lunghezza n da i a j. Infine, vale la relazione $i \leftrightarrow j$ se $i \to j$ e $j \to i$, ovvero se esiste un cammino da i a j e uno da j a i.

Il grafo G si dice *fortemente connesso* se, per ogni coppia di nodi i, j, vale la relazione $i \leftrightarrow j$. In questo caso ogni nodo è connesso a qualunque altro nodo del grafo. Più in generale invece, è facile verificare che la relazione $\leftrightarrow$ è una relazione di equivalenza, soddisfa cioè le proprietà riflessiva, simmetrica e transitiva ([1]). Essa quindi suddivide l'insieme dei nodi di G in classi di equivalenza che chiamiamo semplicemente *classi* di nodi (o *classi irriducibili*). Il sottografo formato da una classe di nodi C e dai lati di G che connettono tali nodi è chiamata *componente fortemente connessa* di G. Per esempio nel grafo rappresentato in figura 2.1 le classi sono date dagli insiemi $\{1\}$, $\{2, 3, 8, 9\}$, $\{4, 12\}$, $\{5, 6, 7, 10\}$, $\{11\}$.

Una classe A è minore di una classe B, in simboli $A \leq B$, se $a \to b$ per qualche $a \in A$ e qualche $b \in B$. Tale relazione $\leq$ è una relazione di ordine parziale definita sull'insieme delle classi di G. Essa può essere facilmente rappresentata dal cosiddetto *grafo ridotto* di G nel quale i vertici sono le classi di G e i lati sono le coppie di classi (A, B), $A \neq B$, tali che per qualche $a \in A$ e qualche $b \in B$, (a, b) è un lato di G. Chiaramente in un grafo ridotto non possono esservi cicli (si tratta quindi di un grafo diretto aciclico). Nell'esempio di figura 2.1 il grafo ridotto è rappresentato dalla seguente immagine.



Una classe di nodi C si dice *essenziale* se, per ogni $i \in C$, $i \to j$ implica $j \in C$. Quindi non è possibile uscire da una classe essenziale seguendo un cammino che parte da un suo nodo. Una classe essenziale è una classe massimale rispetto alla relazione $\leq$ definita sopra. Nota che per ogni classe non essenziale C e per ogni nodo $i \in C$, esiste $j \notin C$ tale che $i \to j$.

[1] Avvisiamo che in molti testi la relazione di comunicazione $\to$ è definita in modo diverso, ponendo $i \to j$ se esiste un cammino da i a j di lunghezza non nulla; qui preferiamo utilizzare la definizione data proprio perché in questo modo la relazione $\to$ è sempre riflessiva.

Nell'esempio di figura 2.1 le classi essenziali sono $\{11\}$ e $\{5, 6, 7, 10\}$. Analogamente, diciamo che un nodo è essenziale se appartiene a una classe essenziale. Questo significa che un nodo i è essenziale se e solo se per ogni nodo j, $i \to j$ implica $j \to i$.

2.1.1 Periodicità

Dato un grafo orientato G, consideriamo un nodo i per il quale passa almeno un ciclo; chiamiamo *periodo* di i, e lo denotiamo $d(i)$, il massimo comun divisore delle lunghezze dei cicli che passano per i:

$$d(i) = \text{mcd}\{n \in \mathbb{N} \mid i \xrightarrow{n} i\}$$

Per esempio, nel grafo di figura 2.1 i nodi 2, 3 e 4 hanno periodo 2, mentre i nodi 5 e 6 hanno periodo 3. Diciamo che un nodo è *aperiodico* se il suo periodo è 1. Nota che ogni nodo dotato di un cappio è aperiodico. In realtà si può provare che il periodo di un nodo dipende dalla sua classe, ovvero tutti i nodi di una data classe hanno lo stesso periodo. In altre parole la periodicità è una proprietà delle classi.

Proposizione 2.1 *Dato un grafo orientato G consideriamo due nodi distinti i, j tali che $i \leftrightarrow j$. Allora $d(i) = d(j)$.*

Dimostrazione. Sia C un qualunque ciclo che passa per j e sia s la sua lunghezza: proviamo innanzitutto che $d(i)$ è divisore di s. Infatti, poiché $i \leftrightarrow j$ esiste un cammino C_1 da i a j ed esiste un cammino C_2 da j a i; siano u e v le lunghezze di tali cammini. Allora C_1 e C_2 formano un ciclo di lunghezza $u + v$ passante per i e quindi $d(i)$ è un divisore di $u + v$; analogamente $d(i)$ è un divisore di $u + s + v$ perché C_1, C e C_2 formano un ciclo per i. Ne segue che $d(i)$ divide anche la differenza $(u+s+v)-(u+v) = s$, e quindi $d(i)$ è divisore della lunghezza di qualsiasi ciclo passante per j; poiché $d(j)$ è il massimo di tali divisori otteniamo $d(i) \leq d(j)$. Ripetendo lo stesso ragionamento con i e j scambiati, otteniamo $d(j) \leq d(i)$ e questo prova l'asserto. □

Chiamiamo quindi periodo di una classe il periodo di uno dei suoi nodi (e quindi di tutti). Nel grafo di figura 2.1 le classi $\{1\}$ e $\{11\}$ hanno periodo 1, le classi $\{4, 12\}$ e $\{2, 3, 8, 9\}$ hanno periodo 2, mentre $\{5, 6, 7, 10\}$ ha periodo 3.

2.2 Matrici e grafi

Ricordiamo anzitutto alcune nozioni di base riguardanti le matrici a coefficienti reali. A questo scopo useremo la notazione tradizionale sulle matrici che in questa sede è descritta in dettaglio nella sezione A.2 dell'Appendice.

Una matrice a coefficienti reali $A = [a_{ij}]$ si dice *positiva*, in simboli $A > 0$, se $a_{ij} > 0$ per ogni i, j; A si dice invece *non negativa*, rispettivamente $A \geq 0$, se $a_{ij} \geq 0$ per tutte le coppie di indici. Più in generale, se $A = [a_{ij}]$ e $B = [b_{ij}]$ sono matrici reali di ugual dimensione, l'espressione $A \geq B$ significa che $a_{ij} \geq b_{ij}$ per ogni coppia di indici i e j. Analogamente si definiscono le relazioni $A > B$, $A \leq B$, $A < B$, $A = B$.

Consideriamo una matrice quadrata $A = [a_{ij}]$ di ordine k a coefficienti reali e supponiamo $A \geq 0$. Sia $G = (V, E)$ il grafo orientato tale che $V = \{1, 2, \ldots, k\}$ ed $E = \{(i, j) \in V \times V \mid a_{ij} > 0\}$. Diciamo che G è il grafo *associato* alla matrice A e che a_{ij} è il peso del lato (i, j) per

ogni $(i, j) \in E$. In questo modo A può essere considerata come una matrice di pesi positivi sui lati di G. Se inoltre i coefficienti di A assumono solo valori in $\{0, 1\}$ (ovvero tutti i lati hanno peso 1), diciamo che A è la *matrice di adiacenza* di G. Per esempio, la matrice di adiacenza del grafo di figura 2.1 è la seguente:

	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0	0	1	0	0	0
4	0	0	1	0	0	0	0	0	0	0	0	1
5	0	0	0	0	0	1	1	0	0	0	0	0
6	0	0	0	0	0	0	1	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	1	0	0
8	0	1	0	0	1	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	1	0	0	1	0
10	0	0	0	0	1	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	1	0
12	0	0	0	1	0	0	0	0	0	0	0	0

(2.1)

La nozione di peso può essere estesa a tutti i cammini di G di lunghezza maggiore di 0. Dato un cammino $S = (i_0, i_1, \ldots, i_n)$ in G, dove $n \geq 1$, chiamiamo *peso* di S il prodotto

$$a_{i_0 i_1} a_{i_1 i_2} \cdots a_{i_{n-1} i_n}.$$

Tali valori sono sempre positivi. Inoltre, se A è la matrice di adiacenza di G allora tutti i cammini hanno peso 1.

Vogliamo ora mettere in rilievo la relazione esistente tra le potenze di A e i pesi dei cammini di data lunghezza. A tale scopo, per ogni $n \in \mathbb{N}$, denotiamo con $a_{ij}^{(n)}$ i coefficienti di A^n, per cui $A^n = [a_{ij}^{(n)}]$. Se $n \geq 2$ è facile verificare che ogni $a_{ij}^{(n)}$ è dato da

$$a_{ij}^{(n)} = \sum_{\ell=1}^{k} a_{i\ell}^{(n-1)} a_{\ell j} = \sum_{\substack{i_0 = i, i_n = j \\ i_t \in V \forall t = 1, \ldots, n-1}} a_{i_0 i_1} a_{i_1 i_2} \cdots a_{i_{n-1} i_n} \tag{2.2}$$

dove la seconda somma è estesa a tutte le sequenze di $n + 1$ indici $(i_0, i_1, i_2, \ldots, i_n)$ tali che $i_0 = i$ e $i_n = j$.

Proposizione 2.2 *Sia $A = [a_{ij}]$ una matrice quadrata non negativa e sia G il grafo associato. Allora, per ogni intero positivo n e ogni coppia di indici i, j, il coefficiente $a_{ij}^{(n)}$ della matrice A^n rappresenta la somma dei pesi di tutti i cammini di lunghezza n in G dal nodo i al nodo j.*

Dimostrazione. Ragioniamo per induzione su n. Per $n = 1$ la proprietà è ovvia. Supponiamo la proprietà vera per un valore $n \geq 1$ e dimostriamola vera per $n + 1$. Sia k la dimensione di

A. Per definizione di prodotto di matrici, sappiamo che ogni coefficiente di A^{n+1} è dato da

$$a_{ij}^{(n+1)} = \sum_{r=1}^{k} a_{ir}^{(n)} a_{rj} \tag{2.3}$$

Per ipotesi di induzione, $a_{ir}^{(n)}$ è la somma dei pesi dei cammini di lunghezza n da i a r e quindi il prodotto $a_{ir}^{(n)} a_{rj}$ è la somma dei pesi dei cammini di lunghezza $n+1$ da i a j che passano da r prima di giungere in j. Sommando tali prodotti $a_{ir}^{(n)} a_{rj}$ al variare r in tutti i modi possibili otteniamo proprio la somma di tutti i cammini di lunghezza $n+1$ da i a j; di conseguenza la proprietà segue dalla relazione (2.3). □

Una conseguenza immediata della proposizione precedente è che, per ogni i, j e n, $a_{ij}^{(n)} > 0$ se e solo se in G esiste un cammino di lunghezza n da i a j.

Inoltre, se A è la matrice di adiacenza di G, allora la relazione (2.2) determina proprio il numero di cammini di lunghezza n che vanno da i a j.

Corollario 2.3 *Se $A = [a_{ij}]$ è la matrice di adiacenza di un grafo orientato G allora, per ogni intero positivo n e ogni coppia di indici i, j, il coefficiente $a_{ij}^{(n)}$ rappresenta il numero di cammini di lunghezza n in G dal nodo i al nodo j.*

2.3 Decomposizione di matrici

Una matrice quadrata non negativa $A = [a_{ij}]$ si dice *irriducibile* se per ogni coppia di indici i, j, esiste un intero $n > 0$, in generale dipendente da i e da j, tale che $a_{ij}^{(n)} > 0$. Questo significa che nel grafo associato ad A, per ogni coppia di nodi i, j esiste un intero $n > 0$ tale che $i \xrightarrow{n} j$ (nota che n non può essere nullo).

Quindi, il grafo associato a una matrice irriducibile è fortemente connesso; inoltre, per la proposizione 2.1, tutti i suoi nodi hanno lo stesso periodo. Definiamo allora il *periodo* di una matrice irriducibile come il periodo d di uno dei nodi del grafo associato. Chiaramente d non dipende dal nodo scelto. Diciamo allora che la matrice è *periodica* se $d > 1$; se invece $d = 1$ la matrice è detta *aperiodica*.

Osserva che l'unico grafo fortemente connesso associato a una matrice non irriducibile è quello formato da un solo nodo e privo di lati. In questo caso la matrice associata è banalmente la matrice 0. Ogni altro grafo fortemente connesso possiede matrice di adiacenza irriducibile.

Una matrice quadrata non negativa A, diversa da 0, si dice *decomponibile* (o anche riducibile) se non è irriducibile. Questo significa che una matrice è decomponibile se e solo se il grafo associato contiene almeno due componenti fortemente connesse.

Le matrici decomponibili possono essere poste in una forma particolare, detta triangolare a blocchi, permutando opportunamente l'ordine delle righe e delle colonne. Infatti, data una matrice decomponibile A, supponiamo che il grafo associato possieda r componenti fortemente connesse. Poiché $r > 1$, possiamo scambiare tra loro alcune righe e le corrispondenti colonne in modo tale che siano verificate le due condizioni seguenti:

1. per ogni classe D le righe (e le colonne) appartenenti a D sono poste consecutivamente,

2. le righe (e le colonne) di ciascuna classe D precedono quelle di un'altra classe F ogniqualvolta $D \leq F$ (cioè vi sia un lato da un nodo in D a uno in F).

Otteniamo così una matrice della forma

$$\begin{bmatrix} A_{11} & A_{12} & A_{13} & \cdots & A_{1r} \\ [0] & A_{22} & A_{23} & \cdots & A_{2r} \\ [0] & [0] & A_{33} & \cdots & A_{3r} \\ & & \cdots & & \\ [0] & [0] & [0] & \cdots & A_{rr} \end{bmatrix} \tag{2.4}$$

dove le matrici A_{ii}, $i = 1, 2, \ldots, r$, si trovano sulla diagonale principale e rappresentano le matrici dei pesi delle r componenti fortemente connesse, mentre le matrici $[0]$ sono a componenti nulle. Nota che le matrici A_{ii} diverse dalla matrice 0, sono irriducibili; invece, le matrici A_{ij} con $i < j$ rappresentano i pesi dei lati che connettono nodi della componente i-esima con nodi della componente j-esima. Le matrici della forma (2.4) sono dette *triangolari a blocchi*. Chiaramente una matrice quadrata non negativa è decomponibile se e solo se mediante una permutazione di righe e delle corrispondenti colonne può essere trasformata in una matrice triangolare a blocchi.

Per esempio, nel caso della matrice (2.1), associata al grafo in figura 2.1, otteniamo la seguente forma triangolare a blocchi.

	1	4	12	2	3	8	9	5	6	7	10	11
1	[1]	0	0	1	0	0	0	0	0	0	0	0
4	0	⌈0	1⌉	0	1	0	0	0	0	0	0	0
12	0	⌊1	0⌋	0	0	0	0	0	0	0	0	0
2	0	0	0	⌈0	1	0	0⌉	0	0	0	0	0
3	0	0	0	|1	0	0	1|	0	0	0	0	0
8	0	0	0	|1	0	0	0|	1	0	0	0	0
9	0	0	0	⌊0	0	1	0⌋	0	0	0	0	1
5	0	0	0	0	0	0	0	⌈0	1	1	0⌉	0
6	0	0	0	0	0	0	0	|0	0	1	0|	0
7	0	0	0	0	0	0	0	|0	0	0	1|	0
10	0	0	0	0	0	0	0	⌊1	0	0	0⌋	0
11	0	0	0	0	0	0	0	0	0	0	0	[1]

(2.5)

Osserviamo che la forma triangolare a blocchi di una matrice decomponibile A è data da un prodotto del tipo PAP', dove P è una matrice di permutazione. Ricordiamo che una matrice di permutazione è una matrice a componenti 0 e 1 ottenuta dalla matrice identità permutando l'ordine delle righe e delle colonne (in modo corrispondente). È noto che ogni matrice di permutazione P è ortogonale, ovvero la sua trasposta P' coincide con la sua inversa ($PP' = I$).

2.4 Matrici irriducibili

Nella sezione precedente abbiamo introdotto le matrici irriducibili e abbiamo visto che ogni matrice quadrata non negativa può essere essenzialmente trasformata in una matrice triangolare a blocchi che possiede sulla diagonale principale matrici irriducibili (o la matrice 0).

Vediamo ora alcune proprietà importanti delle matrici irriducibili, riguardanti le lunghezze dei cicli e dei cammini che connettono i vari nodi del grafo associato. Si tratta principalmente di risultati sulla periodicità di tali lunghezze, basati su proprietà classiche del massimo comun divisore di interi ricordate nella sezione A.4 dell'Appendice.

Nelle seguenti proposizioni supponiamo che $A = [a_{ij}]$ sia una matrice irriducibile di dimensione k e che d sia il suo periodo.

Proposizione 2.4 *Per ogni indice i, $1 \leq i \leq k$, esiste un intero $N(i) > 0$ tale che*

$$a_{ii}^{(nd)} > 0$$

per ogni intero $n \geq N(i)$.

Dimostrazione. Sia $L(i)$ l'insieme $\{t \in \mathbb{N} \mid a_{ii}^{(t)} > 0\}$. Nota che $L(i)$ è la famiglia delle lunghezze dei cicli che passano per i nel grafo associato ad A e quindi d è il suo massimo comun divisore. Si verifica che $L(i)$ è chiuso rispetto alla somma: infatti, se $t_1, t_2 \in L(i)$ allora

$$a_{ii}^{(t_1+t_2)} \geq a_{ii}^{(t_1)} a_{ii}^{(t_2)} > 0$$

e quindi anche $t_1 + t_2 \in L(i)$. Di conseguenza, per il teorema A.4 della Appendice A.4, $L(i)$ contiene tutti i multipli di d a partire da un certo intero in poi e questo prova il risultato. □

Proposizione 2.5 *Fissato un indice i arbitrario, per ogni indice j esistono due interi r_j e q_j, $0 \leq r_j < d$, $0 < q_j$, tali che*

a) *se $a_{ij}^{(s)} > 0$ allora $s \equiv r_j \pmod{d}$;*

b) *$a_{ij}^{(r_j+nd)} > 0$ per ogni $n \geq q_j$.*

Dimostrazione. Siano s_1 e s_2 tali che $a_{ij}^{(s_1)} > 0$ e $a_{ij}^{(s_2)} > 0$; poiché $j \to i$, esiste $t \in N$ tale che $a_{ji}^{(t)} > 0$. Ne segue che $s_1 + t$ e $s_2 + t$ sono lunghezze di cicli passanti per i e quindi d è un loro divisore. Di conseguenza d divide anche la loro differenza, ovvero $s_1 + t - (s_2 + t) = s_1 - s_2 \equiv 0 \pmod{d}$ e questo implica $s_1 \equiv s_2 \pmod{d}$. In questo modo abbiamo provato la proprietà a).

Sia ora s tale $a_{ij}^{(s)} > 0$. Per la a) sappiamo che $s = r_j + n_0 d$, per qualche $n_0 \in \mathbb{N}$. Inoltre, per la proposizione 2.4, esiste $N(j)$ tale che $a_{jj}^{(nd)} > 0$, per ogni $n > N(j)$. Di conseguenza, posto $q_j = n_0 + N(j)$ e preso un intero $n \geq q_j$, abbiamo

$$a_{ij}^{(r_j+nd)} \geq a_{ij}^{(r_j+n_0 d)} a_{jj}^{((n-n_0)d)} > 0$$

e questo implica la proprietà b). □

La proposizione precedente consente di raggruppare gli indici j a seconda della classe di resto r_j determinata dalla proprietà a). Più precisamente, fissato un indice iniziale i, per ogni $r \in \{0, 1, \ldots, d-1\}$ consideriamo l'insieme C_r degli indici j tali che $r_j = r$. Si verifica che $C_r \neq \emptyset$ per ogni r e che l'unione $\bigcup_{r=0}^{d-1} C_r$ coincide con l'insieme di tutti i possibili indici $\{1, 2, \ldots, k\}$. La famiglia $\{C_r \mid r = 0, 1, \ldots, d-1\}$ forma così una partizione di $\{1, 2, \ldots, k\}$. Si può dimostrare che tale partizione non dipende dall'indice iniziale i. Cambiando l'indice

iniziale si ottiene la stessa famiglia di sottoinsiemi C_r a meno di una permutazione ciclica dei coefficienti r.

Si può verificare facilmente quest'ultima proprietà. Infatti, sia r_j la classe di resto corrispondente all'indice j rispetto all'indice iniziale i e sia r'_j lo stesso valore assumendo l'indice iniziale $i' \neq i$. Dalla proposizione precedente deduciamo che per s e t abbastanza grandi, abbiamo

$$a_{ij}^{(r_{i'}+sd+r'_j+td)} \geq a_{ii'}^{(r_{i'}+sd)} a_{i'j}^{(r'_j+td)} > 0$$

e quindi per la proprietà a)

$$r_{i'} + sd + r'_j + td \equiv r_j \pmod{d}$$

ovvero $r_{i'} + r'_j \equiv r_j \pmod{d}$. Questo significa appunto che tutti i valori r'_j sono ottenuti dai valori r_j attraverso una permutazione ciclica determinata dalla lunghezza $r_{i'}$.

Usando la partizione $\{C_r \mid r = 0, 1, \ldots, d-1\}$, possiamo allora permutare le righe e le corrispondenti colonne trasfomando la matrice in una forma canonica nella quale tutti gli indici nella stessa classe sono posti consecutivamente e le classi C_r sono disposte in ordine crescente rispetto a r. La matrice ottenuta è del tipo

$$A' = \begin{bmatrix} [0] & A_0 & [0] & \cdots & [0] \\ [0] & [0] & A_1 & \cdots & [0] \\ [0] & [0] & [0] & \cdots & [0] \\ & & \cdots & & \\ [0] & [0] & [0] & \cdots & A_{d-2} \\ A_{d-1} & [0] & [0] & \cdots & [0] \end{bmatrix}$$

dove le sottomatrici [0] sulla diagonale principale sono quadrate e ogni A_i è la sottomatrice (non necessariamente quadrata) dei pesi dei lati da indici in C_i a indici in $C_{i+1 (\mathrm{mod}\ d)}$.

2.5 Matrici primitive

Le matrici primitive sono un tipo particolare di matrici irriducibili. Formalmente, una matrice non negativa A si dice *primitiva* se esiste un intero $n > 0$ tale che $A^n > 0$. Questo significa che nel grafo associato, per ogni coppia di nodi i e j abbiamo $i \xrightarrow{n} j$. Per esempio la matrice

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

è una matrice primitiva perché $B^2 > 0$, ovvero tutte le coppie di nodi possono essere connesse da un cammino di lunghezza 2.

Dalla definizione segue immediatamente che una matrice primitiva è anche irriducibile. Viceversa, vi sono matrici irriducibili che non sono primitive. Per esempio, nella seguente figura la matrice D è irriducibile ma non primitiva; essa rappresenta il grafo G_1 ed è facile verificare che nessuna delle sue potenze è strettamente positiva.

$$D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad ; \quad G_1 = \quad$$

In particolare, se m è pari abbiamo $D^m = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$; mentre se m è dispari si verifica $D^m = D$.

Inoltre, se A è una matrice primitiva e $A^n > 0$, allora $A^m > 0$ per ogni $m \geq n$: di conseguenza tutti gli indici di A sono aperiodici perché possiedono un ciclo di lunghezza m per ogni $m \geq n$. Più in generale si può provare il seguente risultato.

Proposizione 2.6 *Una matrice non negativa A è primitiva se e solo se A è irriducibile e aperiodica.*

Dimostrazione. Se A è primitiva, per la discussione precedente sappiamo che A è irriducibile e aperiodica. Viceversa, supponiamo che A sia irriducibile e abbia periodo $d = 1$. Applichiamo la proposizione 2.5 alla matrice A. Chiaramente, tutti i coefficienti r_j in questo caso sono uguali a 0. Inoltre, per l'enunciato b), sappiamo che per ogni i, j esiste un intero $q(i, j) > 0$ tale che $a_{ij}^{(n)} > 0$ per ogni $n \geq q(i, j)$; scegliamo allora $N = \max\{q(i, j) \mid i, j\}$ e otteniamo che, per ogni $n \geq N$, $a_{ij}^{(n)} > 0$ per tutti gli indici i, j. Questo significa $A^n > 0$ e quindi A è primitiva. □

A questo punto è naturale chiedersi, per una matrice primitiva $A \in \mathbb{R}_+^{k\times k}$, quale sia il minimo intero positivo n tale che $A^n > 0$. Tale n è il più piccolo intero per il quale, nel grafo associato ad A, esiste un cammino di lunghezza n che va da un nodo i a un nodo j per ogni possibile coppia di nodi (i, j). Questo valore n dipende in generale dalla matrice A, e non può essere lo stesso per tutte le matrici primitive di data dimensione. Per esempio, è chiaro che se $A > 0$ allora $n = 1$. Tuttavia in generale il valore di n può essere maggiore di k, come mostra il seguente esempio.

Esempio 2.1 Considera un grafo $G = (V, E)$ di $k \geq 3$ nodi, $V = \{1, 2 \ldots, k\}$, formato semplicemente da un cappio per un nodo qualsiasi e da un ciclo semplice che passa (una e una volta sola) per ogni vertice. Sia $A = [a_{ij}] \in \{0, 1\}^{k\times k}$ la matrice di adiacenza di G. Chiaramente A è primitiva perché G è fortemente connesso e possiede un nodo di periodo 1. Nota che, scambiando opportunamente righe e colonne, $A = [a_{ij}]$ può essere ridotta a una matrice nella quale $a_{11} = 1$, tutti i coefficienti sopra la diagonale principale sono uguali a 1 (ovvero $a_{i,i+1} = 1$ per ogni $i = 1, 2, \ldots, k-1$) e $a_{k1} = 1$, mentre tutti gli altri coefficienti sono uguali a 0. In queste ipotesi il minimo $n \in \mathbb{N}$ per cui $A^n > 0$ risulta essere $n = 2k - 2$.

Per dimostrare questa proprietà proviamo innanzitutto che per ogni coppia di nodi i, j esiste sempre un cammino di lunghezza $2k - 2$ da i a j: infatti, supponendo la matrice A nella forma descritta sopra, basta partire dal nodo i, seguire il ciclo e giungere nel nodo 1 (dotato di cappio), transitare eventualmente per il cappio un numero opportuno di volte, e quindi arrivare in j sempre seguendo il ciclo. Chiaramente questo cammino non è semplice, sia perché potrebbe attraversare il cappio, sia perché potrebbe passare 2 volte dal nodo i. Nota che per $i = 2$ e $j = k$ tale cammino non attraversa il cappio (ma passa due volte per il nodo 2). In ogni caso la sua esistenza implica $a_{ij}^{(2k-2)} > 0$ per ogni ogni coppia di indici i, j e quindi $A^{2k-2} > 0$.

D'altra parte è evidente che per ogni $\ell = 1, 2, \ldots, k-1$ si verifica $a_{jj}^{(\ell)} = 0$, per tutti i nodi j che non possiedono il cappio. Questo implica che A^ℓ non è una matrice positiva per alcun $\ell \in \{1, 2, \ldots, k-1\}$. Inoltre, è facile verificare che per ogni $\ell = k, k+1, \ldots, 2k-3$ abbiamo $a_{2k}^{(\ell)} = 0$. Infatti, per andare dal nodo 2 al nodo k con un cammino più lungo di

$k-1$, dobbiamo per forza giungere nel nodo 1 con $k-1$ passi, e poi usare altri $k-1$ lati per andare da 1 a k, non ne possiamo cioé usare di meno. Questo prova $A^\ell \not> 0$ per ogni $\ell \in \{k, k+1, \ldots, 2k-3\}$. Di conseguenza $n = 2k-2$ è il più piccolo intero positivo tale che $A^n > 0$.

2.6 Il teorema di Perron-Frobenius

La proprietà principale delle matrici primitive è costituita dal seguente teorema riguardante gli autovalori e gli autovettori di tali matrici. In questa sede ci preme innanzitutto mettere in rilievo questa proprietà e ricordare alcune importanti conseguenze senza entrare nel dettaglio della prova, abbastanza lunga e complessa, che comunque si può trovare in [21]. Le nozioni di autovalore e autovettore, insieme alle loro proprietà di base, sono invece ricordate nella sezione A.3 dell'Appendice.

Teorema 2.7 *(Teorema di Perron-Frobenius per matrici primitive) Sia $A \geq 0$ una matrice primitiva. Allora esiste un autovalore λ di A che gode delle seguenti proprietà:*

1. *λ è reale e maggiore di 0;*
2. *ogni autovalore μ di A diverso da λ verifica la relazione $|\mu| < \lambda$;*
3. *λ ammette autovettori destri e sinistri strettamente positivi;*
4. *λ è radice semplice dell'equazione caratteristica di A (la sua molteplicità algebrica è 1).*

La costante λ è anche chiamata autovalore di Perron-Frobenius della matrice A.

Diverse proprietà utili possono essere derivate dal teorema precedente. La principale riguarda l'ordine di grandezza delle potenze di matrici primitive. Essa asserisce che la potenza A^n di una matrice primitiva A cresce con ordine di grandezza uguale a λ^n, la differenza inoltre è determinata dal modulo massimo degli altri autovalori e dalla loro molteplicità.

Teorema 2.8 *Sia A una matrice primitiva, e siano $\lambda, \mu_1, \mu_2, \ldots, \mu_t$ i suoi autovalori distinti, disposti in modo tale che $\lambda > |\mu_1| \geq |\mu_2| \geq \ldots \geq |\mu_t|$ e la molteplicità m di μ_1 sia maggiore o uguale a quella degli autovalori aventi lo stesso modulo di μ_1. Allora, al crescere di n, abbiamo*

$$A^n = \lambda^n uv' + O(n^{m-1}|\mu_1|^n) \tag{2.6}$$

dove v' e u sono rispettivamente autovettore sinistro e autovettore destro corrispondenti a λ, normalizzati in modo tale che $v'u = 1$.

Nota che l'uguaglianza (2.6) può essere interpretata come una estensione della equazione (A.2) al caso delle matrici primitive (che in generale possono avere autovalori di molteplicità algebrica maggiore di 1).

Ricordiamo infine le ulteriori seguenti proprietà nelle quali $A = [a_{ij}]$ è sempre una matrice primitiva e λ il suo autovalore di Perron-Frobenius. Anche in questo caso le dimostrazioni si possono trovare in [21].

1. λ soddisfa la relazione
$$\min_i \sum_j a_{ij} \leq \lambda \leq \max_i \sum_j a_{ij}$$
con l'uguaglianza che vale solo se i valori $\sum_j a_{ij}$ sono uguali per tutte le righe i (inoltre una proprietà analoga vale per le colonne);

2. se B è una matrice delle stesse dimensioni di A tale che $0 \leq B \leq A$ e β è un suo autovalore, allora $|\beta| \leq \lambda$ e inoltre $|\beta| = \lambda$ se e solo se $B = A$;

3. se v e u sono rispettivamente autovettore sinistro e autovettore destro di λ, normalizzati in modo tale che $v'u = 1$ (ovvero definiti come nel teorema 2.8), allora la matrice uv' è data da
$$uv' = \frac{Adj(\lambda I - A)}{\varphi'(\lambda)}$$
dove $\varphi(x) = \det(xI - A)$.

Concludiamo osservando che un analogo del teorema 2.7 vale anche per le matrici irriducibili; l'unica differenza è che nel caso di matrici periodiche esistono più autovalori di modulo massimo.

Teorema 2.9 *Se $A \geq 0$ è una matrice irriducibile allora esiste un autovalore λ di A che verifica le proprietà 1, 3, 4 del teorema 2.7 e tale che $|\mu| \leq \lambda$ per ogni autovalore μ di A. Inoltre, se il periodo di A è $d \geq 1$ allora le costanti $\lambda e^{i2s\pi/d}$, $s = 0, 1, \ldots, d-1$, sono gli autovalori di A di modulo λ.*

Nota che gli autovalori di modulo massimo di una matrice irriducibile di periodo d coincidono con le radici complesse dell'equazione $x^d - \lambda^d = 0$.

2.7 Matrici stocastiche

Finora abbiamo considerato generiche matrici a coefficienti non negativi. Tuttavia, nei capitoli successivi utilizzeremo matrici i cui coefficienti sono probabilità e risulterà naturale supporre che la somma dei valori disposti su ogni riga sia uguale a uno. Le matrici che godono di questa proprietà sono dette stocastiche.

Formalmente, un vettore riga $v = (v_1, v_2, \ldots, v_r) \in \mathbb{R}^r$ si dice *stocastico* se $0 \leq v_i \leq 1$ per ogni indice i e inoltre $\sum_{i=1}^r v_i = 1$ (e lo stesso dicasi per i vettori colonna). Analogamente, una matrice $P = [p_{ij}]$ si dice *stocastica* se ogni sua riga è un vettore stocastico, ovvero se $0 \leq p_{ij} \leq 1$ per ogni coppia di indici i, j, e inoltre $\sum_{j \geq 1} p_{ij} = 1$ per ogni i. Nel seguito supporremo sempre che una matrice stocastica sia quadrata. Inoltre una matrice doppiamente stocastica è una matrice stocastica P nella quale anche le colonne sono vettori stocastici, ovvero $\sum_{i \geq 1} p_{ij} = 1$ per ogni j. È facile verificare che il prodotto di due matrici stocastiche è ancora una matrice stocastica. Valgono inoltre le seguenti proposizioni.

Proposizione 2.10 *Sia P una matrice stocastica di dimensione r. Allora 1 è autovalore di P e ammette come corrispondente autovettore destro il vettore e di dimensione r tale che $e' = (1, 1, \ldots, 1)$.*

Dimostrazione. Sia $P = [p_{ij}]$. Per la stessa definizione di matrice stocastica abbiamo, per ogni $i = 1, \ldots, r$, $(Pe)_i = \sum_j p_{ij} = 1$ e quindi vale

$$Pe = e$$

Questo prova che 1 è autovalore di P e che e è un autovettore destro di P corrispondente a 1. □

Per lo stesso motivo, se P è una matrice doppiamente stocastica allora $e'P = e'$; di conseguenza, e è anche autovettore sinistro di P corrispondente a 1.

Proposizione 2.11 *Se λ è un autovalore di una matrice stocastica allora $|\lambda| \leq 1$.*

Dimostrazione. Sia $P = [p_{ij}]$ una matrice stocastica di dimensione r e sia λ un suo autovalore. Consideriamo un autovettore sinistro v di P corrispondente a λ. Allora $v'P = \lambda v'$ e quindi abbiamo

$$\sum_{j=1}^{r} |\lambda v_j| = \sum_{j=1}^{r} |\sum_{i=1}^{r} p_{ij} v_i| \leq \sum_{i=1}^{r} |v_i| \, |\sum_{j=1}^{r} p_{ij}| = \sum_{i=1}^{r} |v_i|$$

Di conseguenza $|\lambda| \sum_{j=1}^{r} |v_j| \leq \sum_{i=1}^{r} |v_i|$ e questo implica $|\lambda| \leq 1$. □

Nel caso di matrici stocastiche primitive possiamo applicare i teoremi 2.7 e 2.8 alle proprietà precendenti ottenendo il seguente risultato.

Proposizione 2.12 *Se P è una matrice stocastica primitiva allora 1 è il suo autovalore di Perron-Frobenius e inoltre, per qualche $0 \leq \varepsilon < 1$, abbiamo*

$$P^n = ev' + O(\varepsilon^n)$$

dove v è l'autovettore sinistro di P corrispondente a 1 tale che $\sum_{i \geq 1} v_i = 1$.

Quindi, nella proposizione precedente v è un vettore stocastico. Inoltre ev' è una matrice *stabile*, cioè possiede tutte le righe uguali, in questo caso coincidenti con v'. Nota anche che, per $n \to +\infty$, P^n converge alla matrice ev' e la velocità di convergenza è esponenziale.

Nel caso di matrici doppiamente stocastiche e è anche autovettore sinistro corrispondente a 1 e quindi otteniamo il seguente enunciato.

Corollario 2.13 *Se P è una matrice primitiva doppiamente stocastica di dimensione r, allora l'autovettore sinistro v definito nella proposizione precedente è dato da $v' = (1/r, 1/r, \ldots, 1/r)$.*

Capitolo 3

Nozioni fondamentali sulle catene di Markov

Le catene di Markov furono di fatto introdotte dal matematico russo A.A. Markov (1856-1922) in una serie di articoli, il primo dei quali apparso nel 1906, dedicati allo studio di sequenze di variabili aleatorie debolmente dipendenti. Lo scopo era quello di estendere a questo caso le note proprietà asintotiche valide nell'ipotesi di indipendenza delle variabili. La nozione di dipendenza qui considerata è relativamente debole, nel senso che una volta fissato il valore di una variabile della sequenza, la distribuzione di probabilità della variabile successiva è pienamente determinata e non dipende dai valori delle variabili precedenti. In parole povere, una volta noto il presente, il futuro non dipende dal passato.

Questo modello probabilistico è del tutto naturale e si applica a numerose situazioni. Negli anni '30 e '40 le catene di Markov sono state studiate e approfondite in maniera sistematica da diversi autori e oggi esiste una vasta letteratura sull'argomento, con innumerevoli applicazioni che riguardano non solo il calcolo delle probabilità ma anche le scienze naturali, quelle economiche, sociali e svariati altri settori. Per una bibliografia aggiornata agli anni '80 si può consultare [9], dove si possono trovare i riferimenti alle collezioni dei lavori originali di Markov e agli articoli dei principali autori successivi. Altri riferimenti più recenti si trovano per esempio in [25, 3, 7].

In questa sede ci occuperemo principalmente delle catene di Markov finite e omogenee. Prima di dare la definizione formale illustriamo la nozione attraverso alcuni classici esempi tratti da vari testi che si possono consultare per ulteriori informazioni [5, 14, 9, 25, 7].

3.1 Esempi

Un modello per il tempo atmosferico [14, 25]

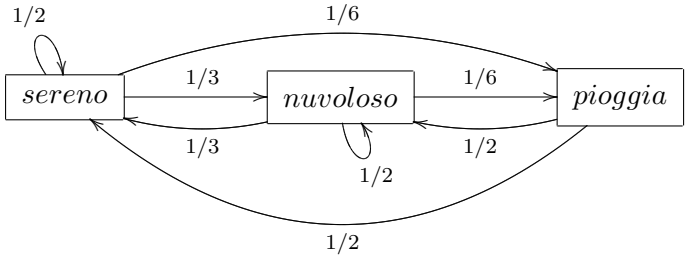
Vogliamo definire un modello probabilistico per descrivere l'evoluzione del tempo in un periodo di riscaldamento climatico, caratterizzato da scarse precipitazioni. Per semplicità, assumiamo tre possibili condizioni del tempo in una giornata qualsiasi: sereno, nuvoloso, pioggia. Supponiamo che le condizioni di domani dipendano sempre dal tempo di oggi ma non da quello dei giorni precedenti. Inoltre, assumiamo che non vi siano mai due giornate di pioggia consecutive; se un giorno piove, la giornata successiva è serena o nuvolosa con

uguale probabilità. Invece, dopo una giornata serena o nuvolosa il tempo rimane invariato con probabilità 1/2; se si verifica un cambiamento allora piove in un terzo dei casi.

In queste ipotesi, le probabilità di transizione tra le varie condizioni atmosferiche in due giorni consecutivi possono essere rappresentate dalla seguente matrice:

	sereno	nuvoloso	pioggia
sereno	1/2	1/3	1/6
nuvoloso	1/3	1/2	1/6
pioggia	1/2	1/2	0

oppure dal grafo pesato riportato di seguito.



Domande naturali che possiamo porci sono le seguenti: se oggi è sereno qual è la probabilità che piova almeno una volta nei prossimi 5 giorni? Mediamente, quante volte piove nell'arco di un mese? Quanto dura in media un periodo di siccità?

La rovina del giocatore [5, 9].

Consideriamo un gioco nel quale due concorrenti, chiamati A e B rispettivamente, si disputano un capitale complessivo di r monete in una successione di partite consecutive. Inizialmente, A possiede k monete, mentre B ne possiede $r-k$, per un dato $k \in \{1, 2, \ldots, r-1\}$. A ogni partita A vince con una probabilità p prefissata, dove $0 < p < 1$, mentre B vince con probabilità $q = 1 - p$. Inoltre, ogni partita è indipendente dalle altre e alla sua conclusione il perdente paga una moneta al vincitore. Il gioco termina quando uno dei due contendenti rimane senza monete.

Questo gioco può essere rappresentato da un insieme di stati $S = \{0, 1, 2, \ldots, r\}$, dove lo stato corrente rappresenta il capitale di A. Quindi, k è lo stato iniziale del gioco, lo stato 0 rappresenta la rovina di A e lo stato r la rovina di B. Ogni partita determina la transizione dallo stato corrente i a uno dei due stati adiacenti $i + 1$ o $i - 1$, a seconda della vittoria di A o di B. Le probabilità di transizione tra i vari stati sono allora definite dalla matrice $P = [P(i, j)]_{i,j=0,1,\ldots,r}$ tale che

$$P(i, i+1) = \begin{cases} p & \text{se } i \neq 0, r \\ 0 & \text{altrimenti} \end{cases}, \quad P(i, i-1) = \begin{cases} q & \text{se } i \neq 0, r \\ 0 & \text{altrimenti} \end{cases}, \quad P(0,0) = P(r,r) = 1 \ ,$$

mentre in tutti gli altri casi $P(i, j) = 0$. La matrice P è quindi la seguente:

	0	1	2	3	...	r-2	r-1	r
0	1	0	0	0	...	0	0	0
1	q	0	p	0	...	0	0	0
2	0	q	0	p	...	0	0	0
.	.	.	.	.	...	.	.	.
.	.	.	.	.	...	.	.	.
.	.	.	.	.	...	.	.	.
r-1	0	0	0	0	...	q	0	p
r	0	0	0	0	...	0	0	1

Lo schema precedente può rappresentare diversi altri processi aleatori. Uno di questi è la nota "passeggiata dell'ubriaco" (vedi per esempio [25]). Sono inoltre state considerate varie estensioni. Possiamo ad esempio sostituire i due stati assorbenti 0 e r con due barriere elastiche o riflettenti. Nel primo caso avremmo $P(0,0) = a$, $P(0,1) = b$, $P(r,r) = c$, $P(r,r-1) = d$, con $a, b, c, d \in (0,1)$, $a + b = 1$ e $c + d = 1$. Mentre nel secondo, $P(0,0) = P(r,r) = 0$ e $P(0,1) = P(r-1,r) = 1$.

Moto rettilineo di una particella

Molti esempi rilevanti possono essere rappresentati dal moto di una particella su un segmento di interi [5, 9]. Questo modello è definito da una particella che si muove sui punti $\{0, 1, \ldots, r\}$, per un intero $r > 0$ fissato. Ad ogni istante, dalla posizione corrente i la particella si muove di una posizione avanti o indietro con probabilità rispettive p_i e q_i, oppure rimane ferma con probabilità m_i, dove $p_i, q_i, m_i \in [0,1]$ e $p_i + q_i + m_i = 1$ (chiaramente $q_0 = p_r = 0$). Le probabilità di transizione sono dunque rappresentate dalla seguente matrice:

	0	1	2	3	...	r-2	r-1	r
0	m_0	p_0	0	0	...	0	0	0
1	q_1	m_1	p_1	0	...	0	0	0
2	0	q_2	m_2	p_2	...	0	0	0
.	.	.	.	.	...	.	.	.
.	.	.	.	.	...	.	.	.
.	.	.	.	.	...	.	.	.
r-1	0	0	0	0	...	q_{r-1}	m_{r-1}	p_{r-1}
r	0	0	0	0	...	0	q_r	m_r

Passeggiate a caso in un grafo

Citiamo infine un altro esempio rilevante che riguarda il moto di un particella in un grafo. Dato un grafo non orientato $G = (V, E)$ supponiamo che una particella si muova tra i nodi di G partendo da un vertice prefissato; ad ogni passo si sceglie il nuovo vertice in modo equiprobabile tra tutti quelli adiacenti al nodo corrente. Per ogni $u \in V$ denotiamo con d_u il numero di vertici adiacenti a u; allora, le probabilità di transizione sono rappresentate dalla matrice $P = [P_{uv}]_{u,v \in V}$ dove, per ogni $u, v \in V$,

$$P_{uv} = \begin{cases} \frac{1}{d_u} & \text{se } \{u,v\} \in E \\ 0 & \text{altrimenti} \end{cases}$$

3.2 Definizione

Per definire formalmente una catena di Markov finita e omogenea abbiamo bisogno di tre quantità:

a) un insieme finito $S = \{1, 2, \ldots, k\}$ di elementi, chiamati *stati*;

b) una distribuzione di probabilità μ definita su S che chiamiamo *distribuzione iniziale*, ovvero una funzione $\mu : S \longrightarrow \mathbb{R}$ tale che

$$\mu(i) \geq 0 \quad \text{per ogni } i \in S \quad \text{e inoltre} \quad \sum_{i \in S} \mu(i) = 1$$

c) una matrice stocastica P con indici in S, detta *matrice di transizione*, ovvero una famiglia di coefficienti $P = [p(i,j)]_{i,j \in S}$ tale che

$$p(i,j) \geq 0 \quad \text{per ogni } i, j \in S \quad \text{e inoltre} \sum_{j \in S} p(i,j) = 1 \quad \text{per ogni } i \in S$$

Una *catena di Markov finita e omogenea* con spazio degli stati S, distribuzione iniziale μ e matrice di transizione $P = [p(i,j)]$, è una sequenza $\{X_n\}_{n \in \mathbb{N}}$ di variabili aleatorie a valori in S tale che:

1. per ogni $i \in S$,
$$\Pr(X_0 = i) = \mu(i) \ ;$$
2. per ogni intero $n > 0$, ogni $i, j \in S$ e ogni n-pla di stati $i_0, i_1, \ldots, i_{n-1}$
$$\Pr(X_{n+1} = j \mid X_0 = i_0, \ldots, X_{n-1} = i_{n-1}, X_n = i) = \Pr(X_{n+1} = j \mid X_n = i) \ ;$$
3. per ogni $n \in \mathbb{N}$ e ogni $i, j \in S$
$$\Pr(X_{n+1} = j \mid X_n = i) = p(i,j) \ .$$

La condizione 2 è nota come *proprietà di Markov*. Essa stabilisce che per ogni $n \in \mathbb{N}$, una volta noto il valore di X_n, l'evento $X_{n+1} = j$ non dipende dai valori assunti dalle variabili $X_0, X_1, \ldots, X_{n-1}$. In modo intuitivo, possiamo dire che la conoscenza del presente è sufficiente a determinare il futuro, nel senso che quest'ultimo non dipende dal passato.

La condizione 3 invece rappresenta l'omogeneità del processo; essa afferma che la probabilità di passare da uno stato i all'istante n-esimo a uno stato j all'istante $n+1$ non dipende da n ma solo da i e j. Tale probabilità rimane quindi la stessa per tutto il processo.

È naturale chiedersi se la definizione appena data descrive un'entità effettiva, che esiste davvero e che può essere costruita a partire dalle ipotesi fissate. In realtà si può provare che una tale sequenza $\{X_n\}$ esiste sempre. Più precisamente, per ogni tripla (S, μ, P) definita dalle condizioni **a)**, **b)**, **c)**, si può sempre costruire una catena di Markov corrispondente, cioè una sequenza di variabili aleatorie $\{X_n\}_{n \in \mathbb{N}}$ che soddisfi le proprietà 1, 2 e 3 date sopra.

Per costruire tale sequenza è necessario fissare lo spazio di probabilità sul quale tutte le X_n sono definite, a partire dalle quantità S, μ e P. A tal fine, chiamiamo *traiettoria* una

qualunque sequenza di infiniti stati, ovvero un elemento $t = (t_0, t_1, \ldots, t_n \ldots)$, dove $t_n \in S$ per ogni $n \in \mathbb{N}$. Denotiamo inoltre con Ω l'insieme di tutte le traiettorie:

$$\Omega = \{t = (t_0, t_1, \ldots, t_n \ldots) \mid t_n \in S \text{ per ogni } n \in \mathbb{N}\}$$

e, per ogni $b \in S^{n+1}$ ($n \in \mathbb{N}$), $b = (b_0, b_1, \ldots, b_n)$, sia $C(b)$ il *cilindro* di base b, ovvero l'insieme di tutte le traiettorie che sono continuazioni di b:

$$C(b) = \{t \in \Omega \mid t_i = b_i \text{ per ogni } i = 0, 1, \ldots, n\}$$

Per convenzione consideriamo anche l'insieme Ω come un cilindro, ponendo $\Omega = C(\epsilon)$, dove ϵ rappresenta il vettore vuoto. Inoltre definiamo la probabilità di un cilindro $C(b)$, con $b = (b_0, b_1, \ldots, b_n)$, ponendo

$$\Pr_\mu(C(b)) = \mu(b_0)p(b_0, b_1)p(b_1, b_2) \cdots p(b_{n-1}, b_n)$$

e fissando in particolare $\Pr_\mu(\Omega) = 1$.

Chiaramente l'insieme dei cilindri non forma una σ-algebra e di conseguenza la funzione $\Pr_\mu$ non è per ora una misura di probabilità. Tuttavia un noto risultato dovuto a Kolmogorov garantisce l'esistenza di un'unica minima σ-algebra $\mathcal{B}$ che include la famiglia di tutti i cilindri: a tale σ-algebra la funzione $\Pr_\mu$ può essere estesa in modo da costituire effettivamente una misura di probabilità. La costruzione della σ-algebra $\mathcal{B}$ e la relativa estensione di $\Pr_\mu$ sono argomenti classici di teoria della misura che esulano dagli scopi della nostra presentazione (per maggiori dettagli si veda [9, sez. 1.5 e 2.1] oppure [25, sez. 1.B]).

In questo modo, la tripla $(\Omega, \mathcal{B}, \Pr_\mu)$ forma uno spazio di probabilità sul quale possiamo definire le variabili aleatorie X_n, $n \in \mathbb{N}$, come semplici proiezioni, ponendo $X_n : \Omega \longrightarrow S$ tale che

$$X_n(t) = t_n \ , \qquad \text{per ogni } t \in \Omega,\ t = (t_0, t1, \ldots, t_k, \ldots) \ .$$

Si può ora verificare facilmente che la sequenza $\{X_n\}$ soddisfa le condizioni 1, 2 e 3 della definizione. In particolare, per ogni $n \in \mathbb{N}$, la probabilità congiunta delle variabili $X_0, X_1, \ldots, X_n$ è definita dalla probabilità dei corrispondenti cilindri: per ogni $b = (b_0, b_1, \ldots, b_n) \in S^{n+1}$,

$$\Pr_\mu(X_0 = b_0, \ldots, X_n = b_n) = \Pr_\mu(C(b)) = \mu(b_0)p(b_0, b_1)p(b_1, b_2) \cdots p(b_{n-1}, b_n)$$

Nel seguito supporremo sempre che ogni catena di Markov $\{X_n\}$ sia definita sullo spazio di probabilità $(\Omega, \mathcal{B}, \Pr_\mu)$ appena descritto (solitamente chiamato *spazio delle traiettorie*). Inoltre, se μ è puntuale, ovvero $\mu = \delta_i$ per qualche $i \in S$, allora rappresenteremo $\Pr_\mu$ nella forma $\Pr_i$. In particolare, per ogni distribuzione iniziale μ abbiamo $\Pr_i(X_n = j) = \Pr_\mu(X_n = j \mid X_0 = i)$. Denoteremo infine con E_i l'operatore di valor medio associato a $\Pr_i$. Se per esempio Y è una variabile aleatoria a valori in $\mathbb{N}$ definita sullo spazio delle traiettorie, allora $E_i(Y) = \sum_{n \in \mathbb{N}} n \Pr_i(Y = n)$.

Osserviamo infine che ogni catena di Markov finita e omogenea, con insieme degli stati S e matrice di transizione $P = [p(i, j)]_{i,j \in S}$, può essere associata a un grafo orientato $G = (V, E)$, dove $V = S$, $E = \{(i, j) \mid p(i, j) > 0\}$ e ogni lato $(i, j) \in E$ è etichettato da $p(i, j)$. Diremo anche che G è il *grafo di comunicazione* della catena di Markov. In questo modo possiamo classificare gli stati della catena usando le relazioni di comunicazione $\rightarrow$ e di connessione $\leftrightarrow$ del grafo, come illustrato nel capitolo 2.

Nota che, per ogni $i, j \in S$, abbiamo $i \to j$ se $i = j$ oppure esiste una sequenza di stati $i_0, i_1, \ldots, i_n$ con $i_0 = i$ e $i_n = j$ tali che

$$\prod_{\ell=1}^{n} p(i_{\ell-1}, i_\ell) \; > \; 0$$

Questa condizione è equivalente a richiedere che $\Pr_i(X_n = j) > 0$ per qualche $n \in \mathbb{N}$.

Inoltre possiamo estendere in modo ovvio agli stati le nozioni e le proprietà introdotte per i nodi. Così una classe di stati non è altro che un insieme di nodi nel corrispondente grafo di comunicazione che forma una classe di equivalenza rispetto alla relazione $\leftrightarrow$. Analogamente parleremo di periodo di uno stato, di stati periodici e aperiodici e diremo che uno stato $i \in S$ è essenziale se i è un nodo essenziale nel grafo di comunicazione.

Una catena di Markov finita eredita anche in modo naturale le proprietà della matrice di transizione associata P. Così diremo che la catena è irriducibile se la matrice P è irriducibile. In modo analogo si definiscono le catene primitive, quelle periodiche e aperiodiche.

Osservazione 3.1 La definizione di catena di Markov che abbiamo introdotta può essere estesa in vari sensi. Se l'insieme degli stati S è infinito (ma numerabile) parleremo di catena di Markov *infinita*. Spesso nella letteratura la nozione di catena di Markov fa riferimento a questa definizione; nota che in questo caso la matrice $P = [p(i, j)]$ possiede infinite righe e infinite colonne.

Ricordiamo inoltre che una catena di Markov *non omogenea* è una sequenza di v.a. $\{X_n\}$ che soddisfa le condizioni 1 e 2 ma non la 3. In questo caso non avremo più un'unica matrice di transizione P ma una sequenza di matrici stocastiche $\{P_n\}$, $P_n = [p_n(i, j)]_{i,j \in S}$, una per ciascun passo del processo: per ogni $n \in \mathbb{N}$ e ogni $i, j \in S$

$$\Pr(X_{n+1} = j \mid X_n = i) = p_n(i, j) \; .$$

Infine, un'altra notevole estensione è data dai cosiddetti *processi di Markov*: supponi che il parametro n non sia più discreto ma continuo; allora avremo una famiglia di variabili aleatorie $\{X(t) \mid t \in \mathbb{R}_+\}$, a valori su un insieme S di stati, dotata di una corrispondente famiglia di matrici $\{P(h) = [p_h(i, j)]_{i,j \in S} \mid h \in \mathbb{R}_+\}$. Qui la proprietà di Markov (analoga alla condizione 2) si fa più complessa e viene espressa dalla seguente relazione

$$\Pr(X(t_{n+1}) = j \mid X(t_0) = i_0, \ldots, X(t_{n-1}) = i_{n-1}, X(t_n) = i) = \Pr(X(t_{n+1}) = j \mid X(t_n) = i)$$

per ogni sequenza di valori $0 \le t_0 < t_1 < \cdots < t_n < t_{n+1}$, ogni $i, j \in S$ e ogni n-pla di stati $i_0, i_1, \ldots, i_{n-1}$. Mentre la proprietà di omogeneità viene data da

$$\Pr(X(t + h) = j \mid X(t) = i) = p_h(i, j)$$

per ogni $t \ge 0$, $h > 0$ e $i, j \in S$.

3.3 Probabilità di transizione

Sia $\{X_n\}$ una catena di Markov finita e omogenea, con spazio degli stati S, distribuzione iniziale μ e matrice di transizione $P = [p(i, j)]_{i,j \in S}$. Valutiamo ora le probabilità di transizione in un numero di passi $n > 1$, in funzione delle potenze della matrice P.

A tale scopo, per ogni $n \in \mathbb{N}$ denotiamo con $p^{(n)}(i,j)$ i coefficienti della matrice P^n. Ovvero poniamo

$$P^n = [p^{(n)}(i,j)]_{i,j\in S}$$

Nota che $p^{(1)}(i,j) = p(i,j)$, mentre $p^{(0)}(i,j)$ coincide con il coefficiente di Kronecker δ_{ij} e, per il prodotto di matrici, si ha

$$p^{(n+1)}(i,j) = \sum_{\ell\in S} p(i,\ell)p^{(n)}(\ell,j)$$

La proposizione seguente è importante perché stabilisce che $p^{(n)}(i,j)$ coincide con la probabilità di passare dallo stato i allo stato j in n passi in un qualunque momento del processo.

Proposizione 3.1 *Per ogni $k, n \in \mathbb{N}$ e ogni $i, j \in S$, supponendo $Pr_\mu(X_k = i) > 0$ abbiamo*

$$Pr_\mu(X_{k+n} = j \mid X_k = i) = p^{(n)}(i,j)$$

Dimostrazione. Per $n = 0$ la proprietà è ovvia. Se $n = 1$ essa coincide con la condizione 3 della definizione (omogeneità). Ragionando per induzione, supponiamo che la proprietà sia vera per $n \geq 1$. Ricordiamo inoltre che per ogni tripla di eventi A, B, C si ha

$$\Pr(A \cap B \mid C) = \Pr(B \mid C) \cdot \Pr(A \mid B \cap C)$$

Otteniamo così la sequente catena di uguaglianze:

$$\begin{aligned}
\Pr_\mu(X_{k+n+1} = j \mid X_k = i) &= \Pr_\mu(X_{k+n+1} = j,\ \exists \ell \in S\ :\ X_{k+1} = \ell \mid X_k = i) \\
&= \sum_{\ell\in S} \Pr_\mu(X_{k+n+1} = j,\ X_{k+1} = \ell \mid X_k = i) \\
&= \sum_{\ell\in S} \Pr_\mu(X_{k+1} = \ell \mid X_k = i) \cdot \Pr_\mu(X_{k+n+1} = j \mid X_{k+1} = \ell, X_k = i)
\end{aligned}$$

Nota che $\Pr_\mu(X_{k+1} = \ell \mid X_k = i) > 0$ implica $\Pr_\mu(X_{k+1} = \ell, X_k = i) > 0$. Quindi per la proprietà di Markov si ottiene

$$\begin{aligned}
\Pr_\mu(X_{k+n+1} = j \mid X_k = i) &= \sum_{\ell\in S} \Pr_\mu(X_{k+1} = \ell \mid X_k = i) \cdot \Pr_\mu(X_{k+n+1} = j \mid X_{k+1} = \ell) \\
&= \sum_{\ell\in S} p(i,\ell) \cdot \Pr_\mu(X_{k+n+1} = j \mid X_{k+1} = \ell)
\end{aligned}$$

che, per ipotesi di induzione, diventa

$$\Pr_\mu(X_{k+n+1} = j \mid X_k = i) = \sum_{\ell\in S} p(i,\ell) \cdot p^{(n)}(\ell,j) = p^{(n+1)}(i,j)$$

□

La proprietà precedente implica inoltre

$$\Pr_\mu(X_{k+n} = j \mid X_k = i) = \Pr_i(X_n = j) = p^{(n)}(i,j)$$

Di conseguenza, assumendo le stesse ipotesi della proposizione precedente otteniamo

$$\Pr_i(X_{k+n} = j) = \sum_{\ell \in S} \Pr_i(X_k = \ell) \cdot \Pr_\ell(X_n = j) \qquad (\forall i, j \in S)$$

equivalente all'identità $P^{k+n} = P^k \cdot P^n$.

Infine, valutiamo la distribuzione della variabile aleatoria X_n per un qualunque $n \in \mathbb{N}$. Possiamo considerare la distribuzione μ di X_0 come un vettore stocastico a indici in S. Analogamente, per ogni $n \in \mathbb{N}$, possiamo rappresentare la distribuzione di X_n mediante il vettore $\mu(n)$ tale che $\mu(n)_j = \Pr_\mu(X_n = j)$ per ogni $j \in S$. Tale vettore verifica la relazione

$$\mu(n)' = \mu' P^n$$

Infatti, per ogni $j \in S$ abbiamo

$$\begin{aligned} \mu(n)_j &= \Pr_\mu(X_n = j) = \sum_{i \in S} \Pr_\mu(X_n = j \mid X_0 = i) \cdot \Pr_\mu(X_0 = i) \\ &= \sum_{i \in S} p^{(n)}(i,j) \cdot \mu_i = (\mu' P^n)_j \end{aligned}$$

Vogliamo ora definire le funzioni generatrici associate ai coefficienti $\{p^{(n)}(i,j)\}_n$. Osserviamo anzitutto che, data una matrice stocastica P, ogni sua potenza P^n, $n \in \mathbb{N}$, è ancora una matrice stocastica e quindi i suoi elementi sono compresi nell'intervallo $[0,1]$. Questo significa che $\lim_{n \to +\infty} (Pz)^n = 0$ per ogni $z \in \mathbb{C}$ tale che $|z| < 1$, e quindi per la proposizione A.1, la matrice $(I - Pz)^{-1} = \sum_{n=0}^{+\infty} P^n z^n$ è ben definita. Possiamo allora dare la seguente definizione.

Definizione 3.1 *La funzione di Green associata a una matrice stocastica P è una matrice di funzioni $G(z)$ data da*

$$G(z) = (I - Pz)^{-1} = \sum_{n=0}^{+\infty} P^n z^n$$

definita per ogni $z \in \mathbb{C}$ tale che $|z| < 1$.

Per ogni $i, j \in S$ possiamo allora considerare la funzione $G_{ij}(z) = ((I - Pz)^{-1})_{ij}$. Per le proprietà presentate nella sezione precedente essa rappresenta la funzione generatrice della sequenza $\{\Pr_i(X_n = j)\}_n$:

$$G_{ij}(z) = \sum_{n=0}^{+\infty} \Pr_i(X_n = j) z^n$$

Poiché $(I - Pz)^{-1} = \frac{\mathrm{adj}(I - Pz)}{\det(I - Pz)}$, ogni funzione $G_{ij}(z)$ è una funzione razionale in z, esistono cioè due polinomi $r(z)$, $s(z)$ a coefficienti in $\mathbb{R}$ (in generale dipendenti da i e j), che soddisfano $\mathrm{gr}(s) < \mathrm{gr}(r)$, tali che

$$G_{ij}(z) = \frac{s(z)}{r(z)}$$

Quindi il problema di determinare la probabilità di transizione in n passi da uno stato all'altro, è ridotto al calcolo del coefficiente n-esimo dello sviluppo in serie di Taylor di una funzione razionale. Più precisamente, per ogni $i, j \in S$ e ogni $n \in \mathbb{N}$, il valore $\Pr_i(X_n = j)$ è il coefficiente n-esimo dello sviluppo in serie di Taylor (con centro in 0) della funzione $\frac{s(z)}{r(z)}$, dove $s(z) = \mathrm{cof}(I - Pz)_{ji}$ e $r(z) = \det(I - Pz)$.

3.4 Tempi di prima entrata

Considera una catena di Markov finita e omogenea $\{X_n\}$, con spazio degli stati S e matrice di transizione $P = [p(i,j)]_{i,j \in S}$. Per ogni $j \in S$ denotiamo con τ_j la variabile aleatoria che rappresenta il minimo $n \geq 1$ tale che $X_n = j$:

$$\tau_j = \min\{n \geq 1 \mid X_n = j\}$$

La variabile τ_j rappresenta quindi il tempo di attesa necessario per entrare in j per la prima volta dopo l'istante 0. Essa assume valori nell'insieme $\mathbb{N}_+ \cup \{+\infty\}$, dove $\mathbb{N}_+ = \{n \in \mathbb{N} \mid n \neq 0\}$. L'evento $\{\tau_j = +\infty\}$ significa che dopo l'istante 0 la catena non entra mai nello stato j, ovvero $X_n \neq j$ per ogni $n \geq 1$.

Definiamo ora i seguenti coefficienti di probabilità per ogni $i, j \in S$:

$$\begin{aligned} f^0(i,j) &= 0 \\ f^{(n)}(i,j) &= \Pr_i(\tau_j = n) \qquad (\forall n \in \mathbb{N}_+) \\ f(i,j) &= \sum_{n \geq 1} f^{(n)}(i,j) = \Pr_i(\tau_j < +\infty) \end{aligned}$$

Nota che la serie precedente è per forza convergente poiché gli eventi $\{\tau_j = n \mid X_0 = i\}$, per $n \geq 1$, sono disgiunti. Chiaramente $f(i,j)$ rappresenta la probabilità di entrare prima o poi in j partendo dallo stato i. Inoltre, è chiaro che

$$\Pr_i(\tau_j = +\infty) = 1 - f(i,j)$$

Nota anche che $f(j,j) = \Pr_j(\exists n \geq 1 : \tau_j = n)$ rappresenta la probabilità di rientrare in j partendo proprio da j, ovvero la probabilità di rientro nel medesimo stato.

Le seguenti osservazioni seguono facilmente dalle definizioni:

1. $f^{(1)}(i,j) = p(i,j)$;
2. $f^{(n)}(i,j) = \Pr_i(X_n = j,\ X_\ell \neq j\ \forall \ell = 1, 2, \ldots, n-1)$;
3. $f(i,j) = \Pr_i(\bigcup_{n \geq 1} \{X_n = j\})$;
4. $\sup_{n \geq 1}\{p^{(n)}(i,j)\} \leq f(i,j) \leq \sum_{n \geq 1} p^{(n)}(i,j)$.

I coefficienti $f^{(n)}(i,j)$ sono inoltre legati alle probabilità di transizione in più passi. La seguente proprietà è abbastanza intuitiva: essa afferma che per andare da i a j in n passi occorre entrare per la prima volta in j alla k-esima mossa, per qualche $k \in \{1, \ldots, n\}$ e quindi rientrare in j nei successivi $n - k$ passi.

Proposizione 3.2 *Per ogni $n \geq 1$ e ogni $i, j \in S$*

$$p^{(n)}(i,j) = \sum_{k=1}^{n} f^{(k)}(i,j) p^{(n-k)}(j,j) \tag{3.1}$$

Dimostrazione. Condizionando sull'evento $\{\tau_j = k\}$, $k = 1, \ldots, n$, abbiamo

$$p^{(n)}(i,j) = \Pr_i(X_n = j) = \sum_{k=1}^{n} \Pr_i(X_n = j \mid \tau_j = k)\Pr_i(\tau_j = k) \tag{3.2}$$

Se $\Pr_i(\tau_j = k) \neq 0$, per la proprietà di Markov e la proposizione 3.1, vale $\Pr_i(X_n = j \mid \tau_j = k) = \Pr_i(X_n = j \mid X_k = j) = p^{(n-k)}(j,j)$. La proprietà segue quindi dalla equazione (3.2) sostituendo opportunamente i valori nella sommatoria. □

La proposizione precedente stabilisce una convoluzione tra sequenze che quindi può essere trasformata in un prodotto di funzioni generatrici. A tale scopo definiamo, per ogni $i, j \in S$, la funzione generatrice $F_{ij}(z)$ ponendo

$$F_{ij}(z) = \sum_{n=0}^{+\infty} f^{(n)}(i,j) z^n$$

Poiché $F_{ij}(1) = f(i,j)$, la serie converge per $z = 1$ e quindi il suo raggio di convergenza è maggiore o uguale a 1.

Ora, osserviamo che se $i \neq j$ allora $p^{(0)}(i,j) = 0 = f^{(0)}(i,j)p^{(0)}(j,j)$. Di conseguenza, per la proposizione 3.2, la sequenza $\{p^{(n)}(i,j)\}_{n\geq 0}$ è la convoluzione di $\{f^{(n)}(i,j)\}_{n\geq 0}$ e di $\{p^{(n)}(j,j)\}_{n\geq 0}$. Questo implica

$$G_{ij}(z) = F_{ij}(z)G_{jj}(z)$$

Se invece $i = j$ allora $p^{(0)}(i,j) = 1$ e per lo stesso ragionamento otteniamo

$$G_{jj}(z) = 1 + F_{jj}(z)G_{jj}(z)$$

Abbiamo così dimostrato il seguente corollario.

Corollario 3.3 *Per ogni $i, j \in S$, se $i \neq j$ allora*

$$G_{ij}(z) = F_{ij}(z)G_{jj}(z) \qquad (|z| < 1)$$

altrimenti abbiamo

$$G_{jj}(z) = \frac{1}{1 - F_{jj}(z)} \qquad (|z| < 1)$$

L'ultima proprietà che presentiamo in questa sezione permette di esprimere attraverso i coefficienti $f(i,j)$ la probabilità di entrare in un dato stato un certo numero di volte.

Proposizione 3.4 *Per ogni $i, j \in S$ e ogni intero $k \geq 1$ vale la seguente relazione*

$$Pr_i(X_n = j \text{ per almeno } k \text{ valori } n > 0) = f(i,j)\,(f(j,j))^{k-1}$$

Dimostrazione. Ragioniamo per induzione su $k \geq 1$. Se $k = 1$ la proprietà è ovvia. Supponiamo l'equazione vera per $k > 1$ e dimostriamola per $k + 1$. Condizionando sul valore

di τ_j abbiamo

$$\begin{aligned}
&\Pr_i(X_n = j \text{ per almeno } k+1 \text{ valori } n > 0) \\
&\quad = \sum_{t \geq 1} \Pr_i(\tau_j = t,\ X_n = j \text{ per almeno } k \text{ valori } n > t) \\
&\quad = \sum_{t \geq 1} \Pr_i(X_n = j \text{ per almeno } k \text{ valori } n > t \mid \tau_j = t)\ \Pr_i(\tau_j = t) \\
&\quad = \sum_{t \geq 1} \Pr_j(X_n = j \text{ per almeno } k \text{ valori } n > 0)\ \Pr_i(\tau_j = t) \\
&\quad = \Pr_j(X_n = j \text{ per almeno } k \text{ valori } n > 0)\ \sum_{t \geq 1} \Pr_i(\tau_j = t) \\
&\quad = (f(j,j))^k f(i,j)
\end{aligned}$$

dove la proprietà di Markov e l'omogeneità sono utilizzate nella terza uguaglianza, mentre l'ipotesi di induzione nell'ultima. □

3.5 Stati ricorrenti

Sia di nuovo $\{X_n\}$ una catena di Markov finita e omogenea, con uno spazio degli stati S e matrice di transizione $P = [p(i,j)]_{i,j \in S}$. Diciamo che uno stato $i \in S$ è *ricorrente* se

$$\Pr_i(X_n = i \text{ per infiniti } n > 0) = 1$$

Dimostriamo innazitutto che la definizione è ben posta, cioè che l'evento

$$\{X_n = i \text{ per infiniti } n > 0\}$$

appartiene alla σ-algebra $\mathcal{B}$. Infatti, per ogni intero $k \geq 1$, l'evento

$$\alpha_k = \{X_n = i \text{ per almeno } k \text{ valori } n > 0\}$$

appartiene a $\mathcal{B}$ (essendo ottenibile mediante unione di cilindri). Inoltre, si vede subito che

$$\alpha_1 \supseteq \alpha_2 \supseteq \cdots \supseteq \alpha_k \supseteq \alpha_{k+1} \supseteq \cdots$$

e che

$$\{X_n = i \text{ per infiniti } n > 0\} = \bigcap_{k \geq 1} \alpha_k$$

Di conseguenza anche $\{X_n = i \text{ per infiniti } n > 0\}$ appartiene a $\mathcal{B}$ e inoltre

$$\Pr_i(X_n = i \text{ per infiniti } n > 0) = \lim_{k \to +\infty} \Pr_i(\alpha_k) \tag{3.3}$$

Diremo inoltre che uno stato $i \in S$ è *transiente* se non è ricorrente.

Proposizione 3.5 *Per ogni stato $i \in S$ le seguenti proprietà sono equivalenti:*

1. *i è ricorrente;*
2. *$f(i,i) = 1$;*
3. *$\sum_{n \geq 0} p^{(n)}(i,i) = +\infty$.*

Dimostrazione. Per provare che la prima proprietà equivale alla seconda osserva che, per la relazione (3.3) e la proposizione 3.4, vale

$$\Pr_i(X_n = i \text{ per infiniti } n > 0) = \lim_{k \to +\infty} (f(i,i))^k \tag{3.4}$$

e tale limite è 1 se $f(i,i) = 1$, mentre è 0 se $f(i,i) < 1$.

Per dimostrare l'equivalenza tra la seconda e la terza proprietà ricordiamo innazitutto il teorema di Abel. Questo afferma che data una serie di potenze $A(z) = \sum_{n \geq 0} a_n z^n$, con raggio di convergenza $R \geq 1$ e coefficienti $a_n \geq 0$ (per ogni $n \in \mathbb{N}$), vale

$$\lim_{z \to 1^-,\, z \in [0,1]} A(z) = A(1)$$

dove il limite è inteso per z che si muove sull'intervallo reale $[0,1]$ e approssima 1 per difetto, mentre $A(1) = \sum_{n \geq 0} a_n$ può anche assumere il valore $+\infty$.

Ora, osserva che per ogni stato i, $f(i,i) = F_{ii}(1)$ è sempre minore o uguale a 1. Se $f(i,i) = 1$, per il teorema di Abel abbiamo

$$1 = F_{ii}(1) = \lim_{z \to 1^-,\, z \in [0,1]} F_{ii}(z)$$

e quindi per il corollario 3.3,

$$G_{ii}(1) = \lim_{z \to 1^-,\, z \in [0,1]} \frac{1}{1 - F_{ii}(z)} = +\infty$$

ovvero $G_{ii}(1) = \sum_{n \geq 0} p^{(n)}(i,i) = +\infty$.

Viceversa, se $f(i,i) < 1$ per lo stesso teorema abbiamo $\lim_{z \to 1^-,\, z \in [0,1]} F_{ii}(z) < 1$ e quindi

$$G_{ii}(1) = \lim_{z \to 1^-,\, z \in [0,1]} \frac{1}{1 - F_{ii}(z)} < +\infty$$

che implica la convergenza della serie $G_{ii}(1) = \sum_{n \geq 0} p^{(n)}(i,i)$. □

Osservazione 3.2 Nota che per la (3.4) l'evento $\{X_n = i \text{ per infiniti } n > 0\}$ obbedisce a una legge 0-1, nel senso che la sua probabilità è 0 oppure 1. Inoltre, un enunciato analogo vale per gli stati transienti: uno stato i è transiente se e solo se $f(i,i) < 1$ ovvero, se e solo se la serie $\sum_{n \geq 0} p^{(n)}(i,i)$ converge.

Osserviamo che quest'ultima proprietà può essere ulteriormente estesa. Infatti, per ogni $i, j \in S$, se j è transiente allora

$$\sum_{n \geq 0} p^{(n)}(i,j) < +\infty \tag{3.5}$$

La prova è ancora basata sul teorema di Abel ed è analoga a quella della proposizione precedente (unica differenza: si tiene conto dell'equazione $G_{ij}(z) = F_{ij}(z) G_{jj}(z)$). Tuttavia non vale il viceversa, ovvero la convergenza della serie non implica che lo stato j sia transiente.

Concludiamo questa sezione mostrando un legame interessante tra la proprietà di ricorrenza ora introdotta e le classi di irriducibilità del grafo associato alla catena di Markov considerata.

Proposizione 3.6 *La ricorrenza è una proprietà delle classi. Ovvero, se $i \in S$ è uno stato ricorrente e C è la sua classe allora ogni stato j in C è ricorrente.*

Dimostrazione. Data una classe C, siano $i, j \in C$ due stati distinti. Allora esistono $a, b > 0$, $a = p^{(r)}(i,j)$ e $b = p^{(s)}(j,i)$ per qualche $r, s \in \mathbb{N}$, tali che per ogni $n \in \mathbb{N}$

$$p^{(n+r+s)}(j,j) \geq b\, a\, p^{(n)}(i,i) \tag{3.6}$$

Per la proposizione 3.5, se i è ricorrente la serie $\sum_{n\geq 0} p^{(n)}(i,i)$ è divergente e per la (3.6) anche $\sum_{n\geq 0} p^{(n)}(j,j)$ diverge, per cui j risulta ricorrente. Nota che per la simmetria di i e j, se i fosse transiente anche j lo sarebbe. □

In parole povere questo significa che in ogni classe tutti gli stati sono ricorrenti, oppure sono tutti transienti.

3.6 Equivalenza tra stati ricorrenti e stati essenziali

In questa sezione proviamo (sempre nell'ipotesi di catene di Markov finite e omogenee) che gli stati ricorrenti coincidono con quelli essenziali. Ricordiamo che in una catena di Markov uno stato i è essenziale se per ogni stato j, $i \to j$ implica $j \to i$ (ovvero se $p^{(n)}(i,j) > 0$ implica $p^{(k)}(j,i) > 0$ per qualche $k \in \mathbb{N}$). Quindi la nozione di ricorrenza, definita in modo probabilistico, coincide con una proprietà dei nodi del grafo di comunicazione della catena.

Consideriamo dunque una catena di Markov $\{X_n\}$ su un insieme finito di stati S con matrice di transizione $P = [p(i,j)]_{i,j\in S}$.

Proposizione 3.7 *Se uno stato i è ricorrente e $i \to j$ allora anche j è ricorrente e inoltre $f(i,j) = 1 = f(j,i)$.*

Dimostrazione. Mostriamo anzitutto che $f(j,i) = 1$. Poiché i è ricorrente, per ogni $n \in \mathbb{N}$ abbiamo

$$\begin{aligned}
1 &= \Pr_i(X_m = i \text{ per infiniti } m > 0) \;\leq\; \Pr_i(X_m = i \text{ per qualche } m > n) \;= \\
&= \sum_{r\in S} \Pr_i(X_m = i \text{ per qualche } m > n,\; X_n = r) \\
&= \sum_{r\in S} p^{(n)}(i,r)\, \Pr_i(X_m = i \text{ per qualche } m > n \mid X_n = r) \\
&= \sum_{r\in S} p^{(n)}(i,r)\, f(r,i)
\end{aligned}$$

Scegliamo ora n tale che $p^{(n)}(i,j) > 0$. Se fosse $f(j,i) < 1$ allora avremmo

$$1 \;\leq\; \sum_{r\in S} p^{(n)}(i,r)\, f(r,i) \;<\; \sum_{r\in S} p^{(n)}(i,r) \;=\; 1$$

che è assurdo. Quindi $f(j,i) = 1$ e questo implica che $j \to i$. Di conseguenza i e j appartengono alla stessa classe e per la proposizione 3.6 anche j è ricorrente. Scambiando infine i e j nel ragionamento precedente otteniamo $f(i,j) = 1$. □

Corollario 3.8 *Ogni stato ricorrente è essenziale.*

Dimostrazione. Infatti nella prova della proposizione 3.7 abbiamo visto che se i è uno stato ricorrente e $i \to j$ allora $j \to i$. Questo significa che i è essenziale. □

Proposizione 3.9 *In una catena di Markov finita e omogenea ogni stato essenziale è ricorrente.*

Dimostrazione. Sia i uno stato essenziale e sia C la sua classe. Ragioniamo per assurdo e supponiamo che i sia transiente. Allora tutti gli stati $j \in C$ sono transienti. Quindi, per la (3.5), otteniamo $\sum_{n\geq 0} p^{(n)}(i,j) < +\infty$ e di conseguenza $\lim_{n\to+\infty} p^{(n)}(i,j) = 0$ per ogni $j \in C$.

Inoltre, poiché C è essenziale, per ogni $n \in \mathbb{N}$ abbiamo

$$\sum_{j\in C} p^{(n)}(i,j) = 1$$

Così, possiamo scrivere

$$1 = \lim_{n\to+\infty} \sum_{j\in C} p^{(n)}(i,j) = \sum_{j\in C} \lim_{n\to+\infty} p^{(n)}(i,j) \tag{3.7}$$

La seconda uguaglianza è giustificata dal fatto che C è finita e che, per ogni $j \in C$, esiste finito il limite $\lim_n p^{(n)}(i,j)$. Tuttavia tali limiti sono tutti nulli e sostituendo i loro valori in (3.7) otteniamo un assurdo (cioè $1 = 0$). Ne segue che i deve essere ricorrente. □

Osservazione 3.3 La dimostrazione precedente è basata sullo scambio tra limite e somma nella (3.7), del tipo

$$\lim_{n\to+\infty} \sum_{j\in C} a_n(j) = \sum_{j\in C} \lim_{n\to+\infty} a_n(j) \qquad (\{a_n(j)\}_n \subseteq \mathbb{R}_+ \text{ per ogni } j \in C)$$

Questa uguaglianza è sempre vera se C è finito e i limiti del termine destro esistono e sono finiti. Se invece C è un insieme infinito la proprietà non è sempre vera. Per esempio:

$$\lim_{n\to+\infty} \sum_{j=0}^{+\infty} \frac{n^j}{j!e^n} = \lim_{n\to+\infty} e^{-n} \sum_{j=0}^{+\infty} \frac{n^j}{j!} = 1$$

mentre

$$\sum_{j=0}^{+\infty} \lim_{n\to+\infty} \frac{n^j}{j!e^n} = 0$$

Il noto teorema di Lebesgue di convergenza dominata fornisce condizioni che permettono lo scambio tra limite e sommatoria anche con infiniti elementi (vedi per esempio [10]).

Corollario 3.10 *Per ogni $i, j \in S$, se j è transiente allora*

$$p^{(n)}(i,j) = O(\varepsilon^n)$$

per qualche $0 < \varepsilon < 1$.

Dimostrazione. Ricordiamo anzitutto che per le proposizioni precedenti uno stato è ricorrente se e solo se è essenziale. Quindi, se i è ricorrente la proprietà è ovvia perché $p^{(n)}(i,j) = 0$ per ogni n. Sia allora $T \subseteq S$ l'insieme degli stati transienti e supponi $i \in T$. Sappiamo che per ogni $\ell \in T$ esiste uno stato ricorrente v tale che $\ell \to v$. Di conseguenza esistono un $t \in \mathbb{N}$ e un numero reale α, $0 < \alpha < 1$, tali che per ogni $\ell \in T$

$$\sum_{u \in T} p^{(t)}(\ell, u) \leq \alpha$$

Ragionando per induzione si può provare che per ogni intero $s > 0$ e ogni $\ell \in T$

$$\sum_{u \in T} p^{(st)}(\ell, u) = \sum_{u,v \in T} p^{(t)}(\ell, v) p^{((s-1)t)}(v, u) \leq \sum_{v \in T} p^{(t)}(\ell, v) \alpha^{s-1} \leq \alpha^s$$

In particolare questo implica

$$\sum_{u \in T} p^{(st)}(i, u) \leq \alpha^s$$

Se ora consideriamo un $n \in \mathbb{N}$ qualsiasi e poniamo $n = st + r$, dove r è il resto della divisione di n per t, abbiamo

$$p^{(n)}(i,j) = \sum_{u \in T} p^{(st)}(i,u)\, p^{(r)}(u,j) \leq \alpha^s = \alpha^{\frac{n-r}{t}} = \mathrm{O}(\alpha^{1/t})^n$$

Poiché $0 < \alpha^{1/t} < 1$ la proprietà è dimostrata. □

Nella prossima proposizione si prova che quasi certamente ogni catena di Markov finita entra definitivamente in una classe essenziale.

Proposizione 3.11 *Con probabilità* 1 *ogni catena di Markov (finita e omogenea) esce definitivamente dall'insieme T degli stati transienti. Ovvero, per ogni stato i,*

$$Pr_i(\exists k \in \mathbb{N} \,:\, X_n \notin T \text{ per ogni } n > k) = 1$$

Dimostrazione. Poiché T è finito, se $X_n \in T$ per ogni $n \in \mathbb{N}$ allora esiste $j \in T$ tale che $X_n = j$ per infiniti n. Quindi, per ogni $i \in S$, abbiamo

$$\begin{aligned} \Pr_i(X_n \in T \text{ per ogni } n \in \mathbb{N}) &\leq \Pr_i(\exists j \in T \,:\, X_n = j \text{ per infiniti } n) \\ &\leq \sum_{j \in T} \Pr_i(X_n = j \text{ per infiniti } n) \\ &= \sum_{j \in T} f(i,j) \Pr_j(X_n = j \text{ per infiniti } n) \end{aligned}$$

Per l'osservazione 3.2, l'evento $(X_n = j \text{ per infiniti } n)$ obbedisce a una legge $0-1$ e inoltre, se j è transiente, la sua probabilità non può essere 1. Quindi $\Pr_j(X_n = j \text{ per infiniti } n) = 0$ per ogni $j \in T$ e di conseguenza dall'ultima disuguaglianza si ricava

$$\Pr_i(X_n \in T \text{ per ogni } n \in \mathbb{N}) = 0$$

Poiché T coincide con l'insieme degli stati non essenziali, una volta uscita da T la catena non vi rientra più. Ne segue che

$$\begin{aligned} \Pr_i(\exists k \in \mathbb{N} \,:\, X_n \notin T \text{ per ogni } n > k) &= \Pr_i(\exists m \in \mathbb{N} \,:\, X_m \notin T) \\ &= 1 - \Pr_i(X_n \in T \text{ per ogni } n \in \mathbb{N}) \;=\; 1 \end{aligned}$$

□

3.7 Tempi medi di rientro

In questa sezione studiamo i tempi medi di rientro in un dato stato. Come al solito, sia $\{X_n\}$ una catena di Markov finita e omogenea, con insieme degli stati S e matrice di transizione $P = [p(i,j)]_{i,j\in S}$. Ricordando la definizione data nella sezione 3.4, per ogni $i \in S$ sia τ_i il tempo di prima entrata nello stato i successivo all'istante 0. Vogliamo valutare il valor medio di τ_i supponendo che $X_0 = i$, ovvero il valore

$$E_i(\tau_i) = \sum_{n\in\mathbb{N}_+\cup\{+\infty\}} n \Pr_i(\tau_i = n)$$

Consideriamo ovviamente il caso in cui lo stato i sia ricorrente; se infatti i fosse transiente, avremmo $E_i(\tau_i) = +\infty$ poiché $\Pr_i(\tau_i = \infty) > 0$.

Se i è ricorrente allora

$$E_i(\tau_i) = \sum_{n\geq 1} n \Pr_i(\tau_i = n) = \sum_{n\geq 1} n\, f^{(n)}(i,i)$$

e l'obiettivo principale di questa sezione è quello di provare che in questo caso $E_i(\tau_i)$ è finito.

Osservazione 3.4 A questo proposito è bene ricordare che esistono naturali variabili aleatorie a valori in $\mathbb{N}$ con valor medio infinito. Per esempio, considera una variabile aleatoria X a valori in $\mathbb{N}$ tale che

$$\Pr(X = n) = \begin{cases} 2^{-i} & \text{se } n = 2^i \text{ per qualche intero } i \geq 1 \\ 0 & \text{altrimenti} \end{cases}$$

e osserva che $E(X) = \sum_{i\geq 1} 2^i \cdot 2^{-i} = \sum_{i\geq 1} 1 = +\infty$.

Un esempio significativo di questo tipo è dato dal paradosso di San Pietroburgo, illustrato in [7].

Sappiamo già dalla sezione 3.4 che la serie di potenze $F_{ii}(z) = \sum_{n\geq 1} f^{(n)}(i,i) z^n$ possiede raggio di convergenza $r \geq 1$. Consideriamo allora la sua derivata $F'_{ii}(z)$:

$$F'_{ii}(z) = \sum_{n\geq 1} n f^{(n)}(i,i) z^{n-1}$$

È facile verificare che il raggio di convergenza di $F'_{ii}(z)$ coincide con quello di $F_{ii}(z)$ ed è quindi maggiore o uguale a 1. Di conseguenza, per il teorema di Abel abbiamo

$$E_i(\tau_i) = F'_{ii}(1) = \lim_{z\to 1^-,\ z\in[0,1]} F'_{ii}(z)$$

Questo significa che per provare $E_i(\tau_i) < +\infty$ è sufficiente dimostrare che $f^{(n)}(i,i) = \mathrm{O}(\varepsilon^n)$ per qualche $0 < \varepsilon < 1$; in questo caso infatti il raggio di convergenza di $F'_{ii}(z)$ risulta maggiore di 1 e quindi $F'_{ii}(1) = E_i(\tau_i) \in \mathbb{R}_+$.

Proposizione 3.12 *Per ogni $i \in S$ ricorrente abbiamo $E_i(\tau_i) < +\infty$.*

Dimostrazione. Per l'osservazione precedente ci limitiamo a provare che $f^{(n)}(i,i) = \mathrm{O}(\varepsilon^n)$ per qualche $0 < \varepsilon < 1$. Inoltre, essendo i essenziale, possiamo restringere l'insieme degli stati S alla classe C di i (infatti nessuno stato fuori da C è raggiungibile da i). Definiamo allora

una nuova catena di Markov sull'insieme degli stati C rendendo i assorbente. Tale catena possiede matrice di transizione $\tilde{P} = [\tilde{p}(k,j)]_{k,j\in C}$ tale che

$$\begin{aligned} \tilde{p}(k,j) &= p(k,j) \qquad \text{per ogni } k,j \in C \text{ con } k \neq i \\ \tilde{p}(i,j) &= \begin{cases} 1 & \text{se } j = i \\ 0 & \text{altrimenti} \end{cases} \end{aligned}$$

Nella nuova catena tutti gli stati $j \neq i$ sono transienti e quindi, per il corollario 3.10,

$$\sum_{j\neq i} \tilde{p}^{(n)}(k,j) = \mathrm{O}(\varepsilon^n)$$

per qualche $0 < \varepsilon < 1$ (e per tutti i $k \in C$). Ne segue allora che per ogni intero $n \geq 2$

$$\begin{aligned} f^{(n)}(i,i) &= \sum_{k,j\in C,\, k,j\neq i} p(i,k)\, \tilde{p}^{(n-2)}(k,j)\, p(j,i) \\ &= \mathrm{O}(\varepsilon^n) \sum_{k,j\in C,\, k,j\neq i} p(i,k)\, p(j,i) \quad = \quad \mathrm{O}(\varepsilon^n) \end{aligned}$$

□

Con una dimostrazione quasi indentica alla precedente si può dimostrare il seguente

Corollario 3.13 *Se P è irriducibile allora per ogni $i,j \in S$ abbiamo*

$$E_i(\tau_j) = \sum_{n\geq 1} n f^{(n)}(i,j) < +\infty$$

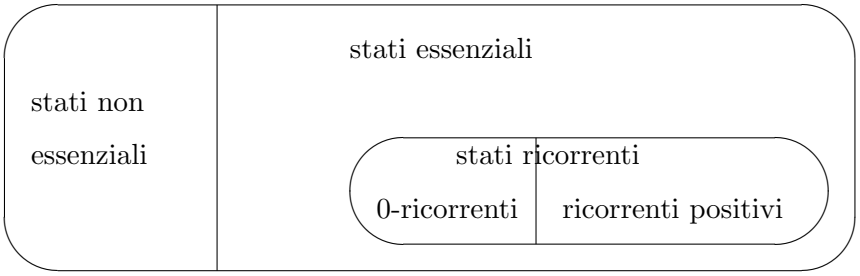
3.8 Catene di Markov infinite

A questo punto una domanda che sorge spontanea è la seguente: cosa cambia se l'insieme degli stati S diventa infinito (numerabile)? Osserviamo infatti che una catena di Markov può essere definita come nella sezione 3.2 anche nel caso in cui l'insieme degli stati S sia infinito e numerabile. Le probabilità di transizioni in più passi si calcolano nello stesso modo, le nozioni di stato ricorrente, transiente, essenziale, nonché i coefficienti $f(i,j)$ e $f^{(n)}(i,j)$ si possono definire in maniera analoga. Tuttavia in questo caso molte delle dimostrazioni presentate nelle sezioni precedenti non sono più vere. Le principali differenze sono le seguenti:

1. Ogni stato ricorrente è anche uno stato essenziale; tuttavia possono esistere stati essenziali che non sono ricorrenti. Quindi in alcuni casi la famiglia degli stati ricorrenti è propriamente inclusa in quella degli stati essenziali.

2. Non è detto che uno stato ricorrente abbia tempo medio di rientro finito: possono esistere stati ricorrenti i tali che $E_i(\tau_i) = +\infty$ (i cosiddetti stati 0-ricorrenti).

3. Non è detto che la catena termini in una classe essenziale. Ovvero può capitare che con probabilità maggiore di 0 la catena rimanga per sempre in stati non essenziali.



In questo contesto, uno stato ricorrente i si dice *ricorrente positivo* se $E_i(\tau_i) < +\infty$, mentre i è chiamato 0-*ricorrente* se $E_i(\tau_i) = +\infty$.

Riassumiamo qui di seguito le principali proprietà:

a) Uno stato i è ricorrente se e solo se $G_{ii}(1) = \sum_{n\geq 0} p^{(n)}(i,i) = +\infty$, ovvero se e solo se $F_{ii}(1) = 1$.

b) Ogni stato ricorrente è essenziale.

c) La ricorrenza è una proprietà delle classi, così come la 0-ricorrenza e la ricorrenza positiva.

d) Ogni classe essenziale finita è anche una classe ricorrente positiva. Come abbiamo segnalato sopra la proprietà inversa non è vera. In particolare esistono classi essenziali che non sono ricorrenti.

Esempio 3.1 *Passeggiata infinita dell'ubriaco* [25]. Consideriamo una catena di Markov sullo spazio degli stati $\mathbb{Z}$, con probabilità di transizione definite mediante due valori $p, q > 0$, $p + q = 1$, ponendo per ogni $k \in \mathbb{Z}$

$$p(k,k+1) = p, \quad p(k,k-1) = q \ \text{ e } \ p(k,i) = 0 \ \text{ per ogni intero } i \neq k+1, k-1.$$

È chiaro che $\mathbb{Z}$ forma un'unica classe essenziale. Inoltre, si può provare che

$$\begin{aligned} F_{00}(z) &= \sum_{n\geq 0} f^{(n)}(0,0) z^n = 1 - \sqrt{1 - 4qpz^2} \\ F_{00}(1) &= f(0,0) = 1 - |p-q| = \begin{cases} 1 & \text{se } p = q \\ 2\min\{p,q\} & \text{se } p \neq q \end{cases} \end{aligned}$$

Quindi lo stato 0 è ricorrente se $p = q$, mentre è transiente se $p \neq q$. Di conseguenza nel primo caso tutti gli stati sono ricorrenti, nel secondo sono tutti transienti.

Inoltre, se $p = q$ si verifica che tutti gli stati sono 0-ricorrenti. Infatti in questo caso abbiamo

$$F_{00}(z) = 1 - \sqrt{1 - z^2}, \qquad F'_{00}(z) = \frac{z}{\sqrt{1 - z^2}}$$

e, per il teorema di Abel,

$$E_0(\tau_0) = \lim_{z \to 1^-} F'_{00}(z) = +\infty$$

da cui si ricava che lo stato 0 è 0-ricorrente.

Modificando l'esempio precedente si può inoltre ottenere una catena di Markov infinita nella quale non è garantita l'entrata in una classe essenziale.

Esempio 3.2 *Passeggiata infinita con barriera assorbente* [25]. Sia $\mathbb{N}$ lo spazio degli stati e, dati $p, q > 0$, $p + q = 1$, definiamo le seguenti probabilità di transizione:

$$p(0,0) = 1, \quad p(k, k+1) = p, \quad p(k, k-1) = q \quad \text{per ogni intero } k > 0$$

mentre $p(i, j) = 0$ per gli altri valori i, j in $\mathbb{N}$. Nella corrispondente catena di Markov, lo stato 0 è assorbente (quindi ricorrente ed essenziale) mentre la famiglia degli interi positivi forma una classe non essenziale infinita.

Inoltre si può dimostrare che

$$F_{10}(z) = \frac{1 - \sqrt{1 - 4pqz^2}}{2pz}, \text{ da cui } \quad f(1,0) = \min\{1, q/p\}.$$

Di conseguenza, nel caso $p > q$, se lo stato iniziale è 1 la catena finirà nell'unico stato essenziale con probabilità $f(1,0) < 1$. In questo caso quindi, con probabilità non nulla, la catena (partendo dallo stato 1) può rimanere per sempre nella classe non essenziale degli stati $i > 0$.

Esercizi

1) Data una catena di Markov finita, sia C una classe ricorrente. Dimostrare che per ogni coppia di stati $i, j \in C$, $f(i, j) = 1$.

2) Nelle stesse ipotesi dell'esercizio precedente, provare che $E_i(\tau_j) < +\infty$ per ogni $i, j \in C$.

Capitolo 4

Catene di Markov ergodiche

In questo capitolo studiamo le proprietà ergodiche delle catene di Markov finite. Intuitivamente, una catena di Markov $\{X_n\}$ si dice ergodica se al crescere di n la distribuzione limite della variabile X_n esiste ed è indipendente dalla distribuzione iniziale μ. Questa proprietà è essenziale in molte applicazioni e rappresenta uno degli aspetti più studiati nella teoria delle catene di Markov.

Formalmente, una catena di Markov finita $\{X_n\}$ su un insieme S di k stati si dice *ergodica* se esiste un vettore stocastico $\pi^* = (\pi_i^*)_{i \in S}$ tale che, per ogni $i, j \in S$,

$$\lim_{n \to +\infty} \Pr_i(X_n = j) \;=\; \pi_j^*$$

ovvero

$$\lim_{n \to +\infty} p^{(n)}(i,j) \;=\; \pi_j^*$$

dove $P = [p(i,j)]_{i,j \in S}$ è la matrice di transizione della catena. Questo equivale a richiedere che per ogni distribuzione μ su S e ogni $j \in S$, $\lim_{n \to +\infty} (\mu' P^n)_j = \pi_j^*$.

L'esempio fondamentale di catena ergodica è fornito dalle catene di Markov primitive. Sappiamo infatti, per la proposizione 2.12, che se P è una matrice stocastica primitiva, allora

$$\lim_{n \to +\infty} P^n = eu' \;,$$

dove e è il vettore i cui elementi sono uguali a 1 e $u = (u_1, \ldots, u_k)$ è l'unico vettore stocastico che è anche autovettore sinistro di P corrispodente all'autovalore 1. Di conseguenza $\lim_{n \to +\infty} p^{(n)}(i,j) = u_j$, per ogni indice j. Quindi, se $\{X_n\}$ è una catena di Markov con matrice di transizione P primitiva, il vettore stocastico u, autovettore sinistro di P rispetto a 1, rappresenta la distribuzione limite di $\{X_n\}$ ed è indipendente dalla distribuzione iniziale della catena.

In questo capitolo studiamo le proprietà ergodiche delle catene di Markov senza l'ausilio del teorema di Perron-Frobenius e quindi di fatto, senza usare la proposizione 2.12. Svilupperemo un'analisi diretta della sequenze $\{p^{(n)}(i,j)\}_n$ che permetterà di mettere in luce il significato probabilistico della distribuzione limite π^* quando questa esiste. In questo caso infatti avremo che per ogni stato i, $\pi_i^* = 1/E_i(\tau_i)$, dove τ_i è il tempo di prima entrata nello stato i studiato nella sezione 3.4.

4.1 Distribuzioni stazionarie

Data una catena di Markov finita $\{X_n\}$ sull'insieme degli stati $S = \{1, 2, \ldots, k\}$, con matrice di transizione P, chiamiamo *distribuzione stazionaria* un vettore $\pi \in \mathbb{R}^k$ che soddisfa le seguenti proprietà:

1. π è un vettore stocastico, ovvero $\pi_i \geq 0$ per ogni $i = 1, 2, \ldots, k$ e inoltre $\sum_{i=1}^{k} \pi_i = 1$.
2. π è autovettore sinistro di P corrispondente a 1, ovvero $\pi' P = \pi'$.

Chiaramente, un tale vettore π verifica l'equazione $\pi' P^n = \pi'$ per ogni intero $n > 0$ e quindi $\Pr_\pi(X_n = i) = \pi_i$ per ogni stato i. Se dunque π coincide con la distribuzione iniziale della catena, la probabilità di trovarsi nei vari stati rimane sempre la stessa durante l'evoluzione del processo.

Proviamo ora a costruire una distribuzione stazionaria per una generica catena di Markov $\{X_n\}$ con famiglia degli stati $S = \{1, 2, \ldots, k\}$ e matrice di transizione P. Poiché ogni catena finita ammette sempre una classe ricorrente, senza perdita di generalità possiamo supporre che lo stato 1 sia ricorrente. Allora, per ogni $i \in S$, definiamo

$$\rho_i = \sum_{n=0}^{+\infty} \Pr_1(X_n = i,\ \tau_1 > n)$$

Tali coefficienti godono delle seguenti proprietà:

1. Ogni ρ_i è finito.

   Infatti abbiamo $\rho_i \leq \sum_{n=0}^{+\infty} \Pr_1(\tau_1 > n) = E_1(\tau_1)$ ed essendo lo stato 1 ricorrente, $E_1(\tau_1) < +\infty$ per la proposizione 3.12.

2. $\rho_1 = 1$.

   Infatti $\Pr_1(X_0 = 1,\ \tau_1 > 0) = 1$, mentre $\Pr_1(X_n = 1,\ \tau_1 > n) = 0$ per ogni intero $n > 0$.

3. Ogni ρ_i rappresenta il numero medio di entrate nello stato i nell'intervallo di tempo $\{0, 1, \ldots, \tau_1 - 1\}$, supponendo $X_0 = 1$.

   Per verificare anche questa proprietà, considera la variabile aleatoria $\nu_i = \sum_{n=0}^{+\infty} b_i(n)$, dove

   $$b_i(n) = \begin{cases} 1 & \text{se } X_n = i \text{ e } \tau_1 > n \\ 0 & \text{altrimenti} \end{cases}$$

   Allora, il valor medio di ν_i nell'ipotesi $X_0 = 1$ è dato da

   $$E_1(\nu_i) \ = \ \sum_{n=0}^{+\infty} E_1(b_i(n)) \ = \ \sum_{n=0}^{+\infty} \Pr_1(X_n = i,\ \tau_1 > n) \ = \rho_i$$

Definiamo ora il vettore π dato da

$$\pi \ = \ \left(\frac{\rho_1}{E_1(\tau_1)}, \frac{\rho_2}{E_1(\tau_1)}, \ldots, \frac{\rho_k}{E_1(\tau_1)} \right) \tag{4.1}$$

Proposizione 4.1 *Il vettore π è stocastico.*

Dimostrazione. Chiaramente $\pi_i \geq 0$ per ogni i. Inoltre abbiamo

$$\begin{aligned}\sum_{i=1}^{k} \rho_i &= \sum_{i=1}^{k}\sum_{n=0}^{+\infty} \Pr_1(X_n = i,\ \tau_1 > n) = \sum_{n=0}^{+\infty}\sum_{i=1}^{k} \Pr_1(X_n = i,\ \tau_1 > n) \\ &= \sum_{n=0}^{+\infty} \Pr_1(\tau_1 > n) = E_1(\tau_1)\end{aligned}$$

□

Il prossimo enunciato stabilisce la proprietà principale di questa sezione.

Proposizione 4.2 *Sia $\{X_n\}$ una catena di Markov sugli stati $\{1, 2, \ldots, k\}$ con matrice di transizione $P = [p(i,j)]$ e supponiamo che lo stato 1 sia ricorrente. Allora il vettore π definito in (4.1) è una distribuzione stazionaria per $\{X_n\}$.*

Dimostrazione. Basta provare che il vettore $\rho = (\rho_1, \rho_2 \ldots, \rho_k)$ è autovettore sinistro di P corrispondente all'autovalore 1. Consideriamo prima il caso $j \neq 1$ e proviamo che $\rho_j = (\rho' P)_j$. A tale scopo si può manipolare la stessa definizione di ρ_j condizionando sullo stato raggiunto al passo n-esimo e successivamente applicare la condizione di Markov. Poiché $j \neq 1$ abbiamo

$$\begin{aligned}\rho_j &= \sum_{n=1}^{+\infty} \Pr_1(X_n = j,\ \tau_1 > n) \ = \ \sum_{n=1}^{+\infty} \Pr_1(X_n = j,\ \tau_1 > n-1) \\ &= \sum_{n=1}^{+\infty}\sum_{i=1}^{k} \Pr_1(X_n = j,\ X_{n-1} = i,\ \tau_1 > n-1) \\ &= \sum_{n=1}^{+\infty}\sum_{i=1}^{k} \Pr_1(X_n = j \mid X_{n-1} = i,\ \tau_1 > n-1)\ \Pr_1(X_{n-1} = i,\ \tau_1 > n-1)\end{aligned}$$

Considera il termine generale dell'ultima sommatoria: se $i \neq 1$ e $n > 1$ (oppure $i = 1 = n$) il primo fattore coincide con $\Pr_1(X_n = j \mid X_{n-1} = i) = p(i,j)$; se invece $i = 1$ e $n > 1$ oppure $i \neq 1$ e $n = 1$ allora il secondo fattore è nullo, cioè $\Pr_1(X_{n-1} = i,\ \tau_1 > n-1) = 0$. Di conseguenza possiamo scrivere

$$\begin{aligned}\rho_j &= \sum_{n=1}^{+\infty}\sum_{i=1}^{k} p(i,j)\ \Pr_1(X_{n-1} = i,\ \tau_1 > n-1) \\ &= \sum_{i=1}^{k} p(i,j)\ \sum_{n=1}^{+\infty} \Pr_1(X_{n-1} = i,\ \tau_1 > n-1) \\ &= \sum_{i=1}^{k} p(i,j)\ \rho_i \ = \ (\rho'\ P)_j\end{aligned}$$

Consideriamo ora ρ_1 che per l'osservazione iniziale coincide con 1. Poiché lo stato 1 è ricorrente abbiamo

$$\begin{aligned}
\rho_1 &= \sum_{n=1}^{+\infty} \Pr_1(\tau_1 = n) \\
&= \sum_{n=1}^{+\infty} \sum_{i=1}^{k} \Pr_1(X_{n-1} = i,\ \tau_1 = n) \qquad \text{(poiché } \{\tau_1 = n\} = \{X_n = 1,\ \tau_1 > n-1\}\text{)} \\
&= \sum_{n=1}^{+\infty} \sum_{i=1}^{k} \Pr_1(X_n = 1 \mid X_{n-1} = i,\ \tau_1 > n-1)\ \Pr_1(X_{n-1} = i,\ \tau_1 > n-1) \\
&= \sum_{n=1}^{+\infty} \sum_{i=1}^{k} p(i,1)\ \Pr_1(X_{n-1} = i,\ \tau_1 > n-1) \\
&= \sum_{i=1}^{k} p(i,1) \sum_{n=1}^{+\infty} \Pr_1(X_{n-1} = i,\ \tau_1 > n-1) \ = \ \sum_{i=1}^{k} p(i,1)\ \rho_i \ = \ (\rho'\ P)_1
\end{aligned}$$

Abbiamo quindi provato che $\rho' = (\rho'\ P)$ e di conseguenza $\pi' = (\pi'\ P)$. □

Corollario 4.3 *Nell'ipotesi della proposizione precedente, se P è una matrice irriducibile allora π è strettamente positivo.*

Dimostrazione. Per la irriducibilità di P, nel grafo associato alla catena di Markov, per ogni nodo $i \neq 1$ esiste un cammino semplice da 1 a i e quindi per qualche $n > 0$, $\Pr_1(X_n = i,\ \tau_1 > n) > 0$. Questo prova che ogni ρ_i è positivo e di conseguenza risulta $\pi > 0$. □

Osservazione 4.1 *Se i è uno stato ricorrente diverso da 1, il vettore π può essere costruito a partire da i invece che da 1. La proposizione 4.2 garantisce che anche in questo caso π è una distribuzione stazionaria per la stessa catena. In particolare la sua componente i-esima risulta $\pi_i = (E_i(\tau_i))^{-1}$. Nelle prossime sezioni dimostreremo che se i due stati i e 1 appartengono alla stessa classe le due distribuzioni stazionarie coincidono.*

4.2 Catene di Markov primitive

In questa sezione mostriamo che le catene di Markov con matrice di transizione primitiva sono ergodiche e che la distribuzione limite coincide con l'unica distribuzione stazionaria.

A tale scopo introduciamo la tradizionale nozione di distanza tra vettori stocastici. Sia $\mathbb{R}_+$ l'insieme dei reali non negativi, cioè $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x \geq 0\}$ e, per ogni intero $k > 0$, denotiamo con M_k l'insieme dei vettori stocastici a k componenti, ovvero

$$M_k = \left\{ v \in \mathbb{R}_+^k : \sum_{i=1}^{k} v_i = 1 \right\}$$

Chiaramente M_k coincide con la famiglia delle distribuzioni di probabilità su $\{1, 2, \ldots, k\}$. Su tale insieme è ben definita la norma ℓ_1: per ogni $v \in M_k$ il valore $\| v \|_1 \in \mathbb{R}_+$ è dato da

$\| v \|_1 = \sum_{i=1}^k |v_i|$. Allora, per ogni $u, v \in M_k$, chiamiamo *distanza di variazione totale* tra u e v la quantità

$$d_{TV}(u,v) \;=\; \frac{1}{2} \| u - v \|_1 = \; \frac{1}{2} \sum_{i=1}^{k} |u_i - v_i|$$

Osserva che $0 \le d_{TV}(u,v) \le 1$ per ogni $u, v \in M_k$ e che d_{TV} definisce una distanza su M_k, ovvero $d_{TV}(u,v) = 0$ se e solo se $u = v$, $d_{TV}(u,v) = d_{TV}(v,u)$ e $d_{TV}(u,v) \le d_{TV}(u,z) + d_{TV}(z,v)$ per ogni $u, v, z \in M_k$ ([1]).

Così (M_k, d_{TV}) forma uno spazio metrico compatibile con la nozione di limite usata in questa sede, ovvero per ogni $\pi \in M_k$ e ogni sequenza $\{u^{(n)}\} \subseteq M_k$, vale $\lim_{n\to+\infty} u^{(n)} = \pi$ (cioè $\lim_{n\to+\infty} u_j^{(n)} = \pi_j$ per ogni $j = 1, \ldots, k$) se e solo se

$$d_{TV}(u^{(n)}, \pi) = \frac{1}{2} \| u^{(n)} - \pi \|_1 \longrightarrow 0 \qquad (\text{per } n \to +\infty)$$

Un modo per dimostrare che le catene di Markov con matrice di transizione primitiva sono ergodiche è basato sulle proprietà del seguente coefficiente che può essere definito su una matrice stocastica qualsiasi.

Definizione 4.1 *Data una matrice stocastica $P = [p(i,j)]$ di dimensione $k \times k$ e un qualsiasi $j \in \{1, 2, \ldots, k\}$, denotiamo con $\alpha(j)$ e $\beta(P)$ i valori*

$$\alpha(j) = \min\{p(i,j) \mid i = 1, 2, \ldots, k\} \;, \qquad \beta(P) = 1 - \sum_{j=1}^{k} \alpha(j)$$

Il coefficiente $\beta(P)$ soddisfa le seguenti proprietà:

1) $0 \le \beta(P) \le 1$ per ogni matrice stocastica P.

Infatti è chiaro che $\beta(P) \le 1$; inoltre $1 = \sum_{j=1}^k p(i,j) \ge \sum_{j=1}^k \alpha(j)$ e quindi $0 \le \beta(P)$.

2) $\beta(P) < 1$ se e solo se P possiede una colonna di valori tutti positivi.

3) $\beta(P) < 1$ se $P > 0$.

Ogni matrice stocastica $P \in \mathbb{R}_+^{k\times k}$ definisce una funzione $f_P : M_k \longrightarrow M_k$ che associa ad ogni $u \in M_k$ il vettore $f_P(u) = u'P$. Il seguente lemma mostra che distanza tra $f_P(u)$ e $f_P(v)$ è sempre minore o uguale alla distanza tra u e v, per ogni coppia di vettori $u, v \in M_k$; inoltre il rapporto tra queste distanze è al più $\beta(P)$. Quindi intuitivamente la funzione f_P non estende mai le distanze tra gli elementi di M_k. Anzi, se $\beta(P) < 1$ allora f_P è una contrazione sullo spazio M_k nel senso che riduce le distanze tra i suoi elementi di un fattore minore di 1.

Lemma 4.4 *Per ogni matrice stocastica $P \in \mathbb{R}_+^{k\times k}$ e ogni coppia di vettori stocastici $u, v \in M_k$ abbiamo*

$$\| u'P - v'P \|_1 \le \; \beta(P) \| u - v \|_1$$

[1] Altre proprietà di d_{TV} saranno presentate nel capitolo 8.

Dimostrazione. Per ogni $j = 1, 2, \ldots, k$ possiamo scrivere

$$\begin{aligned}
(u'P)_j - (v'P)_j &= \sum_{i=1}^{k}(u_i - v_i)p(i,j) = \\
&= \sum_{i=1}^{k}|u_i - v_i|p(i,j) - \left[\sum_{i=1}^{k}(|u_i - v_i| - (u_i - v_i))p(i,j)\right] = \\
&\leq \sum_{i=1}^{k}|u_i - v_i|p(i,j) - \left[\sum_{i=1}^{k}(|u_i - v_i| - (u_i - v_i))\right]\alpha(j) = \\
&= \sum_{i=1}^{k}|u_i - v_i|\,[p(i,j) - \alpha(j)]
\end{aligned}$$

In maniera analoga si prova che $(v'P)_j - (u'P)_j \leq \sum_{i=1}^{k}|u_i - v_i|\,[p(i,j) - \alpha(j)]$ e quindi si ottiene

$$|(u'P)_j - (v'P)_j| \leq \sum_{i=1}^{k}|u_i - v_i|\,[p(i,j) - \alpha(j)]$$

Questo implica

$$\begin{aligned}
\| u'P - v'P \|_1 &= \sum_{j=1}^{k}|(u'P)_j - (v'P)_j| \leq \sum_{j=1}^{k}\sum_{i=1}^{k}|u_i - v_i|\,[p(i,j) - \alpha(j)] = \\
&\leq \sum_{i=1}^{k}|u_i - v_i|\sum_{j=1}^{k}(p(i,j) - \alpha(j)) = \sum_{i=1}^{k}|u_i - v_i|\beta(P) = \\
&\leq \beta(P)\,\| v - u \|_1
\end{aligned}$$

□

Iterando la disuguaglianza ottenuta in questo lemma, ricaviamo la seguente relazione valida nelle medesime ipotesi per ogni $n \in \mathbb{N}$:

$$\| u'P^n - v'P^n \|_1 \leq (\beta(P))^n \,\| u - v \|_1 \tag{4.2}$$

Proposizione 4.5 *Per ogni matrice stocastica $P \in \mathbb{R}_+^{k\times k}$ primitiva esistono una costante $C > 0$ e un valore ε, $0 \leq \varepsilon < 1$ tali che per ogni coppia di vettori stocastici $u, v \in M_k$ e ogni $n \in \mathbb{N}$*

$$\| u'P^n - v'P^n \|_1 \leq C\varepsilon^n$$

Dimostrazione. Poiché P è primitiva esiste $t \in \mathbb{N}$ tale che $P^t > 0$ e di conseguenza $0 \leq \beta(P^t) < 1$. Ora per ogni $n \in \mathbb{N}$ abbiamo $n = qt + r$ per qualche $q \in \mathbb{N}$ e $r \in \{0, 1, \ldots, t-1\}$; quindi applicando il Lemma precedente e in particolare la disuguaglianza (4.2), si ottiene

$$\begin{aligned}
\| u'P^n - v'P^n \|_1 &= \| u'P^r(P^t)^q - v'P^r(P^t)^q \|_1 \leq \left(\beta(P^t)\right)^q \| u'P^r - v'P^r \|_1 = \\
&\leq 2\left(\beta(P^t)\right)^{\frac{n-r}{t}} \leq 2\left(\beta(P^t)\right)^{-1}\left[\beta(P^t)^{1/t}\right]^n = C\varepsilon^n
\end{aligned}$$

dove $C = 2\beta(P^t)^{-1}$ e $\varepsilon = \beta(P^t)^{1/t} < 1$. □

Teorema 4.6 *Sia $\{X_n\}$ è una catena di Markov con matrice di transizione primitiva sull'insieme di stati $S = \{1, 2, \ldots, k\}$. Allora valgono le seguenti proprietà:*

1. *$\{X_n\}$ possiede una sola distribuzione stazionaria $\pi^* = (\pi_1^*, \pi_2^*, \ldots, \pi_k^*)$;*

2. *per ogni $i \in S$*
$$\pi_i^* \;=\; \frac{1}{E_i(\tau_i)} \;=\; \frac{1}{\sum_{n\geq 1} n f^{(n)}(i,i)}$$

3. *$\{X_n\}$ è ergodica e per ogni $i, j \in S$*
$$\lim_{n\to+\infty} Pr_i(X_n = j) \;=\; \pi_j^*$$

Dimostrazione. Sia $P = [p(i,j)]$ la matrice di transizione della catena. Per la proposizione precedente sappiamo che, per ogni coppia di distribuzioni u, v su S,

$$\| u'P^n - v'P^n \|_1 \to 0 \qquad (\text{per } n \to +\infty) \tag{4.3}$$

Se u e v sono due distribuzioni stazionarie per la catena allora $u'P^n = u'$ e $v'P^n = v'$ per ogni $n \in \mathbb{N}$ e, per la relazione (4.3), otteniamo $\| u' - v' \|_1 = 0$, ovvero $u = v$. Di conseguenza la catena ammette un'unica distribuzione stazionaria che denotiamo $\pi^* = (\pi_1^*, \ldots, \pi_k^*)$ e questo prova il punto 1.

Osserva ora che nel nostro caso tutti gli stati sono ricorrenti e quindi la distribuzione stazionaria π^* può essere costruita come nella sezione 4.1 a partire da un qualunque stato $i \in S$ invece che dallo stato 1. Ne segue che $\pi_i^* = 1/E_i(\tau_i)$ per ogni $i \in S$ e questo prova il punto 2.

Infine per quanto riguarda il punto 3 considera la relazione (4.3). Assumendo $v = \pi^*$ per ogni distribuzione u su S abbiamo $\| u'P^n - \pi^{*\prime} \|_1 \to 0$ e questo significa che $(u'P^n)_j \to \pi_j^*$, per ogni stato $j = 1, \ldots, k$. Pertanto, quando u coincide con il vettore caratteristico di uno stato $i \in S$ si ottiene il risultato. □

4.3 Catene di Markov irriducibili periodiche

Nelle sezioni precedenti abbiamo visto che le catene di Markov primitive sono ergodiche. Invece, per le catene di Markov irriducibili di periodo maggiore di 1 questa proprietà non è più vera. In questo caso infatti la sequenza $\{p^{(n)}(i,j)\}_n$ in generale non ammette limite.

Esempio 4.1 Considera una catena formata da due soli stati $\{1, 2\}$ con matrice di transizione

$$P \;=\; \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Chiaramente P è irriducibile di periodo 2 e si verifica subito che $p^{(n)}(1,2) = 1$ se n è dispari, mentre $p^{(n)}(1,2) = 0$ per n pari. Quindi, al crescere di n, $\{p^{(n)}(1,2)\}_n$ non ammette limite e lo stesso vale per ogni altra coppia di stati.

Si può però dimostrare che anche nel caso irriducibile periodico la distribuzione stazionaria è unica e coincide con il vettore π^* definito nel teorema 4.6. Valgono inoltre proprietà di limite per sottosequenze di $\{p^{(n)}(i,j)\}$ e si può provare una forma di convergenza più debole, relativa cioè alla sequenza delle somme $\{\frac{1}{n}\sum_{k=0}^{n} p^{(k)}(i,j)\}_n$ (intuitivamente, una sorta di media dei valori $p^{(n)}(i,j)$, al variare di n).

Prima di illustrare questi risultati ricordiamo alcune proprietà delle matrici irriducibili presentate nel capitolo 2 adattandole alla nostra situazione.

Data una matrice stocastica irriducibile $P = [p(u,v)]$ di periodo $d > 1$ e dimensione k, esistono d famiglie di indici $C_0, C_1, \ldots, C_{d-1}$ ($C_d = C_0$) che formano una partizione dell'insieme $\{1, 2, \ldots, k\}$ e che rappresentano le "classi di periodicità" di P. Esse verificano in particolare le seguenti proprietà.

1) Se $u \in C_i$ e $p(u,v) > 0$ allora $v \in C_{i+1}$.

2) Due stati u, v appartengono allo stesso insieme C_i se e solo se $p^{(nd)}(u,v) > 0$ per qualche $n \in \mathbb{N}$.

3) Per ogni $u \in C_i$ e ogni $v \in C_j$, posto $r \in \{0, 1, \ldots, d-1\}$ tale che $r \equiv i - j \pmod d$, allora

$$p^{(n)}(u,v) > 0 \quad \text{implica} \quad n \equiv r \pmod d$$

4) La restrizione di P^d agli indici in C_i forma una matrice stocastica primitiva. Quindi, permutando l'ordine di righe e colonne, P^d può essere trasformata in una forma diagonale a blocchi

$$(P^d)^* = \begin{bmatrix} U_0 & 0 & \cdots & 0 \\ 0 & U_1 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & U_{d-1} \end{bmatrix}$$

nella quale le matrici U_i sono disposte sulla diagonale principale, sono quadrate e coincidono con la restrizione di P^d agli indici in C_i (risultano quindi primitive); viceversa, ogni altro elemento della matrice è nullo.

5) Analoghe proprietà di periodicità valgono per i coefficienti $f^{(n)}(u,v)$ introdotti nella sezione 3.4. Poiché $f^{(n)}(u,v) > 0$ implica $p^{(n)}(u,v) > 0$ abbiamo

$$f^{(n)}(u,u) = 0 \qquad \text{per ogni} \quad n \not\equiv 0 \pmod d, \quad \text{e ogni} \quad u. \tag{4.4}$$

Per lo stesso motivo, se $u \in C_i$, $v \in C_j$ e $r \in \{0, 1, \ldots, d-1\}$ tale che $r \equiv i - j \pmod d$, allora

$$f^{(n)}(u,v) = 0 \qquad \text{per ogni} \quad n \not\equiv r \pmod d \tag{4.5}$$

e quindi, essendo P irriducibile,

$$1 = f(u,v) = \sum_{n \geq 1} f^{(n)}(u,v) = \sum_{n \geq 1} f^{(nd+r)}(u,v) \tag{4.6}$$

Ricordiamo infine che, essendo ogni stato $u \in \{1, 2, \ldots, k\}$ ricorrente, il valor medio di τ_u è sempre ben definito:

$$E_u(\tau_u) \quad = \quad \sum_{n \geq 1} n f^{(n)}(u, u) \quad < +\infty$$

Per una tale matrice P possiamo allora definire il vettore $\pi^* = (\pi_1^*, \ldots, \pi_k^*)$ tale che

$$\pi_u^* \quad = \quad \frac{1}{E_u(\tau_u)} \quad = \quad \frac{1}{\sum_{n \geq 1} n f^{(n)}(u, u)} \qquad\qquad (\forall\, u \in \{1, 2, \ldots, k\})$$

Proposizione 4.7 *Se P è una matrice stocastica irriducibile di dimensione k e periodo d allora*

$$\lim_{n \to +\infty} p^{(nd)}(u, u) \quad = \quad d\pi_u^* \qquad\qquad (\forall\, u \in \{1, 2, \ldots, k\})$$

Nota che per la proprietà 3) data sopra, $p^{(n)}(u, u) = 0$ per ogni $n \not\equiv 0 \pmod d$. Quindi, se $d > 1$ la proposizione implica che $p^{(n)}(u, u)$ non ammette limite al crescere di n. Ne segue che una catena di Markov irriducibile periodica non può essere ergodica.

Dimostrazione. Sia u un indice in $\{1, 2, \ldots, k\}$. Innanzitutto osserviamo che per l'equazione (4.4) il coefficiente π_u^* verifica $\pi_u^* = 1/\sum_{n \geq 1} nd\, f^{(nd)}(u, u)$.

Denotata con C la classe di periodicità di u, per ogni $n \in \mathbb{N}$ e ogni $x, y \in C$, definiamo

$$h^{(n)}(x, y) = p^{(nd)}(x, y)\ , \qquad g^{(n)}(x, y) = f^{(nd)}(x, y)$$

Chiaramente la matrice $H = [h^{(1)}(x, y)]_{x,y \in C}$ è la restrizione di P^d alle componenti in C e quindi è stocastica primitiva. Analogamente, i valori $g^{(n)}(x, y)$ rappresentano le probabilità di prima entrata da x a y in n passi in una catena di Markov con spazio degli stati C e matrice di transizione H. Essendo H primitiva, per il teorema 4.6, abbiamo

$$\lim_{n \to +\infty} h^{(n)}(u, u) \quad = \quad \frac{1}{\sum_{n \geq 1} n\, g^{(n)}(u, u)}$$

ovvero

$$\lim_{n \to +\infty} p^{(nd)}(u, u) \quad = \quad \frac{1}{\sum_{n \geq 1} n\, f^{(nd)}(u, u)} \quad = \quad d\pi_u^*$$

□

Proposizione 4.8 *Sia P una matrice stocastica irriducibile di periodo $d > 1$ e siano C_i e C_j due classi di periodicità. Allora, per ogni $u \in C_i$ e ogni $v \in C_j$ abbiamo*

$$\lim_{n \to +\infty} p^{(nd+r)}(u, v) \quad = \quad d\, \pi_v^*$$

dove $r \equiv i - j \ (mod\, d)$, $r \in \{0, 1, \ldots, d-1\}$.

Omettiamo la prova di questa proposizione. Segnaliamo solo che la dimostrazione si ottiene essenzialmente in due passi: prima si considera la relazione tra i coefficienti $p^{(n)}(i, j)$ e gli $f^{(n)}(i, j)$ data nella proposizione 3.2, che nel nostro caso diventa

$$p^{(nd+r)}(u, v) = \sum_{j=0}^{nd+r} f^{(j)}(u, v) p^{(nd+r-j)}(v, v) = \sum_{j=0}^{n} f^{(jd+r)}(u, v) p^{(n-j)d}(v, v) \quad ;$$

quindi si applica la proposizione 4.7 al termine destro della sommatoria e si ricorda che

$$\lim_{n\to+\infty} f^{(n)}(u,v) = 0$$

Osserviamo infine che nelle stesse ipotesi precedenti $p^{(n)}(u,v) = 0$ per ogni $n \not\equiv r \pmod{d}$. Si può così dedurre il seguente risultato.

Corollario 4.9 *Se P è una matrice stocastica irriducibile allora, per ogni coppia di indici i, j abbiamo*

$$\lim_{n\to+\infty} \frac{1}{n} \sum_{\ell=0}^{n} p^{(\ell)}(i,j) \quad = \quad \pi_j^*$$

Per quanto riguarda le distribuzioni stazionarie delle catene irriducibili, sappiamo già dalla sezione 4.1 che ogni matrice stocastica e irriducibile P ammette una distribuzione stazionaria π definita in (4.1). Il prossimo enunciato afferma che π coincide con π^* e che questa è l'unica distribuzione stazionaria di P.

Teorema 4.10 *Ogni catena di Markov irriducibile ammette un'unica distribuzione stazionaria che coincide con il vettore π^*.*

Dimostrazione. Sia $P = [p(u,v)]$ la matrice di transizione della catena e sia μ una sua distribuzione stazionaria. Poiché P è irriducibile, per l'osservazione precedente sappiamo che ne esiste almeno una. Denotiamo con d il periodo di P e con C_0, C_1, $\cdots$, C_{d-1} le classi di periodicità corrispondenti ($C_d = C_0$). Allora

$$\begin{aligned} \sum_{v\in C_{i+1}} \mu_v \quad &= \quad \sum_{v\in C_{i+1}} \sum_{u\in C_i} \mu_u p(u,v) \\ &= \quad \sum_{u\in C_i} \mu_u \sum_{v\in C_{i+1}} p(u,v) \quad = \quad \sum_{u\in C_i} \mu_u \end{aligned}$$

Questo prova che $\sum_{u\in C_i} \mu_u = 1/d$ per ogni $i = 0, 1 \ldots, d-1$.

Inoltre, essendo μ stazionario, $\mu' P^{nd} = \mu'$ per ogni $n \in \mathbb{N}$ e per ogni stato v abbiamo

$$(\mu' P^{nd})_v \quad = \quad \mu_v$$

Applicando la proposizione 4.8 al termine sinistro, posto $v \in C_{i+1}$, abbiamo

$$(\mu' P^{nd})_v \quad = \quad \sum_{u\in C_i} \mu_u p^{(nd)}(u,v) \quad \longrightarrow \quad \sum_{u\in C_i} \mu_u \cdot d\, \pi_v^* \quad = \quad \pi_v^*$$

e per l'equazione precedente deve essere $\mu_v = \pi_v^*$. □

4.4 Catene di Markov riducibili

È ora naturale chiedersi quale sia il comportamento asintotico di $\{p^{(n)}(i,j)\}_n$ per le catene di Markov riducibili, nelle quali cioè il grafo di comunicazione contiene più componenti fortemente connesse. In questo caso non esiste una risposta univoca e il comportamento dipende

dalla relazione di comunicazione tra le varie componenti e dalla periodicità dei loro elementi. Si può però provare che se vi è una sola classe essenziale e quest'ultima è aperiodica allora la catena è ergodica. Viceversa, se vi sono più classi essenziali, oppure se l'unica classe essenziale è periodica, allora la catena non può essere ergodica.

Per illustrare questi risultati, consideriamo come sempre una catena di Markov $\{X_n\}$ su un insieme finito di stati S, con matrice di transizione $P = [p(i,j)]_{i,j\in S}$.

Osserviamo innanzitutto che per il corollario 3.10 se $j \in S$ è uno stato transiente allora per ogni $i \in S$

$$\lim_{n\to+\infty} p^{(n)}(i,j) \;=\; 0$$

Rimane quindi da indagare il comportamento di $\{p^{(n)}(i,j)\}_n$ nel caso di j ricorrente.

Proposizione 4.11 *Se la catena di Markov $\{X_n\}$ possiede una sola classe essenziale C e quest'ultima è aperiodica allora, per ogni $j \in C$ e ogni $i \in S$,*

$$\lim_{n\to+\infty} p^{(n)}(i,j) \;=\; \frac{1}{\sum_{n\geq 1} n f^{(n)}(j,j)}$$

Per l'osservazione precedente la catena è quindi ergodica.

Dimostrazione. Proviamo innanzitutto che $f(i,j) = 1$. Se $i \in C$ la proprietà segue dalla proposizione 3.7. Supponiamo che i appartenga all'insieme T degli stati transienti e denotiamo con σ_T il tempo di permanenza della catena in T, cioè $\sigma_T = \max\{n \in \mathbb{N} \mid X_n \in T\}$. Per la proposizione 3.11, sappiamo che $\Pr_i(\sigma_T = +\infty) = 0$ e quindi, essendo $C = S\backslash T$, abbiamo

$$1 \;=\; \sum_{\ell=0}^{+\infty} \Pr_i(\sigma_T = \ell) \;=\; \sum_{\ell=0}^{+\infty} \sum_{u\in C} \Pr_i(\sigma_T = \ell, X_{\ell+1} = u) \tag{4.7}$$

Per valutare $f(i,j)$ possiamo allora condizionare sull'evento $\{\sigma_T = \ell, X_{\ell+1} = u\}$:

$$\begin{aligned}
f(i,j) \;&=\; \Pr_i(\exists\, n \;:\; \tau_j = n) \;=\; \sum_{\ell=0}^{+\infty} \sum_{u\in C} \Pr_i(\exists\, n \;:\; \tau_j = n,\; \sigma_T = \ell, X_{\ell+1} = u) \\
&=\; \sum_{\ell=0}^{+\infty} \sum_{u\in C} \Pr_i(\exists\, n > \ell \;:\; \tau_j = n,\; \sigma_T = \ell, X_{\ell+1} = u) \\
&=\; \sum_{\ell=0}^{+\infty} \sum_{u\in C} \Pr_i(\exists\, n > \ell \;:\; \tau_j = n \mid\; \sigma_T = \ell, X_{\ell+1} = u)\, \Pr_i(\sigma_T = \ell, X_{\ell+1} = u) \\
&=\; \sum_{\ell=0}^{+\infty} \Pr_i(\sigma_T = \ell, X_{\ell+1} = j) + \sum_{u\in C, u\neq j} \Pr_u(\exists\, n > 0 \;:\; \tau_j = n)\, \Pr_i(\sigma_T = \ell, X_{\ell+1} = u) \\
&=\; \sum_{\ell=0}^{+\infty} \sum_{u\in C} f(u,j)\, \Pr_i(\sigma_T = \ell, X_{\ell+1} = u)
\end{aligned}$$

Per la proposizione 3.7 $f(u,j) = 1$ per ogni $u \in C$ e quindi dalla (4.7) ricaviamo

$$f(i,j) = \sum_{\ell=0}^{+\infty} \sum_{u\in C} \Pr_i(\sigma_T = \ell, X_{\ell+1} = u) = 1$$

Poiché C è una classe essenziale e aperiodica, la restrizione di P agli indici in C forma una matrice primitiva. Possiamo quindi applicare il teorema 4.6, ottenendo

$$\lim_{n\to+\infty} p^{(n)}(j,j) \;=\; \pi_j^* \;= \frac{1}{\sum_{n\geq 1} n f^{(n)}(j,j)}$$

Questo significa che, per ogni $\varepsilon > 0$, esiste $m_\varepsilon \in \mathbb{N}$ tale che per ogni intero $n > m_\varepsilon$, $|p^{(n)}(j,j) - \pi_j^*| \leq \varepsilon$. Di conseguenza, per n abbastanza grande, la nota equazione (3.1) che lega i coefficienti $p^{(n)}(j,j)$ e $f^{(n)}(j,j)$, può essere riscritta nella forma seguente:

$$\begin{aligned} p^{(n)}(i,j) &= \sum_{k=1}^{n} f^{(k)}(i,j)p^{(n-k)}(j,j) \\ &= \sum_{k=1}^{n-m_\varepsilon-1} f^{(k)}(i,j)p^{(n-k)}(j,j) \;+\; \sum_{k=n-m_\varepsilon}^{n} f^{(k)}(i,j)p^{(n-k)}(j,j) \\ &= \sum_{k=m_\varepsilon+1}^{n-1} f^{(n-k)}(i,j)p^{(k)}(j,j) \;+\; \sum_{k=0}^{m_\varepsilon} f^{(n-k)}(i,j)p^{(k)}(j,j) \end{aligned} \tag{4.8}$$

Poiché i termini della seconda sommatoria sono positivi o nulli, per la scelta di m_ε abbiamo

$$p^{(n)}(i,j) \;\geq\; (\pi_j^* - \varepsilon) \sum_{k=m_\varepsilon+1}^{n-1} f^{(n-k)}(i,j)$$

Per ogni $\varepsilon > 0$, la sommatoria nel termine destro tende a $f(i,j) = 1$ per $n \to +\infty$ e quindi

$$\liminf_{n\to+\infty} p^{(n)}(i,j) \;\geq\; (\pi_j^* - \varepsilon) \tag{4.9}$$

Un limite analogo vale per l'estremo superiore e questo conclude la prova; infatti, dall'equazione (4.8), sempre per la scelta di m_ε otteniamo la disuguaglianza

$$p^{(n)}(i,j) \;\leq\; (\pi_j^* + \varepsilon) + \sum_{k=0}^{m_\varepsilon} f^{(n-k)}(i,j)$$

e poiché $f^{(n)}(i,j) \to 0$ per $n \to +\infty$, si ricava

$$\limsup_{n\to+\infty} p^{(n)}(i,j) \;\leq\; (\pi_j^* + \varepsilon) \tag{4.10}$$

Per l'arbitrarietà di ε, le relazioni (4.9) e (4.10) implicano

$$\lim_{n\to+\infty} p^{(n)}(i,j) \;=\; \pi_j^* \tag{4.11}$$

□

Osserviamo che una catena di Markov finita con due classi essenziali non può essere ergodica. Infatti, denotando con C_1 e C_2 due tali classi e con i, j due stati in C_1 e C_2 rispettivamente, abbiamo

$$p^{(n)}(i,j) \;=\; 0 \qquad \text{per ogni } \; n \in \mathbb{N}$$

mentre

$$\lim_{n\to+\infty} p^{(n)}(j,j) \;=\; \pi_j^* \;=\; \frac{1}{\sum_{n\geq 1} n f^{(n)}(j,j)} \;\neq 0$$

quindi il limite di $p^{(n)}(u,j)$ per $n \to +\infty$ dipende dallo stato di partenza u.

Corollario 4.12 *Una catena di Markov finita è ergodica se e solo se possiede un'unica classe essenziale e quest'ultima è aperiodica.*

Notiamo infine che la precedente dimostrazione della relazione (4.11) può essere adattata per provare che, se vi sono più componenti essenziali, j è uno stato essenziale aperiodico e i uno stato transiente, allora

$$\lim_{n\to+\infty} p^{(n)}(i,j) \;=\; f(i,j)\pi^*_j$$

In questo caso infatti avremo $f(i,j) \leq 1$ e non è detto che $f(i,j) = 1$, mentre le altre proprietà sono del tutto valide e la formula ottenuta è assolutamente intuitiva.

Capitolo 5

Catene reversibili

In questo capitolo introduciamo anzitutto la nozione di reversibilità di una catena di Markov. Si tratta di una proprietà delle catene che consente in molte applicazioni di determinare in maniera semplice una distribuzione stazionaria e quindi, nei casi ergodici, la distribuzione limite della catena. Nella seconda sezione invece mostreremo alcuni esempi tipici di catene reversibili, legate alle passeggiate a caso su grafi non orientati, che hanno numerosi risvolti applicativi. Il famoso algoritmo di Metropolis, che introdurremo nella sezione 7.4, può essere visto come una variante di tali procedimenti. Un altro esempio di rilievo è dato dalle passeggiate a caso su grafi formati da una semplice lista di vertici; queste infatti consentono di studiare un interessante esempio di algoritmo probabilistico per la soluzione di un problema classico (2-CNF SODD) e di valutarne la probabilità di errore.

5.1 Catene reversibili

Una catena di Markov $\{X_n\}_n$, definita sullo spazio degli stati $S = \{1, 2, \ldots, k\}$ con matrice di transizione $P = [p(i,j)]_{i,j \in S}$, si dice *reversibile* se esiste un vettore stocastico π su S tale che per ogni $i, j \in S$

$$\pi_i p(i,j) = \pi_j p(j,i) \tag{5.1}$$

Diciamo anche che π è una distribuzione reversibile per la catena $\{X_n\}_n$.

La proprietà appena definita può essere considerata una forma di simmetria della catena, essa equivale infatti a porre

$$\Pr_\pi(X_0 = i, X_1 = j) \;=\; \Pr_\pi(X_0 = j, X_1 = i)$$

Più in generale la reversibilità implica che per ogni sequenza finita di stati $i_0, i_1, \ldots, i_k$,

$$\Pr_\pi(X_0 = i_0, X_1 = i_1, \ldots, X_k = i_k) \;=\; \Pr_\pi(X_0 = i_k, X_1 = i_{k-1}, \ldots, X_k = i_0)$$

La proprietà fondamentale delle catene reversibili è la seguente.

Proposizione 5.1 *Se π è una distribuzione reversibile per una catena $\{X_n\}_n$ allora π è anche distribuzione stazionaria per $\{X_n\}_n$.*

Dimostrazione. Siano S e $P = [p(i,j)]_{i,j\in S}$, rispettivamente, l'insieme degli stati e la matrice di transizione della catena. Poiché π è una distribuzione reversibile, per ogni $j \in S$ abbiamo

$$(\pi' P)_j \;=\; \sum_{i=1}^{m} \pi_i p(i,j) \;=\; \sum_{i=1}^{m} \pi_j p(j,i) \;=\; \pi_j$$

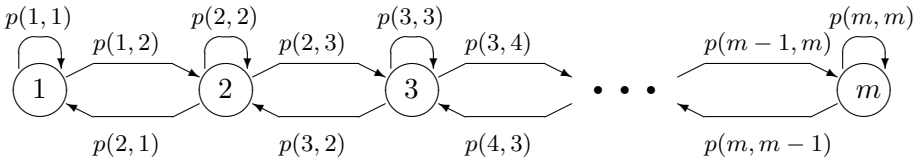
Di conseguenza $\pi' P = \pi'$ e quindi π risulta stazionaria. □

Allora, se $\{X_n\}_n$ è una catena di Markov irriducibile e reversibile, la sua distribuzione stazionaria coincide con la distribuzione reversibile π (che soddisfa le equazioni (5.1)).

Esempi classici di catene reversibili sono forniti dai cosiddetti processi di nascita e morte. Formalmente, un *processo di nascita e morte* è una catena di Markov su un insieme di stati $S = \{1, 2, \ldots, m\}$ con matrice di transizione $P = [p(i,j)]_{i,j\in S}$, tale che

$$p(i,j) > 0 \;\text{ se }\; |i-j| = 1 \text{ , e}$$
$$p(i,j) = 0 \;\text{ se }\; |i-j| \geq 2.$$

Il grafo di comunicazione della catena è descritto dalla seguente figura.



Chiaramente tale catena è irriducibile e risulta inoltre aperiodica se $p(i,i) > 0$ per qualche $i \in S$. Mostriamo ora la sua reversibilità. A tale scopo definiamo m coefficienti reali positivi $r_1, r_2, \ldots, r_m$, dove $r_1 > 0$ è un valore qualsiasi, mentre i successivi sono dati da

$$r_2 = r_1 \frac{p(1,2)}{p(2,1)},\; r_3 = r_2 \frac{p(2,3)}{p(3,2)},\; \ldots\;,\; r_m = r_{m-1} \frac{p(m-1,m)}{p(m,m-1)}\;.$$

Questo equivale a porre, per ogni $i = 2, \ldots, m$,

$$r_i = r_1 \frac{p(1,2)p(2,3)\cdots p(i-1,i)}{p(i,i-1)\cdots p(3,2)p(2,1)}.$$

Consideriamo ora il vettore stocastico π dato dalle equazioni

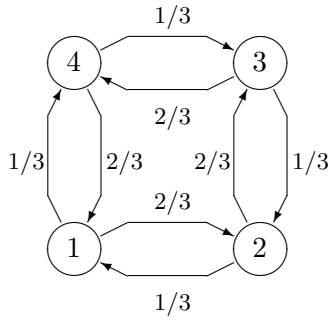
$$\pi = (\pi_1, \pi_2, \ldots, \pi_m) = \left(\frac{r_1}{\sum_{i=1}^m r_i}, \frac{r_2}{\sum_{i=1}^m r_i}, \ldots, \frac{r_m}{\sum_{i=1}^m r_i} \right)$$

Per la stessa definizione dei coefficienti r_i è facile verificare che π è una distribuzione reversibile per la catena considerata. Di conseguenza, π è anche l'unica distribuzione stazionaria. Nota che i suoi valori non dipendono dalle probabilità $p(i,i)$, per $i \in S$.

Proposizione 5.2 *Sia $\{X_n\}_n$ un catena di Markov con matrice di transizione P irriducibile e bistocastica. Se $\{X_n\}_n$ è reversibile allora P è simmetrica.*

Dimostrazione. Infatti, essendo P irriducible e bistocastica, la sua unica distribuzione stazionaria è quella uniforme $\pi = (1/k, 1/k, \ldots, 1/k)$, dove k è la dimensione di P. Inoltre, per la reversibilità della catena π è anche l'unica distribuzione reversibile. Di conseguenza, $\pi_i P_{ij} = \pi_j P_{ji}$ per ogni coppia di indici i, j, il che implica $P_{ij} = P_{ji}$. □

La proposizione precedente permette di fornire facilmente esempi di catene che non sono reversibili. È sufficiente considerare matrici irriducibili bistocastiche e non simmetriche. Le corrispondenti catene di di Markov non possono essere reversibili. Per esempio, la catena definita dal seguente grafo di comunicazione non è reversibile.



5.2 Passeggiate a caso su grafi

Un altro esempio fondamentale di catena reversibile è fornito dalle passeggiate a caso in un grafo non orientato. Tale catena è definita nel modo seguente. Sia $G = (V, E)$ un grafo non orientato, con $V = \{1, 2, \ldots, k\}$ insieme dei nodi, E insieme degli archi dove $\sharp E = m$ (cioè supponiamo che la cardinalità di E sia m). Per ogni $i \in V$ denotiamo inoltre con d_i il grado di i, ovvero $\sharp\{\{i, j\} \in E \mid j \in V\}$. Chiaramente abbiamo $\sum_{i \in V} d_i = 2m$.

Consideriamo ora una catena di Markov $\{X_n\}_n$ sullo spazio degli stati V, con matrice di transizione $P = [p(i, j)]_{i,j \in V}$ tale che, per ogni $i, j \in V$,

$$p(i,j) = \begin{cases} 1/d_i & \text{se } \{i,j\} \in E \\ 0 & \text{altrimenti} \end{cases}$$

Diciamo che $\{X_n\}_n$ è la catena delle *passeggiate a caso* su G. Essa rappresenta un processo naturale di visita dei nodi di grafo a partire da un vertice dato; ad ogni passo il nuovo nodo viene scelto in maniera equiprobabile tra tutti i vertici adiacenti al nodo corrente. Definiamo il vettore stocastico π su V dato da

$$\pi = \left(\frac{d_1}{2m}, \frac{d_2}{2m}, \ldots, \frac{d_k}{2m} \right) \tag{5.2}$$

È facile verificare che π è un vettore reversibile per la catena $\{X_n\}_n$. Infatti, per ogni coppia di nodi distinti $i, j \in V$, se $\{i, j\} \notin E$ allora $\pi_i p(i, j) = 0 = \pi_j p(j, i)$. Viceversa, se $\{i, j\} \in E$ si verifica immediatamente che $\pi_i p(i, j) = \frac{1}{2m} = \pi_j p(j, i)$.

Inoltre, osserviamo che se G è connesso la catena è irriducibile. Applicando allora la proposizione 5.2 e le proprietà della sezione 4.3, otteniamo il seguente risultato.

Proposizione 5.3 *Se G è un grafo non orientato connesso allora la catena delle passeggiate a caso su G gode delle seguenti proprietà:*

a) la catena è irriducibile e reversibile,

b) la sua periodicità è al più 2,

c) la sua distribuzione stazionaria è data dal vettore π definito in (5.2),

d) per ogni nodo i di G il tempo medio di rientro in i è dato da

$$E_i(\tau_i) \;=\; 2m/d_i$$

dove m è il numero di lati di G e d_i è il grado di i.

Solitamente sono due i parametri di interesse nelle passeggiate a caso in un grafo: il tempo medio di passaggio da un nodo i a un nodo j, ovvero $E_i(\tau_j)$, e il tempo medio necessario per visitare tutti i nodi del grafo, detto anche tempo medio di copertura del grafo. Tali quantità dipendono dalla forma del grafo e qui nel seguito le studiamo per due famiglie particolari di grafi: i grafi completi e i cammini semplici, che rappresentano rispettivamente i grafi connessi con il massimo e con il minimo numero di lati.

5.2.1 Passeggiate in un grafo completo

Sia G un grafo completo di $k \geq 3$ nodi e sia u un nodo di G. Denotiamo con $\{X_n\}_n$ la catena di Markov delle passeggiate a caso su G assumendo che lo stato iniziale sia u. Chiaramente tale catena è irriducibile e aperiodica e, per le proprietà precedenti, la sua distribuzione stazionaria è $\pi = (1/k, 1/k, \ldots, 1/k)$. Di conseguenza, il tempo medio di rientro in ciascun nodo v è proprio $E_v(\tau_v) = k$, dove con τ_v rappresentiamo il tempo di prima entrata in v.

Vogliamo ora valutare $E_u(\tau_v)$, ovvero il tempo medio di prima entrata in un nodo generico v partendo dal nodo iniziale u e supponendo che $v \neq u$. In questo caso la passeggiata casuale entra in v al primo passo con probabilità $\frac{1}{k-1}$ mentre entra in un nodo diverso da v con probabilità $\frac{k-2}{k-1}$; in quest'ultimo caso il processo si ripete per simmetria con le stesse probabilità. La variabile aleatoria τ_v è quindi una geometrica di parametro $\frac{1}{k-1}$. Come sappiamo la sua media è $k-1$ e questo prova la seguente proprietà.

Proposizione 5.4 *Per ogni nodo v diverso dal nodo iniziale u abbiamo $E_u(\tau_v) = k - 1$.*

Denotiamo ora con Γ_G il tempo di copertura di G, ovvero il minimo numero di passi compiuti da $\{X_n\}_n$ per entrare almeno una volta in ogni stato della catena. Formalmente, si tratta della variabile aleatoria definita da

$$\Gamma_G = \min\{n \in \mathbb{N} \mid \forall v \in V \; \exists i \leq n \;:\; X_i = v\}$$

dove V rappresenta l'insieme dei nodi di G. Tale variabile è ben definita perché la famiglia degli stati della catena è composta da un'unica classe essenziale. (quindi con probabilità 1 la catena entrerà in ogni stato).

Proposizione 5.5 *Il tempo medio di copertura di un grafo completo G di k nodi è dato da*

$$E_u(\Gamma_G) = (k-1)\sum_{i=1}^{k-1} \frac{1}{i} \sim k \log k$$

Dimostrazione. È facile verificare che Γ_G è una somma di $k-1$ variabili aleatorie

$$\Gamma_G \;=\; \sum_{i=1}^{k-1} \delta_i$$

dove ogni δ_i è il minimo numero di passi compiuti dalla passeggiata a caso, dopo aver visitato esattamente i nodi distinti, per entrare in un nuovo nodo diverso dai precedenti. Chiaramente $\delta_1 = 1$ mentre, per ogni $i = 2, 3, \ldots, k-1$, δ_i è una geometrica di parametro $\frac{k-i}{k-1}$. Il valor medio di Γ_G è quindi la somma delle medie

$$\sum_{i=1}^{k-1} \frac{k-1}{k-i} = (k-1) \sum_{i=1}^{k-1} \frac{1}{i}$$

□

Intuitivamente, questo significa che nella passeggiata a caso di un grafo completo, ogni nodo viene visitato in media circa $\log k$ volte prima che tutti i vertici siano stati visitati.

Osserviamo che le variabili aleatorie δ_i sono indipendenti e quindi la varianza di Γ_G può essere ricavata dalla somma delle varianze, ottenendo

$$Var(\Gamma_G) \;=\; (k-1)^2 \sum_{i=1}^{k-1} \frac{1}{i^2} - (k-1) \sum_{i=1}^{k-1} \frac{1}{i} \;\sim\; \frac{\pi^2}{6} k^2$$

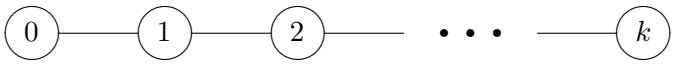
Vale la pena di osservare infine che, pur essendo una somma di variabili aleatorie indipendenti, Γ_G non converge in distribuzione ad una normale. È stato infatti provato che per ogni $t \in \mathbb{R}$ vale la relazione

$$\lim_{k \to +\infty} \Pr\{ \frac{\Gamma_G - k \log k}{k} \leq t \} \;=\; e^{-e^{-t}}$$

La distribuzione $e^{-e^{-t}}$ è chiamata distribuzione di Gumbel ed è nota in letteratura come distribuzione limite di statistiche d'ordine.

5.2.2 Passeggiate in un cammino semplice

Consideriamo ora un grafo G formato semplicemente da un cammino semplice di $k+1$ nodi numerati da 0 a k.



Consideriamo la catena di Markov $\{X_n\}_n$ definita da una passeggiata a caso nel grafo. Per ogni $i \in \{0, 1, \ldots, k\}$, denotiamo con u_i la variabile aleatoria che rappresenta il numero di passi necessari per raggiungere il nodo k, supponendo di partire da i. Ovvero $u_i = \min\{n \in \mathbb{N} : X_n = k / X_0 = i\}$. Per semplicità, denotiamo inoltre con U_i il valor medio di u_i, $U_i = E(u_i)$. Condizionando sul primo passo della passeggiata è facile verificare che i valori U_i soddisfano il sistema di equazioni

$$\begin{aligned}
U_0 &= 1 + U_1 \\
U_1 &= 1 + \frac{U_0 + U_2}{2} \\
&.... \\
U_i &= 1 + \frac{U_{i-1} + U_{i+1}}{2} \\
&.... \\
U_{k-1} &= 1 + \frac{U_{k-2}}{2}
\end{aligned}$$

che può essere risolto mediante una semplice sostituzione ottenendo

$$U_i \;=\; \sum_{j=i}^{k-1}(2j+1) \;=\; k^2 - i^2 \qquad (\forall i = 0, 1, \ldots, k)$$

Proposizione 5.6 *Compiendo una passeggiata a caso in un grafo formato da un cammino semplice di k nodi il numero medio di passi necessari per raggiungere una estremità del grafo a partire da un vertice qualunque è minore o uguale a* k^2*.*

Il risultato appena provato può essere utilizzato nell'analisi di un semplice algoritmo probabilistico per risolvere il problema 2-CNF SODD (soddisfacibilità di formule booleane in forma normale 2 congiunta). Con un approccio simile è possibile definire un analogo algoritmo probabilistico per 3-CNF SODD (si veda per esempio [8, sez. 5.3]). Prima di descrivere il problema, ricordiamo che un *letterale* è una variabile Booleana o una sua negazione, mentre una *clausola* è un "or" di letterali, ovvero una formula Booleana del tipo $(u_1 \vee u_2 \vee \cdots \vee u_m)$ dove ogni u_i è un letterale.

PROBLEMA 2-CNF SODD

Istanza : una formula booleana $\Phi = \bigwedge_{i=1}^{m} C_i$ su un insieme di variabili $V = \{v_1, v_2, \ldots, v_k\}$, nella quale ogni C_i è una clausola di due letterali.

Domanda : esiste un assegnamento di valori booleani alle variabili in V che rende Φ vera?

La procedura che presentiamo è tipico esempio di algoritmo probabilistico *one-sided error*; esso infatti restituisce il valore esatto nel caso in cui la formula Φ non ammetta un assegnamento che la rende vera, mentre se un tale assegnamento esiste la procedura può sbagliare con una certa probabilità. Sarà ovviamente opportuno progettare l'algoritmo in modo tale che la probabilità di errore sia piccola a piacere.

L'idea dell'algoritmo è molto semplice: si ripete un certo numero di volte un ciclo principale di istruzioni nel quale partendo da un assegnamento casuale A di valori alle variabili in V si verifica se A soddisfa Φ. In caso affermativo abbiamo effettivamente trovato un assegnamento che rende vera la formula. In caso contrario si modifica il valore di una variabile che compare in una clausola non soddisfatta da A, ripetendo il procedimento per il nuovo assegnamento. L'algoritmo è formalmente descritto dalla seguente procedura che dipende da un parametro di iterazione h:

```
Ripeti h volte il seguente blocco
   begin
      i := 1
      scegli un assegnamento A per V a caso
      while A non soddisfa Φ e i ≤ 2k² do
                  { determina una clausola C_j non soddisfatta da A
                  { scegli a caso con probabilità uniforme una variabile v che compare in C_j
                  { cambia l'assegnamento A attribuendo a v il valore complementare
                  { i := i + 1
      if A soddisfa Φ then { return 1
                           { stop
   end
return 0
```

Come vedremo più precisamente nella sezione 6.1, la generazione casuale di un assegnamento A può essere eseguita in $O(k)$ passi. Inoltre, verificare se A soddisfa Φ richiede un tempo $\Theta(m)$. Il tempo complessivo è quindi dell'ordine $\Theta(hmk^2)$.

Studiamo ora la probabilità di errore dell'algoritmo. Se Φ non è soddisfatta da alcun assegnamento, l'algoritmo non commette errore perché la procedura termina sempre restituendo la risposta negativa.

Supponiamo ora che Φ ammetta un assegnamento che la rende vera. In questo caso è possibile che l'algoritmo non trovi un assegnamento del genere e quindi fornisca una risposta sbagliata. Valutiamo la probabilità η di un simile errore. Il valore η è massimo quando vi è un solo assegnamento α che rende vera Φ. In questo caso possiamo considerare la distanza tra α e l'assegnamento corrente A calcolato dalla procedura, cioè il numero di variabili cui i due assegnamenti attribuiscono valore diverso. Chiaramente, tale distanza è un intero compreso tra 0 e k. Ad ogni iterazione interna essa viene incrementata o diminuita di 1 cambiando il valore di una variabile in una clausola C_j non soddisfatta da A. Poiché A e α attribuiscono valore diverso ad almeno una delle due variabili di C_j, la probabilità di diminuire la distanza è almeno $1/2$ mentre la probabilità di aumentarla è al più $1/2$. Possiamo rappresentare l'esecuzione di un ciclo esterno dell'algoritmo come una passeggiata a caso in un cammino semplice formato dalla sequenza di nodi $\{0, 1, 2, \ldots, k\}$, nella quale si parte da un nodo qualsiasi i e ci si arresta non appena si giunge nel nodo 0.

Ne segue che la probabilità di errore in una singola iterazione del ciclo più esterno è minore o uguale alla probabilità che in una passeggiata a caso in una sequenza di $k+1$ nodi non si raggiunga il nodo 0 entro i primi $2k^2$ passi. Poiché l'algoritmo esegue h cicli esterni, denotando con $\{X_n\}_n$ la catena di Markov che rappresenta tale passeggiata, abbiamo

$$\eta \;\leq\; \left(\Pr\{X_n \neq 0,\ \forall\ n \leq 2k^2\}\right)^h$$

Qualunque sia il nodo di partenza i (ottenuto dalla generazione di un assegnamento a caso), denotiamo con u_i la variabile aleatoria che rappresenta il numero di passi necessari per raggiungere 0. Per la proposizione 5.6 sappiamo che $E(u_i) \leq k^2$ per qualunque i. Quindi per la disuguaglianza di Markov abbiamo

$$\Pr\{X_n \neq 0,\ \forall\ n \leq 2k^2\} \;=\; \Pr(u_i > 2k^2) \;\leq\; \frac{E(u_i)}{2k^2} \;\leq \frac{1}{2}$$

Dalle due disuguaglianze precedenti si ricava

$$\eta \;\leq\; (1/2)^h$$

È quindi sufficiente compiere $h \geq \log_2 \frac{1}{\varepsilon}$ iterazioni principali nella procedura per ottenere una probabilità di errore $\eta \leq \varepsilon$, per qualunque $\varepsilon > 0$.

Capitolo 6

Simulazione di catene di Markov

In questo capitolo vogliamo descrivere l'algoritmo tradizionale di simulazione di una catena di Markov, supponendo sempre che la catena sia finita e omogenea. Come è facile immaginare l'algoritmo utilizza ripetutamente un procedimento di generazione casuale di elementi estratti da un insieme finito secondo un'arbitraria distribuzione di probabilità. Per questo motivo descriviamo innanzitutto il metodo classico utilizzato generalmente per risolvere questo problema. Tale metodo è ampiamente utilizzato come sottoprogramma fondamentale nella progettazione di algoritmi per la generazione casuale delle più comuni strutture combinatorie [6].

6.1 Generazione casuale non uniforme

Dato un intero positivo k, consideriamo l'insieme $S = \{1, 2, \ldots, k\}$ e una qualsiasi distribuzione di probabilità su S, ovvero una funzione $p : S \to [0, 1]$ tale che $p(1) + p(2) + \cdots + p(k) = 1$. Chiaramente possiamo considerare p come un vettore stocastico

$$p = (p(1), p(2), \ldots, p(k)) \ \in \ [0, 1]^k$$

Vogliamo generare un elemento a caso in S secondo la distribuzione p. Più precisamente vogliamo definire un algoritmo probabilistico che su input p restituisca un valore $y \in S$ tale che, per ogni $i \in S$,

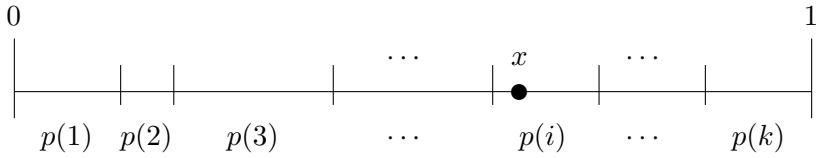
$$\Pr(y = i) = p(i)$$

La procedura che illustriamo è semplice e intuitiva: si genera a caso un numero reale x uniformemente distribuito nell'intervallo $[0, 1]$ e quindi si determina il minimo $i \in S$ tale che

$$x \leq p(1) + p(2) + \cdots + p(i) \tag{6.1}$$

Qui supponiamo di poter utilizzare una funzione *random*$[0, 1]$ in grado di generare un valore reale nell'intervallo $[0, 1]$ secondo la distribuzione uniforme. Ricordiamo che gran parte dei linguaggi e dei sistemi di manipolazione simbolica dispongono di funzioni in grado di eseguire efficacemente un simile calcolo.

Il procedimento appena descritto è giustificato dalla seguente considerazione: la distribuzione p può essere vista come una partizione dell'intervallo $[0, 1]$ in k intervallini consecutivi t_1, t_2,..., t_k, di dimensione $p(1)$, $p(2)$, . . ., $p(k)$, rispettivamente, come mostrato nella seguente figura.



Quindi, scegliendo un valore reale x uniformemente distribuito in $[0, 1]$, la probabilità che x cada nell'intervallo t_i è proprio uguale a $p(i)$, per ogni $i = 1, 2, \ldots, k$. Si tratta quindi di trovare l'intervallo nel quale x è caduto; il metodo più semplice è quello di determinare il minimo i che soddisfi la relazione (6.1).

Formalmente l'algoritmo è descritto dalla seguente procedura.

```
Procedure Genera(p)
begin
    x := random[0, 1]
    i := 1
    u := p(1)
    while u < x do
        { i := i + 1
        { u := u + p(i)
    return i
end
```

Nella valutazione del tempo di calcolo e dello spazio di memoria richiesti assumeremo sempre un criterio di costo uniforme (si veda per esempio [1, 4]). In queste ipotesi è ragionevole assumere che anche il calcolo della funzione *random*$[0, 1]$ richieda tempo costante. Ne segue che il tempo di calcolo richiesto dalla procedura di generazione casuale appena descritta è $\mathrm{O}(k)$. Inoltre, anche lo spazio di memoria richiesto dall'algoritmo è $\mathrm{O}(k)$, poiché per l'esecuzione del procedimento dobbiamo mantenere il vettore stocastico p.

6.2 Algoritmo di simulazione

Consideriamo ora una catena di Markov $\{X_n\}$ definita su un insieme di stati $S = \{1, 2, \ldots, k\}$, con distribuzione iniziale μ e matrice di transizione $P = [p(i, j)]_{i,j \in S}$. Vogliamo generare una istanza delle prime n transizioni compiute dalla catena a partire da uno stato iniziale, per un qualsiasi $n \in \mathbb{N}$.

L'algoritmo che descriviamo utilizza direttamente i parametri k, μ e P che definiscono la catena e che supponiamo letti e memorizzati in una fase iniziale di precomputazione. La procedura quindi riceve in input l'intero n e, dopo aver generato lo stato iniziale secondo la distribuzione μ, determina i successivi n passi scegliendo il nuovo stato corrente mediante le righe della matrice P. La procedura restituisce gli $n + 1$ stati consecutivi visitati durante la simulazione.

```
Procedure Simula(n)
begin
    d := μ
    for i = 0, 1, ..., n do
```

$$\left\{ \begin{array}{l} j := \text{Genera}(d) \\ \text{stampa } j \\ d := (p(j,1), p(j,2), \cdots, p(j,k)) \end{array} \right.$$

`end`

La procedura è chiaramente basata sull'algoritmo di generazione non uniforme presentato nella sezione precedente. Per svolgere l'analisi dei tempi di calcolo e dello spazio di memoria richiesti dall'algoritmo, dobbiamo innanzitutto fissare le dimensioni dell'input che nel nostro caso dipende in modo naturale da due parametri: il numero degli stati k e il numero di passi della simulazione n. È facile verificare che il tempo di calcolo richiesto dalla procedura `Simula` (sempre secondo un criterio di costo uniforme) è $\mathrm{O}(nk)$. A tale quantità dobbiamo aggiungere il tempo necessario per leggere e memorizzare i parametri che definiscono la catena di Markov: questo richiede un tempo $\mathrm{O}(k^2)$ se manteniamo in memoria l'intera matrice P. In questo caso è chiaro che anche lo spazio richiesto dall'algoritmo è $\mathrm{O}(k^2)$. Altrimenti, se possiamo calcolare di volta in volta il vettore delle probabilità necessario (senza memorizzare l'intera matrice), il procedimento richiede solo uno spazio $\mathrm{O}(k)$.

6.3 Catene a grado limitato

Come abbiamo osservato, la procedura descritta nella sezione precedente richiede (nel caso peggiore) uno spazio di memoria almeno proporzionale al numero di stati. In molte applicazioni tuttavia tale numero è troppo elevato e rende l'algoritmo del tutto inefficiente. Vedremo nel capitolo 7 come, in molte applicazioni rilevanti, il numero degli stati della catena sia esponenziale rispetto alle dimensione del problema originale. Per questo motivo è importante definire procedure di simulazione che non dipendano direttamente dal numero di stati e, in particolare, che evitino di memorizzare l'intera matrice di transizione.

Possiamo definire una procedura di questo genere quando, per ogni stato, esiste un numero limitato (facilmente calcolabile) di stati raggiungibili in un passo; in questo caso il grafo di comunicazione della catena ha grado piccolo rispetto al numero di stati. In questa situazione, possiamo limitarci a mantenere, per ogni stato corrente solo le probabilità di transizione negli stati adiacenti, che vengono calcolate di volta in volta. Così il tempo di calcolo e lo spazio di memoria necessari per eseguire la procedura non dipendono più dal numero di stati ma solo dal numero di passi della simulazione e dal grado del grafo di comunicazione della catena.

Per formalizzare la descrizione dell'algoritmo in questo caso, per ogni stato $q \in S$, denotiamo con A_q l'insieme $A_q = \{r \in S \mid p(q,r) > 0\}$. Chiamiamo inoltre *grado* della catena il massimo delle cardinalità degli insiemi A_q e lo denotiamo con g, quindi $g = \max\{\sharp A_q : q \in S\}$.

L'algoritmo può essere allora descritto dalla seguente procedura nella quale si suppone di poter sempre calcolare in un tempo $\mathrm{O}(g)$ l'insieme A_q e la distribuzione $p_q = \{p(q,r)\}_{r \in A_q}$, per ogni $q \in S$. Per semplicità supporremo inoltre che lo stato iniziale sia un valore $q_0 \in S$ fissato a priori.

```
Procedure Simula(n, q_0)
begin
    q := q_0
    for  i = 1, 2, ..., n do
```

$$\begin{cases} \text{calcola la distribuzione } p := \{p(q,r)\}_{r \in A_q} \\ r := \text{Genera}(p) \\ \text{stampa } r \\ q := r \end{cases}$$

`end`

Nelle ipotesi date è evidente che il tempo di calcolo è $O(ng)$. Inoltre, non è più necessario mantenere in memoria la matrice P e neppure un vettore stocastico di dimensione k come avveniva nell'algoritmo precedente. Nel nostro caso il vettore stocastico, di volta in volta utilizzato nella generazione casuale, ha una dimensione limitata dal valore di g. Di conseguenza lo spazio necessario per eseguire la procedura è ridotto a $O(g)$.

La complessità dell'algoritmo risulta quindi nettamente migliore del precedente proprio quando il valore di g è molto piccolo rispetto a quello di k. Questo si verifica per esempio per le catene di Markov definite nella sezione 3.1 relative alla rovina del giocatore o al moto rettilineo di una particella, oppure per i tradizionali processi di nascita e morte, descritti nella sezione 5.1, o ancora nelle passeggiate casuali considerate nella sezione 5.2.2. In tutti questi casi il grado della catena è costante (al più 3), indipendentemente dal numero di stati: quindi il tempo di calcolo richiesto dalla simulazione diventa $O(n)$ e lo spazio di memoria $O(1)$.

Altri esempi significativi saranno considerati nel capitolo 7, dove presenteremo catene di Markov che hanno un grado logaritmico rispetto al numero di stati. In questi casi il tempo di calcolo diventa $O(n \log k)$ e lo spazio di memoria $O(\log k)$.

Capitolo 7

Generazione casuale mediante catene di Markov

In questo capitolo illustriamo un metodo naturale per la generazione casuale basato su catene di Markov ergodiche. Supponiamo di voler generare un elemento a caso da un insieme finito S secondo una distribuzione di probabilità π definita su S. In alcuni casi l'algoritmo tradizionale illustrato nella sezione 6.1 non è facilmente utilizzabile. Questo capita tipicamente quando l'insieme S non è ben definito, oppure la probabilità π_i dei suoi elementi $i \in S$ è difficile da calcolare . In questi casi un metodo alternativo spesso utilizzato consiste nel definire una catena di Markov irriducible e aperiodica $\{X_n\}$ sull'insieme di stati S che abbia π come distribuzione stazionaria; poiché la catena è ergodica, sappiamo che qualunque sia il valore di X_0, per n grande la probabilità che $X_n = i$ approssima π_i per ogni stato i. Possiamo quindi simulare la catena a partire da uno stato qualunque, per un numero di passi n abbastanza elevato, restituendo lo stato raggiunto al passo n-esimo. In letteratura, un algoritmo, o in generale un procedimento di calcolo di questo tipo, è chiamato *MCMC corretto* per la distribuzione π, dove con MCMC si intende "Markov Chain Monte Carlo" (in parole povere, un metodo Monte Carlo basato su catena di Markov). Questi metodi sono stati formalizzati e sistemati in vari articoli apparsi negli anni '90 (si veda per esempio [12, 13]), anche se di fatto essi erano già stati utilizzati nella letteratura precedente in diversi ambiti scientifici [7]. Esempi classici sono quelli dell'Annealing simulato o dell'algoritmo di Metropolis. In questo capitolo e in quelli successivi presentiamo i tratti essenziali e le proprietà principali di questi metodi, basandoci in molti casi su materiale didattico sviluppato in [7, 15, 16]. Rimandiamo ai testi classici (per esempio [3, 7, 12, 13, 15, 16]) gli approfondimenti e gli sviluppi più recenti.

Per descrivere i metodi MCMC e presentare alcune delle problematiche che si incontrano nella loro applicazione, presentiamo un esempio concreto che può essere considerato tipico di questo approccio.

7.1 Generazione di insiemi indipendenti

Ricordiamo innanzitutto che in un grafo non orientato $G = (V, E)$ un insieme indipendente è un sottoinsieme di vertici $A \subseteq V$ tra i quali non vi sono lati, ovvero, per ogni $u, v \in A$ si verifica $\{u, v\} \notin E$. Nota che il numero di insiemi indipendenti può essere esponenziale rispetto alle dimensioni del grafo (numero dei nodi). Di conseguenza, se vogliamo generare un

insieme indipendente secondo la distribuzione uniforme, l'algoritmo presentato nella sezione 6.1 non è sempre utilizzabile perché può richiedere un tempo di calcolo troppo elevato.

Per inciso, ricordiamo che molti problemi tradizionali definiti su questi insiemi sono di difficile soluzione e rappresentano classici esempi ampiamente studiati nell'area della complessità computazionale. Per esempio, è ben noto che il problema di stabilire se in un grafo non orientato esiste un insieme indipendente di dimensione data è NP-completo. Di conseguenza, calcolare il numero di insiemi indipendenti di data dimensione in un grafo è ♯P-completo, così come risulta NP-hard determinare il massimo insieme indipendente in un grafo. Inoltre, si può provare che lo stesso problema di ottimizzazione non è approssimabile in tempo polinomiale con un errore relativo minore di una costante fissata (a meno che P=NP). Si tratta quindi di problemi difficili che non ammettono algoritmi di approssimazione efficienti [4].

Definiamo allora una catena di Markov per generare a caso in modo uniforme un insieme indipendente in un grafo non orientato $G = (V, E)$. Qui assumiamo che $E \neq \emptyset$ e denotiamo con k il numero dei nodi di G, ovvero $k = \sharp V$. Inoltre sia S la famiglia di tutti gli insiemi indipendenti in $G = (V, E)$,

$$S = \{A \subseteq V \mid \forall u, v \in A \ \{u, v\} \notin E\}$$

Denotiamo inoltre con Z_G la cardinalità di S e rappresentiamo con π la distribuzione di probabilità uniforme su S, ovvero la funzione

$$\pi : S \longrightarrow [0, 1] \text{ tale che, per ogni } A \in S,\ \pi(A) = \frac{1}{Z_G}$$

La catena di Markov $\{X_n\}$ è definita quindi assumendo S come insieme di stati e fissando la probabilità di transizione da uno stato all'altro attraverso la seguente procedura, nella quale A è lo stato corrente e B lo stato successivo. In pratica, si sceglie un nodo v in V a caso in maniera uniforme: se $v \in A$ allora si toglie v da A; se invece $v \notin A$ e v non possiede nodi adiacenti in A, allora si aggiunge v ad A.

```
begin
    A := insieme indipendente corrente
    scegli v ∈ V a caso secondo la distribuzione uniforme
    if v ∈ A then B := A\{v}
            else if (∀w ∈ A {w, v} ∉ E) then B := A ∪ {v}
                                        else B := A
    return B
end
```

Nota che il nuovo stato B coincide con lo stato precedente A ogniqualvolta $v \notin A$ ed esiste in A un nodo adiacente a v. In ogni caso, la differenza tra uno stato corrente e il successivo consiste al più di un solo nodo.

Più precisamente, denotiamo con $A \div B$ la differenza simmetrica tra due insiemi A e B, ovvero $A \div B = (A \cup B) \setminus (A \cap B)$. Allora è facile verificare che, per ogni coppia di stati $A, B \in S$, la probabilità $P(A, B)$ di passare da A a B in un passo è data da

$$P(A,B) = \begin{cases} 0 & \text{se } \sharp(A \div B) > 1 \\ \frac{1}{k} & \text{se } \sharp(A \div B) = 1 \\ 1 - \frac{\sharp\{C \in S \mid \sharp(A \div C) = 1\}}{k} & \text{se } A = B \end{cases}$$

Proposizione 7.1 *La matrice di transizione $P = [P(A,B)]_{A,B\in S}$ è irriducibile e aperiodica. Inoltre la distribuzione π è reversibile per la catena $\{X_n\}$ definita sopra.*

Dimostrazione. Per dimostrare l'irriducibilità di P, consideriamo due stati qualsiasi $A, B \in S$. Allora un cammino da A a B può essere facilmente costruito togliendo prima tutti i nodi nell'insieme $A\backslash B$, raggiungendo così lo stato $A \cap B$, poi aggiungendo tutti quelli in $B\backslash A$. Per la definizione della catena è facile verificare che ciascuno di questi passi ha probabilità non nulla e quindi la probabilità dell'intero cammino è positiva. Questo implica che per un opportuno intero $n > 0$ abbiamo $P^n(A,B) > 0$ e di conseguenza la matrice è irriducibile.

Osserviamo inoltre che la matrice è aperiodica poiché $E \neq \emptyset$ e per ogni lato $\{a,b\} \in E$, se la catena si trova nello stato $\{a\}$ può scegliere con probabilità $1/k$ il nodo $v = b$ e di conseguenza rimanere in $\{a\}$. Ne segue che $P(\{a\},\{a\}) > 0$

Infine per provare la reversibilità di π basta osservare che P è una matrice simmetrica mentre π è una distribuzione uniforme. Di conseguenza per ogni $A, B \in S$ abbiamo $\pi(A) = \pi(B)$ e $P(A,B) = P(B,A)$, che implica

$$\pi(A)P(A,B) = \pi(B)P(B,A)$$

□

Questo risultato mostra che la catena $\{X_n\}$ è ergodica e che π è l'unica distribuzione stazionaria. Di conseguenza, per ogni coppia di insiemi indipendenti A, B di G abbiamo

$$\lim_{n\longrightarrow+\infty} \Pr_A(X_n = B) \;=\; \pi(B)$$

La catena definisce quindi un algoritmo MCMC corretto per generare un insieme indipendente di un grafo secondo una distribuzione uniforme. La procedura è del tutto naturale: si sceglie un insieme indipendente qualsiasi, anche formato da un solo nodo e, a partire da questo si simula la catena per un numero di passi n grande abbastanza, restituendo in uscita l'insieme indipendente ottenuto. Nel capitolo 8 tratteremo il problema della velocità di convergenza, ovvero il problema di determinare il numero n di passi sufficienti a garantire una buona approssimazione della probabilità di generazione alla distribuzione stazionaria.

Usando la funzione random, la procedura può essere descritta nel modo seguente:

Generatore(V,E)
`begin`
    assumi $V = \{v_1, v_2, \ldots, v_k\}$
    scegli un nodo $v_i \in V$ qualsiasi
    $A := \{v_i\}$
    scegli $n \in \mathbb{N}$ abbastanza grande
    `for` $i = 1, 2, \ldots, n$ `do`
        `begin`
            $r :=$random$(0,1]$
            determina $j \in \{1, 2, \ldots, k\}$ tale che $\frac{j-1}{k} < r \leq \frac{j}{k}$
            `if` $v_j \in A$ `then` $A := A\backslash\{v_j\}$
                `else if` v_j non ha nodi adiacenti in A `then` $A := A \cup \{v_j\}$
        `end`
    `return` A
`end`

7.2 Campionatori di Gibbs

L'esempio presentato nella sezione precedente può anche essere considerato come un tipico campionatore di Gibbs (Gibbs sampler). Tali algoritmi sono generatori casuali di funzioni che dipendono da una distribuzione fissata e sono definiti da una opportuna catena di Markov.

Per definire formalmente il problema, consideriamo due insiemi finiti arbitrari V e R, entrambi di cardinalità maggiore di 1, ponendo $k = \sharp V$ e $q = \sharp R$. Denotiamo con R^V l'insieme delle funzioni definite su V a valori in R

$$R^V \;=\; \{f : V \longrightarrow R\}$$

Sia inoltre π una distribuzione di probabilità su R^V. Nota che la cardinalità di R^V è q^k, un valore esponenziale rispetto a k. Quindi per generare un elemento a caso in tale insieme secondo una distribuzione fissata, avendo in input V e R, le procedure viste nella sezione 6.1 non sono efficienti.

Osserva anche che il problema di generare a caso un insieme indipendente in un grafo $G = (V, E)$ può essere ricondotto al problema precedente: basta porre $R = \{0, 1\}$ e denotare con π la distribuzione che assegna ugual probabilità a tutte le $f \in \{0, 1\}^V$ che sono funzioni caratteristiche di insiemi indipendenti e assegna invece probabilità 0 ad ogni altra funzione in $\{0, 1\}^V$.

Un campionatore di Gibbs per generare un elemento di R^V secondo una distribuzione π è definito da una catena di Markov sull'insieme degli stati

$$S = \{A \in R^V : \pi(A) > 0\}$$

Il nuovo stato della catena viene ottenuto da uno stato corrente $A \in S$ estraendo a caso in modo uniforme un elemento $v \in V$ e scegliendo per v un nuovo valore $c \in R$ con probabilità π condizionata a conservare uguali ad A i valori degli altri elementi di V. Più formalmente, il passo generico della catena da uno stato A a uno stato B è descritto dalla seguente procedura:

```
begin
```
$A :=$ stato corrente
scegli $v \in V$ a caso secondo la distribuzione uniforme
scegli $c \in R$ a caso con probabilità
$$\Pr(c) = \pi(U \in R^V : U(v) = c \mid \forall\ w \neq v\ U(w) = A(w))$$
definisci il nuovo stato $B \in R^V$ nel modo seguente:
$B(v) = c$
$B(w) = A(w)$ per tutti i $w \in V$ tali che $w \neq v$
```
end
```

Nota che il nuovo stato B differisce da A al più per il solo valore attribuito all'elemento v estratto. Inoltre, vi è sempre una probabilità non nulla che B coincida con A poiché, qualunque sia il nodo scelto v, la probabilità che $c = A(v)$ è sempre maggiore di 0.

Per ogni $A, B \in S$, denotiamo ora con $P(A, B)$ la probabilità di scegliere il nuovo stato B partendo da A. Abbiamo

$$P(A,B) = \begin{cases} 0 & \text{se esistono } u, v \in V, u \neq v \text{ tali che} \\ & A(u) \neq B(u) \text{ e } A(v) \neq B(v) \\ \dfrac{\pi(B)}{k\ \pi(C \in R^V : C(u) = A(u)\ \forall u \neq v)} & \text{se esiste un solo } v \in V \text{ tale che} \\ & A(v) \neq B(v) \\ \dfrac{\pi(A)}{k} \displaystyle\sum_{v \in V} \dfrac{1}{\pi(C \in R^V : C(u) = A(u)\ \forall u \neq v)} & \text{se } A = B \end{cases}$$

La matrice $P = [P(A, B)]_{A,B \in S}$ è quindi la matrice di transizione della catena.

Proposizione 7.2 *La distribuzione π è reversibile per la catena di Markov definita sopra.*

Dimostrazione. Vogliamo provare che per ogni $A, B \in S$, vale la relazione

$$\pi(A) \cdot P(A, B) \ = \ \pi(B) \cdot P(B, A)$$

Chiaramente se $A = B$ la proprietà è ovvia. Lo stesso vale se A e B si differenziano per più di un valore, infatti in questo caso abbiamo $P(A, B) = 0 = P(B, A)$. Se invece A e B si differenziano per il valore attribuito a un solo elemento $v \in V$, allora per la definizione del passo generico della catena abbiamo

$$P(A,B) \ = \ \frac{1}{k} \cdot \frac{\pi(B)}{\pi(U \in R^V : U(w) = A(w)\ \forall\ w \neq v)}$$

e

$$P(B,A) \ = \ \frac{1}{k} \cdot \frac{\pi(A)}{\pi(U \in R^V : U(w) = B(w)\ \forall\ w \neq v)}$$

Poiché in entrambe le espressioni precedenti i denominatori sono uguali, con una semplice sostituzione si verifica immediatamente che $\pi(A) \cdot P(A, B) = \pi(B) \cdot P(B, A)$. □

Di conseguenza, se la catena è irriducibile, la matrice P risulta primitiva e π è quindi l'unica distribuzione stazionaria.

Il campionatore di Gibbs per π è dunque definito dall'algoritmo che su input V e R sceglie anzitutto una funzione iniziale $I \in R^V$ tale che $\pi(I) > 0$. Quindi esegue n passi della catena di Markov sopra descritta a partire da I, per un opportuno intero n abbastanza grande. Se la matrice è irriducibile, siamo sicuri che la distribuzione di probabilità dello stato raggiunto al passo n-esimo approssimi π.

Una variante del metodo sopra illustrato prevede di selezionare ciclicamente l'elemento v in V in modo tale che in ogni sequenza di k passi consecutivi tutti gli elementi siano stati estratti esattamente una volta. La selezione diventa quindi deterministica e non più casuale. Più precisamente, posto $V = \{v_1, v_2, \ldots, v_k\}$, al passo n-esimo la catena sceglie un nuovo valore per l'elemento v_j di indice $j = 1 + [n-1]_k$, dove con $[n-1]_k$ denotiamo il resto della divisione di $n-1$ per k. In questo caso il campionatore di Gibbs è detto *ciclico*. Il passo casuale è qui ristretto alla scelta del valore del nodo estratto, scelta che viene compiuta nello stesso modo precedente. La catena di Markov che si ottiene in questo caso non è più omogenea. Essa è definita da k matrici stocastiche $\{P_i\}_{i=1,\ldots,k}$, una per ogni elemento v_i. È facile tuttavia verificare che π è distribuzione reversibile per ciascuna matrice P_i e quindi rimane distribuzione stazionaria della catena.

7.3 Generazione di colorazioni di grafi

Un altro classico esempio di campionatore Gibbs è dato da un noto algoritmo per la generazione casuale di una colorazione di un grafo. In questa sezione descriviamo tale procedura, apparsa in letteratura in [11, 13], che prevede anche una variante ciclica.

Il problema è definito da un grafo non orientato $G = (V, E)$ di k nodi e da un insieme di colori $Q = \{1, 2, \ldots, q\}$. Come è noto, una q-colorazione di G è una funzione $f : V \longrightarrow Q$ tale che, per ogni $\{u, v\} \in E$, $f(u) \neq f(v)$. Denotiamo con $Z_{G,q}$ il numero di q-colorazioni di G. Inoltre, con π rappresentiamo la distribuzione uniforme sulle q-colorazioni, ovvero la funzione $\pi : Q^V \longrightarrow [0, 1]$ tale che, per ogni $f \in Q^V$,

$$\pi(f) \;=\; \begin{cases} \frac{1}{Z_{G,q}} & \text{se } f \text{ è una } q\text{-colorazione di } G \\ 0 & \text{altrimenti} \end{cases}$$

Il nostro obiettivo è quello di generare una funzione $f \in Q^V$ secondo la distribuzione di probabilità π.

È bene ricordare che anche in questo caso ci troviamo di fronte a un problema considerato generalmente difficile. Innanzitutto non è detto che un grafo non orientato G ammetta una q-colorazione. Anzi, lo stesso problema di stabilire se un grafo ammette una q-colorazione è NP-completo. Di conseguenza risulta ♯P-completo il problema di calcolare $Z_{G,q}$ su input G e q; così come è NP-hard il problema di determinare il minimo numero di colori necessari per colorare un grafo. Anche in questo caso il problema di ottimizzazione non è risolubile in tempo polinomiale in modo approssimato con errore relativo limitato (a meno che $P = NP$). Si tratta quindi di problemi difficili per i quali non sono noti nemmeno algoritmi polinomiali di approssimazione. Infine il problema di decisione resta difficile anche in casi particolari. Per esempio, è NP-completo stabilire se un grafo planare è 3-colorabile (mentre è noto che ogni grafo planare ammette una 4-colorazione).

L'idea dell'algoritmo per il nostro problema è quella di definire una catena di Markov sull'insieme di stati $S = \{f \in Q^V \mid f \text{ è } q\text{-colorazione di } G\}$ e quindi, come al solito, simulare la catena per un numero opportuno di passi. Osserviamo subito che la scelta dello stato iniziale può non essere banale se il numero di colori è piccolo. Addirittura, potrebbero non esistere q colorazioni per il grafo dato oppure, anche quando queste esistono, se il numero dei colori non è abbastanza grande può darsi sia computazionalmente difficile calcolarne una. Per questo supponiamo che si possa sempre facilmente determinare una q-colorazione di partenza. È facile verificare che questo avviene sicuramente se q è maggiore del grado di ogni nodo del grafo.

Quindi, una volta fissata la q-colorazione iniziale la catena di Markov passa da uno stato all'altro mediante il seguente procedimento che modifica lo stato corrente $f \in S$:

```
begin
      scegli a caso v ∈ V secondo la distribuzione uniforme
      calcola l'insieme U_f(v) = {c ∈ Q : f(w) ≠ c per ogni w vicino di v}
                (nota che U_f(v) ≠ ∅ poiché f(v) ∈ U_f(v) )
      scegli a caso c ∈ U_f(v) secondo la distribuzione uniforme
      f(v) = c
end
```

È facile verificare che tale catena definisce proprio un campionatore di Gibbs per la generazione di una q-colorazione di G secondo la distribuzione uniforme π.

Inoltre la stessa π è una distribuzione reversibile per la catena di Markov sopra descritta. Infatti, denotando con $P(f,g)$ la probabilità di andare in un passo dallo stato f allo stato g (per ogni coppia di q-colorazioni distinte f, g di G), abbiamo che

$$P(f,g) = \begin{cases} 0 & \text{se } f \text{ e } g \text{ si differenziano per il valore attribuito ad almeno 2 nodi} \\ \frac{1}{k} \cdot \frac{1}{\sharp U_f(v)} & \text{se } f \text{ e } g \text{ si differenziano per il valore attribuito ad un solo nodo } v \end{cases}$$

Di conseguenza, vale l'equazione $\pi(f)P(f,g) = \pi(g)P(g,f)$ e quindi π è reversibile. Inoltre, si verifica facilmente che $P(f,f) > 0$ per ogni q-colorazione f di G; infatti

$$P(f,f) = \sum_{v \in V} \frac{1}{k} \, \frac{1}{q - \sharp f(\text{Adiacenza}(v))} > 0$$

Questo implica che la matrice di transizione della catena è aperiodica. Non è detto tuttavia che la matrice sia irriducibile, questo dipende dai valori di G e di q.

Nella sezione 8.5 illustreremo una versione non omogenea del campionatore di Gibbs appena descritto, nella quale, a ogni passo, il nodo corrente $v \in V$ non è più scelto a caso ma viene determinato ciclicamente. Più precisamente, posto $V = \{v_1, v_2, \ldots, v_k\}$, al passo n-esimo si sceglie il nodo v_j di indice $j = 1 + [n-1]_k$. In questo modo, ad ogni sequenza di k passi, si ridefinisce in modo casuale il colore da attribuire a tutti i nodi del grafo. Mostreremo nel seguito che, nel caso $q > 2d^2$, la catena così ottenuta è ergodica.

7.4 L'algoritmo di Metropolis

Un altro procedimento classico basato su catene di Markov per generare a caso un elemento secondo una distribuzione fissata è dato dall'algoritmo di Metropolis. Il metodo è molto generale e può essere interpretato come una estensione dei procedimenti di visita casuale dei grafi illustrati nella sezione 5.2.

Consideriamo un insieme finito S e una distribuzione di probabilità π su S tale che $\pi(i) > 0$ per ogni $i \in S$. Per generare a caso un elemento in S secondo la distribuzione π, definiamo innanzitutto un grafo non orientato $G = (S, E)$ che goda delle seguenti proprietà:

1. S sia l'insieme dei nodi di G,
2. G sia connesso,
3. il grado di G (cioè il massimo grado dei suoi nodi) sia limitato da una opportuna costante.

Se denotiamo con d_i il grado del generico nodo $i \in S$, possiamo definire la probabilità $P(i,j)$ di passare da un nodo i a un nodo j nel modo seguente:

$$P(i,j) = \begin{cases} 0 & \text{se } i \neq j \text{ e } \{i,j\} \notin E \\ \frac{1}{d_i} \cdot \min\left\{\frac{\pi_j d_i}{\pi_i d_j}, 1\right\} & \text{se } \{i,j\} \in E \\ 1 - \frac{1}{d_i} \cdot \sum_{\ell : \{i,\ell\} \in E} \min\left\{\frac{\pi_\ell d_i}{\pi_i d_\ell}, 1\right\} & \text{se } i = j \end{cases}$$

La matrice $P = [P(i,j)_{i,j \in S}]$ è quindi la matrice di transizione della catena di Markov. Nella simulazione della catena, il generico passo dallo stato corrente i allo stato successivo j, può essere eseguito (con probabilità $P(i,j)$) applicando la seguente procedura:

```
begin
    scegli a caso ℓ nell'insieme {u ∈ S : {i, ℓ} ∈ E} in modo casuale uniforme
    if  π_ℓ d_i ≥ π_i d_ℓ then j := ℓ
                else scegli a caso j nell'insieme {ℓ, i} con le seguenti probabilità:
                                        Pr(ℓ) = π_ℓ d_i / π_i d_ℓ
                                        Pr(i) = 1 − π_ℓ d_i / π_i d_ℓ
    return j
end
```

Per tale catena valgono inoltre le seguenti proprietà.

1. Poiché G è connesso la catena è irriducibile.

2. La catena è aperiodica se esistono $i, j \in S$ tali che $\pi_j d_i < \pi_i d_j$, perché questa condizione garantisce un cappio su i. Un'altra condizione che implica l'aperiodicità è l'esistenza di un ciclo di lunghezza dispari nel grafo G.

3. La distribuzione π è reversibile per la catena. Infatti, la relazione

$$\pi_i P(i,j) = \pi_j P(j,i)$$

è chiaramente vera quando $i = j$ e quando $\{i,j\} \notin E$ e $i \neq j$. Inoltre si dimostra facilmente che la stessa vale nel caso $\{i,j\} \in E$. Quindi π è sempre la distribuzione stazionaria della catena.

È bene osservare che non sempre la catena è aperiodica. Per esempio, se per ogni $\{i,j\} \in E$ vale $\pi_i d_j = \pi_j d_i$ allora la condizione indicata nel punto 2 non è vera e l'aperiodicità non è garantita. Questo capita per esempio nelle passeggiate a caso in un grafo quando non vi sono cicli di lunghezza dispari e la probabilità di passare da un nodo i a un nodo j è data da $P(i,j) = 1/d_i$.

In ogni caso, se l'aperiodicità vale, allora la catena è ergodica con π distribuzione stazionaria. Possiamo quindi adottare il solito criterio: simuliamo la catena a partire da uno stato qualsiasi per un numero sufficientemente grande di passi e restituiamo il valore dello stato raggiunto. Al crescere del numero di passi sappiamo che la probabilità di restituire un valore i approssima π_i, per ogni $i \in S$.

Capitolo 8

Analisi della velocità di convergenza

Un problema naturale che finora abbiamo trascurato è quello di valutare la velocità con la quale la distribuzione di probabilità di una catena di Markov ergodica converge alla distribuzione stazionaria.

Se infatti $\{X_n\}$ è una catena di Markov ergodica e π è la sua distribuzione stazionaria, sappiamo che, qualunque sia lo stato di partenza, la distribuzione di probabilità della variabile X_n approssima π al crescere di n. Tuttavia, in generale le due distribuzioni di probabilità non sono uguali, ed è quindi lecito chiedersi quanto deve essere grande n affinché la loro differenza sia minore di una quantità fissata. L'utilità pratica di questa valutazione è evidente: dato un algoritmo MCMC corretto per generare a caso un elemento con una certa probabilità, ci chiediamo quanti passi della catena dobbiamo eseguire per ottenere uno stato con una probabilità che si discosta da quella desiderata per una quantità ritenuta trascurabile.

Per valutare tale velocità di convergenza possiamo individuare in prima istanza due metodi rilevanti. Il primo è un metodo generale, sempre valido per ogni catena di Markov ergodica, il quale però non fornisce sempre una valutazione significativa ed effettivamente utile per definire procedure efficienti di generazione casuale. Tale valutazione della velocità dipende infatti da vari parametri tra i quali vi è anche il numero degli stati della catena e spesso questo è uno svantaggio, perché nelle applicazioni reali tale quantità in molti casi è esponenziale rispetto alle dimensioni del problema che si sta considerando. Un secondo metodo tradizionale è invece quello dell'accoppiamento, il quale permette spesso di fornire valutazioni efficienti degli algoritmi di generazione casuale. Tale metodo però non è sempre utilizzabile e la sua applicabilità dipende dalla matrice di transizione della catena. Il cosiddetto *lemma di accoppiamento* fornisce uno strumento spesso utile per mostrare che la distribuzione di probabilità di una catena ergodica si avvicina rapicamente alla sua distribuzione stazionaria, ovvero, come si usa dire, che la catena è *rapidly mixing*.

Prima di affrontare il problema in dettaglio, ricordiamo nella prossima sezione alcune proprietà della distanza di variazione totale introdotta nel capitolo 4.2. Quest'ultima infatti rappresenta la naturale misura utilizzata per valutare la differenza complessiva tra due distribuzioni di probabilità discrete definite sullo stesso insieme finito.

8.1 Distanza di variazione totale

Per ogni coppia di distribuzioni di probabilità μ e ν, definite sullo stesso insieme finito $S = \{1, 2, \ldots, k\}$, il valore $d_{TV}(\mu, \nu)$ è dato da

$$d_{TV}(\mu, \nu) = \frac{1}{2} \sum_{i \in S} |\mu_i - \nu_i| = \frac{1}{2} ||\mu - \nu||_1$$

Sappiamo che d_{TV} è una distanza in senso tradizionale. Inoltre si possono dimostrare le seguenti proprietà.

Proposizione 8.1 *Se μ e ν sono due distribuzioni di probabilità definite sullo stesso insieme finito S allora $d_{TV}(\mu, \nu)$ è la massima differenza tra le due distribuzioni valutate su un qualunque sottoinsieme di S, ovvero*

$$d_{TV}(\mu, \nu) = \max_{A \subseteq S} |\mu(A) - \nu(A)|$$

Proposizione 8.2 *Se X e Y sono due variabili aleatorie definite sullo stesso spazio di probabilità a valori in un insieme finito S e hanno distribuzione μ e ν, rispettivamente, allora*

$$d_{TV}(\mu, \nu) \ \leq \ Pr(X \neq Y)$$

Dimostrazione. Sia $A = \{i \in S \mid \mu_i \geq \nu_i\}$. Allora

$$\sum_{i \in S} |\mu_i - \nu_i| = \sum_{i \in A} (\mu_i - \nu_i) + \sum_{i \in A^c} (\nu_i - \mu_i)$$

La prima sommatoria nella parte destra dell'equazione può essere maggiorata nel modo seguente:

$$\begin{aligned} \sum_{i \in A} (\mu_i - \nu_i) &= \mu(A) - \nu(A) = \Pr(X \in A) - \Pr(Y \in A) \\ &\leq \Pr(X \in A) - \Pr(X \in A, Y \in A) \\ &= \Pr(X \in A, Y \notin A) \ \leq \ \Pr(X \neq Y) \end{aligned}$$

In maniera analoga si prova che

$$\sum_{i \in A^c} (\nu_i - \mu_i) \ \leq \ \Pr(Y \in A^c, X \notin A^c) \ \leq \ \Pr(X \neq Y)$$

Applicando quindi le due disuguaglianze alla prima equazione otteniamo

$$\sum_{i \in S} |\mu_i - \nu_i| \ \leq \ 2 \Pr(X \neq Y)$$

che prova il risultato. □

8.2 Approssimazione generale alla distribuzione stazionaria

Torniamo ora al problema di valutare la velocità di convergenza di una catena di Markov ergodica. Per definire il problema formalmente, consideriamo una catena di Markov $\{X_n\}$ su un insieme finito di stati S, con matrice di transizione P primitiva e sia π la sua distribuzione stazionaria. Per il teorema 4.6 sappiamo che, per ogni distribuzione iniziale μ della catena,

$$\lim_{n\to+\infty} \| \mu P^n - \pi \|_1 = 0$$

Vogliamo trovare una funzione $g_P : \mathbb{R}_+ \to \mathbb{N}$, dipendente dalla matrice P, tale che per ogni distribuzione iniziale μ, ogni $\varepsilon > 0$ e ogni $n \geq g_P(\varepsilon)$, vale

$$d_{TV}(\mu P^n, \pi) \leq \varepsilon$$

Una funzione g_P generale, che può sempre essere usata quando la matrice P è primitiva, deriva dallo stesso teorema 4.6 ed è basata sul coefficiente ergodico β introdotto nella definizione 4.1. Infatti poiché P è primitiva esiste un intero $t \in \mathbb{N}$, tale che $P^t > 0$ e quindi $\beta(P^t) < 1$. Sappiamo inoltre per il lemma 4.4 che

$$\| \mu P^t - \pi \|_1 \leq \beta(P^t) \| \mu - \pi \|_1$$

Quindi per ogni intero $n > t$, ponendo $n = mt + r$ con $r \in \{0, 1, \ldots, t-1\}$, otteniamo

$$\begin{aligned} d_{TV}(\mu P^n, \pi) &= \frac{1}{2} \| \mu P^n - \pi \|_1 = \frac{1}{2} \| \mu P^r \cdot P^{tm} - \pi \|_1 \\ &\leq \frac{1}{2} \beta(P^t)^m \| \mu P^r - \pi \|_1 \leq \beta(P^t)^{\frac{n-r}{t}} \\ &\leq \beta(P^t)^{\frac{n}{t}-1} \end{aligned}$$

Quest'ultima quantità è minore o uguale a ε per $\left(\frac{n}{t} - 1\right) \log(\beta(P^t)) \leq \log(\varepsilon)$, ovvero per ogni intero n tale che $n \geq t\left(1 + \frac{\log(\varepsilon)}{\log(\beta(P^t))}\right)$. Abbiamo quindi provato il seguente risultato.

Proposizione 8.3 *Sia P una matrice stocastica primitiva di dimensione $k \times k$ con distribuzione stazionaria π e sia t il minimo intero in $\mathbb{N}$ tale che $P^t > 0$. Allora, per ogni $\varepsilon > 0$ e ogni vettore stocastico μ di dimensione k, si verifica che $d_{TV}(\mu P^n, \pi) \leq \varepsilon$ per tutti gli interi n tali che*

$$n \geq t\left(1 + \frac{\log(\varepsilon)}{\log(\beta(P^t))}\right) \tag{8.1}$$

Questo implica che la funzione $g_P(\varepsilon) = t\left(1 + \frac{\log \varepsilon}{\log \beta(P^t)}\right)$ soddisfa la condizione richiesta. Nota che entrambi i valori $\log \varepsilon$ e $\log \beta(P^t)$ sono in generale valori negativi. Inoltre è chiaro che per ε decrescente, il valore $g_P(\varepsilon)$ cresce. Osserva anche che il valore t può essere prossimo o anche superiore al numero di stati, perché rappresenta la lunghezza minima di cammino necessaria a collegare tutte le coppie di stati. Infatti, nell'esempio 2.1 della sezione 2.5, abbiamo mostrato (per ogni $k \geq 3$) l'esistenza di matrici primitive di dimensione k per le quali il valore di t è $2k - 2$. Questo fatto rende quindi la formula (8.1) poco utile nelle applicazioni quando il numero degli stati della catena è elevato (per esempio esponenziale) rispetto alle dimensioni del problema che si sta considerando. Viceversa la formula può essere

utile in quelle situazioni in cui t è piccolo rispetto al numero di stati, per esempio nel caso in cui tutte le coppie di nodi sono collegabili con cammini di lunghezza limitata.

Un altro parametro che può determinare un valore elevato di $g_P(\varepsilon)$ è il valore $\beta(P^t)$. Infatti se quest'ultimo è molto vicino a 1 allora $g_P(\varepsilon)$ è grande e può rendere la formula poco utile nella pratica.

Osserviamo infine che valori tradizionali di ε che nella pratica consentono spesso una buona approssimazione alla distribuzione stazionaria sono dati da $\varepsilon = 10^{-3}$ o $\varepsilon = 10^{-4}$.

8.3 Il metodo dell'accoppiamento

Diamo ora uno strumento formale utile per determinare una funzione g_P adeguata e quindi per valutare la velocità di convergenza alla distribuzione stazionaria. Anche in questa sezione supponiamo che $\{X_n\}$ sia una catena di Markov finita sull'insieme di stati $S = \{1, \ldots, k\}$, con matrice di transizione P primitiva e distribuzione stazionaria π.

Definizione 8.1 *Per ogni $i \in S$ e ogni $n \in \mathbb{N}$ sia ${P^n}_i$ la i-esima riga di P^n. Definiamo allora i valori $\Delta_i(n)$ e $\Delta(n)$ mediante le relazioni*

$$\Delta_i(n) = d_{TV}({P^n}_i, \pi) \ , \qquad \Delta(n) = \max\{\Delta_i(n) : i \in S\}$$

Inoltre, per ogni $\varepsilon > 0$ definiamo

$$\tau(\varepsilon) = \min\{n \in \mathbb{N} : \Delta(n) \leq \varepsilon\}$$

La funzione $\tau(\varepsilon)$ è chiamata mixing time della catena.

Nelle nostre ipotesi le seguenti proprietà sono facilmente verificate:

1. per ogni $i \in S$ abbiamo $\lim_{n\to+\infty} \Delta_i(n) = 0$ e quindi $\lim_{n\to+\infty} \Delta(n) = 0$;
2. per il lemma 4.4 le distanze $\Delta_i(n)$ non crescono mai al crescere di n, ovvero

   $$\Delta_i(n+1) = d_{TV}({P^{n+1}}_i, \pi) \leq \beta(P) d_{TV}({P^n}_i, \pi) \leq \Delta_i(n) \qquad \forall\ i,\ n$$

   e lo stesso vale per i coefficienti $\Delta(n)$;
3. di conseguenza per ogni $n \geq \tau(\varepsilon)$ vale $\Delta(n) \leq \varepsilon$ e quindi

   $$\tau(\varepsilon) = \min\{n \in \mathbb{N} : \Delta(m) \leq \varepsilon\ \forall m \geq n\}$$

4. per ogni distribuzione iniziale μ di $\{X_n\}$ e ogni $\varepsilon > 0$, se $n \geq \tau(\varepsilon)$ allora

   $$d_{TV}(\mu P^n, \pi) \leq \varepsilon$$

L'ultima proprietà mostra che $\tau(\varepsilon)$ rappresenta intuitivamente la miglior funzione $g_P(\varepsilon)$ che garantisce una approssimazione alla distribuzione stazionaria con errore al più ε. In altre parole $\tau(\varepsilon)$ fornisce sempre il più piccolo n per cui la approssimazione è garantita da n in poi (cioè per ogni $\mu \in M_k$, $d_{TV}(\mu P^m, \pi) \leq \varepsilon$ per qualsiasi $m \geq n$).

La dimostrazione della 4) data sopra è conseguenza della seguente disuguaglianza che può essere provata per ogni $\mu \in M_k$ usando le proprietà delle distribuzioni stazionarie e della distanza di variazione totale:

$$d_{TV}(\mu P^n, \pi) \ \leq \ \sum_{i \in S} \mu_i \ d_{TV}(P^n{}_i, \pi)$$

Nelle applicazioni degli algoritmi MCMC siamo chiaramente interessati a trovare i valori di $\tau(\varepsilon)$ più piccoli possibile. Se denotiamo con n la dimensione dell'istanza del problema cui applichiamo l'algoritmo, si dice che la catena di Markov considerata è *rapidly mixing* se $\tau(\varepsilon)$ è un valore polinomialmente limitato rispetto a n e a $\log 1/\varepsilon$. Osserviamo che in molte applicazioni di interesse il numero degli stati della catena è esponenziale rispetto a n.

Uno dei metodi principali per valutare $\tau(\varepsilon)$ è basato sulla costruzione di una coppia di catene di Markov sullo stesso insieme di stati, aventi la medesima matrice di transizione. Questa nozione è formalizzata dalla seguente definizione.

Definizione 8.2 *Dato un insieme finito di stati S e una matrice stocastica $P = [p(i,j)]_{i,j \in S}$, un accoppiamento è una catena di Markov $\{Z_n\}$ sull'insieme degli stati $S \times S$, tale che $Z_n = (X_n, Y_n)$ per ogni $n \in \mathbb{N}$ e per ogni $i, j, \ell \in S$*

$$Pr(X_{n+1} = j \mid X_n = i, Y_n = \ell) = p(i,j)$$
$$Pr(Y_{n+1} = j \mid X_n = \ell, Y_n = i) = p(i,j)$$

In questa definizione $\{X_n\}$ e $\{Y_n\}$ possono essere pensate come due catene di Markov sul medesimo spazio degli stati S che si muovono in parallelo ad ogni passo, mediante le stesse probabilità di transizione P. Nota che per ogni coppia di insiemi $A, B \subseteq S$ l'evento $(X_n \in A, Y_n \in B)$ è sempre ben definito e di conseguenza anche il valore $\Pr(X_n \in A, Y_n \in B)$. Inoltre non si pone alcun vincolo di dipendenza tra le due catene, che possono quindi risultare del tutto indipendenti, oppure fortemente condizionate tra loro a patto che la definizione data sopra sia valida. Anche le distribuzioni iniziali delle due catene non sono soggette ad alcuna restrizione e di conseguenza possono essere arbitrarie.

Infine osserviamo che per ogni accoppiamento (X_n, Y_n) possiamo considerare la variabile aleatoria $T = \min\{n \in \mathbb{N} : X_n = Y_n\}$ che rappresenta l'eventuale primo istante di incontro delle due catene, e definire un nuovo accoppiamento (X_n, Y'_n) tale che

$$Y'_n = \begin{cases} Y_n & \text{se } n < T \\ X_n & \text{altrimenti} \end{cases}$$

Nota che oper ogni n le due variabili Y_n e Y'_n hanno la stessa distribuzione, ovvero $\Pr(Y_n = i) = \Pr(Y'_n = i)$ per ogni $i \in S$. Inoltre è chiaro che $X_n = Y'_n$ per tutti gli $n \geq T$, ovvero una volta che si incontrano le due catene restano uguali.

Il seguente lemma consente di valutare il mixing time di una catena con matrice di transizione primitiva, avendo a disposizione un accoppiamento nel quale le due catene si incontrano rapidamente.

Lemma 8.4 *Sia (X_n, Y_n) un accoppiamento di catene di Markov con matrice di transizione P primitiva, insieme di stati S. Supponi che esista $t \in \mathbb{N}$ tale che, per ogni $i, j \in S$,*

$$Pr(X_t \neq Y_t \mid X_0 = i, Y_0 = j) \leq \varepsilon$$

Allora

$$\tau(\varepsilon) \leq t$$

ovvero $d_{TV}({P^t}_i, \pi) \leq \varepsilon$ *per ogni* $i \in S$*, dove* π *è la distribuzione stazionaria.*

Dimostrazione. Le ipotesi del lemma non dipendono dalle distribuzioni iniziali delle due catene $\{X_n\}$, $\{Y_n\}$. Possiamo allora supporre che $X_0 = i$ per qualche $i \in S$ e Y_0 abbia distribuzione π (stazionaria). Allora per la proposizione 8.2 e l'ipotesi data abbiamo

$$\begin{aligned} d_{TV}({P^t}_i, \pi) &\leq \Pr(X_t \neq Y_t) \\ &= \sum_{j \in S} \Pr(X_t \neq Y_t \mid X_0 = i, Y_0 = j) \Pr(X_0 = i, Y_0 = j) \\ &\leq \varepsilon \sum_{j \in S} \pi_j = \varepsilon \end{aligned}$$

Questo implica che $d_{TV}({P^t}_i, \pi) \leq \varepsilon$ per ogni $i \in S$ e quindi $\tau(\varepsilon) \leq t$. □

Esempio Consideriamo il problema di mischiare un mazzo di carte. Formalmente abbiamo un insieme di n carte e vogliamo generare una permutazione (allineamento) casuale uniforme di tale insieme. È facile mostrare che il problema si può risolvere usando ripetutamente una procedura simile a quelle utilizzate nella sezione 6.1 senza usare i metodi esposti sopra. Tuttavia, presentiamo come esempio una catena di Markov rapidly mixing che fornisce un algoritmo MCMC per il problema, basandosi proprio sul metodo dell'accoppiamento.

Sia S l'insieme delle permutazioni delle n carte. Definiamo una catena di Markov $\{X_t\}$ con insieme di stati S nella quale ogni X_t è ottenuta da X_{t-1} scegliendo una carta a caso con probabilità uniforme $(1/n)$, qualunque sia la sua posizione nell'allineamento raggiunto e mettendola all'inizio di X_{t-1}. È facile verificare che tale catena è irriducibile e aperiodica (esercizio). Inoltre la matrice di transizione è bistocastica, perché ogni $y \in S$ può essere raggiunto in un passo esattamente da n stati. Quindi la catena è ergodica e la distribuzione stazionaria coincide con quella uniforme.

Definiamo ora un accoppiamento (X_t, Y_t). Ad ogni passo X_t è ottenuta da X_{t-1} con il procedimento descritto sopra. Se C è la carta scelta in questa transizione allora Y_t è ottenuta da Y_{t-1} prelevando la stessa carta C, ovunque essa si trovi in Y_{t-1}, e spostandola all'inizio dell'allineamento. È chiaro che la matrice di transizione di $\{Y_t\}$ è la medesima poiché la carta scelta ad ogni passo è sempre generata in modo casuale uniforme. Inoltre se dopo m passi tutte le carte sono state scelte almeno una volta allora $X_m = Y_m$ e, da questo momento in poi le due catene ad ogni passo entrano nello stesso stato, ovvero $X_t = Y_t$ per ogni $t \geq m$.

Proposizione 8.5 *La catena appena descritta è rapidly mixing.*

Dimostrazione. Vogliamo applicare il Lemma 8.4. Per questo dobbiamo valutare $\Pr(X_t \neq Y_t \mid X_0 = i, Y_0 = j)$ per $t \in \mathbb{N}$. A questo scopo, sia $A_t(C)$ l'evento per il quale la carta C non è stata scelta in t passi. Allora è chiaro che

$$\Pr(A_t(C)) = \left(1 - \frac{1}{n}\right)^t$$

Inoltre, denotando con M l'insieme di tutte le carte, abbiamo $(X_t \neq Y_t) = \bigcup_{C \in M} A_t(C)$ e quindi, per ogni $i, j \in S$

$$\Pr(X_t \neq Y_t \mid X_0 = i, Y_0 = j) \leq n \left(1 - \frac{1}{n}\right)^t \leq n\, e^{-t/n}$$

Quest'ultima quantità è minore o uguale a ε per ogni $t \in \mathbb{N}$ tale che $t \geq n \log n + n \log 1/\varepsilon$. Applicando ora il Lemma 8.4 si ottiene $\tau(\varepsilon) \leq n \log n + n \log 1/\varepsilon$ che prova il risultato. □

8.4 Generatore di Indipendent Set di dimensione fissata

In questa sezione presentiamo un algoritmo MCMC per la generazione casuale uniforme di indipendent set di dimensione fissata in un grafo dato per il quale la corrispondente catena di Markov è rapidly mixing. Anche in questo caso il risultato è basato sul metodo dell'accoppiamento descritto nella sezione precedente.

Consideriamo un grafo non orientato $G = (V, E)$ di n nodi, con grado massimo Δ e sia $k \in \mathbb{N}$ un intero positivo tale che

$$k \leq \frac{n}{3(\Delta + 1)}$$

Denotiamo con S_k l'insieme degli indipendent set di G di dimensione k

$$S_k = \{A \subseteq V \mid \sharp A = k, \forall u, v \in A\ \{u, v\} \notin E\}$$

Sia inoltre $Z_k(G)$ la cardinalità di S_k, in simboli $Z_k(G) = \sharp S_k$. Vogliamo generare un elemento $A \in S_k$ con probabilità uniforme e denotiamo con π tale misura di probabilità sull'insieme S_k

$$\pi(A) = \frac{1}{Z_k(G)} \qquad A \in S_k$$

Osserva che per il vincolo posto sul valore k l'insieme S_k non è vuoto ed è facile costruire un elemento $A \in S_k$ in $O(n^2)$ passi.

Definiamo ora una catena di Markov sull'insieme di stati S_k. Il passo generico della catena è definito dalla seguente procedura che modifica lo stato corrente $A \in S_k$:

```
begin
    scegli a caso v ∈ A secondo la distribuzione uniforme
    scegli a caso w ∈ V secondo la distribuzione uniforme
    if w ∉ A ∧ (A\{v}) ∪ {w} ∈ S_k then A := (A\{v}) ∪ {w}
end
```

Quindi, per ogni $A, B \in S_k$ la probabilità di transizione da A a B è data da

$$P(A,B) = \begin{cases} 0 & \text{se } \sharp(A \div B) > 2 \\ \frac{1}{kn} & \text{se } \sharp(A \div B) = 2 \\ 1 - \frac{\sharp\{C \in S_k \mid \sharp(A \div C) = 2\}}{kn} & \text{se } A = B \end{cases}$$

Proposizione 8.6 *La matrice $P = [P(A,B)]_{A,B \in S_k}$ è primitiva e la distribuzione uniforme π coincide con la distribuzione stazionaria della catena.*

Dimostrazione. È chiaro che $P(A, A) > 0$ per ogni $A \in S_k$ e quindi la matrice è aperiodica. Inoltre la matrice P è simmetrica per cui la distribuzione uniforme π è reversibile e quindi stazionaria. Rimane solo da dimostrare che P è irriducibile.

A questo scopo, per ogni $B \subseteq V$ definiamo $\mathrm{Ad}(B) = \{w \in V \mid \exists v \in B : \{v, w\} \in E\}$. Nota che $\mathrm{Ad}(A) \cap A = \emptyset$ per ogni $A \in S_k$. Siano ora A, B due elementi in S_k. Vogliamo costruire un cammino da A a B nella catena. Se $B \cap \mathrm{Ad}(A) = \emptyset$ allora $A \cup B$ è un indipendent set e possiamo passare da A a B con al più k passi nei quali l'elemento v da togliere dallo stato corrente viene scelto in $A \backslash B$ e l'elemento w da aggiungere viene preso in $B \backslash A$.

Se invece $B \cap \mathrm{Ad}(A) \neq \emptyset$ allora si può dimostrare che esiste $C \in S_k$ tale che $C \cap \mathrm{Ad}(A) = \emptyset = C \cap \mathrm{Ad}(B)$. Una volta noto tale insieme C si possono costruire un cammino da A a C e uno da C a B ragionando come nel caso precedente. L'esistenza di C è provata dal fatto che l'insieme $A \cup B \cup \mathrm{Ad}(A) \cup \mathrm{Ad}(B)$ possiede al più $2k(\Delta + 1) \leq n - k(\Delta + 1)$ elementi e quindi il suo complementare contiene almeno $k(\Delta + 1)$ nodi dai quali è sempre possibile ricavare un indipendent set C di k vertici. □

Costruiamo ora un accoppiamento (X_t, Y_t) su S_k con matrice di transizione P. Poiché i valori di X_t e Y_t sono insiemi di k nodi, per ogni $t \in \mathbb{N}$ abbiamo $\sharp(X_t \backslash Y_t) = \sharp(Y_t \backslash X_t)$; possiamo quindi considerare una corrispondenza biunivoca tra i due insiemi $f : X_t \backslash Y_t \to Y_t \backslash X_t$. La transizione da X_t a X_{t+1} viene eseguita come descritto sopra: si scelgono $v \in X_t$ e $w \in V$ in modo casuale uniforme, se $w \notin X_t$ e $(X_t \backslash \{v\}) \cup \{w\} \in S_k$ allora $X_{t+1} = (X_t \backslash \{v\}) \cup \{w\}$, altrimenti $X_{t+1} = X_t$. Invece, il nuovo stato Y_{t+1} si ottiene da Y_t scegliendo $v' \in Y_t$ e $w' \in V$ tali che

$$w' = w \ , \qquad v' = \begin{cases} v & \text{se } v \in Y_t \\ f(v) & \text{altrimenti} \end{cases}$$

e operando in maniera analoga.

Osserva che la definizione dell'accoppiamento (X_t, Y_t) è corretta. Inoltre, se per qualche $t \in \mathbb{N}$ abbiamo $X_t = Y_t$ allora $X_\ell = Y_\ell$ per ogni $\ell \geq t$.

La velocità di convergenza della catena è basata sulla seguente proprietà la cui dimostrazione, che qui omettiamo per brevità, si può trovare in [15].

Proposizione 8.7 *Per ogni $A, B \in S_k$ e ogni $\varepsilon > 0$, $Pr(X_t \neq Y_T \mid X_0 = A, Y_0 = B) \leq \varepsilon$ per ogni $t \in \mathbb{N}$ tale che*

$$t \ \geq \ \frac{kn(\log k + \log 1/\varepsilon)}{3(\Delta + 1)}$$

Applicando ora il Lemma 8.4 si ottiene, per ogni $\varepsilon > 0$,

$$\tau(\varepsilon) \ \leq \ \frac{kn(\log k + \log 1/\varepsilon)}{3(\Delta + 1)}$$

e questo prova che la catena descritta è rapidly mixing.

8.5 Velocità di convergenza della colorazione di grafi

Valutiamo ora la velocità di convergenza del campionatore di Gibbs descritto nella sezione 7.3. In questa sede, tuttavia, consideriamo una versione ciclica del campionatore, nella quale cioè tutti i nodi vengono ricolorati dopo un numero fissato di passi. Per definire la procedura, ricordiamo anzitutto i dati del problema.

Dato un grafo non orientato $G = (V, E)$ di k nodi $V = \{v_1, v_2, \ldots, v_k\}$ e un insieme di colori $Q = \{1, 2, \ldots, q\}$, sia $S = \{f \in Q^V \mid f(u) \neq f(v)\ \forall \{u, v\} \in E\}$ l'insieme delle q-colorazioni di G e denotiamo con $Z_{G,q}$ il loro numero, $Z_{G,q} = \sharp S$. Denotiamo inoltre con d il *grado* di G, cioè il massimo tra i gradi dei suoi nodi. Supponiamo che il numero di colori sia abbastanza grande, per esempio $q > d$. In questo modo siamo sicuri che $S \neq \emptyset$ ed è facile determinare una q-colorazione di G. Vogliamo generare a caso un elemento di S secondo una distribuzione di probabilità che approssimi la distribuzione uniforme, definita dalla funzione π tale che

$$\text{per ogni } f \in Q^V, \quad \pi(f) = \begin{cases} \frac{1}{Z_{G,q}} & \text{se } f \in S \\ O & \text{altrimenti} \end{cases}$$

La procedura definisce una catena di Markov non omogenea $\{X_n\}$ sull'insieme degli stati S. Di fatto al primo passo si sceglie un elemento $X_0 \in S$ qualsiasi. Quindi si eseguono n passi nella catena, all'i-esimo passo si ricolora il nodo v_j dove $j = 1 + [i-1]_k$, scegliendo il nuovo colore in modo uniforme sull'insieme dei colori compatibili con quelli dei nodi adiacenti a v_j. Formalmente l'algoritmo definito nel modo seguente:

```
begin
    calcola una q-colorazione f ∈ S qualsiasi
    for i = 1, 2, ..., n do
        begin
            j := 1 + [i − 1]_k
            v := v_j
            U = {c ∈ Q : f(w) ≠ c per ogni w ∈ V tale che {w, v} ∈ E}
            scegli a caso c ∈ U secondo la distribuzione uniforme
            f(v) := c (lasciando inalterati gli altri valori di f(w) con w ≠ v)
        end
    return f
end
```

Chiaramente la catena di Markov $\{X_n\}$ definita implicitamente dalla procedura precedente non è omogenea; piuttosto essa è definita da k matrici stocastiche $P_1, P_2, \ldots, P_k$, dove ciascuna P_j è associata al nodo v_j. È facile provare, ragionando come nella sezione 7.3, che π è reversibile per tutte le matrici P_j, $j = 1, 2, \ldots, k$, e quindi π rimane distribuzione stazionaria della catena.

Studiamo ora la velocità di convergenza del campionatore appena descritto nell'ipotesi ulteriore che $q > 2d^2$, seguendo essenzialmente la presentazione svolta in [7] che consente di semplificare notevolmente la prova.

Teorema 8.8 *Dato un insieme di colori $Q = \{1, 2, \ldots, q\}$, sia $G = (V, E)$ un grafo non orientato di k nodi, sia d il grado di G e sia $\{X_n\}$ la catena di Markov descritta sopra sulle q-colorazioni di G. Denotiamo inoltre con $\mu^{(n)}$ la distribuzione di probabilità di X_n (per ciascun $n \in \mathbb{N}$) e con π la distribuzione uniforme sull'insieme delle q-colorazioni di G. Se $q > 2d^2$, allora esiste una costante $C > 0$, dipendente solo da d e da q, tale che per ogni $\varepsilon > 0$ vale*

$$d_{TV}(\mu^{(n)}, \pi) \leq \varepsilon$$

per tutti gli $n \in \mathbb{N}$ *che soddisfano*

$$n \;>\; Ck(\log k + \log(1/\varepsilon))$$

Prima di illustrare la dimostrazione, elenchiamo le seguenti osservazioni:

1. Nota che il teorema garantisce l'ergodicità di una catena non uniforme, provando che, qualunque sia lo stato iniziale, $\mu^{(n)}$ converge a π.

2. Il tempo di calcolo richiesto per ottenere una approssimazione con errore minore o uguale a ε è dell'ordine $\mathrm{O}(k \log k + k \log(1/\varepsilon))$ poiché, assumendo d e q costanti, è chiaro che un passo della catena richiede al più tempo costante. Osserva che questo valore è molto buono perché dipende dal numero di nodi del grafo e non dal numero di stati della catena, che in questo caso potrebbe essere troppo elevato (coincide infatti con il numero di q-colorazioni del grafo).

3. La condizione $q > 2d^2$ può in realtà essere rilassata; in effetti il risultato originale ottenuto in [11] richiede solo la condizione $q > 2d$, la prova è tuttavia più complicata e poco adatta ad una presentazione in questa sede.

4. Nella dimostrazione si mostrerà un'espressione precisa della costante C che quindi potrà essere utilizzata nelle applicazioni.

Dimostrazione. La prova è basata sulla tecnica di accoppiamento. Dobbiamo quindi definire una nuova catena di Markov $\{Y_n\}$ sullo stesso spazio di probabilità di $\{X_n\}$, a valori nello stesso insieme di stati S, dotata delle stesse matrici di transizione di $\{X_n\}$ ma con distribuzione iniziale π. Di conseguenza avremo, per ogni $n \in \mathbb{N}$,

$$\Pr(Y_n = f) = \pi(f), \quad \forall f \in S$$

Per la proposizione 8.2 sappiamo che $d_{TV}(\mu^{(n)}, \pi) \leq \Pr(X_n \neq Y_n)$. Quindi il nostro problema sarà ridotto a maggiorare la probabilità che X_n e Y_n siano diversi. Per questo motivo siamo interessati a definire $\{Y_n\}$ in modo che le due catene, evolvendo in parallelo, una volta incontratesi nel medesimo stato rimangano uguali.

Al generico passo n-esimo, note le funzioni X_{n-1} e Y_{n-1}, consideriamo il nodo corrente $v = v_{1+[n-1]_k}$. I nuovi valori $X_n(v)$ e $Y_n(v)$ si possono ottenere nel modo seguente: si genera una permutazione casuale uniforme

$$(c_1^n, c_2^n, \ldots, c_q^n)$$

degli elementi di Q; si assegna a $X_n(v)$ il primo colore c_i^n diverso dai colori $X_{n-1}(w)$ per tutti i w adiacenti a v; in modo analogo, sempre usando la stessa permutazione, si sceglie il colore $Y_n(v)$. Formalmente, abbiamo

$$X_n(v) = c_i^n \;\text{ dove }\; i = \min\{j : c_j^n \neq X_{n-1}(w) \;\text{ per ogni } w \text{ tale che } \{v, w\} \in E\}$$
$$Y_n(v) = c_{i'}^n \;\text{ dove }\; i' = \min\{j : c_j^n \neq Y_{n-1}(w) \;\text{ per ogni } w \text{ tale che } \{v, w\} \in E\}$$

Osserva anche che, se per qualche ℓ vale $X_\ell = Y_\ell$, allora $X_n = Y_n$ per tutti gli $n \geq \ell$.

A questo punto vogliamo valutare $\Pr(X_n(v) \neq Y_n(v))$, dove v è il nodo corrente relativo al passo n-esimo. In seguito chiameremo "fallimento(v)" l'evento $(X_n(v) \neq Y_n(v))$. Consideriamo inizialmente il primo ciclo, ovvero quando $n \leq k$. Possiamo suddividere l'insieme dei colori in tre sottoinsiemi con le seguenti cardinalità:

1. B_0 sia il numero di colori in Q diversi da $X_{n-1}(w)$ e $Y_{n-1}(w)$ per tutti i nodi w adiacenti a v
$$B_0 = \sharp\{c \in Q \mid X_{n-1}(w) \neq c \neq Y_{n-1}(w) \ \forall \ w : \{v, w\} \in E\}$$
2. B_1 sia il numero di colori assegnati ai nodi adiacenti a v in una sola delle due colorazioni X_{n-1} e Y_{n-1}.
3. B_2 sia il numero di colori assegnati ai nodi adiacenti a v in entrambe le colorazioni X_{n-1} e Y_{n-1}.

Chiaramente $q = B_0 + B_1 + B_2$ e inoltre è facile verificare che

$$\Pr(X_n(v) \neq Y_n(v)) = \frac{B_1}{B_0 + B_1}$$

Poiché $B_2 \leq d$ e $B_1 \leq 2d - 2B_2$ otteniamo

$$\Pr(X_n(v) \neq Y_n(v)) \leq \frac{2d - 2B_2}{q - B_2} \leq \frac{2d}{q} \frac{\left(1 - \frac{B_2}{d}\right)}{\left(1 - \frac{B_2}{q}\right)} \leq \frac{2d}{q}$$

Di conseguenza, se $n = k$ la disuguaglianza precedente vale per ogni nodo v del grafo e possiamo quindi scrivere

$$\Pr(X_k(v) \neq Y_k(v)) \leq \frac{2d}{q} \ , \quad \text{per ogni } v \in V$$

Consideriamo ora il secondo ciclo: $k < n \leq 2k$. Per semplicità, se v è il nodo corrente al passo n-esimo, chiamiamo "discrepanza(v)" l'evento ($\exists$ w adiacente a v tale che $X_n(w) \neq Y_n(w)$). Dalla disuguaglianza precedente otteniamo

$$\Pr(\text{discrepanza}(v)) \leq \frac{2d^2}{q}$$

Inoltre, poiché "fallimento(v)" implica "discrepanza(v)", con una prova analoga a quella illustrata per il primo ciclo si dimostra che

$$\Pr(\text{fallimento}(v)/\text{discrepanza}(v)) \leq \frac{2d}{q}$$

e quindi si ottiene

$$\Pr(\text{fallimento}(v)) \ = \ \Pr(\text{fallimento}(v)/\text{discrepanza}(v)) \ \Pr(\text{discrepanza}(v)) \ \leq \ \frac{2d}{q}\left(\frac{2d^2}{q}\right)$$

Questo implica che per ogni $v \in V$

$$\Pr(X_{2k}(v) \neq Y_{2k}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right)$$

Ragionando nello stesso modo per il terzo ciclo ricaviamo, per ogni $v \in V$,

$$\Pr(X_{3k}(v) \neq Y_{3k}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right)^2$$

Le stesse considerazioni applicate all'm-esimo ciclo (per un $m \in \mathbb{N}$ qualsiasi) portano alla disuguaglianza

$$\Pr(X_{mk}(v) \neq Y_{mk}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right)^{m-1}$$

Di conseguenza

$$\Pr(X_{mk} \neq Y_{mk}) \leq \sum_{v \in V} \Pr(X_{mk}(v) \neq Y_{mk}(v)) \leq \frac{k}{d}\left(\frac{2d^2}{q}\right)^{m}$$

La parte destra dell'ultima maggiorazione è minore o uguale a ε se

$$m \geq \frac{\log k - \log \varepsilon - \log d}{\log \frac{q}{2d^2}}$$

Ricordando che all'ultimo passo dell'm-esimo ciclo abbiamo $n = mk$, possiamo concludere che

$$d_{TV}(\mu^{(n)}, \pi) \leq \varepsilon$$

per tutti gli interi n tali che

$$n \;\geq\; k\left(1 + \frac{\log k - \log \varepsilon - \log d}{\log \frac{q}{2d^2}}\right)$$

e questo prova il risultato. □

Capitolo 9

Approssimazione per problemi di conteggio

I problemi di conteggio o di enumerazione consistono generalmente nel determinare la cardinalità di un dato insieme di elementi. Molti problemi classici trattati nell'area algoritmica rientrano in questa famiglia e la loro complessità computazionale è stata studiata in letteratura accanto a quella dei tradizionali problemi di decisione [23, 24]. In molti casi rilevanti tali problemi sono difficili da risolvere esattamente in modo efficiente, e si è spesso portati a considerare procedure di approssimazione probabilistiche che, in tempo polinomiale, forniscono una soluzione approssimata la quale, con elevata probabilità, si discosta dalla soluzione esatta per un errore trascurabile.

Tra tali procedure vi sono anche quelle basate sulle catene di Markov e in particolare sull'utilizzo iterato di algoritmi MCMC. In questo capitolo illustriamo un esempio classico di procedure di questo genere, progettato per determinare il numero di colorazioni di un grafo. Questa procedura di approssimazione si basa sugli algoritmo MCMC per la generazione casuale di colorazioni, presentati nei capitoli precedenti.

9.1 Generalità sui problemi di conteggio

Formalmente un problema di conteggio può essere rappresentato da una funzione $F : I \to \mathbb{N}$, dove I è l'insieme delle istanze. Esempi tipici sono i seguenti:

1. Dato un grafo orientato G, due nodi u, v in G e un intero $n > 0$, determinare il numero di cammini da u a v di lunghezza n.

2. Determinare il numero di alberi di copertura in un grafo non orientato G.

3. Data una formula booleana $f(x_1, x_2, \ldots, x_n)$, dove $x_1, x_2, \ldots, x_n$ sono le variabili, determinare il numero di assegnamenti di valori alle variabili che rendono vera la formula.

4. Dato un grafo non orientato G e un intero k, determinare il numero di clique di dimensione k in G.

Per molti problemi di conteggio sono noti algoritmi esatti efficienti, cioè procedure che su ogni input restituiscono la soluzione esatta e che funzionano in tempo polinomiale. Questo è il caso dei primi due esempi illustrati sopra.

Per altri problemi di conteggio invece algoritmi polinomiali non esistono o non sono stati trovati e si congettura che non sia possibile trovare la soluzione in maniera efficiente. La complessità computazionale dei problemi di enumerazione è stata formalizzata in [24], dove è stata introdotta e studiata la classe $\sharp P$ che contiene molti problemi notoriamente difficili per i quali non si conoscono algoritmi che funzionano in tempo polinomiale. Più precisamente, è possibile definire la classe dei problemi $\sharp P$-completi che rappresenta intuitivamente la famiglia dei problemi più difficili in $\sharp P$. Per esempio è noto che i problemi definiti negli esempi 3 e 4 illustrati sopra sono $\sharp P$-completi. Per tali problemi dunque non si conoscono algoritmi di soluzione esatti che funzionano in tempo polinomiale e la loro esistenza è considerata molto improbabile visto che implicherebbe l'equivalenza $P = NP$. Tuttavia è spesso possibile definire degli algoritmi di approssimazione efficienti, ovvero procedure che forniscono una soluzione approssimata in un tempo polinomiale. Un aspetto importante nell'analisi di queste procedure consiste nella valutazione dell'errore; in generale si cerca di garantire che l'errore relativo sia minore di una quantità abbastanza piccola (per una analisi degli algoritmi di approssimazione si può consultare [2]).

Vi sono due nozioni formali di algoritmo di approssimazione, una deterministica e una probabilistica. Entrambe hanno per input una istanza del problema di conteggio e un valore reale $\varepsilon > 0$ che rappresenta l'errore relativo massimo che il procedimento può compiere. Per questo motivo l'algoritmo è chiamato solitamente *schema di approssimazione*.

Dato un problema di conteggio definito da una funzione $F : I \to \mathbb{N}$, uno schema di approssimazione polinomiale (PTAS) per F è un algoritmo che riceve in input una coppia (x, ε), dove $x \in I$, $\varepsilon > 0$, e che soddisfa le seguenti condizioni:

1. per ogni $\varepsilon > 0$ esiste un polinomio $p_\varepsilon(y)$ tale che l'algoritmo su input (x, ε) richiede un tempo minore o uguale a $p_\varepsilon(n)$, dove $n = |x|$;

2. il valore $R(x, \varepsilon)$ restituito dall'algoritmo su input (x, ε) verifica la relazione

$$(1 - \varepsilon)F(x) \leq R(x, \varepsilon) \leq (1 + \varepsilon)F(x)$$

Se inoltre $p_\varepsilon(y)$ è polinomialmente limitato anche rispetto a $1/\varepsilon$, allora l'algoritmo è chiamato schema di approssimazione *pienamente* polinomiale (FPTAS).

Tale schema di approssimazione garantisce quindi sempre un errore relativo minore della quantità ε ricevuta in input:

$$\frac{|R(x, \varepsilon) - F(x)|}{F(x)} \ \leq \ \varepsilon$$

Tuttavia in molti casi anche questo tipo di approssimazione sembra difficile da stabilire. In particolare, per certi problemi di conteggio si è dimostrato che non esiste un PTAS a meno che la classe P non coincida con NP. Questo significa che quasi certamente il problema non è approssimabile mediante un algoritmo deterministico. In questi casi l'unica possibilità per trattare il problema con un algoritmo efficiente è quella di trovare uno schema di approssimazione probabilistico che fornisca un errore relativo il quale, con alta probabilità, sia minore della quantità ε fissata a priori.

Formalmente, uno schema *probabilistico* di approssimazione polinomiale (RPTAS) per una funzione $F : I \to \mathbb{N}$, è un algoritmo probabilistico che su input (x, ε) verifica la condizione 1 della definizione precedente e inoltre, su ogni input (x, ε), restituisce il valore $R(x, \varepsilon)$ tale che

$$\Pr\left((1 - \varepsilon)F(x) \leq R(x, \varepsilon) \leq (1 + \varepsilon)F(x)\right) \geq 2/3$$

Anche in questo caso diremo che lo schema è *pienamente* polinomiale (RFPTAS) se $p_\varepsilon(y)$ è polinomialmente limitato rispetto a $1/\varepsilon$. Ovvero, esiste un polinomio $q(y,z)$ in y e z, tale che $p_\varepsilon(n) \leq q(n, 1/\varepsilon)$, per ogni $n \in \mathbb{N}$ e ogni $\varepsilon > 0$.

Il valore $2/3$ nella definizione precedente può essere sostituito da un qualunque numero reale δ tale che $1/2 < \delta < 1$. Vale infatti la seguente proprietà.

Proposizione 9.1 *Consideriamo un problema di conteggio definito da una funzione $F : I \to \mathbb{N}$ e sia δ una costante tale che $1/2 < \delta < 1$. Supponiamo che per tale problema vi sia un RPTAS che su ogni input (x, ε) restituisce un valore $R(x, \varepsilon)$ tale che*

$$Pr(|R(x,\varepsilon) - F(x)| \leq \varepsilon F(x)) \geq \delta \quad .$$

Allora, per ogni $\alpha > 0$, esiste un RPTAS per lo stesso problema che su ogni input (x, ε) restituisce un valore $R'(x, \varepsilon)$ tale che

$$Pr(|R'(x,\varepsilon) - F(x)| > \varepsilon F(x)) < \alpha$$

Per la dimostrazione basta usare la mediana di un certo numero di ripetizioni dell'algoritmo sullo stesso input e applicare la disuguaglianza di Chebychev sulle binomiali.

9.2 Conteggio approssimato di colorazioni

Un esempio rilevante di RPTAS per un problema di conteggio difficile riguarda il calcolo del numero di q-colorazioni. L'algoritmo che consideriamo è stato proposto in [11] e la versione semplificata che qui illustriamo è dovuta a [7]. Tale procedura si base principalmente sul procedimento di generazione casuale di q-colorazioni presentato nella sezione 7.3.

Anche in questo caso l'istanza del problema è data da un grafo non orientato $G = (V, E)$ e da un numero q di colori. Denotiamo con k il numero di nodi del grafo, con d il massimo grado dei suoi vertici e con m il numero dei suoi lati. Così la coppia (k, m) rappresenta la dimensione dell'istanza del problema. Inoltre, rappresentiamo con $Q = \{1, 2, \ldots, q\}$ l'insieme dei colori e ricordiamo che una q-colorazione è una funzione $f : V \longrightarrow Q$ tale che, per ogni $\{u, v\} \in E$, $f(u) \neq f(v)$. La soluzione del problema è il numero di q-colorazioni del grafo, che denotiamo con $Z_{G,q}$; poiché il problema è notoriamente un problema difficile ($\sharp P$-completo) vogliamo definire uno schema di approssimazione probabilistico (RPTAS). Osserviamo che per questo problema non esistono schemi di approssimazione polinomiale deterministici (PTAS). L'unico modo per approssimare la soluzione sembra dunque quella di utilizzare una procedura probabilistica.

Descriviamo ora il procedimento adottato dall'algoritmo. Consideriamo l'insieme dei lati $E = \{e_1, e_2, \ldots, e_m\}$ del grafo e, per ogni $j = 0, 1, \ldots, m$, definiamo il grafo $G_j = (V, \{e_1, \ldots, e_j\})$ con la convenzione che $G_0 = (V, \emptyset)$. Nota che tutti questi grafi hanno lo stesso insieme di vertici V. Inoltre $G_m = G$ e ciascun G_j è ottenuto da G_{j-1} aggiungendo il lato e_j, $j = 1, 2, \ldots, m$. Possiamo anche denotare con Z_j il numero di q-colorazioni di G_j, per ogni $j = 0, 1, \ldots, m$. Di conseguenza $Z_m = Z_{G,q}$ ed è facile verificare che $Z_0 = q^k$ poiché nel grafo G_0 ogni assegnamento di colori ai nodi è una q-colorazione. Quindi il valore Z_m che vogliamo calcolare può essere ottenuto mediante la produttoria seguente:

$$Z_m \;=\; Z_0 \cdot \frac{Z_1}{Z_0} \cdot \frac{Z_2}{Z_1} \cdot \;\cdots\; \cdot \frac{Z_m}{Z_{m-1}} \tag{9.1}$$

Possiamo quindi valutare i rapporti $\frac{Z_j}{Z_{j-1}}$ e moltiplicare queste frazioni tra loro. Osserva che ciascun Z_j può essere visto come il numero di q-colorazioni di G_{j-1} che assegnano colori diversi ai nodi del lato e_j. Denotiamo ora con x_j e y_j i due nodi del lato e_j, per ciascun $j = 1, 2, \ldots, m$. Allora

$$Z_j \;=\; \sharp\{f \in Q^V \mid f \text{ è } q\text{-colorazione di } G_{j-1} \text{ tale che } f(x_j) \neq f(y_j)\}$$

Di conseguenza $\frac{Z_j}{Z_{j-1}}$ è la probabilità che una q-colorazione f di G_{j-1} estratta con distribuzione uniforme, sia anche una colorazione di G_j, ovvero

$$\frac{Z_j}{Z_{j-1}} \;=\; \Pr\left(f(x_j) \neq f(y_j)\right)$$

L'idea dell'algoritmo è allora la seguente: per ogni $j = 1, 2, \ldots, m$, usando il campionatore di Gibbs descritto nella sezione 7.3, si generano diverse q-colorazioni casuali del grafo G_{j-1} e si verifica quante di queste attribuiscono colori diversi ai nodi x_j e y_j; si ottiene così una stima Y_j della probabilità $\frac{Z_j}{Z_{j-1}}$. Moltiplicando tutti questi valori tra di loro insieme alla quantità $Z_0 = q^k$ si ottiene il risultato R fornito dall'algoritmo

$$R \;=\; q^k \cdot \prod_{j=1}^{m} Y_j$$

che per la relazione (9.1) rappresenta una approssimazione di Z_m.

Osserviamo che questo procedimento dipende da due parametri importanti, che denotiamo con ℓ e n, rispettivamente:

- ℓ è il numero di q-colorazioni casuali di G_{j-1}, generate mediante il campionatore di Gibbs, utilizzate per calcolare ciascuna stima Y_j della probabilità $\frac{Z_j}{Z_{j-1}}$, $j = 1, 2, \ldots, m$. Così risulta $Y_j = H_j/\ell$, dove H_j è il numero di q-colorazioni di G_{j-1} generate a caso che attribuiscono colori diversi ai nodi x_j e y_j.

- n è il numero di passi principali eseguiti da ciascun campionatore di Gibbs per determinare la q-colorazione casuale corrispondente (ovvero il numero delle transizioni compiute sulla catena di Markov associata).

L'algoritmo è riassunto dalla seguente procedura ad alto livello:

```
begin
    R = q^k
    for j = 1, 2, ..., m do
        begin
            % calcola Y_j %
            H := 0
            for i = 1, 2, ..., ℓ do
                begin
                    % esegui una simulazione del campionatore di Gibbs su G_{j-1} %
                    f := colorazione iniziale di G_{j-1}
```

```
                    for  t = 1, 2, ..., n do
                         { esegui una transizione del campionatore di Gibbs su G_{j-1}
                         { sia g la nuova colorazione ottenuta
                         { f := g
                    if f(x_j) ≠ f(y_j) then H := H + 1
                end
            Y_j := H/ℓ
            R := R · Y_j
        end
    return R
end
```

Affinché questo procedimento sia davvero un RPTAS per il problema considerato dovremo garantire che l'errore relativo compiuto sia piccolo a piacere con alta probabilità. Questo significa determinare i valori dei due parametri ℓ e n per i quali il risultato R della procedura soddisfi la relazione

$$\Pr\left(|R - Z_m| > \varepsilon Z_m\right) \leq 1/3$$

La seguente proposizione afferma proprio che sotto certe ipotesi, riguardanti q e d, tali valori esistono e quindi l'algoritmo illustrato è davvero un RPTAS per il nostro problema.

Teorema 9.2 *Assumendo la notazione illustrata sopra, supponiamo che $d \geq 2$ e $q > 2d^2$. Allora esiste un RPTAS per il problema di determinare il numero di q-colorazioni di G.*

Prima di descrivere la dimostrazione, osserviamo che la condizione $d \geq 2$ è del tutto naturale perché nel caso $d \leq 1$ il numero di q-colorazioni si determina facilmente. L'ipotesi $q > 2d^2$ invece deriva dall'utilizzo del Teorema 8.8. Tuttavia, poiché lo stesso teorema vale nell'ipotesi più debole $q > 2d$, anche nel nostro caso quest'ultima condizione è sufficiente a garantire la validità dell'enunciato.

La dimostrazione del teorema 9.2 si basa sui seguenti lemmi.

Lemma 9.3 *Per ogni $\varepsilon > 0$ e ogni sequenza $a_1, a_2, \ldots, a_k$ tali che*

$$\left(1 - \frac{\varepsilon}{2k}\right) \;\leq\; a_i \;\leq\; \left(1 + \frac{\varepsilon}{2k}\right) \qquad \textit{per ogni } i = 1, \ldots, k$$

vale

$$1 - \varepsilon \;\leq\; \prod_{i=1}^{k} a_i \;\leq\; 1 + \varepsilon$$

Dimostrazione. Ragionando per induzione si prova che per ogni $i \in \mathbb{N}$

$$\left(1 - \frac{\varepsilon}{2k}\right)^i \;\geq\; 1 - \frac{i\varepsilon}{2k}$$

Di conseguenza

$$\prod_{i=1}^{k} a_i \;\geq\; \left(1 - \frac{\varepsilon}{2k}\right)^k \;\geq\; 1 - \frac{\varepsilon}{2} \;\geq\; 1 - \varepsilon$$

e questo prova la prima disuguaglianza. Per provare la seconda osserva che, per ogni $0 \leq x \leq 1$, vale

$$1 + x \;\leq\; e^x \;\leq\; 1 + 2x$$

e quindi

$$\prod_{i=1}^{k} a_i \;\leq\; \left(1 + \frac{\varepsilon}{2k}\right)^k \;\leq\; e^{\varepsilon/2} \;\leq\; 1 + \varepsilon$$

□

Lemma 9.4 *Supponi $d \geq 2$ e $q \geq 2d$ per due interi positivi d, q. Sia G un grafo di grado massimo d e sia f una q-colorazione di G estratta uniformemente a caso. Allora, per ogni coppia di nodi distinti x, y di G abbiamo*

$$Pr(f(x) \neq f(y)) \;\geq\; 1/2$$

Dimostrazione. Supponi che $\{x, y\}$ non sia un lato del grafo (altrimenti la proprietà è ovvia). Denotiamo con $Ad(x)$ l'insieme dei nodi adiacenti a x in G e con $Q = \{1, 2, \ldots, q\}$ l'insieme dei possibili colori. Osserva che una volta fissati i colori $f(w)$ dei nodi $w \in Ad(x)$, la variabile aleatoria $f(x)$ possiede una distribuzione uniforme sull'insieme dei colori disponibili, cioè quelli diversi dai valori $f(Ad(x)) = \{f(z) \mid z \text{ vicino di } x\}$. I colori disponibili sono almeno $q - d$ e quindi la probabilità condizionata che $f(x)$ assuma uno di questi è minore o uguale a $\frac{1}{q-d} \leq 1/2$. Allora per ogni $c \in Q$ e ogni $U \subset Q$, abbiamo

$$\Pr\left(f(x) = c \mid f(Ad(x)) = U\right) \begin{cases} = 0 & \text{se } c \in U \text{ oppure } \Pr(f(Ad(x)) = U) = 0 \\ \leq \frac{1}{q-d} \leq \frac{1}{2} & \text{altrimenti} \end{cases}$$

Di conseguenza possiamo scrivere

$$\begin{aligned} &\Pr\left(f(x) = f(y)\right) = \\ &\quad = \sum_{c \in Q, U \subset Q} \Pr\left(f(x) = c \mid f(y) = c, f(Ad(x)) = U\right) \Pr\left(f(y) = c, f(Ad(x)) = U\right) \\ &\quad \leq \frac{1}{2} \sum_{c \in Q, U \subset Q} \Pr\left(f(y) = c, f(Ad(x)) = U\right) \;=\; \frac{1}{2} \end{aligned}$$

□

Dimostrazione del teorema 9.2. Valutiamo anzitutto l'errore relativo compiuto dall'algoritmo. Vogliamo mostrare che per opportuni valori dei parametri n e ℓ il risultato R ottenuto su input (G, q, ε) soddisfa la relazione

$$\Pr\left((1 - \varepsilon)Z_m \leq R \leq (1 + \varepsilon)Z_m\right) \;\geq\; 2/3 \tag{9.2}$$

A tale scopo supponi che, per ogni $j = 1, 2, \ldots, m$, valga la disuguaglianza

$$\left(1 - \frac{\varepsilon}{2m}\right) \frac{Z_j}{Z_{j-1}} \leq Y_j \leq \left(1 + \frac{\varepsilon}{2m}\right) \frac{Z_j}{Z_{j-1}} \tag{9.3}$$

Allora, poiché $R = q^k \prod_{j=1}^{m} Y_j$, per il lemma 9.3, si ottiene esattamente l'evento

$$(1 - \varepsilon)Z_m \leq R \leq (1 + \varepsilon)Z_m$$

di cui vogliamo stimare la probabilità .

Per il lemma 9.4 sappiamo che $\frac{Z_j}{Z_{j-1}} \geq 1/2$ e quindi la relazione (9.3) è conseguenza delle disuguaglianze

$$-\frac{\varepsilon}{4m} \leq Y_j - \frac{Z_j}{Z_{j-1}} \leq \frac{\varepsilon}{4m} \qquad j = 1, 2, \ldots, m$$

Quest'ultima può essere spezzata nelle due disuguaglianze seguenti

$$(i) \quad |Y_j - \Pr(X_n(x_j) \neq X_n(y_j))| \leq \frac{\varepsilon}{8m}$$
$$(ii) \quad \left|\Pr(X_n(x_j) \neq X_n(y_j)) - \frac{Z_j}{Z_{j-1}}\right| \leq \frac{\varepsilon}{8m}$$

dove X_n è la q-colorazione ottenuta all'n-esimo passo dal campionatore di Gibbs corretto che genera q-colorazioni del grafo G_{j-1}.

Per dimostrare il teorema dobbiamo quindi provare che le disuguaglianze (i) e (ii) valgono per tutti i $j = 1, 2, \ldots, m$ con probabilità almeno $2/3$. La disuguaglianza (i) rappresenta l'errore dovuto alla differenza tra la stima empirica Y_j ottenuta dalla valutazione di ℓ q-colorazioni generate dal campionatore di Gibbs e il suo valor medio $\Pr(X_n(x_j) \neq X_n(y_j))$ che possiamo denotare più semplicemente con p_j.

La disuguaglianza (ii) rappresenta invece l'errore nella valutazione della probabilità dell'evento $(f(x_j) \neq f(y_j)$ ottenuto assumendo $f = X_n$ (cioè f generata in n passi dal campionatore di Gibbs sul grafo G_{j-1}) invece che supponendo f generata a caso in modo uniforme tra tutte le q-colorazioni del grafo G_{j-1}.

Osserviamo subito che per il Teorema 8.8 la (ii) è sempre vera per tutti i j a patto che n soddisfi la relazione

$$n \geq k\left(1 + \frac{\log k + \log \frac{8m}{\varepsilon} - \log d}{\log \frac{q}{2d^2}}\right)$$

Poiché $m \leq kd$ la relazione precedente è soddisfatta se

$$n \geq k\left(1 + \frac{2\log k - \log \varepsilon + \log 8}{\log \frac{q}{2d^2}}\right) \tag{9.4}$$

Per quanto riguarda la (i) invece, osserva che $H_j = \ell Y_j$ è una binomiale di parametri ℓ e $p_j = \Pr(X_n(x_j) \neq X_n(y_j))$. Quindi la disuguaglianza (i) equivale a

$$|H_j - \ell p_j| \leq \frac{\varepsilon \ell}{8m}$$

Applicando ora la disuguaglianza di Chernoff sulle binomiali otteniamo

$$\Pr\left(|H_j - \ell p_j| > \frac{\varepsilon \ell}{8m}\right) \leq 2e^{-2\left(\frac{\varepsilon}{8m}\right)^2 \ell}$$

Il termine destro è minore o uguale a $\frac{1}{3m}$ per

$$\ell \geq \frac{32m^2}{\varepsilon^2} \log 6m \tag{9.5}$$

Di conseguenza per tali valori di ℓ abbiamo che per ogni $j = 1, 2, \ldots, m$

$$\Pr\left(|H_j - \ell p_j| > \frac{\varepsilon \ell}{8m}\right) \leq \frac{1}{3m}$$

e quindi

$$\Pr\left(\exists\, j \in \{1, \ldots, m\} \;:\; |H_j - \ell p_j| > \frac{\varepsilon \ell}{8m}\right) \;\leq\; \frac{1}{3}$$

Valutando ora la probabilità dell'evento complementare, si ricava

$$\Pr\left(\forall j = 1, \ldots, m \;:\; |H_j - \ell p_j| \leq \frac{\varepsilon}{8m}\right) \;\geq\; \frac{2}{3}$$

Ciò significa che se ℓ soddisfa la (9.5) la (i) vale per tutti i $j = 1, 2, \ldots, m$ con probabilità almeno $2/3$ e di conseguenza la (9.2) è dimostrata.

Valutiamo infine il tempo di calcolo richiesto dalla procedura su un grafo di k nodi (nelle ipotesi date) per garantire un errore relativo minore o uguale a ε con probabilità almeno $2/3$. L'algoritmo ripete tre cicli, rispettivamente m, ℓ e n volte. Supponendo constante il grado d del grafo possiamo assumere che il passo generico del campionatore di Gibbs richieda tempo $O(1)$. Di conseguenza, tenendo conto di (9.5) e (9.4), l'algoritmo richiede un tempo

$$T(k, \varepsilon) = O(m\ell n) = O\left(\frac{k^4}{\varepsilon^2} \log k (\log k + \log 1/\varepsilon)\right)$$

Questo significa che l'algoritmo appena descritto può essere considerato un RFPTAS per il problema di calcolare il numero di q-colorazioni di un grafo. □

Appendice A

Richiami di base

In questa appendice ricordiamo le nozioni matematiche di base utilizzate nei capitoli precedenti, molte delle quali sono state introdotte in corsi iniziali di laurea triennale. I temi principali riguardano la teoria della probabilità, l'algebra lineare e alcune proprietà elementari di teoria dei numeri. La presentazione di questi argomenti è necessariamente sintetica e non ha alcuna pretesa di completezza. Lo scopo è anche quello di fissare la notazione usata in questo lavoro, riassumendo concetti e proprietà fondamentali, solitamente presentati nei libri di testo specifici in maniera più estesa.

A.1 Probabilità

Ricordiamo innanzitutto che uno *spazio di probabilità* è una tripla $(\Omega, \mathcal{B}, Pr)$ che gode delle seguenti proprietà:

1. Ω è un insieme, detto *spazio campione*, i cui elementi sono chiamati punti campione;
2. $\mathcal{B}$ è una σ-algebra su Ω, ovvero una famiglia di sottoinsiemi di Ω tale che
   - $\Omega \in \mathcal{B}$,
   - per ogni $A \in \mathcal{B}$ il complementare A^c appartiene a $\mathcal{B}$,
   - per ogni sequenza $\{A_i\}_{i\geq 1}$ di elementi di $\mathcal{B}$, abbiamo $\bigcup_{i\geq 1} A_i \in \mathcal{B}$.

   Gli elementi di $\mathcal{B}$ sono chiamati eventi casuali o semplicemente *eventi*;
3. Pr è una misura di probabilità su $\mathcal{B}$, ovvero $Pr : \mathcal{B} \longrightarrow [0,1]$ tale che
   - $Pr(\Omega) = 1$,
   - per ogni sequenza $\{A_i\}_{i\geq 1}$ di elementi disgiunti di $\mathcal{B}$
     $$Pr(\bigcup_{i\geq 1} A_i) = \sum_{i\geq 1} Pr(A_i) \qquad \text{(additività numerabile)}.$$

Possiamo facilmente costruire uno spazio di probabilità su un qualunque insieme finito. Sia per esempio Ω un insieme finito e sia $\mathcal{B}$ la famiglia di tutti i sottoinsiemi di Ω. Considera una funzione $p : \Omega \longrightarrow \mathbb{R}$ tale che $0 \leq p(\omega) \leq 1$ per ogni $\omega \in \Omega$ e inoltre $\sum_{\omega\in\Omega} p(\omega) = 1$; definiamo allora Pr come la funzione che ad ogni $A \in \mathcal{B}$ associa il valore $Pr(A) = \sum_{\omega\in A} p(\omega)$. Si verifica facilmente che la tripla $(\Omega, \mathcal{B}, Pr)$ appena definita è uno spazio di probabilità.

Varie altre proprietà possono essere derivate dagli assiomi precedenti. Elenchiamo nel seguito solo le più semplici. Dato uno spazio di probabilità $(\Omega, \mathcal{B}, Pr)$ si verifica che:

- per ogni $A \in \mathcal{B}$, $Pr(A^c) = 1 - Pr(A)$;
- per ogni $A, B \in \mathcal{B}$, se $A \subseteq B$ allora $Pr(A) \leq Pr(B)$;
- se $\{A_1, A_2, \ldots, A_n\}$ è un insieme finito di elementi di $\mathcal{B}$ disgiunti allora
$Pr(\bigcup_{i=1}^n A_i) = \sum_{i=1}^n Pr(A_i)$ (additività finita).

Inoltre, data una sequenza $\{A_n\}_{n\geq 1}$ di eventi casuali (appartenenti a $\mathcal{B}$), definiamo il limite inferiore e il limite superiore di $\{A_n\}_{n\geq 1}$ mediante le relazioni

$$\liminf_{n\to+\infty} A_n = \bigcup_{n\geq 1} \bigcap_{k\geq n} A_k \qquad \limsup_{n\to+\infty} A_n = \bigcap_{n\geq 1} \bigcup_{k\geq n} A_k \ .$$

Entrambi tali limiti sono anche loro eventi casuali. Il limite inferiore è l'insieme di tutti gli elementi $\omega \in \Omega$ che appartengono a tutti gli insiemi A_n, $n \geq 1$, tranne al più ad un numero finito di questi; il limite superiore è invece l'insieme di tutti gli elementi $\omega \in \Omega$ che appartengono a infiniti insiemi A_n, $n \geq 1$. Lo loro probabilità è data da

$$Pr(\liminf_{n\to+\infty} A_n) = \lim_{n\to+\infty} Pr(\bigcap_{k\geq n} A_k) \qquad Pr(\limsup_{n\to+\infty} A_n) = \lim_{n\to+\infty} Pr(\bigcup_{k\geq n} A_k)$$

Si dice anche che $\{A_n\}_{n\geq 1}$ converge a un insieme A se i due limiti inferiore e superiore coincidono e il loro valore è proprio A.

Un'altra nozione fondamentale è quella di indipendenza. Dato uno spazio di probabilità $(\Omega, \mathcal{B}, Pr)$, due eventi casuali A, B $(\in \mathcal{B})$ si dicono *indipendenti* se $Pr(A \cap B) = Pr(A)Pr(B)$. Intuitivamente, due eventi sono indipendenti se l'occorrenza di uno dei due non influisce sulla probabilità di occorrenza dell'altro. Più in generale, una famiglia qualsiasi di eventi casuali $\{A_j\}_{j\in I}$ si dice indipendente se, per ogni sottoinsieme finito di indici $S \subseteq I$,

$$Pr(\bigcap_{j\in S} A_j) = \prod_{j\in S} Pr(A_j)$$

Dati due eventi A, B, dove $Pr(A) > 0$, la *probabilità condizionata* di B rispetto ad A, denotata $Pr(B \mid A)$, è definita da

$$Pr(B \mid A) = \frac{Pr(A \cap B)}{Pr(A)}$$

e intuitivamente rappresenta la probabilità di occorrenza di B dato che si è verificato A. Nota che la tripla $(\Omega, \mathcal{B}, Pr_A)$, dove $Pr_A(B) = Pr(B \mid A)$ per ogni $B \in \mathcal{B}$, è uno spazio di probabilità. Se invece $Pr(A) = 0$ si pone per convenzione $Pr(B \mid A) = 0$. Chiaramente, se A e B sono indipendenti allora $Pr(B \mid A) = Pr(B)$ e $Pr(A \mid B) = Pr(A)$. Inoltre, le seguenti proprietà possono essere facilmente dimostrate a partire dalle definizioni e sono spesso utilizzate per calcolare la probabilità di un evento casuale:

- data una famiglia finita di eventi $A_1, A_2, \ldots, A_n \in \mathcal{B}$ tali che $Pr(\bigcap_i A_i) > 0$, abbiamo
$$Pr(\bigcap_{i=1}^n A_i) = Pr(A_1)\ Pr(A_1 \mid A_2)\ Pr(A_3 \mid A_1 \cap A_2) \cdots Pr(A_n \mid A_1 \cap \cdots \cap A_{n-1}).$$
- Sia $\{A_j\}_{j\in I}$ una famiglia finita o numerabile di eventi che formano una partizione di Ω. Allora, per ogni $B \in \mathcal{B}$, abbiamo $Pr(B) = \sum_{j\in I} Pr(B \cap A_j)$ e quindi
$$Pr(B) = \sum_{j\in I'} Pr(B \mid A_j) Pr(A_j)$$
dove I' è il sottoinsieme di I degli indici j tali che $Pr(A_j) > 0$.

Una variabile aleatoria X su uno spazio di probabilità $(\Omega, \mathcal{B}, Pr)$ è una funzione $X : \Omega \longrightarrow \mathbb{R}$ tale che, per ogni $a \in \mathbb{R}$, l'insieme $\{\omega \in \Omega \mid X(\omega \leq a\}$ appartiene a $\mathcal{B}$. Nota che in tale definizione X dipende da Ω e da $\mathcal{B}$ ma non dalla misura di probabilità Pr. Si può inoltre provare che se X è variabile aleatoria su $(\Omega, \mathcal{B}, Pr)$ allora, per ogni insieme di Borel[1] $A \subseteq \mathbb{R}$, l'insieme $\{\omega \in \Omega \mid X(\omega) \in A\}$ appartiene a $\mathcal{B}$. Per semplificare la notazione si è soliti rappresentare tali insiemi senza menzionare i punti campione $\omega \in \Omega$; così per esempio, gli insiemi $\{\omega \in \Omega \mid X(\omega) \in A\}$ e $\{\omega \in \Omega \mid X(\omega \leq a\}$ sono denotati rispettivamente dalle espressioni $\{X \in A\}$ e $\{X \leq a\}$, mentre le loro probabilità sono espresse da $Pr(X \in A)$ e $Pr(X \leq a)$.

Ogni variabile aleatoria X su $(\Omega, \mathcal{B}, Pr)$ è dotata di una funzione distribuzione $F_X : \mathbb{R} \longrightarrow [0, 1]$, definita da

$$F_X(a) = Pr(X \leq a) \qquad \text{per ogni } a \in \mathbb{R}.$$

È facile verificare che F_X è sempre non decrescente, che $\lim_{a \to -\infty} F_X(a) = 0$, $\lim_{a \to +\infty} F_X(a) = 1$ e inoltre che F_X è una funzione continua dalla destra su tutto $\mathbb{R}$, cioè $\lim_{0<h\to 0} F_X(a+h) = F_X(a)$ per ogni $a \in \mathbb{R}$. Infine si verifica facilmente che $Pr(a < X \leq b) = F_X(b) - F_X(a)$, per ogni $a < b$.

Una variabile aleatoria X su $(\Omega, \mathcal{B}, Pr)$ si dice *discreta* se l'insieme dei suoi valori $X(\Omega)$ è finito o infinitamente numerabile. In questo caso, posto $X(\Omega) = \{a_1, a_2, \ldots\}$, possiamo definire la funzione $p_X : \{a_1, a_2, \ldots\} \longrightarrow [0, 1]$, tale che $p_X(a_i) = Pr(X = a_i)$, per ogni i. Otteniamo così $Pr(X \in A) = \sum_{a_i \in A} p_X(a_i)$, per ogni $A \subseteq X(\Omega)$. La funzione p_X è chiamata *funzione probabilità* di X. Si verifica facilmente che, per ogni indice i

$$F_X(a_i) = \sum_{j : a_j \leq a_i} p_X(a_j), \qquad \text{mentre} \qquad p_X(a_j) = \lim_{0<h\to 0} (F_X(a_j) - F_X(a_j - h))$$

permettendo così di calcolare F_X conoscendo i valori di p_X e viceversa.

Un esempio tradizionale è dato dalla variabile aleatoria binomiale X_{np} di parametri n e p, dove $n \in \mathbb{N}$ e $0 \leq p \leq 1$; essa rappresenta il numero di successi in una sequenza di n prove bernoulliane indipendenti, dove ogni prova ha probabilità di successo p e probabilità di insuccesso $q = 1 - p$. I possibili valori di X_{np} sono $\{0, 1, \ldots, n\}$ e la sua funzione probabilità è data da

$$p_{X_{np}}(k) = \binom{n}{k} p^k q^{n-k}, \qquad \text{per ogni } k = 0, 1, \ldots, n.$$

Un altro esempio è costituito dalla variabile aleatoria geometrica X_p di parametro p, $0 < p \leq 1$. Essa è definita come il numero di prove necessarie per ottenere il primo successo in una sequenza illimitata di prove bernoulliane indipendenti (dove p rappresenta di nuovo la probabilità di successo). In questo caso, l'insieme dei valori di X_p è quello degli interi positivi, mentre sua funzione di probabilità è definita da $p_{X_p}(k) = (1-p)^{k-1}p$, per ogni $k = 1, 2, \ldots$.

Un variabile aleatoria X su $(\Omega, \mathcal{B}, Pr)$ si dice *continua* se esiste una funzione $f_X : \mathbb{R} \longrightarrow \mathbb{R}$ tale che $f_X(t) \geq 0$ per ogni $t \in \mathbb{R}$, e inoltre $F_X(a) = \int_{-\infty}^{a} f_X(t)dt$ per ogni $a \in \mathbb{R}$. La funzione f_X è detta *funzione densità* di X e coincide con la derivata di F_X. Essa è chiaramente integrabile in $\mathbb{R}$, $\int_a^b f_X(t)dt = Pr(a < X < b)$ per ogni $a < b$ e, più generalmente, $Pr(X \in A) = \int_A f(t)dt$ per ogni insieme di Borel $A \subseteq \mathbb{R}$ (integrale di Lebesgue). Osserviamo infine che, per ogni variabile aleatoria continua X, $Pr(X = a) = 0$ per ogni $a \in \mathbb{R}$.

[1] La famiglia degli insiemi di Borel in $\mathbb{R}$ è definita come la più piccola σ-algebra su $\mathbb{R}$ che contiene gli intervalli della retta reale.

Un esempio classico è quello della funzione densità normale (o gaussiana) di parametri $m, s \in \mathbb{R}$, $s > 0$. Essa è definita dalla funzione

$$f(t) = \frac{1}{s\sqrt{2\pi}} e^{-\frac{(t-m)^2}{2s^2}}, \qquad -\infty < t < +\infty$$

Una variabile aleatoria si dice normale se è la sua funzione densità è normale. Tali variabili aleatorie devono la loro importanza al teorema del limite centrale (che ricordiamo nel seguito) e sono legate alla valutazione degli errori nelle approssimazioni di un valore casuale basate sulla media aritmetica di un insieme di osservazioni.

Un altro esempio è quello della densità esponenziale di parametro $\lambda > 0$, definita dalla funzione

$$f(t) = \begin{cases} 0 & \text{se } t < 0 \\ \lambda e^{-\lambda t} & \text{se } t \geq 0 \end{cases}$$

Anche in questo caso una variabile aleatoria si dice esponenziale se la sua funzione densità è esponenziale. Tali variabili aleatorie godono della seguente notevole proprietà che ne giustifica l'utilizzo come modello per lo studio di tempi di attesa di certi eventi casuali: se X è una variabile aleatoria esponenziale allora $Pr(X > a + b \mid X > a) = Pr(X > b)$ per ogni coppia di valori reali $a, b > 0$. Questo significa intuitivamente che X è priva di memoria; in altre parole, se X rappresenta il tempo di attesa di un dato evento, allora la proprietà precedente asserisce che se abbiamo già aspettato un tempo a la probabilità di attesa di un successivo tempo b è la stessa che si avrebbe all'inizio del processo.

Ricordiamo ora la definizione dei momenti di una variabile aleatoria. Sia g una funzione di variabile reale, definita su tutto $\mathbb{R}$, a valori reali o complessi. Data una variabile aleatoria discreta X, a valori nell'insieme $\{a_1, a_2, \ldots\}$, definiamo il valor medio $E[g(X)]$ di $g(X)$ mediante l'uguaglianza $E[g(X)] = \sum_i g(a_i) p_X(a_i)$, assumendo che la serie sia assolutamente convergente (ovvero che $\sum_i |g(a_i)| p_X(a_i) < +\infty$). Analogamente, data una variabile aleatoria X continua, definiamo il valor medio $E[g(X)]$ di $g(X)$ mediante $E[g(X)] = \int_{-\infty}^{+\infty} g(t) f_X(t) dt$, assumendo anche in questo caso che la funzione sia assolutamente integrabile.

In particolare, se g è la funzione identità, otteniamo il *valor medio* (o semplicemente *media*) della variabile aleatoria X,

$$E[X] = \sum_i a_i p_X(a_i) \qquad \text{oppure} \qquad E[X] = \int_{-\infty}^{+\infty} t f_X(t) dt.$$

Osserviamo che, se X è una variabile aleatoria discreta e assume valori in $\mathbb{N}$, allora

$$E[X] = \sum_{k \geq 1} Pr(X \geq k)$$

Per ogni $m > 0$, $E[X^m]$ è il momento m-esimo di X, rispettivamente

$$E[X^m] = \sum_i a_i^m p_X(a_i) \qquad \text{oppure} \qquad E[X^m] = \int_{-\infty}^{+\infty} t^m f_X(t) dt.$$

Inoltre, il momento m-esimo di $X - E[X]$, ovvero $E[(X - E[X])^m]$, è chiamato momento centrale m-esimo di X. Di particolare importanza è il momento centrale secondo di X, denotato $var(X)$ e solitamente chiamato *varianza* di X. Si verifica facilmente che

$$var(X) = E[(X - E[X])^2] = E[X^2] - (E[X])^2$$

La varianza di X è intuitivamente una misura della dispersione di X intorno al suo valor medio. Vale inoltre la nota disuguaglianza di Chebyshev

$$Pr(|X - E[X]| \geq a) \leq \frac{Var(X)}{a^2} \qquad \text{per ogni } a > 0$$

che consente di valutare attraverso la varianza la probabilità di distanza di X da $E[X]$. Un'altra disuguaglianza utile è quella di Markov che vale però solo per le variabili aleatorie positive: Se Y è una variabile casuale che assume solo valori in $\mathbb{R}_+$ allora, per ogni reale $a > 0$, abbiamo

$$Pr(Y \geq a) \leq \frac{E[Y]}{a}$$

Altre proprietà derivabili dalle definizioni sono le seguenti (nelle quali c è una costante qualsiasi):

1. $E[c] = c$;
2. $E[cX] = cE[X]$;
3. $var(cX) = c^2 var(X)$;
4. $E[cg(X)] = cE[g(X)]$;
5. $E[c_1 g_1(X) + c_2 g_2(X)] = c_1 E[g_1(X)] + c_2 E[g_2(X)]$
6. $E[g_1(X)] \leq E[g_2(X)]$ se $g_1(x) \leq g_2(x)$ per ogni $x \in \mathbb{R}$.

Come esempi, ricordiamo che la media di una variabile aleatoria binomiale X_{np} è $E(X_{np}) = np$ mentre $var(X_{np}) = np(1-p)$. Nel caso di una variabile aleatoria geometrica X_p abbiamo $E(X_p) = 1/p$ e $var(X_p) = (1-p)/p^2$. Inoltre, una variabile aleatoria esponenziale di parametro λ possiede media $1/\lambda$ e varianza $1/\lambda^2$, mentre m e s^2 sono rispettivamente la media e la varianza di una variabile aleatoria gaussiana di parametri m e s.

Ricordiamo infine che la media di una variabile aleatoria non è sempre definita. Questo si verifica quando la serie (o l'integrale) che definisce il valor medio non è convergente. Per esempio, se definiamo $Y = 2^{X_p}$, dove X_p è una variabile aleatoria geometrica di parametro p $(0 < p < 1)$, allora abbiamo

$$E[Y] = E[2^{X_p}] = \sum_{n \geq 1} 2^n (1-p)^{n-1} p = 2p \sum_{n \geq 0} (2(1-p))^n$$

Quest'ultima serie è convergente solo nel caso $1/2 < p < 1$; quindi, per ogni $0 < p \leq 1/2$ il valor medio di Y non è definito.

L'operatore E permette infine di definire la funzione caratteristica $\varphi_X(t)$ di una variabile aleatoria X. Essa è definita come la funzione $\varphi_X : \mathbb{R} \to \mathbb{C}$, che associa ad ogni $t \in \mathbb{R}$ il valore $\varphi_X(t) = E[e^{itX}]$, dove i è l'unità immaginaria, $i = \sqrt{-1}$. Poiché $|e^{itx}| = 1$, la funzione $\varphi_X(\cdot)$ è ben definita su tutto $\mathbb{R}$, per qualunque variabile aleatoria X. Inoltre $\varphi_X(0) = 1$, $|\varphi_X(t)| \leq 1$ per ogni $t \in \mathbb{R}$, e $\varphi_X(\cdot)$ è (uniformemente) continua su tutto $\mathbb{R}$. Come esempio ricordiamo che se X è una variabile aleatoria gaussiana di media 0 e varianza 1, allora la sua funzione caratteristica è data da $\varphi_X(t) = e^{-t^2/2}$.

La proprietà fondamentale di $\varphi_X(\cdot)$, per una generica variabile aleatoria X, è che essa caratterizza la funzione distribuzione di X. In altre parole, due variabili aleatorie hanno la stessa funzione distribuzione se e solo se possiedono la stessa funzione caratteristica. Inoltre, essa consente di determinare la distribuzione limite di sequenze di variabili aleatorie: data una sequenza di variabili aleatorie $\{X_n\}_{n\geq 1}$, ciascuna delle quali possiede funzione distribuzione F_n e funzione caratteristica φ_n, e una variabile aleatoria Y con funzione distribuzione G e funzione caratteristica ψ, si verifica che

$$\lim_{n\to+\infty} F_n(x) = G(x) \quad \text{per tutti i punti } x \in \mathbb{R} \text{ di continuità di } F$$

se e solo se

$$\lim_{n\to+\infty} \varphi_n(t) = \psi(t) \quad \text{per ogni } t \in \mathbb{R}.$$

Discutiamo ora la nozione di indipendenza per variabili aleatorie. Innanzitutto osserviamo che se X e Y sono variabili aleatorie definite sul medesimo spazio di probabilità, anche $X+Y$ è una variabile aleatoria definita su tale spazio, essa associa ad ogni punto campione ω il valore $X(\omega)+Y(\omega)$. Per lo stesso motivo, $X-Y$, XY, X/Y (assumendo $Y \neq 0$) sono variabili aleatorie. In particolare si verifica che

$$E[X+Y] = E[X] + E[Y],$$

mentre

$$var(X+Y) = var(X) + var(Y) + 2cov(X,Y),$$

dove $cov(X,Y)$ è la covarianza di X e Y, definita da $cov(X,Y) = E\left[(X-E[X])(Y-E[Y])\right]$, che rappresenta intuitivamente il grado di correlazione tra X e Y.

Detto questo, consideriamo n variabili aleatorie $X_1, X_2, \ldots, X_n$ definite sullo stesso spazio di probabilità; tali variabili sono dette *indipendenti* se per ogni n-pla $B_1, \ldots, B_n$ di insiemi di Borel in $\mathbb{R}$, abbiamo

$$Pr(X_1 \in B_1, \ldots, X_n \in B_n) = \prod_{i=1}^{n} Pr(X_i \in B_i)$$

In particolare, se le variabili aleatorie X_i sono discrete, la condizione precedente equivale a porre

$$Pr(X_1 = a_1, \ldots, X_n = a_n) = \prod_{i=1}^{n} Pr(X_i = a_i)$$

per ogni n-pla di valori reali $a_1, \ldots, a_n$. La definizione si estende alle sequenze infinite di variabili aleatorie $\{X_i\}_{i\geq 1}$ dicendo che tali variabili sono indipendenti se, per ogni n, le $X_1, X_2, \ldots, X_n$ sono variabili aleatorie indipendenti.

Tra le proprietà più semplici ricordiamo che se le variabili aleatorie X e Y sono indipendenti allora $E[XY] = E[X]E[Y]$ e quindi $cov(X,Y) = 0$, il che implica $var(X+Y) = var(X) + var(Y)$.

In generale possiamo dire che lo studio del comportamento di sequenze di variabili aleatorie indipendenti è tra gli argomenti principali del tradizionale calcolo delle probabilità. Ricordiamo qui in una forma relativamente semplice due proprietà fondamentali, ovvero la legge dei grandi numeri e il teorema del limite centrale. Esse riguardano le somme parziali di una

sequenza di variabili aleatorie. Intuitivamente, la prima stabilisce che, con alta probabilità, tale somma si concentra intorno al suo valor medio; la seconda mostra che la funzione distribuzione di tale somma approssima una distribuzione normale. Più precisamente, supponiamo che $\{X_i\}_{i\geq 1}$ sia una sequenza di variabili aleatorie indipendenti aventi la stessa distribuzione. In tale ipotesi valgono le seguenti proprietà:

1. (Legge dei grandi numeri) Se m è il valor medio di X_1 (e quindi di tutte le $X_i, i \geq 1$) allora, con probabilità 1,

$$\lim_{n\to+\infty} \frac{X_1 + X_2 + \cdots + X_n}{n} = m$$

   Questo implica in particolare una proprietà più debole, ovvero che per ogni $\varepsilon > 0$,

$$\lim_{n\to+\infty} Pr\left\{\left|\frac{X_1 + X_2 + \cdots + X_n}{n} - m\right| > \varepsilon\right\} = 0.$$

2. (Teorema del limite centrale) Se m e s sono la media e la varianza di X_1 (e quindi di tutte le $X_i, i \geq 1$) allora, per ogni $x \in \mathbb{R}$

$$\lim_{n\to+\infty} Pr\left\{\frac{X_1 + \cdots + X_n - nm}{\sqrt{sn}} \leq x\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$$

   Lo strumento tradizionale utilizzato per provare questa proprietà è quello delle funzioni caratteristiche: si fa cioè vedere che la funzione caratteristica della somma parziale (opportunamente normalizzata) converge in ogni punto alla funzione caratteristica della normale standard (quella di media 0 e varianza 1).

Un tema di studio e di ricerca naturale in questo contesto è quello di determinare le ipotesi che consentono di estendere il teorema del limite centrale o la legge dei grandi numeri al caso di sequenze di variabili aleatorie dipendenti o non ugualmente distribuite. Il più semplice esempio di variabili aleatorie dipendenti è proprio fornito dalle catene di Markov e alcune funzioni di tali quantità hanno proprio una distribuzione limite normale.

A.2 Matrici e vettori

Dati due interi positivi r e s, una matrice di dimensione $r \times s$ è una famiglia di $r \cdot s$ valori a_{ij}, dove $i \in \{1, 2, \ldots, r\}$ e $j \in \{1, 2, \ldots, s\}$, che noi rappresentiamo come tavola bidimensionale nella forma

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \cdots & \cdots & & \cdots \\ a_{r1} & a_{r2} & \cdots & a_{rs} \end{pmatrix}$$

oppure mediante l'espressione $[a_{ij}]_{1\leq i\leq r,\ 1\leq j\leq s}$ o ancora, più semplicemente, da $[a_{ij}]$ quando la dimensione $r \times s$ è nota. Il valore r è il numero di righe di A mentre s è il numero di colonne. Gli elementi a_{ij} sono detti coefficienti (o componenti) della matrice. Se $r = s$ diremo che la matrice è quadrata e che r è il suo ordine. Un vettore riga è una matrice di dimensione $1 \times r$ mentre un vettore colonna è una matrice di dimensione $r \times 1$; in entrambi i casi diremo che

r è la dimensione del vettore. Un vettore a di dimensione r è generalmente considerato come vettore colonna e rappresentato nella forma

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_r \end{pmatrix}$$

Dato un insieme T denotiamo con $T^{r\times s}$ la famiglia di tutte le matrici di dimensione $r \times s$ a coefficienti in T. Analogamente, con T^r denoteremo l'insieme di tutti i vettori (colonna) di dimensione r a coefficienti in T. Così, $\mathbb{R}^{3\times 7}$ è l'insieme di tutte le matrici a coefficienti reali di dimensione 3×7, mentre $\mathbb{C}^4$ è l'insieme di tutti vettori di dimensione 4 a coefficienti complessi.

La matrice trasposta di una matrice $A = [a_{ij}]$ di dimensione $r \times s$ è la matrice $[b_{ji}]$ di dimensione $s \times r$, tale che $b_{ji} = a_{ij}$ per ogni $1 \le i \le r,\ 1 \le j \le s$; la matrice trasposta di A si ottiene quindi scambiando le righe e le colonne e viene solitamente rappresentata da A'. Così, se a è un vettore colonna, il suo trasposto a' è il corrispondente vettore riga. Per esempio, posto

$$A = \begin{pmatrix} 3 & 7 & 1 & 5 \\ 2 & 3 & 1 & 0 \\ 1 & -3 & 4 & -1 \end{pmatrix}\ , \qquad a = \begin{pmatrix} 2 \\ -3 \\ 6 \end{pmatrix}$$

allora

$$A' = \begin{pmatrix} 3 & 2 & 1 \\ 7 & 3 & -3 \\ 1 & 1 & 4 \\ 5 & 0 & -1 \end{pmatrix}\ , \qquad a' = (2,\ -3,\ 6)\ .$$

Una sottomatrice di una matrice A si ottiene cancellando da A alcune righe e/o alcune colonne.

Ricordiamo ora le tradizionali relazioni ed operazioni tra matrici. D'ora in poi consideriamo solo matrici e vettori a coefficienti reali o complessi. Due matrici $A = [a_{ij}]$ e $B = [b_{ij}]$ di dimensione $r \times s$ si dicono uguali, in simboli $A = B$, se $a_{ij} = b_{ij}$ per ogni coppia di indici i e j ($1 \le i \le r$, $1 \le j \le s$). Analogamente, $A < B$ significa che A e B sono a coefficienti reali e che $a_{ij} < b_{ij}$ per ogni $i = 1, \ldots, r$ e ogni $j = 1, \ldots, s$. In modo del tutto simile si definiscono le relazioni $A \le B$, $A \ge B$, $A > B$. Inoltre una matrice reale $A = [a_{ij}]$ si dice positiva, in simboli $A > 0$, se $a_{ij} > 0$ per ogni i e ogni j; A si dice invece non negativa, $A \ge 0$, se $a_{ij} \ge 0$ per tutte le coppie di indici.

Una matrice quadrata A si dice *simmetrica* se coincide con la sua trasposta, ovvero $A = A'$. Inoltre una matrice quadrata $[a_{ij}]$ si dice *diagonale* se tutti i suoi coefficienti sono nulli tranne gli elementi a_{ii}. Tali elementi formano la cosiddetta diagonale principale della matrice. Chiaramente, tutte le matrici diagonali sono simmetriche. Tra queste ricordiamo la matrice identità di ordine r, solitamente denotata con I_r, definita ponendo $I_r = [\delta_{ij}]$, dove i valori δ_{ij} sono i coefficienti di Kronecker, definiti dalle equazioni $\delta_{ii} = 1$ e $\delta_{ij} = 0$ per ogni $i \ne j$. Quando l'ordine r è sottinteso, I_r sarà più semplicemente rappresentata con I, omettendo l'indice r.

Altre due matrici spesso usate sono la matrice $0_{r\times s}$ di dimensione $r \times s$, le cui componenti sono tutte 0 e la matrice $E_{r\times s}$ della stessa dimensione, i cui coefficienti sono tutti 1. I

corrispondenti vettori (colonna) sarano rappresentati da 0_r e e_r. Anche in questo caso gli indici saranno omessi quando le dimensioni sono sottointese.

Tre sono le operazioni principali tra matrici a coefficienti complessi: il prodotto per uno scalare, la somma e la moltiplicazione. Il prodotto cA di una matrice $A = [a_{ij}]$ per una costante $c \in \mathbb{C}$ è la matrice $cA = [ca_{ij}]$. In particolare, abbiamo $(-1)A = -A = [-a_{ij}]$, $0A = [0]$. La somma $A + B$ di due matrici $A = [a_{ij}]$ e $B = [b_{ij}]$ della stessa dimensione è data da $A+B = [a_{ij}+b_{ij}]$. La somma di matrici è un'operazione associativa e commutativa; inoltre il prodotto per una costante è distributivo rispetto alla somma, ovvero $c(A + B) = cA + cB$ e $(c + d)A = cA + dA$.

Il prodotto di due matrici $A = [a_{ij}]$ e $B = [b_{ij}]$ è definito quando il numero di colonne di A è uguale al numero di righe di B; se $r \times s$ è la dimensione di A e $s \times t$ quella di B allora il prodotto AB è la matrice $AB = [c_{ij}]$ di dimensione $r \times t$, tale che $c_{ij} = \sum_{k=1}^{s} a_{ik}b_{kj}$ per tutti gli indici i,j.

Il prodotto di matrici è associativo ma non commutativo; tale operazione è distributiva rispetto alla somma di matrici, ovvero $(A + B)C = AC + BC$ e $A(B + C) = AB + AC$. Per ogni matrice A di dimensione $r \times s$ valgono anche le seguenti identità: $I_r A = AI_s = A$, $0_{t\times r}A = 0_{t\times s}$, $A0_{s\times t} = 0_{r\times t}$. Inoltre la trasposta di un prodotto è sempre il prodotto inverso delle trasposte, ovvero $(AB)' = B'A'$. Infine, per ogni $n \in \mathbb{N}$, la potenza A^n di una matrice quadrata A è il prodotto di A per sè stessa n volte, con la convenzione che $A^0 = I$. Il prodotto di potenze di una stessa matrice è commutativo.

Il determinante di una matrice quadrata $A = [a_{ij}]$ di ordine r è definito da

$$\det(A) = \sum_{*} \pm a_{1j_1} a_{2j_2} \cdots a_{rj_r}$$

dove la somma è estesa a tutte le permutazioni $(j_1, j_2, \ldots, j_r)$ di $(1, 2, \ldots, r)$ e il segno $\pm$ è positivo se la permutazione è pari, negativo se è dispari. Se $\det(A) = 0$ diciamo che A è singolare e questo avviene se e solo se una delle sue righe (o colonne) si può esprimere come combinazione lineare delle altre. Viceversa, se $\det(A) \neq 0$ diremo che A è regolare o non singolare e in questo caso le righe (e le colonne) di A sono linearmente indipendenti. Il determinante può essere calcolato usando i cofattori; il cofattore $\mathrm{cof}(A)_{ij}$ è il valore

$$\mathrm{cof}(A)_{ij} = (-1)^{i+j}\det(A_{ij}) \ ,$$

dove A_{ij} è la sottomatrice che si ottiene cancellando da A la riga i-esima e la colonna j-esima. Si può provare che per ogni $1 \leq i, j \leq r$,

$$\det(A) = \sum_{k=1}^{r} a_{ik}\mathrm{cof}(A)_{ik} = \sum_{k=1}^{r} a_{kj}\mathrm{cof}(A)_{kj} \ .$$

Inoltre l'aggiunto di A, denotato $\mathrm{adj}(A)$, è la trasposta della matrice dei cofattori, ovvero

$$\mathrm{adj}(A) = [\mathrm{cof}(A)_{ij}]' \ . \tag{A.1}$$

Infine, se A e B sono matrici quadrate dello stesso ordine, allora $\det(AB) = \det(A)\det(B)$.

L'inversa di una matrice quadrata A è la matrice A^{-1} tale che $AA^{-1} = A^{-1}A = I$. Si può dimostrare che A^{-1} esiste se e solo se A non è singolare, ovvero $\det(A) \neq 1$, nel qual caso abbiamo

$$A^{-1} = \frac{1}{\det(A)}\mathrm{adj}(A)$$

Chiaramente $I_r^{-1} = I_r$ per ogni intero $r > 0$ e si può provare che, se A e B sono matrici quadrate non singolari dello stesso ordine, allora $(AB)^{-1} = B^{-1}A^{-1}$ e $(A')^{-1} = (A^{-1})'$.

Molte proprietà delle catene di Markov sono basate sullo studio delle potenze di matrici. Per questo motivo in questa sezione ricordiamo alcune caratteristiche di base di tali quantità.

Proposizione A.1 *Se A è una matrice quadrata tale che $A^n \to 0$ (matrice nulla) per $n \to +\infty$, allora $(I - A)^{-1}$ esiste e inoltre*

$$(I - A)^{-1} = I + A + A^2 + \cdots + A^n + \cdots$$

Dimostrazione. È facile verificare che per ogni intero $n > 0$

$$I - A^n = (I - A)(I + A + A^2 + \cdots + A^{n-1})$$

Sappiamo inoltre che il determinante della matrice a sinistra dell'uguaglianza tende a 1; quindi per ogni n abbastanza grande $\det(I - A^n) \neq 0$. Allora anche il determinante della matrice a destra dell'uguaglianza è diverso da 0 e, poiché il determinante di un prodotto è il prodotto dei determinanti, otteniamo $\det(I - A) \neq 0$. Questo implica che $(I - A)^{-1}$ è ben definita. Se ora moltiplichiamo l'equazione precedente per $(I - A)^{-1}$ otteniamo

$$(I - A)^{-1}(I - A^n) = I + A + A^2 + \cdots + A^{n-1}$$

e facendo tendere n all'infinito si ricava il risultato. □

A.3 Autovalori e autovettori

Data una matrice quadrata $A = [a_{ij}]$ di ordine r, diciamo che un numero complesso $\lambda \in \mathbb{C}$ è un *autovalore* di A se esiste un vettore $u \neq 0_r$ tale che

$$u'A = \lambda u' \ .$$

In questo caso si dice che u è *autovettore sinistro* corrispondente a λ. L'insieme S_λ ottenuto considerando tutti gli autovettori sinistri di A corrispondenti a λ e aggiungendo il vettore 0_r, forma uno spazio vettoriale, sottospazio di $\mathbb{C}^r$; S_λ è anche chiamato autospazio sinistro di A corrispondente a λ e la sua dimensione è detta *molteplicità geometrica* di λ.

Gli autovalori di A possono anche essere definiti come le radici (nella variabile x) dell'equazione

$$\det(xI_r - A) = 0$$

chiamata *equazione caratteristica* di A. Si mostra facilmente che le due definizioni sono equivalenti. Inoltre si chiama *molteplicità algebrica* di λ la sua molteplicità come radice del polinomio $\det(xI_r - A)$. Poiché l'equazione caratteristica ha grado r ci possono essere al più r autovalori distinti di A e in questo caso tutti hanno molteplicità algebrica 1. Si può dimostrare che la molteplicità geometrica di un autovalore è sempre minore o uguale alla sua molteplicità algebrica. Chiaramente, se la molteplicità algebrica di un autovalore è 1 anche quella geometrica è 1. Il viceversa non è sempre vero.

Così come abbiamo definito l'autospazio sinistro, possiamo definire l'autospazio destro. Dato un autovalore λ di A chiamiamo *autovettore destro* corrispondente a λ un vettore $v \neq 0_r$

di dimensione r, tale che $Av = \lambda v$. L'insieme di tutti questi vettori con l'aggiunta di 0_r forma uno spazio vettoriale D_λ, chiamato autospazio destro corrispondente a λ. Si verifica che la sua dimensione coincide con quella di S_λ e quindi con la molteplicità geometrica di λ.

Si può anche provare che se $\lambda_1, \lambda_2, \ldots, \lambda_t$ sono autovalori distinti di A allora ogni t-pla di autovettori sinistri $u_1, \ldots, u_t$, dove $u_i \in S_{\lambda_i}$ per ogni i, forma un insieme di vettori indipendenti. Una proprietà analoga vale per gli autovettori destri. Questo implica che il massimo numero di autovettori sinistri (destri) indipendenti è minore o uguale alla somma delle molteplicità geometriche degli autovalori; a sua volta tale somma può essere minore di r e questo capita quando un autovalore possiede molteplicità geometrica minore di quella algebrica.

Un modo per calcolare facilmente la potenza A^n di una matrice A passa attraverso la sua diagonalizzazione. Una matrice quadrata A si dice *diagonalizzabile* se esiste una matrice non singolare U e una matrice diagonale D tali che

$$D = UAU^{-1} \ .$$

In questo caso i coefficienti che si trovano sulla diagonale principale di D sono gli autovalori di A, cioè $D = [\lambda_i \delta_{ij}]$, dove i λ_i sono gli autovalori di A. Inoltre le righe di U e le colonne di U^{-1} sono rispettivamente autovettori sinistri e autovettori destri corrispondenti agli autovalori. Questo implica che una matrice è diagonalizzabile se e solo se le molteplicità geometriche di tutti gli autovalori coincidono con quelle algebriche. Chiaramente abbiamo $A^n = U^{-1}D^nU$ dove D^n è la matrice diagonale data da $D^n = [\lambda_i^n \delta_{ij}]$.

Due sono i casi di matrici diagonalizzabili particolarmente importanti: il caso delle matrici reali simmetriche e quello delle matrici con autovalori distinti. Se A è una matrice reale simmetrica allora valgono le seguenti proprietà: 1) tutti gli autovalori di A sono reali; 2) gli autovettori destri e sinistri di uno stesso autovalore coincidono; 3) A è diagonalizzabile, cioè $A = U^{-1}DU$ con D e U definiti come sopra e 4) si può scegliere la matrice degli autovettori U in modo che sia una matrice ortogonale, ovvero $U^{-1} = U'$ (i.e., A possiede r autovettori tra loro ortogonali).

Se invece A è una matrice quadrata di ordine r che possiede r autovalori distinti $\lambda_1, \ldots, \lambda_r$, allora è facile provare che per ogni $i = 1, \ldots, r$ esistono un autovettore sinistro u_i e uno destro v_i, entrambi corrispondenti a λ_i, tali che $u_i'v_i = 1$ e $u_i'v_j = 0$, per ogni $i \neq j$. Possiamo allora considerare la matrice U che si ottiene accostando le r righe $u_1', \ldots, u_r'$ e la matrice V ottenuta accostando le colonne $v_1, \ldots v_r$. Tali matrici, entrambe quadrate di ordine r, sono non singolari e inoltre abbiamo $UV = I$, cioè $U = V^{-1}$ e $V = U^{-1}$. Esse consentono di diagonalizzare la matrice A; dallo loro stessa definizione infatti si ricava $UA = DU$ e $AV = VD$, dove $D = [\lambda_i \delta_{ij}]$ e quindi otteniamo

$$A = U^{-1}DU = VDU \ .$$

Quest'ultima relazione può essere riscritta nella forma

$$A = \sum_{i=1}^{r} \lambda_i v_i u_i'$$

che solitamente è chiamata *rappresentazione spettrale* di A e deve la sua importanza alla immediata deduzione della equazione

$$A^n = \sum_{i=1}^{r} \lambda_i^n v_i u_i' \tag{A.2}$$

valida per ogni intero $n > 0$, che consente di calcolare facilmente le potenze di A.

A.4 Massimo comun divisore

In questa sede ricordiamo alcune proprietà del massimo comun divisore con particolare riferimento alle famiglie di interi chiuse rispetto alla somma. L'obiettivo principale è quello di provare che i sottoinsiemi di $\mathbb{N}$ chiusi rispetto alla somma contengono tutti i multipli positivi del loro massimo comun divisore eccetto al più un numero finito di questi. Tale proprietà, qui enunciata nel teorema A.4, è utile in particolare nell'analisi del periodo delle matrici irriducibili sviluppata nel capitolo 2. La presentazione è qui ripresa da [21].

Sia S un insieme di numeri interi, eventualmente infinito, contenente almeno un elemento a diverso da 0. Il massimo comun divisore di S può essere definito nel modo tradizionale: consideriamo la famiglia dei divisori comuni a tutti gli elementi di S; essa non è vuota perché contiene il numero 1, ed è certamente finita perché il numero di divisori di a è finito. Possiamo quindi considerare il massimo valore in tale famiglia, detto appunto *massimo comun divisore* di S.

Ricordiamo infine che un insieme $S \subseteq \mathbb{Z}$ è chiuso rispetto alla somma se, per ogni $a, b \in S$, anche l'intero $a + b$ appartiene a S. Chiaramente un tale insieme contiene infiniti elementi se possiede almeno un intero diverso da 0. Definizione analoghe si possono dare per la sottrazione e le altre operazioni aritmetiche.

Lemma A.2 *Sia $S \subseteq \mathbb{Z}$ un insieme chiuso rispetto alla somma e alla sottrazione, contenente un intero diverso da 0. Allora S possiede un minimo elemento positivo m e inoltre S coincide con l'insieme dei multipli di m, ovvero $S = \{cm \mid c \in \mathbb{Z}\}$.*

Dimostrazione. Se $a \neq 0$ appartiene a S allora anche $0 = a - a$ e $-a = 0 - a$ appartengono a S. Quindi S contiene almeno un elemento positivo e possiamo considerare il minimo m dei suoi elementi positivi, $m = \min\{t \in S \mid t > 0\}$. Per le proprietà di chiusura di S, gli interi $-km$ e km appartengono a S per ogni $k = 1, 2, \ldots$. Mostriamo ora che ogni elemento di S è un multiplo di m. Infatti, se $t \in S$ allora, dividendo t per m, determiniamo due interi q e r, $0 \leq r < m$ tali che $t = qm + r$; di conseguenza anche $r = t - qm$ appartiene a S e quindi $r = 0$ perché m è il minimo elemento positivo in S ed r deve essere minore di m. Ne segue che t è un multiplo di m. □

Lemma A.3 *Il massimo comun divisore d di un insieme finito di numeri interi $\{b_1, b_2, \ldots, b_k\}$ è combinazione lineare a coefficienti interi di $b_1, b_2, \ldots, b_k$, ovvero esistono k coefficienti $c_1, c_2, \ldots, c_k \in \mathbb{Z}$ tali che $d = \sum_{j=1}^{k} c_j b_j$.*

Dimostrazione. Sia S l'insieme delle combinazioni lineari $\sum_{j=1}^{k} i_j b_j$ al variare degli interi i_j in $\mathbb{Z}$. Poiché S è chiuso rispetto alla somma e alla sottrazione, per il Lemma A.2, esiste un elemento positivo minimo $m \in S$ tale che ogni elemento di S è multiplo di m. Mostriamo che $d = m$. Infatti, si verifica che $0 < d \leq m$, poiché d, essendo divisore di ogni b_j, è divisore di ogni intero in S. D'altra parte, poiché ogni b_j appartiene a S, m divide ogni intero b_j per cui $m \leq d$. Quindi $m = d$ e questo prova che anche d è combinazione lineare dei b_j. □

Teorema A.4 *Ogni insieme non vuoto di interi positivi chiuso rispetto alla somma contiene tutti i multipli positivi del suo massimo comun divisore eccetto al più un numero finito di questi.*

Dimostrazione. Sia U un insieme non vuoto di interi positivi chiuso rispetto alla somma e sia d il suo massimo comun divisore. Proviamo il teorema supponendo $d = 1$. Se infatti fosse $d > 1$ basterebbe dividere tutti gli elementi di U per d per ricondursi al caso precedente. Allora, $d = 1$ è anche il massimo comun divisore di un numero finito di elementi di U, che denotiamo $b_1, b_2, \ldots, b_k$; quindi, per il Lemma A.3, esistono k interi $i_1, i_2, \ldots, i_k \in \mathbb{Z}$ tali che

$$1 = \sum_{j=1}^{k} i_j b_j = u - v \tag{A.3}$$

dove u è la somma degli elementi positivi nella sommatoria e $-v$ la somma di quelli negativi. Se $v = 0$ allora, nella sommatoria precedente, tutti gli elementi sono positivi o nulli, il che implica che qualche $b_j \in U$ è uguale a 1, ed essendo U chiuso rispetto alla somma U deve contenere tutti gli interi positivi. Se invece $v > 0$ allora abbiamo $u, v \in U$ perché somme di elementi di U. Consideriamo allora un qualunque intero $n \geq v^2$ e mostriamo che $n \in U$. Infatti, dividendo n per v otteniamo due interi q e r tali che $n = qv + r$, $0 \leq r < v$ e $v \leq q$. Per la (A.3) abbiamo $n = qv + r(u - v) = ru + (q - r)v$, ed essendo $q > r$, otteniamo che n è somma di elementi di U e di conseguenza appartiene a U. □

Bibliografia

[1] A. Aho, J. Hopcroft, J. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley Publishing Company, Reading (Massachusetts), 1974.

[2] G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, M. Protasi, *Complexity and Approximation*, Springer-Verlag, Berlin Heidelberg, 1999.

[3] P. Brémaud, *Markov Chains: Gibbs fields, Monte Carlo Simulation and Queues*, Springer, New York, 1998.

[4] T. Cormen, C. Leiserson, R. Rivest, *Introduction to Algorithms*, The MIT Press, Cambridge (Massachusetts), 1990.

[5] W. Feller, *An Introduction to Probability Theory and Applications*, John Wiley & Sons, New York, 1968.

[6] P. Flajolet, P. Zimmerman, B. Van Cutsem. A calculus for the random generation of labelled combinatorial structures. *Theoretical Computer Science*, vol. 132(1-2), 1-35, 1994.

[7] O. Häggström, *Finite Markov Chains and Algorithmic Applications*, Cambridge Unversity Press, New York, 2003.

[8] J. Hromkovic, *Desing and Analysis of Randomized Algorithms*, Springer, Berlin Heidelberg New York, 2005.

[9] M. Iosifescu, *Finite Markov Processes and Their Applications*, John Wiley & Sons, New York, 1980.

[10] D. Isaacson, R. Madsen, *Markov Chains Theory and Applications*, R.E. Krieger Publishing Company, 1985.

[11] M. Jerrum, A very simple algorithm for estimating the number of k-colorings of a low-degree graph. *Random Structures and Algorithms*, vol. 7, 157-165, 1995.

[12] M. Jerrum, Mathematical foundations of the Markov chain Monte Carlo method, in *Probabilistic Methods for Algorithmic Discrete Mathematics*, M. Habib, C. McDiarmid, J. Ramirez-Alfonsin and B. Reed editors, Springer, 116-165, 1998.

[13] M. Jerrum, A. Sinclair, A Markov chain Monte Carlo method: an approach to approximate counting and integration, Chapter 12 in *Approximations for NP-hard problems*, D. Hochbaum editor, PSW Publishing, 482-520, 1996.

[14] J.G. Kemeny, J.L. Snell, *Finite Markov Chains*, Van Nostrand Company, Princeton (New Jersey), 1960.

[15] M. Mitzenmacher, E. Upfal, *Probability and Computing*, Cambridge University Press, New York, 2005.

[16] R. Motwani, P. Raghavan, *Randomized Algorithms*, Cambridge University Press, New York, 1995.

[17] J.R. Norris, *Markov Chains*, Cambridge University Press, New York, 2009.

[18] C.H. Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Reading (Massachusetts), 1994.

[19] A. Paz, *Introduction to Probabilistic Automata*, Academic Press, 1971.

[20] R. Sedgewick, P. Flajolet, *An Introduction to the Analysis of Algorithms*, Addison-Wesley Publishing Company, Reading (Massachusetts), 1996.

[21] E. Seneta, *Non-negative Matrices and Markov Chains*, Springer–Verlag, New York Heidelberg Berlin, 1981.

[22] G. Strang, *Linear Algebra and its Applications*, Harcourt Brace Jovanovich College Publisher, Fort Worth (Texas), 1988.

[23] L.G. Valiant, The complexity of computing the permanent, *Theoretical Computer Science*, vol. 8, 189-201, 1979.

[24] L.G. Valiant, The complexity of enumeration and reliability problems, *SIAM Journal on Computing*, vol. 8, 410-421, 1979.

[25] W. Woess, *Catene di Markov e teoria del potenziale nel discreto*, Quaderni dell'Unione Matematica Italiana, n.41, Pitagora Editrice, Bologna, 1996.

Catene di Markov e applicazioni algoritmiche

Massimiliano Goldwurm

Le catene di Markov rappresentano un argomento di studio classico, di carattere matematico e probabilistico, che ha trovato un grande numero di applicazioni in varie discipline, dall'informatica alla matematica, dalla fisica alla biologia e alle scienze naturali, dalla sociologia all'economia e in molti altri contesti. Esempi tipici di modelli markoviani riguardano l'analisi e l'interpretazione di sequenze di DNA, il riconoscimento di segnali vocali, il disegno di procedure di esplorazione e analisi della rete web. In un ambito informatico e soprattutto algoritmico le catene di Markov hanno dato origine ai cosiddetti metodi Markov Chain Monte Carlo (MCMC), che consentono di definire algoritmi probabilistici di approssimazione per problemi difficili dal punto di vista computazionale. Questo testo presenta le catene di Markov e alcune loro applicazioni algoritmiche in uno stile matematico con un taglio principalmente didattico, rivolto in particolare agli studenti dei corsi di laurea magistrale a carattere scientifico delle università italiane.

In copertina: disegno dell'autore.

ISBN 9791255100997 (print)
ISBN 9791255101000 (PDF)
ISBN 9791255101017 (EPUB)
DOI 10.54103/milanoup.158