UNIVERSIDADE FEDERAL DE ALAGOAS

INSTITUTO DE MATEMÁTICA

CURSO EM MATEMÁTICA BACHARELADO

TRABALHO DE CONCLUSÃO DE CURSO

DAVI MATHEUS COSTA BARROS

CADEIAS DE MARKOV: DECIFRANDO CRIPTOGRAFIAS

MACEIÓ

2022

DAVI MATHEUS COSTA BARROS

CADEIAS DE MARKOV: DECIFRANDO CRIPTOGRAFIAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Matemática do Instituto de Matemática da Universidade Federal de Alagoas, como requisito parcial à obtenção do grau de bacharel em Matemática.

Orientador: Prof. Dr. Alan Anderson da Silva Pereira .

MACEIÓ

2022

Catalogação na Fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecário: Marcelino de Carvalho Freitas Neto – CRB-4 – 1767

B277c Barros, Davi Matheus Costa.
Cadeias de Markov : decifrando criptografias / Davi Matheus Costa Barros. - 2022.
68 f. : il.

Orientador: Alan Andeson da Silva Pereira.
Monografia (Trabalho de Conclusão de Curso em Matemática : Bacharelado) – Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2022.

Bibliografia: f. 68.

1. Markov, Processos de. 2. Monte Carlo, Método de. 3. Criptografia. I. Título.

CDU: 519.217.2

AGRADECIMENTOS

Em primeiro lugar, gradeço a Deus, por ter permitido que eu tivesse saúde e, assim, fez com que meus objetivos fossem alcançados durante todos os meus anos de estudos. Agradeço também aos amigos e familiares, por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho. Aos professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação ao longo do curso. Aos meus colegas de curso, com quem convivi intensamente durante os últimos anos, pelo companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando.

"A persistência é o caminho do êxito."

(Charles Chaplin)

RESUMO

O presente trabalho consiste no estudo das cadeias de Markov e o algoritmo de Monte Carlo como ferramenta de descriptografia.

Cadeia de Markov é um sistema probabilístico de tempo discreto e sem memória, ou seja, o "amanhã" depende do "hoje" e independe do "ontem". O algoritmo de Monte Carlo em Cadeias de Markov é útil para otimizar longas simulações que modelam um fenômeno probabilístico.

Palavras-chave: Cadeias de Markov, Monte Carlo, Criptografia.

ABSTRACT

The present work consists of the study of Markov chains and the Monte Carlo algorithm as a decryption tool.

Markov chain is a discrete-time, memoryless probabilistic system, that is, the "tomorrow"depends on "today"and is independent of "yesterday". The Markov Chain Monte Carlo Algorithm is useful for optimizing long simulations that model a probabilistic phenomenon.

Keywords: Markov Chains, Monte Carlo, Cryptography.

SUMÁRIO

1 INTRODUÇÃO

O objetivo deste trabalho é expor alguns resultados básicos de probabilidade utilizando algoritmos de Monte Carlo para Cadeias de Markov. Inicialmente, vamos abordar conceitos iniciais de Probabilidade. Depois exploraremos algumas propriedades de Cadeias de Markov como a aperiodicidade e irredutibilidade. Por fim, mostraremos o algoritmo de Monte Carlo e uma de suas aplicações.

No capítulo 2, veremos alguns conceitos básicos da teoria de probabilidade que serão imprescindíveis para o nosso estudo. Veremos os conceitos, por exemplo, de probabilidade condicional, variáveis aleatórias, esperança de variável aleatória, distribuição de probabilidade. Daremos motivações a estes conceitos para que fiquem o mais claro possível através de exemplos paupáveis.

No capítulo 3, introduziremos a definição e conceito de Cadeias de Markov. Vamos abordar as definições importantes como, por exemplo, espaço de estados, matriz de transição, o fenômeno da perda de memória, entre outros tópicos. Além de trazer exemplos que aproxime esses objetos de estudos para o cotidiano do leitor.

No capítulo 4, vamos desenvolver ferramentas matemáticas que permitam realizar simulações das cadeias de Markov de acordo com nossas necessidades. Nos capítulo 5 e 7, vamos estudar as principais propriedades que uma cadeia de Markov pode ter: aperiodicidade, irredutibilidade e reversibilidade.

No capítulo 6, estudaremos o conceito de distribuição estacionária e, na sequência, três teoremas importantes a respeito da convergência da distribuição de probabilidade em cadeias aperiódicas e irredutíveis.

Nos capítulo 8 e 9, seremos apresentados ao Algoritmo de Monte Carlo para otimizações em Cadeias de Markov. Por fim, no capítulo 10, aplicaremos uma otimização via algoritmo de Monte Carlo para otimizar a descriptografia de um texto por meio de sua plausibilidade.

2 O BÁSICO DE PROBABILIDADE

Nesse capítulo, vamos introduzir algumas noções importantes de probabilidade como variavéis aleatórias, distribuição de probabilidade, esperança, probabilidade condicional, etc. Esses conceitos serão importantes para a compreensão de Cadeias de Markov no capítulo seguinte.

Definição 1. *Sejam X um conjunto qualquer e $P(X)$ a coleção de todos os subconjuntos de X. Dizemos que $\mathbb{X} \subseteq P(X)$ é uma σ-álgebra de subconjuntos de X se, e somente se:*

1. $X \in \mathbb{X}$
2. *Se $A \in \mathbb{X}$, então $A^c \in \mathbb{X}$*
3. *Se $(A_n)_{n\in\mathbb{N}}$ é uma sequência em X, então*

$$\bigcup_{n=1}^{\infty} A_n \in \mathbb{X}$$

Sejam Ω um conjunto qualquer e Σ uma família de subconjuntos de Ω, satisfazendo certas condições (operações básicas fechadas no próprio conjunto). Elementos de Σ são chamados de eventos. Para $A \subseteq \Omega$, escrevemos A^c para o complementar de A em Ω que significa: $A^c = \{s \in \Omega : s \notin A\}$

Uma medida de em Ω é uma função $P : \Sigma \to [0,1]$, satisfazendo:

1. $P(\emptyset) = 0$.
2. P(A^c) = 1 - P(A) para todo $A \subseteq \Omega$.
3. Se A e B são dois eventos disjutos, ou seja, $A \cap B = \emptyset$, então $P(A \cup B) = P(A) + P(B)$. Em geral, se $A_1, A_2, \ldots, A_n$ é uma sequência enumerável de eventos disjuntos ($A_i \cap B_j = \emptyset$ para todo i $\neq$ j), então $P(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$.

Note que (1) e (2) juntos implicam que P(Ω) = 1.

Se A e B são eventos, e $P(B) > 0$, então definimos a probabilidade condicional de A dado B e denotamos por

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}.$$

A interpretação intuitiva de P($A \mid B$) é a probabilidade do evento A acontecer, visto que ocorreu o

evento B.

Dois eventos A e B são ditos independentes se P($A \cap B$) = $P(A)P(B)$. Em geral, os eventos $A_1,\ldots,A_k$ são ditos independentes se para qualquer $l \leq k$ e quaisquer $i_1,\ldots,i_l \in \{1,\ldots,k\}$ com $i_1 < i_2 < \ldots < i_l$ nós temos que:

$$P(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_l}) = \prod_{n=1}^{l} P(A_{i_n}).$$

Para uma sequência infinita de eventos $(A_1,\ldots,A_n,\ldots)$, nós dizemos que $A_1,A_2,\ldots$ são independentes se $A_1,A_2,\ldots,A_k$ são independentes para todo k. Note que se $P(B) > 0$, então a independência entre A e B implica que $P(A \mid B) = P(A)$, ou seja, a ocorrência de B não afeta a ocrrência do evento A.

Uma variável aleatória deve ser considerada como uma quantidade aleatória que depende do acaso. Normalmente, uma variável aleatória tem valor real, caso em que é uma função da forma $X : \Omega \to \mathbb{R}$. Iremos, no entanto, também considerar variáveis aleatórias em um sentido mais geral, permitindo que sejam funções $X : \Omega \to S$ onde S pode ser qualquer conjunto.

Um evento A é definido em termos da variável aleatória X se podemos ler se A aconteceu ou não a partir do valor de X. Exemplos de eventos definidos em termos da variável aleatória X são

$$A = \{X \leq 4.7\} = \{\omega \in \Omega \mid X(\omega) \leq 4.7\} \text{ e } B = \{X \text{ é um número inteiro par}\}.$$

Definição 2. *Duas variáveis aleatórias X e Y são consideradas independentes quando, para quaisquer eventos $A = A(X)$ e $B = B(Y)$, definidos em termos das variavéis aleatórias X e Y respectivamente, são independentes. Da mesma forma, se $X_1,\ldots,X_k,\ldots$ são variáveis aleatórias, então elas são consideradas independentes quando os eventos $A_1 = A_1(X_1),\ldots,A_k = A_k(X_k)$, $\ldots$ são independentes.*

Uma distribuição é a mesma coisa que uma medida de probabilidade. Se X é uma variável aleatória de valor real, então a distribuição μ_X é a medida de probabilidade em $\mathbb{R}$ satisfazendo $\mu_X(A) = P(X \in A)$ para todos (apropriados) $A \subseteq \mathbb{R}$. A distribuição de uma variável aleatória de valor real é caracterizada em termos de sua função de distribuição $F_X : \mathbb{R} \to [0,1]$ definida por $F_X(x) = P(X \leq x)$ para todo $x \in \mathbb{R}$. Uma distribuição μ em um conjunto finito

$S = \{s_1, ..., s_k\}$ é frequentemente representada como um vetor $(\mu_1, ..., \mu_k)$, onde $\mu_i = \mu_{s_i}$. Pela definição de uma medida de probabilidade, temos então que $\mu_i \in [0,1]$ para cada i, e que $\sum_{i=1}^{k} \mu_i = 1$.

Uma sequência de variáveis aleatórias $X_1, X_2, ...$ é dita *i.i.d.*, que é abreviação de independente e identicamente distribuída, se as variáveis aleatórias:

1. são independentes, e
2. possuem a mesma função distribuição, isto é, $P(X_i \leq x) = P(X_j \leq x)$ para todos i, j e x.

Muitas vezes, uma sequência $(X_1, X_2, ...)$ é interpretada como a evolução no tempo de alguma quantidade aleatória: X_n é a quantidade no tempo n. Essa sequência é então chamada de processo aleatório (ou, às vezes, processo estocástico). Cadeias de Markov, a serem introduzidos no próximo capítulo, é uma classe especial de processos aleatórios.

Estaremos lidando apenas com dois tipos de variáveis aleatórias de valor real: variáveis aleatórias discretas e contínuas. Os discretos assumem seus valores em algum subconjunto finito ou contável de $\mathbb{R}$; em todas as nossas aplicações, este subconjunto é (ou está contido em) $\{0, 1, 2, ...\}$, caso em que dizemos que eles são não negativos variáveis aleatórias discretas com valor inteiro.

Uma variável aleatória contínua X é uma variável aleatória para a qual existe uma função de densidade chamada $f_X : \mathbb{R} \to [0, \infty)$ de modo que:

$$\int_{-\infty}^{x} f_X(x)\, dx = F_X(x) = P(X \leq x) \text{ para todo } x \in \mathbb{R}$$

Um exemplo muito conhecido de uma variável aleatória contínua X surge ao deixar X ter a função de densidade gaussiana $f_X(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/2\sigma^2}$ com parâmetros μ e $\sigma > 0$. No entanto, as únicas variáveis aleatórias contínuas que serão consideradas neste texto são as uniformes [0, 1], que têm função de densidade

$$f_X(x) = \begin{cases} 1, & \text{se} \quad x \in [0,1], \\ 0, & \text{se} \quad x \notin [0,1] \end{cases}$$

e função distribuição dada por

$$F_X(x) = \int_{-\infty}^{x} f_X(t\,dt \begin{cases} 0, & \text{se} \quad x \leq 0, \\ x, & \text{se} \quad x \in [0,1], \\ 1, & \text{se} \quad x \geq 1 \end{cases}$$

Intuitivamente, se X for uma variável aleatória uniforme $[0,1]$, então X é igualmente provável para tomar seu valor em qualquer lugar no intervalo $[0,1]$. Mais precisamente, para cada intervalo I de comprimento a dentro de $[0,1]$, temos $P(X \in I) = a$

A esperança (ou valor esperado, ou média) $E[X]$ de uma variável aleatória de valor real X é, em certo sentido, o valor "médio" que esperamos de x. Se X for uma variável aleatória contínua com função de densidade $f_X(x)$, então sua esperança é definido como

$$E[X] = \int_{-\infty}^{\infty} x f_X(x)\,dx.$$

que no caso em que X é uniforme $[0,1]$ se reduz a

$$E[X] = \int_0^1 x\,dx = \frac{1}{2}.$$

Para o caso em que X é uma variável aleatória de valor inteiro não negativa, a esperança é definida como

$$E[X] = \sum_{k=1}^{\infty} kP(X = k).$$

Pode ser demonstrado que isso é equivalente à fórmula alternativa

$$\sum_{k=1}^{\infty} P(X \geq k).$$

É importante entender que a esperança $E[X]$ de uma variável aleatória pode ser infinito, mesmo se o próprio X assumir apenas valores finitos. Um exemplo famoso é o seguinte:

Exemplo 1. *O paradoxo de São Petersburgo. Considere o seguinte jogo. Uma moeda justa é jogada repetidamente até a primeira vez que sai coroa. Deixe X ser o número (aleatório) de caras que aparecem antes da primeira ocorrência de coroas. Suponha que o banco pague* 2^X *rublos dependendo de X. Quanto você está disposto a pagar para entrar neste jogo? De acordo*

com a teoria clássica dos jogos de risco, você deve concordar em pagar para $E[Y]$, onde $Y = 2^X$ é o valor que você recebe do banco no final do jogo. Então, vamos calcular $E[Y]$. Nós temos:

$$P(X = n) = \left(\frac{1}{2}\right)^{n+1} \text{ para cada n, de modo que}$$

$$\begin{aligned} E[Y] &= \sum_{k=1}^{\infty} kP(Y = k) = \sum_{n=0}^{\infty} 2^n P(Y = 2^n) \\ &= \sum_{n=0}^{\infty} 2^n P(X = n) = \sum_{n=0}^{\infty} 2^n (\frac{1}{2})^{n+1} \\ &= \sum_{n=0}^{\infty} \frac{1}{2} = \infty. \end{aligned}$$

Outra característica importante, além de $E[X]$, de uma variável aleatória X, é a variância $Var[X]$, definida por

$$Var[X] = E[(X - \mu)^2] \text{ onde } \mu = E[X].$$

A variância é, portanto, o desvio médio quadrático de X de sua esperança. Isto pode ser calculado usando a fórmula de definição ou pela identidade

$$Var[X] = E[X^2] - (E[X])^2$$

conhecida como fórmula de Steiner.

Utilizando a linearidade, temos

$$E[X_1 + ... + X_n] = E[X_1] + ... + E[X_n]$$

e, se c for uma constante,

$$E[cX] = cE[X]$$

Para variâncias, temos

$$Var[cX] = c^2 Var[X]$$

e, quando $X_1, \ldots, X_n$ são independentes

$$Var[X_1 + ... + X_n] = Var[X_1] + ... + Var[X_n]$$

Vamos calcular as esperanças e variações em alguns casos simples.

Fixe $p \in [0,1]$ e seja

$$X = \begin{cases} 1, & \text{com probabilidade p} \\ 0, & \text{com probabilidade 1-p.} \end{cases}$$

Esse tipo de X é chamado de variável aleatória $Bernoulli(p)$. A esperança de X torna-se

$$E[X] = 0 \cdot P(X = 0) + 1 \cdot P(X = 1) = p.$$

Além disso, uma vez que X apenas assume os valores 0 e 1, temos $X^2 = X$, de modo que $E[X^2] = E[X]$, e

$$Var[X] = E[X^2] - E[X]^2$$

$$= p - p^2 = p(1-p).$$

Exemplo 2. *Seja Y a soma de n variáveis aleatórias $Bernoulli(p)$ independentes $X_1, ..., X_n$. Por exemplo, Y pode ser o número de caras em n lançamentos de uma moeda com probabilidade de caras p.) Tal Y é dito ser uma variável aleatória $binomial(n,p)$. Então,*

$$E[Y] = E[X_1] + ... + E[X_n] = np,$$

$$Var[Y] = Var[X_1] + ... + Var[X_n] = np(1-p).$$

Variâncias são úteis, por exemplo, para limitar a probabilidade de que uma variável aleatória desvia muito de sua média. Temos, por exemplo, o seguinte resultado bem conhecido.

Teorema 1 (Desigualdade de Chebyshev)**.** *Seja X uma variável aleatória com média μ e variância σ^2. Para qualquer $a > 0$, temos que a probabilidade $P[|X-\mu| \geq a]$ de um desvio da média de pelo menos a, satisfaz*

$$P(|X-\mu| \geq a) \leq \frac{\sigma^2}{a^2}.$$

Demonstração. Defina outra variável aleatória Y dada por

$$Y = \begin{cases} a^2, & \text{se} \quad |X-\mu| \geq a, \\ 0, & \text{se} \quad |X-\mu| < a \end{cases}$$

Então sempre temos $Y \leq (X-\mu)^2$, de forma que $E[Y] \leq E[(X-\mu)^2]$. Além disso, $E[Y] = a^2 P(|X-\mu| \geq a)$, de modo que

$$P(|X-\mu| \geq a) = \frac{E[Y]}{a^2}$$

$$\leq \frac{E[(X-\mu)^2]}{a^2}$$

$$= \frac{Var[X]}{a^2} = \frac{\sigma^2}{a^2}.$$

□

Teorema 2 (**A Lei dos Grandes Números**)**.** *Sejam $X_1, X_2, \ldots$ variáveis aleatórias i.i.d com média finita μ e variância finita σ^2. Deixe M_n denotar a média dos n primeiros X_i's, ou seja, $M_n = \frac{1}{n}(X_1 + \ldots + X_n)$. Então, para qualquer $\varepsilon > 0$, temos*

$$\lim_{n\to\infty} P(|M_n - \mu| \geq \varepsilon) = 0$$

Demonstração. Usando a linearidade, temos

$$E[M_n] = \frac{1}{n}(\mu + \ldots + \mu) = \mu$$

Analogamente, como $Var[cX] = c^2 X$, então

$$Var[M_n] = \frac{1}{n^2}(\sigma^2 + \ldots + \sigma^2) = \frac{\sigma^2}{n}$$

Portanto, a desigualdade de Chebyshev dá

$$P(|M_n - \mu| \geq \varepsilon) \leq \frac{\sigma^2}{n\varepsilon^2} \text{ que tende a 0 quando } n \to \infty.$$

□

3 CADEIAS DE MARKOV

Uma cadeia de Markov nada mais é que uma modelagem de um sistema probabilístico com tempo discreto. Nesse capítulo vamos introduzir os conceitos do nosso objeto de estudo. Para isso, vamos começar com um exemplo simples.

Nós consideramos um "andarilho"em uma pequena cidade composta por quatro ruas e quatro esquinas v_1, v_2, v_3 e v_4 organizado como na Figura 1. No tempo 0, o andarilho fica no canto v_1. No tempo 1, ele joga uma moeda justa e se move imediatamente para v_2 ou v_4 de acordo com se a moeda dá cara ou coroa. No tempo 2, ele joga a moeda novamente para decidir para qual dos dois cantos adjacentes se mover, com a regra de decisão que se a moeda der cara, então ele se move um passo no sentido horário na Figura 1, enquanto se sair coroa, ele dá um passo no sentido anti-horário. Este procedimento é então iterado n vezes.

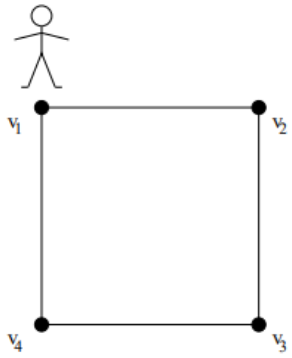


Figura 1

Para cada n, seja X_n o índice da esquina em que o andarilho está no tempo n. Portanto, $(X_0, X_1, \dots)$ é um processo aleatório tomando valores em $\{1,2,3,4\}$. Como o andarilho começa no tempo 0 em v_1, temos:

$$P(X_0 = 1) = 1.$$

Em seguida, ele se moverá para v_2 ou v_4 com probabilidade $1/2$ cada, de modo que

$$P(X_1 = 2) = \frac{1}{2} \quad \text{e} \quad P(X_1 = 4) = \frac{1}{2}$$

Calcular a distribuição de X_n para $n \geq 2$ requer um pouco mais de reflexão. Para este fim, é útil considere as probabilidades condicionais. Suponha que no momento n, o andarilho se posicione em, digamos, v_2. Então, obtemos as probabilidades condicionais:

$$P(X_{n+1} = v_1 | X_n = v_2) = \frac{1}{2} \quad \text{e} \quad P(X_{n+1} = v_3 | X_n = v_2) = \frac{1}{2}$$

por causa do mecanismo de cara ou coroa para decidir para onde ir a seguir. Na verdade, obtemos as mesmas probabilidades condicionais se condicionarmos ainda mais na totalidade história do processo até o tempo n, ou seja,

$$P(X_{n+1} = v_1 | X_0 = i_0, X_1 = i_1, \ldots, X_{n-1} = i_{n-1}, X_n = v_2) = \frac{1}{2}$$

e

$$P(X_{n+1} = v_3 | X_0 = i_0, X_1 = i_1, \ldots, X_{n-1} = i_{n-1}, X_n = v_2) = \frac{1}{2}$$

para qualquer escolha de $i_0, \ldots, i_{n-1}$. (Isso ocorre porque o cara ou coroa no tempo $n+1$ é independente de todos os lançamentos de moeda anteriores e, portanto, também independente de $X_0, \ldots, X_n$). Este fenômeno é chamado de propriedade sem memória, também conhecida como propriedade de Markov: a distribuição condicional de X_{n+1} dada $(X_0, \ldots, X_n)$ depende apenas de X_n. Ou, em outras palavras, fazer o melhor possível previsão do que acontece "amanhã"(tempo $n+1$), só precisamos considerar o que acontece “hoje” (tempo n), como o “passado” (tempos $0, \ldots, n-1$) não fornecem informações úteis adicionais.

Outra característica interessante deste processo aleatório é que a condicional distribuição de X_{n+1} dado que $X_n = v_2$ (digamos) é a mesma para todos os n. (Isso é porque o mecanismo que o andarilho usa para decidir para onde ir a seguir é o mesmo em todos os momentos). Esta propriedade é conhecida como homogeneidade do tempo, ou simplesmente homogeneidade.

Definição 3. *Seja P seja uma matriz $k \times k$ com elementos $\{P_{i,j} : i, j = 1, \ldots, k\}$. Um processo aleatório $(X_0, X_1, \ldots)$ com espaço de estado finito $S = \{s_1, \ldots, s_k\}$ é dito ser uma cadeia de Markov (homogênea) com matriz de transição P, se para todos n, todos $i, j \in \{1, \ldots, k\}$ e todos*

$i_0, \ldots, i_{n-1} \in \{1, ..., k\}$ *temos*

$$\begin{aligned} P(X_{n+1} = s_j \,|\, X_0 = s_{i_0}, X_1 = s_{i_1}, \ldots, X_{n-1} = s_{i_{n1}}, X_n = s_i) \\ &= P(X_{n+1} = s_j | X_n = s_i) \\ &= P_{i,j}. \end{aligned}$$

Os elementos da matriz de transição P são chamados de probabilidades de transição. A probabilidade de transição $P_{i,j}$ é a probabilidade condicional de estar no estado s_j "amanhã"dado que estamos no estado s_i "hoje". O termo homogêneo é frequentemente descartado, e dado como certo quando se fala sobre cadeias de Markov. Por exemplo, o exemplo de passeio aleatório acima é uma cadeia de Markov, com espaço de estados $\{1,2,3,4\}$ e matriz de transição

$$\mathbf{P} = \begin{bmatrix} 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 \end{bmatrix}$$

Cada matriz de transição satisfaz:

$$P_{i,j} \geq 0 \text{ para todo } i, j \in \{1, \ldots, k\} \tag{3.1}$$

e

$$\sum_{j=1}^{k} P_{i,j} = 1 \text{ para todo } i \in \{1, \ldots, k\}. \tag{3.2}$$

A propriedade anterior é apenas o fato de que as probabilidades condicionais são sempre não negativas, e que somam 1, ou seja,

$$P(X_{n+1} = s_1 | X_n = s_i) + P(X_{n+1} = s_2 | X_n = s_i) + \cdots + P(X_{n+1} = s_k | X_n = s_i) = 1.$$

A seguir consideramos outra característica importante (além da matriz de transição) de uma cadeia de Markov $(X_0, X_1, \ldots)$, a distribuição inicial, que nos diz como a cadeia de Markov começa. A distribuição inicial é representada como um vetor linha $\mu^{(0)}$ dado por

$$\begin{aligned} \mu^{(0)} &= (\mu_1^{(0)}, \mu_2^{(0)}, \ldots, \mu_k^{(0)}) \\ &= (P(X_0 = s_1), P(X_0 = s_2), \ldots, P(X_0 = s_k)). \end{aligned}$$

Uma vez que $\mu^{(0)}$ representa uma distribuição de probabilidade, temos

$$\sum_{i=1}^{k} \mu_i^{(0)} = 1.$$

No exemplo de passeio aleatório acima, temos

$$\mu^{(0)} = (1,0,0,0).$$

Da mesma forma, deixamos os vetores linha $\mu^{(1)}, \mu^{(2)}, \ldots$ denotam as distribuições de a cadeia de Markov nos tempos $1,2,\ldots$ de modo que

$$\begin{aligned}\mu^{(n)} &= (\mu_1^{(n)}, \mu_2^{(n)}, \ldots, \mu_k^{(n)}) \\ &= (P(X_n = s_1), P(X_n = s_2), \ldots, P(X_n = s_k)).\end{aligned}$$

Para o exemplo do passeio aleatório, temos que

$$\mu^{(1)} = \left(0, \frac{1}{2}, 0, \frac{1}{2}\right).$$

Acontece que uma vez que conhecemos a distribuição inicial $\mu^{(0)}$ e a matriz de transição P, podemos calcular todas as distribuições $\mu^{(1)}, \mu^{(2)}, \ldots$ da cadeia de Markov. O seguinte resultado nos diz que isso é simplesmente uma questão de multiplicação de matrizes. Escrevemos P^n para a n-ésima potência da matriz P.

Teorema 3. *Para uma cadeia de Markov $(X_0, X_1, \ldots)$ com espaço de estado $\{s_1, \ldots, s_k\}$, distribuição inicial $\mu^{(0)}$ e matriz de transição P, temos para qualquer n que o distribuição $\mu^{(n)}$ no tempo n satisfaz*

$$\mu^{(n)} = \mu^{(0)} P^n.$$

Demonstração. Considere primeiro o caso $n = 1$. Obtemos, para $j = 1, \ldots, k$, que

$$\begin{aligned}\mu_j^{(1)} = P(X_1 = s_j) &= \sum_{i=1}^{k} P(X_0 = s_i, X_1 = s_j) \\ &= \sum_{i=1}^{k} P(X_0 = s_i) P(X_1 = s_j | X_0 = s_i) \\ &= \sum_{i=1}^{k} \mu_i^{(0)} P_{i,j} = (\mu^{(0)} P)_j\end{aligned}$$

onde $(\mu^{(0)}P)_j$ denota o j-ésimo elemento do vetor linha $\mu^{(0)}P$.

Portanto,

$$\mu^{(1)} = \mu^{(0)} P.$$

Para provar para o caso geral, usamos a indução. Fixe m, e suponha que o resultado é válido para $n = m$. Para $n = m+1$, obtemos

$$\begin{aligned}\mu_j^{(m+1)} &= P(X_{m+1} = s_j) = \sum_{i=1}^{k} P(X_m = s_i, X_{m+1} = s_j) \\ &= \sum_{i=1}^{k} P(X_m = s_i) P(X_{m+1} = s_j | X_m = s_i) \\ &= \sum_{i=1}^{k} \mu_i^{(m)} P_{i,j} = (\mu^{(m)} P)_j\end{aligned}$$

de modo que $\mu^{(m+1)} = \mu^{(m)} P$. Mas $\mu^{(m)} = \mu^{(0)} P^m$ pela hipótese de indução, então

$$\mu^{(m+1)} = \mu^{(m)} P = \mu^{(0)} P^m P = \mu^{(0)} P^{m+1}.$$

□

Exemplo 3 (**O tempo de Gotemburgo**). *Às vezes, é afirmado que a melhor maneira de prever o tempo de amanhã é simplesmente adivinhar que será o mesmo amanhã como é hoje. Se assumirmos que esta afirmação está correta, então é natural modelar o tempo como uma cadeia de Markov. Para simplificar, assumimos que existem apenas dois tipos de tempo: chuva e sol. Se o preditor acima estiver correto 75% do tempo (independentemente de o tempo de hoje ser chuva ou sol), então o tempo forma uma cadeia de Markov com espaço de estado $S = \{s_1, s_2\}$ (com s_1 = "chuva" e s_2 = "luz do sol") e matriz de transição*

$$\mathbf{P} = \begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix}.$$

Exemplo 4 (**O tempo de Los Angeles**). *Observe que no Exemplo 2, há uma simetria perfeita entre "chuva"e "sol", no sentido de que a probabilidade que o tempo de hoje vai persistir amanhã é o mesmo, independentemente do tempo de hoje. Isso pode ser razoavelmente realista em Gotemburgo, mas não em Los Angeles onde o sol é muito mais comum do que a chuva. Uma transição mais razoável matriz para o tempo de Los Angeles pode, portanto, ser (ainda com s_1 = "chuva"e s_2 = "luz do sol")*

$$\mathbf{P} = \begin{bmatrix} 0.50 & 0.50 \\ 0.10 & 0.90 \end{bmatrix}.$$

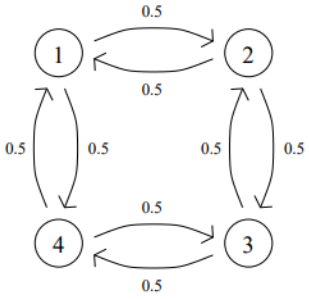


Figura 2

Exemplo 5 (**A Internet como uma cadeia de Markov**). *Imagine que você está navegando na Internet, e que cada vez que encontrar uma página da web, você clica em uma de seus hiperlinks escolhidos aleatoriamente (uniformemente). Se X_n denota onde você está depois n cliques, então $(X_0, X_1, \dots)$ pode ser descrito como uma cadeia de Markov com espaço de estado S igual ao conjunto de todas as páginas da web na Internet, e a matriz de transição P dada por*

$$P_{ij} = \begin{cases} \dfrac{1}{d_i}, & \text{se a página } s_i \text{ tiver um link para a página } s_j \\ 0, & \text{caso contrário} \end{cases}$$

onde d_i é o número de links da página s_i. (Para tornar esta cadeia bem definida, também precisamos definir o que acontece se não houver nenhum link de s_i. Nós podemos, por exemplo, defina $P_{ii} = 1$ (e $P_{ij} = 0$ para todo $i \neq j$) nesse caso, o que significa que quando você encontra uma página sem links, você fica preso.) cadeia de Markov complicada (especialmente em comparação com os Exemplos 2 e 3), mas no entanto, acabou por ser um modelo útil que, sob várias formas de simplificação suposições admite análises interessantes. Uma variante recente deste modelo é levar em consideração também a possibilidade de usar "botões voltar" em navegadores da web. No entanto, o resultado processo $(X_0, X_1, \dots)$ não é mais uma cadeia de Markov, desde o que acontece quando o botão voltar é pressionado não depende apenas do estado atual X_n, mas em geral também em $X_0, \dots, X_{n-1}$.

Uma maneira útil de imaginar uma cadeia de Markov é o chamado gráfico de transição. O gráfico de transição consiste em nós que representam os estados da cadeia de Markov, e setas entre os nós, representando probabilidades de transição. Isso é mais facilmente explicado apenas mostrando os gráficos de transição dos exemplos considerado até agora. Em todos os exemplos acima, bem como na Definição 1, a "regra"para obter X_{n+1} de X_n não mudou com o tempo. Em algumas situações, é mais realista, ou por outras razões mais desejáveis, para deixar essa regra mudar com o tempo. Esta nos traz ao tópico das cadeias de Markov não homogêneas, e o seguinte definição, que generaliza a Definição 2.1.

Aos meus pais, por nunca terem medido esforços para me proporcionar um ensino de qualidade durante todo o meu período escolar.

Definição 4. *Sejam $P^{(1)}, P^{(2)}, \ldots$ ser uma sequência de matrizes $k \times k$, cada uma das que satisfaz* (3.1) *e* (3.2). *Um processo aleatório $(X_0, X_1, \ldots)$ com espaço de estados finito $S = \{s_1, ..., s_k\}$ é dito ser uma cadeia de Markov não homogênea com matrizes de transição $P^{(1)}, P^{(2)}, \ldots$, se para todo n, todo $i, j \in \{1, \ldots, k\}$ e todos $i_0, \ldots, i_{n-1} \in \{1, \ldots, k\}$ nós temos*

$$\begin{aligned} P(X_{n+1} = s_j | X_0 = s_{i_0}, X_1 = s_{i_1}, \ldots, X_{n-1} = s_{i_{n-1}}, X_n = s_i) \\ = P(X_{n+1} = s_j | X_n = s_i) \\ = P_{i,j}^{(n+1)} \end{aligned}$$

Exemplo 6 (Um modelo refinado para o tempo de Gotemburgo). *Há muitas maneiras pelas quais o modelo bruto do Exemplo 2 pode ser feito mais realista. Uma maneira é levar em consideração as mudanças sazonais: não parece razoável ignorar se o calendário diz "janeiro"ou "julho"ao prever o tempo de amanhã. Para este fim, estendemos o espaço de estado para $\{s_1, s_2, s_3\}$, onde s_1 = "chuva" e s_2 = "luz do sol" como antes e s_3 = "neve". Sejam*

$$\mathbf{P_{verao}} = \begin{bmatrix} 0.75 & 0.25 & 0 \\ 0.25 & 0.25 & 0 \\ 0.50 & 0.50 & 0 \end{bmatrix} \text{ e } \mathbf{P_{inverno}} = \begin{bmatrix} 0.5 & 0.30 & 0.20 \\ 0.15 & 0.70 & 0.15 \\ 0.20 & 0.30 & 0.50 \end{bmatrix}.$$

e suponha que o tempo evolua de acordo com o P_{verao} em maio-setembro, e de acordo com $P_{inverno}$ em outubro-abril. Essa é uma cadeia de Markov homogênea que modela o tempo de Gotemburgo. Observe que em maio-setembro, o modelo se comporta exatamente como o do Exemplo 2, exceto por algum possível resíduo tempo de neve em 1ł de maio.

O seguinte resultado, que é uma generalização do Teorema 3, nos diz como para calcular as distribuições $\mu^{(1)}, \mu^{(2)}, \ldots$, nos momentos $1, 2, \ldots$ de uma cadeia de Markov não homogênea com distribuição inicial $\mu^{(0)}$ e matrizes de transição $P^{(1)}, P^{(2)}, \ldots$

Teorema 4. *Suponha que* $(X_0, X_1, \dots)$ *seja uma cadeia de Markov não homogênea com espaço de estado* $\{s_1, \dots, s_k\}$*, distribuição inicial* $\mu^{(0)}$ *e matrizes de transição* $P^{(1)}, P^{(2)}, \dots$*. Para qualquer n, então temos que*

$$\mu^{(n)} = \mu^{(0)} P^{(1)} P^{(2)} \dots P^{(n)}.$$

Demonstração. Segue por um cálculo semelhante ao da prova do Teorema 3. □

4 SIMULAÇÃO COMPUTACIONAL DE CADEIAS DE MARKOV

Uma questão fundamental em muitas aplicações práticas da teoria de Markov é o capacidade de simular cadeias de Markov em um computador. Este capítulo trata de como isso pode ser feito.

Como simulamos um Cadeia de Markov $(X_0, X_1, \dots)$ com determinado espaço de estado $S = \{s_1, \dots, s_k\}$, distribuição inicial $\mu^{(0)}$ e matriz de transição P? Considere variavéis aleatórias $U_0, U_1, \dots$ com distribuição uniforme no intervalo $[0,1]$ (chamaremos também de números aleatórios). Outros ingredientes principais são duas funções, que chamamos de **função de iniciação** e a **função de atualização**.

A função de iniciação $\Psi : [0,1] \to S$ é uma função do intervalo $[0,1]$ para o espaço de estado S, que usamos para gerar o valor inicial X_0. Nós presumimos:

1. Ψ é constante por partes (ou seja, que $[0,1]$ pode ser dividido em finitamente muitos subintervalos de tal forma que Ψ seja constante em cada intervalo)
2. para cada $s \in S$, o comprimento dos intervalos em que $\Psi(x) = s$ é igual a $\mu^{(0)}(s)$

Outra forma de declarar a propriedade $(2.)$ é que:

$$\int_0^1 I_{\{\Psi(x)=s\}} dx = \mu^{(0)}(s) \tag{4.1}$$

para cada $s \in S$; aqui, $I_{\{\Psi(x)=s\}}$ é a chamada função indicadora de $\{\Psi(x) = s\}$, o que significa que:

$$I_{\{\Psi(x)=s\}} = \begin{cases} 1, & \text{se} \quad \Psi(x) = s, \\ 0, & \text{se} \quad \Psi(x) \neq s \end{cases}$$

Desde que tenhamos tal função Ψ, podemos gerar X_0 a partir do primeiro número aleatório U_0 definindo $X_0 = \Psi(U_0) = s$. Isso dá a distribuição correta de X_0, porque para qualquer $s \in S$ obtemos

$$P(X_0 = s) = P(\Psi(U_0) = s) = \int_0^1 I_{\{\Psi(x)=s\}} dx = \mu^{(0)}.$$

Portanto, chamamos Ψ uma função de iniciação válida para a cadeia de Markov $(X_0, X_1, \dots)$ se (2.) vale para todos $s \in S$. As funções de iniciação válidas são fáceis de construir.

Com $S = \{s_1, ..., s_k\}$ e distribuição inicial $\mu^{(0)}$, podemos definir

$$\Psi(x) = \begin{cases} s_1, & \text{se} \quad x \in [0, \mu^{(0)}(s_1)) \\ s_2, & \text{se} \quad x \in [\mu^{(0)}(s_1), \mu^{(0)}(s_1) + \mu^{(0)}(s_2)) \\ \vdots & \\ s_i, & \text{se} \quad x \in \left[\sum_{j=1}^{i-1} \mu^{(0)}(s_j), \sum_{j=1}^{i} \mu^{(0)}(s_j) \right) \\ \vdots & \\ s_k, & \text{se} \quad x \in \left[\sum_{j=1}^{k-1} \mu^{(0)}(s_j), 1 \right] \end{cases} \tag{4.2}$$

Precisamos verificar se esta escolha de Ψ satisfaz as propriedades $(1.)$ e $(2.)$ acima. A propriedade $(1.)$ é óbvia. Quanto à propriedade $(2.)$, basta verificar que (4.1) é válido para cada estado. Isso se mantém, uma vez que

$$\int_0^1 I_{\{\Psi(x)=s_1\}} dx = \sum_{j=1}^{i} \mu^{(0)}(s_j) - \sum_{j=1}^{i-1} \mu^{(0)}(s_j) = \mu^{(0)}(s_i) \quad \text{para } i = 1, \ldots, k.$$

Isso significa que Ψ conforme definido em (4.2) é uma função de iniciação válida para a cadeia de Markov $(X_0, X_1, \ldots)$.

Portanto, agora sabemos como gerar o valor inicial X_0. Se descobrirmos como gerar X_{n+1} de X_n para qualquer n, então podemos usar este procedimento iterativamente para obter toda a cadeia $(X_0, X_1, \ldots)$. Para ir de X_n a X_{n+1}, usaremos o número aleatório U_{n+1} e uma função de atualização $\Phi : S \times [0,1] \to S$, que toma como entrada um estado $s \in S$ e um número entre 0 e 1, e produz outro estado $s \in S$ como saída. Da mesma forma que para a função de iniciação Ψ, nós precisamos Φ para obedecer a certas propriedades, a saber

1. que para s_i fixo, a função $\Phi(s_i, x)$ é constante por partes (quando vista como uma função de x), e
2. que para cada s_i fixo, $s_j \in S$, o comprimento total dos intervalos em que $\Phi(s_i, x) = s_j$ é igual a $P_{i,j}$.

Novamente, quanto à função de iniciação, a propriedade $(2.)$ pode ser reescrita como

$$\int_0^1 I_{\{\phi(s_i,x)=s_j(x)\}} dx = P_{i,j} \quad \text{para todo } s_i, s_j \in S. \tag{4.3}$$

Se a função de atualização ϕ satisfizer (4.3), então

$$\begin{aligned} P(X_{n+1} = s_j | X_n = s_i) &= P(\phi(s_i, U_{n+1}) = s_j | X_n = s_i) \\ &= P(\phi(s_i, U_{n+1}) = s_j) \\ &= \int_0^1 I_{\{\phi(s_i,x)=s_j\}}(x)dx \end{aligned} \tag{4.4}$$

A razão pela qual o condicionamento em (4.4) pode ser descartado é que U_{n+1} é independente de $(U_0, \ldots, U_n)$ e, portanto, também de X_n. O mesmo argumento mostra que a probabilidade condicional permanece a mesma se condicionarmos mais adiante os valores $(X_0, X_1, \ldots, X_{n-1})$. Portanto, isso dá uma simulação correta do Cadeia de Markov. Uma função ϕ satisfazendo (4.4) é, portanto, considerada uma função válida função de atualização para a cadeia de Markov $(X_0, X_1, \ldots)$.

Resta construir uma função de atualização válida, mas isso não é mais difícil do que a construção de uma função de iniciação válida: Defina, para cada $s_i \in S$,

$$\phi(s_i, x) = \begin{cases} s_1, & \text{se} \quad x \in [0, P_{i,1}) \\ s_2, & \text{se} \quad x \in [P_{i,1}, P_{i,1} + P_{i,2}) \\ \vdots & \\ s_j, & \text{se} \quad x \in \left[\sum_{l=1}^{j-1} P_{i,l}, \sum_{l=1}^{j} P_{i,l} \right) \\ \vdots & \\ s_k, & \text{se} \quad x \in \left[\sum_{l=1}^{k-1} P_{i,l}, 1 \right] \end{cases} \tag{4.5}$$

Para ver que esta é uma função de atualização válida, note que para qualquer $s_i, s_j \in S$, temos

$$\int_0^1 I_{\{\phi(s_i,x)=s_j\}} dx = \sum_{l=1}^{j} P_{i,l} - \sum_{l=1}^{j-1} P_{i,l} = P_{i,j}$$

Assim, temos uma receita completa para simular uma cadeia de Markov: Primeiro construir funções válidas de iniciação e atualização ψ e ϕ (por exemplo, como em (4.2) e (4.5)),

e então definir

$$X_0 = \psi(U_0)$$
$$X_1 = \phi(X_0, U_1)$$
$$X_2 = \phi(X_1, U_2)$$
$$X_3 = \phi(X_2, U_3)$$

e assim por diante.

Exemplo 7 (**Simulando o clima de Maceió**). *Considere a cadeia de Markov no Exemplo* 2*, cujo espaço de estado é* $S = \{s_1, s_2\}$ *onde* s_1 = *"chuva"e* s_2 = *"luz do sol", e cuja matriz de transição é dada por*

$$\mathbf{P} = \begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix}.$$

Suponha que iniciemos a cadeia de Markov em um dia chuvoso, de modo que $\mu^{(0)} = (1,0)$*. Para simular esta cadeia de Markov usando o esquema acima, aplicamos* (4.2) *e* (4.5) *para obter a função de iniciação*

$$\psi(x) = s_1 \quad \textit{para todo } x$$

e função de atualização fornecida por

$$\phi(s_1, x) = \begin{cases} s_1, & se \quad x \in [0, 0.75), \\ s_2, & se \quad x \in [0.75, 1] \end{cases}$$

e

$$\phi(s_2, x) = \begin{cases} s_1, & se \quad x \in [0, 0.25), \\ s_2, & se \quad x \in [0.25, 1] \end{cases}$$

Antes de encerrar este capítulo, vamos finalmente apontar como o método acima pode ser generalizado para lidar com a simulação de cadeias de Markov não-homogêneas. Seja $(X_0, X_1, \dots)$ Uma cadeia de Markov não-homogênea com espaço de estado $S = \{s_1, \dots, s_k\}$, distribuição inicial $\mu^{(0)}$, e matrizes de transição $P^{(0)}, P^{(1)}, \dots$ Podemos então obter a função de iniciação ψ e o valor inicial X_0 como no caso homogêneo. A atualização é feita de forma semelhante ao homogêneo caso, exceto que, uma vez que a cadeia não é homogênea, precisamos de vários atualizando funções $\phi^{(1)}, \phi^{(2)}, \dots$, e para estes precisamos ter

$$\int_0^1 I_{\{\phi^{(n)}(s_i,x)=s_j\}}(x)dx = P_{i,j}^{(n)}$$

para cada n e cada $s_i, s_j \in S$. Tais funções podem ser obtidas pela generalização de (4.5):

$$\phi^{(n)}(s_i,x) = \begin{cases} s_1, & \text{se} \quad x \in [0, P_{i,1}^{(n)}) \\ s_2, & \text{se} \quad x \in [P_{i,1}^{(n)}, P_{i,1}^{(n)} + P_{i,2}^{(n)}) \\ \vdots & \\ s_j, & \text{se} \quad x \in \left[\sum_{l=1}^{j-1} P_{i,l}^{(n)}, \sum_{l=1}^{j} P_{i,l}^{(n)}\right) \\ \vdots & \\ s_k, & \text{se} \quad x \in \left[\sum_{l=1}^{k-1} P_{i,l}^{(n)}, 1\right] \end{cases}$$

A cadeia de Markov não-homogênea é, então, simulada pela configuração

$$\begin{aligned} X_0 &= \psi(U_0) \\ X_1 &= \phi^{(1)}(X_0, U_1) \\ X_2 &= \phi^{(2)}(X_1, U_2) \\ X_3 &= \phi^{(3)}(X_2, U_3) \end{aligned}$$

e assim por diante.

5 CADEIAS DE MARKOV IRREDUTÍVEIS E APERIÓDICAS

Neste capítulo, discutiremos duas condições importantes em cadeias de Markov: **irredutibilidade** e **aperiodicidade**. Essas condições são de importância central na teoria de Cadeias de Markov e, em particular, eles desempenham um papel fundamental no estudo de distribuições estacionárias, que é o tópico do Capítulo 6.

Começamos com a irredutibilidade, que, falando vagamente, é a propriedade que "Todos os estados da cadeia de Markov podem ser alcançados de todos os outros". Mais precisamente, considere uma cadeia de Markov $(X_0, X_1, \dots)$ com espaço de estado $S = \{s_1, \dots, s_k\}$ e a matriz de transição P. Dizemos que um estado s_i se comunica com outro estado s_j, escrevendo $s_i \to s_j$, se a cadeia tem probabilidade positiva de alguma vez alcançar s_j quando partimos de s_i. Em outras palavras, s_i se comunica com s_j se existe um n que depende dos estados i e j tal que

$$P(X_{m+n} = s_j \mid X_m = s_i) > 0.$$

Esta probabilidade é independente de m (devido à homogeneidade da cadeia de Markov), e é igual a $(P^n)_{ij}$. Se $s_i \to s_j$ e $s_j \to s_i$, dizemos que os estados s_i e s_j se intercomunicam e escrevemos $s_i \leftrightarrow s_j$. Isso nos leva diretamente à definição de irredutibilidade.

Definição 5. *Outra forma de expressar a definição seria dizer que a cadeia é irredutível se para qualquer $s_i, s_j \in S$ podemos encontrar um n tal que $(P^n)_{ij} > 0$.*

Uma maneira fácil de verificar se uma cadeia de Markov é irredutível é olhar para seu gráfico de transição, e observar se cada estado existe uma sequência de setas que levam a qualquer outro estado. Uma olhada na Figura 2, portanto, revela que o Cadeias de Markov nos Exemplos 2 e 3, bem como o exemplo de passeio aleatório na Figura 1, são todos irredutíveis. Vamos a seguir dar uma olhada em um exemplo que não é irredutível:

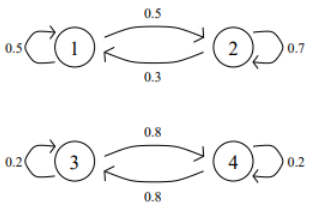


Figura 3

Exemplo 8 (Uma cadeia de Markov redutível). *Considere uma cadeia de Markov* $(X_0, X_1, \dots)$ *com espaço de estado* $S = \{1,2,3,4\}$ *e matriz de transição*

$$\mathbf{P} = \begin{bmatrix} 0.5 & 0.5 & 0 & 0 \\ 0.3 & 0.7 & 0 & 0 \\ 0 & 0 & 0.2 & 0.8 \\ 0 & 0 & 0.8 & 0.2 \end{bmatrix}.$$

Ao dar uma olhada em seu gráfico de transição (veja a Figura 3*), vemos imediatamente que se a cadeia começa no estado* 1 *ou estado* 2*, então é restrita aos estados* 1 *e* 2 *para sempre. Da mesma forma, se começar no estado* 3 *ou* 4*, então nunca poderá deixar o subconjunto* $\{3,4\}$ *do espaço de estado. Portanto, a cadeia é redutível. Observe que se a cadeia começa no estado* 1 *ou estado* 2*, ela se comporta exatamente como se fosse eram uma cadeia de Markov com espaço de estado* $\{1,2\}$ *e matriz de transição*

$$\begin{bmatrix} 0.5 & 0.5 \\ 0.7 & 0.3 \end{bmatrix}.$$

Se começar no estado 3 *ou* 4*, então se comporta como uma cadeia de Markov com espaço de estado* $\{3,4\}$ *e matriz de transição*

$$\begin{bmatrix} 0.2 & 0.8 \\ 0.8 & 0.2 \end{bmatrix}.$$

Isso ilustra uma característica das cadeias de Markov redutíveis, que também explica o termo "redutível": Se uma cadeia de Markov é redutível, então a análise de seu comportamento de longo prazo pode ser reduzido à análise do comportamento de longo prazo de uma ou mais cadeias de Markov com espaço de estado menor.

Passamos a considerar o conceito de aperiodicidade. Para um finito ou infinito conjunto $\{a_1, a_2, \dots\}$ de inteiros positivos, escrevemos $mdc\{a_1, a_2, \dots\}$ para o maior divisor comum de $a_1, a_2, \dots$ O período $d(s_i)$ de um estado $s_i \in S$ é definido como

$$d(s_i) = mdc\{n \geq 1 : (P^n)_{ii} > 0\}.$$

Em palavras, o período de s_i é o maior divisor comum do conjunto de vezes que a cadeia pode retornar (ou seja, tem probabilidade positiva de retornar) para s_i, dado que começamos com $X_0 = s_i$. Se $d(s_i) = 1$, então dizemos que o estado s_i é aperiódico

Definição 6. *Uma cadeia de Markov é considerada aperiódica se todos os seus estados forem* ***aperiódico****. Caso contrário, a cadeia é considerada* ***periódica****.*

Considere, por exemplo, o Exemplo 2 (o clima de Gotemburgo). Veja que, independentemente de o tempo hoje ser chuva ou sol, temos para qualquer n que a probabilidade de ter o mesmo clima n dias depois é estritamente positivo. Ou, expresso de forma mais compacta: $(P^n)_{ii} > 0$ para todo n e todos os estados s_i. Isso obviamente implica que a cadeia de Markov no Exemplo 2 é aperiódico. Claro, o mesmo raciocínio se aplica ao Exemplo 3 (o Los Tempo de Angeles).

Por outro lado, vamos considerar o exemplo de passeio aleatório na Figura 1, onde o caminhante aleatório está no canto v_1 no tempo 0. Claramente, ele tem que pegar um número par de etapas para voltar à v_1. Isso significa que $(P^n)_{1,1} > 0$ apenas para $n = 2,4,6,\ldots$ Portanto,

$$mdc\{n \geq 1 : (P^n)_{ii} > 0\} = mdc\{2,4,6,\ldots\} = 2$$

e a cadeia é, portanto, periódica.

Uma razão para a utilidade da aperiodicidade é o seguinte resultado:

Teorema 5. *Suponha que tenhamos uma cadeia de Markov aperiódica $(X_0, X_1, \ldots)$ com espaço de estado $S = \{s_1, \ldots, s_k\}$ e matriz de transição P. Então existe um $N < \infty$ tal que*

$$(P^n)_{ii} > 0$$

para todo $i \in \{1, \ldots, k\}$ e todo $n \geq N$. Para provar este resultado, devemos tomar emprestado o seguinte lema da teoria dos números

Lema 1. *Seja $A = \{a_1, a_2, \ldots\}$ um conjunto de inteiros positivos que é*

1. *sem rede, o que significa que $mdc\{a_1, a_2, \ldots\} = 1$, e*
2. *fechado sob adição, o que significa que se $a \in A$ e $b \in A$, então $a + b \in A$.*

Então existe um inteiro $N < \infty$ tal que $n \in A$ para todo $n \geq N$

Demonstração. (do Teorema 5) Para $s_i \in S$, seja $A_i = \{n \geq 1 : (P^n)_{ii} > 0\}$, de modo que em outras palavras, A_i é o conjunto de tempos de retorno possíveis para o estado s_i a partir de s_i. Assumimos que a cadeia de Markov é aperiódica e, portanto, o estado s_i é aperiódico, de modo

que A_i é sem rede. Além disso, A_i está fechada sob adição, pelo seguinte motivo: Se $a,b \in A_i$, então $P(X_a = s_i \mid X_0 = s_i) > 0$ e $P(X_{a+b} = s_i \mid X_a = s_i) > 0$. Isso implica que

$$\begin{aligned} P(X_{a+b} = s_i \mid X_0 = s_i) &\geq P(X_a = s_i, X_{a+b} = s_i \mid X_0 = s_i) \\ &= P(X_a = s_i \mid X_0 = s_i) \cdot P(X_{a+b} = s_i \mid X_a = s_i) \\ &> 0 \end{aligned}$$

de modo que $a+b \in A_i$. Em resumo, A_i satisfaz as premissas $(1.)$ e $(2.)$ do Lema 1, que portanto, implica que existe um inteiro $N_i < \infty$ tal que $(P^n)_{ii} > 0$ para todos $n \geq N_i$. O Teorema 5 agora segue com $N = max\{N_1, \ldots, N_k\}$. □

Ao combinar aperiodicidade e irredutibilidade, obtemos o seguinte importante resultado, que será usado no próximo capítulo para provar o teorema da convergência da cadeia de Markov (Teorema 7).

Teorema 6. *Seja $(X_0, X_1, \ldots)$ Uma cadeia de Markov irredutível e aperiódica com espaço de estado $S = \{s_1, \ldots, s_k\}$ e matriz de transição P. Então existe um $M < \infty$ tal que $(P^n)_{ij} > 0$ para todo $i, j \in \{1, \ldots, k\}$ e todo $n \geq M$.*

Demonstração. Pela aperiodicidade assumida e Teorema 4.1, existe um número inteiro $N < \infty$ tal que $(P^n)_{ii} > 0$ para todo $i \in \{1, \ldots, k\}$ e todo $n \geq N$. Fixe dois estados $s_i, s_j \in S$. Pela irredutibilidade assumida, podemos encontrar algum n_{ij} tal que $(P^{n_{ij}})_{ij} > 0$. Seja $M_{ij} = N + n_{ij}$. Para qualquer $m \geq M_{ij}$, temos

$$\begin{aligned} P(X_m = s_j \mid X_0 = s_i) &\geq P(X_{m-n_{ij}} = s_i, X_m = s_j \mid X_0 = s_i) \\ &= P(X_{m-n_{ij}} = s_i \mid X_0 = s_i) P(X_m = s_j \mid X_{m-n_{ij}} = s_i) \\ &> 0 \end{aligned}$$

(o primeiro fator na segunda linha de é positivo porque $m - n_{ij} \geq N$, e a segunda é positiva pela escolha de n_{ij}. Portanto, mostramos que $(P^m)_{ij} > 0$ para todo $m \geq M_{ij}$. O corolário agora segue com

$$M = max\{M_{1,1}, M_{1,2}, \ldots, M_{1,k}, M_{2,1}, \ldots, M_{2,k}, \ldots, M_{k,k}\}$$

□

6 DISTRIBUIÇÕES ESTACIONÁRIAS

Neste capítulo, consideramos uma das questões centrais da teoria de Markov: a assintótica para o comportamento de longo prazo das cadeias de Markov. O que podemos dizer sobre um Cadeia de Markov que está em execução há muito tempo?

Se $(X_0, X_1, \dots)$ for qualquer cadeia de Markov não trivial, não podemos obter resultados sobre a convergência de X_n para um limite. No entanto, podemos esperar que a distribuição de X_n se estabeleça até um limite. Este é realmente o caso se a cadeia de Markov é irredutível e aperiódica, que é o principal resultado neste capítulo, o chamado teorema da convergência da cadeia de Markov (Teorema 8).

Definição 7. *Seja $(X_0, X_1, \dots)$ uma cadeia de Markov com espaço de estado $\{s_1, \dots, s_k\}$ e matriz de transição P. Um vetor linha $\pi = (\pi_1, \dots, \pi_k)$ é dito ser uma distribuição estacionária para a cadeia de Markov, se*

1. $\pi_i \geq 0$ *para* $i = 1, \dots, k$ *e* $\sum_{i=1}^{k} \pi_i = 1$,
2. $\pi P = \pi$, *significa que* $\sum_{i=1}^{k} \pi_i P_{ij} = \pi_j$ *para todo* $j \in \{1, \dots, k\}$.

Propriedade $(1.)$ *significa simplesmente que* π *deve descrever uma distribuição de probabilidade em* $\{s_1, \dots, s_k\}$. *A propriedade* $(2.)$ *implica que se a distribuição inicial* $\mu^{(0)}$ *for igual a* π, *então a distribuição* $\mu^{(1)}$ *da cadeia no tempo* 1 *satisfaz*

$$\mu^{(1)} = \mu^{(0)} P = \pi P = \pi,$$

e iterando vemos que $\mu^{(n)} = \pi$ *para todo n.*

Uma vez que a definição de uma distribuição estacionária realmente depende apenas do matriz de transição P, também às vezes dizemos que uma distribuição π *satisfazendo a as suposições* $(1.)$ *e* $(2.)$ *na definição* 5 *são estacionárias para a matriz P (em vez do que para a cadeia de Markov).*

O restante deste capítulo tratará de três questões: a existência de distribuições estacionárias, a unicidade das distribuições estacionárias e a convergência para a estacionariedade a partir de qualquer distribuição inicial. Vamos trabalhar sob as condições introduzidas no

capítulo anterior (irredutibilidade e aperiodicidade), embora para alguns dos resultados essas condições possam ser relaxadas um pouco. Começamos com a questão da existência.

Teorema 7 (Existência de distribuições estacionárias). *Para qualquer irredutível e aperiódica cadeia de Markov, existe pelo menos uma distribuição estacionária*

Para provar este teorema da existência, primeiro precisamos provar um lema sobre tempos de rebatida para cadeias de Markov. Se uma cadeia de Markov $(X_0, X_1, \dots)$ com espaço de estados $\{s_1, \dots, s_k\}$ e matriz de transição P começa no estado s_i, então podemos definir o tempo de rebatida

$$T_{ij} = min\{n \geq 1 : X_n = s_j\}$$

com a convenção de que $T_{ij} = \infty$ se a cadeia de Markov nunca visita s_j. Também definiremos tempo médio de rebatida

$$\tau_{ij} = E[T_{ij}]$$

Isso significa que τ_{ij} é o tempo esperado até chegarmos ao estado s_j, a partir do estado s_i. Para o caso $i = j$, chamamos τ_{ii} o tempo médio de retorno para o estado s_i. Enfatizamos que ao lidar com o tempo de rebatida τ_{ij}, há sempre a suposição implícita de que $X_0 = s_i$.

Lema 2. *Para qualquer cadeia de Markov aperiódica e irredutível com espaço de estado $S = \{s_1, \dots, s_k\}$ e matriz de transição P, temos para quaisquer dois estados $s_i, s_j \in S$ que se a cadeia começa no estado s_i, então*

$$P(T_{ij} < \infty) = 1 \tag{6.1}$$

Além disso, o tempo médio de acerto τ_{ij} é finito, ou seja,

$$E[T_{ij}] < \infty. \tag{6.2}$$

Demonstração. Pelo Corolário 1, podemos encontrar um $M < \infty$ tal que $(P^M)_{ij} > 0$ para todos $i, j \in \{1, \dots, k\}$. Fixe tal M, defina

$$\alpha = min\{(P^M)_{ij} : i, j \in \{1, \dots, k\}\},$$

e note que $\alpha > 0$. Fixe dois estados s_i e s_j como no lema, e suponha que a cadeia começa em s_i.

Claramente,

$$P(T_{ij} > M) \leq P(X_M \neq s_j) \leq 1 - \alpha$$

Além disso, dado tudo o que aconteceu até o momento M, temos probabilidade condicional de pelo menos α de atingir o estado s_j no tempo $2M$, de modo que:

$$\begin{aligned} P(T_{ij} > 2M) &= P(T_{ij} > M) \cdot P(T_{ij} > 2M \mid T_{ij} > M) \\ &\leq P(T_{ij} > M) \cdot P(X_{2M} \neq s_j \mid T_{ij} > M) \\ &\leq (1-\alpha)^2 \end{aligned}$$

Iterando este argumento, obtemos para qualquer l que

$$\begin{aligned} P(T_{ij} > lM) = P(T_{ij} > M) &\cdot P(T_{ij} > 2M \mid T_{ij} > M) \cdots \\ &\cdots P(T_{ij} > lM \mid T_{ij} > (l-1)M) \\ &\leq (1-\alpha)^l, \end{aligned}$$

que tende a 0 quando $l \to \infty$. Logo, $P(T_{ij} = \infty) = 0$, então (6.1) é estabelecido. Para provar (6.2), usamos a fórmula para a expectativa, obtemos

$$\begin{aligned} E[T_{ij}] &= \sum_{n=1}^{\infty} P(T_{ij} \geq n) = \sum_{n=0}^{\infty} P(T_{ij} > n) \qquad (6.3) \\ &= \sum_{l=0}^{\infty} \left(\sum_{n=lM}^{(l+1)M-1} P(T_{ij} > n) \right) \\ &\leq \sum_{l=0}^{\infty} \left(\sum_{n=lM}^{(l+1)M-1} P(T_{ij} > lM) \right) = M \sum_{l=0}^{\infty} P(T_{ij} > lM) \\ &\leq M \sum_{l=0}^{\infty} (1-\alpha)^l = M \frac{1}{1-(1-\alpha)} = \frac{M}{\alpha} < \infty. \end{aligned}$$

□

Vamos inciar a prova do teorema 7.

Demonstração. Escreva, como de costume, $(X_0, X_1, \dots)$ Para a cadeia de Markov, $S = \{s_1, \dots, s_k\}$ para o espaço de estados e P para a matriz de transição. Suponha que a cadeia começa no estado s_1, e define, para $i \in \{1, \dots, k\}$

$$\rho_i = \sum_{n=0}^{\infty} P(X_n = s_i, T_{1,1} > n)$$

de modo que, em outras palavras, ρ_i é o número esperado de visitas ao estado i até o momento $T_{1,1}-1$. Como o tempo de retorno médio $E[T_{1,1}] = \tau_{1,1}$ é finito, e $\rho_i < \tau_{1,1}$, vejamos que ρ_i também é finito. Nosso candidato a uma distribuição estacionária é

$$\pi = (\pi_1, \ldots, \pi_k) = \left(\frac{\rho_1}{\tau_{1,1}}, \frac{\rho_2}{\tau_{1,1}}, \ldots, \frac{\rho_k}{\tau_{1,1}} \right).$$

Precisamos verificar se esta escolha de π satisfaz as condições $(1.)$ e $(2.)$ da definição 5. Primeiro mostramos que a relação $\sum_{i=1}^{k} \pi_i P_{ij} = \pi_j$ na condição $(2.)$ vale para $j \neq 1$ (o caso $j = 1$ será tratado separadamente).

$$\begin{aligned}
\pi_j = \frac{\rho_j}{\tau_{1,1}} &= \frac{1}{\tau_{1,1}} \sum_{n=0}^{\infty} P(X_n = s_j, T_{1,1} > n) \\
&= \frac{1}{\tau_{1,1}} \sum_{n=1}^{\infty} P(X_n = s_j, T_{1,1} > n) && (6.4) \\
&= \frac{1}{\tau_{1,1}} \sum_{n=1}^{\infty} P(X_n = s_j, T_{1,1} > n-1) && (6.5) \\
&= \frac{1}{\tau_{1,1}} \sum_{n=1}^{\infty} \sum_{i=1}^{k} P(X_{n-1} = s_i, T_{1,1} > n-1) \cdot P(X_n = s_j \mid X_{n-1} = s_i) \\
&= \frac{1}{\tau_{1,1}} \sum_{n=1}^{\infty} \sum_{i=1}^{k} P_{i,j} \cdot P(X_{n-1} = s_i, T_{1,1} > n-1) && (6.6) \\
&= \frac{1}{\tau_{1,1}} \sum_{i=1}^{k} P_{i,j} \sum_{n=1}^{\infty} P(X_{n-1} = s_i, T_{1,1} > n-1) \\
&= \frac{1}{\tau_{1,1}} \sum_{i=1}^{k} P_{i,j} \sum_{m=0}^{\infty} P(X_m = s_i, T_{1,1} > m) \\
&= \frac{\sum_{i=1}^{k} \rho_i P_{i,j}}{\tau_{1,1}} = \sum_{i=1}^{k} \pi_i P_{i,j} && (6.7)
\end{aligned}$$

onde nas linhas (6.4), (6.5) e (6.6) usamos a suposição de que $j \neq 1$; observe também que (6.6) usa o fato de que o evento $\{T_{1,1} > n-1\}$ é determinado unicamente pelo variáveis $X_0, \ldots, X_{n-1}$.

A seguir, verificamos a condição $(2.)$ também para o caso $j = 1$. Observe primeiro

que $\rho_1 = 1$; isso é imediato da definição de ρ_i. Nós temos

$$\begin{aligned}
\rho_1 = 1 = P(T_{1,1} < \infty) &= \sum_{n=1}^{\infty} P(T_{1,1} = n) \\
&= \sum_{n=1}^{\infty} \sum_{i=1}^{k} P(X_{n-1} = s_i, T_{1,1} = n) \\
&= \sum_{n=1}^{\infty} \sum_{i=1}^{k} P(X_{n-1} = s_i, T_{1,1} > n-1) \cdot P(X_n = s_1 \mid X_{n-1} = s_i) \\
&= \sum_{n=1}^{\infty} \sum_{i=1}^{k} P_{i,1} \cdot P(X_{n-1} = s_i, T_{1,1} > n-1) \\
&= \sum_{i=1}^{k} P_{i,1} \sum_{n=1}^{\infty} P(X_{n-1} = s_i, T_{1,1} > n-1) \\
&= \sum_{i=1}^{k} P_{i,1} \sum_{m=0}^{\infty} P(X_m = s_i, T_{1,1} > m) \\
&= \sum_{i=1}^{k} \rho_i P_{i,1}.
\end{aligned}$$

Portanto,

$$\pi_1 = \frac{\rho_1}{\tau_{1,1}} = \sum_{i=1}^{k} \frac{\rho_i P_{i,1}}{\tau_{1,1}} = \sum_{i=1}^{k} \pi_i P_{i,1}$$

Ao combinar isso com (6.7), estabelecemos que a condição (2.) é válida para nossa escolha de π. Resta mostrar que a condição (1.) também é válida. Que $\pi_i \geq 0$ para $i \in \{1, \ldots, k\}$ é imediato. Para ver que $\sum_{i=1}^{k} \pi_i = 1$ também é válido, observe que

$$\begin{aligned}
\tau_{1,1} = E[T_{1,1}] &= \sum_{n=0}^{\infty} P(T_{1,1} > n) \qquad (6.8) \\
&= \sum_{n=0}^{\infty} \sum_{i=1}^{k} P(X_n = s_i, T_{1,1} > n) \\
&= \sum_{i=1}^{k} \sum_{n=0}^{\infty} P(X_n = s_i, T_{1,1} > n) \\
&= \sum_{i=1}^{k} \rho_i
\end{aligned}$$

(onde a equação (6.8) usa (6.3)) de modo que

$$\sum_{i=1}^{k} \pi_i = \frac{1}{\tau_{1,1}} \sum_{i=1}^{k} \rho_i = 1, \text{ a condição } (1.) \text{ é verificada.}$$

□

Devemos continuar a considerar o comportamento assintótico da distribuição $\mu^{(n)}$ de uma cadeia de Markov com distribuição inicial arbitrária $\mu^{(0)}$. Para estabelecer o principal resultado (Teorema 7), precisamos definir o que significa uma sequência de distribuições de probabilidade $\nu^{(1)}, \nu^{(2)}, \ldots$ convergir para outra distribuição de probabilidade ν, e para esse fim é útil ter uma métrica sobre distribuições de probabilidade. Existem várias dessas métricas; aquele que é útil aqui é o chamada **distância de variação total**.

Definição 8. *Se $\nu^{(1)} = (\nu_1^{(1)}, \ldots, \nu_k^{(1)})$ e $\nu^{(2)} = (\nu_1^{(2)}, \ldots, \nu_k^{(2)})$ são distribuições de probabilidade em $S = \{s_1, \ldots, s_k\}$, então definimos a distância de variação total entre $\nu^{(1)}$ e $\nu^{(2)}$ como*

$$d_{TV}(\nu^{(1)}, \nu^{(2)}) = \frac{1}{2} \sum_{i=1}^{k} \mid \nu_i^{(1)} - \nu_i^{(2)} \mid . \tag{6.9}$$

Se $\nu^{(1)}, \nu^{(2)}, \ldots$ e ν são distribuições de probabilidade em S, então dizemos que $\nu^{(n)}$ converge para ν na variação total quando $n \to \infty$, escrevendo $\nu^{(n)} \overset{TV}{\to} \nu$, se

$$\lim_{n \to \infty} d_{TV}(\nu^{(n)}, \nu) = 0.$$

A constante $1/2$ em (6.9) é projetada para fazer a variação total da distância de d_{TV} tomar valores entre 0 e 1. Na ausência dessa contante, d_{TV} tomaria valores entre 0 e 2 devido a desigualdade triangular. A variação total de distância também tem a interpretação

$$d_{TV}(\nu^{(1)}, \nu^{(2)}) = max_{A \subseteq S} \mid \nu^{(1)}(A) - \nu^{(2)}(A) \mid \tag{6.10}$$

Em palavras, a distância de variação total entre $\nu^{(1)}$ e $\nu^{(2)}$ é a diferença máxima entre as probabilidades que as duas distribuições atribuem a qualquer evento.

Agora estamos prontos para apresentar o principal resultado sobre convergência para estacionariedade.

Teorema 8 (**Teorema de convergência da cadeia de Markov**). *Seja $(X_0, X_1, \ldots)$ uma cadeia de Markov aperiódica e irredutível com espaço de estado $S = \{s_1, \ldots, s_k\}$, matriz de transição P e distribuição inicial arbitrária $\mu^{(0)}$. Então, para qualquer distribuição π que é estacionária para a matriz de transição P, temos*

$$\mu^{(n)} \overset{TV}{\to} \pi. \tag{6.11}$$

O que o teorema diz é que se executarmos uma cadeia de Markov por um período suficientemente longo de tempo *n*, então, independentemente de qual foi a distribuição inicial, a

distribuição no tempo n estará próximo da distribuição estacionária π.

Para a prova, usaremos o chamado argumento de acoplamento; acoplamento é um das técnicas mais úteis e elegantes em probabilidade contemporânea.

Demonstração. Ao estudar o comportamento de $\mu^{(n)}$, podemos assumir que $(X_0, X_1, \dots)$ foi obtido pelo método de simulação descrito no Capítulo 3, ou seja,

$$\begin{aligned} X_0 &= \psi_{\mu^{(0)}}(U_0) \\ X_1 &= \phi(X_0, U_1) \\ X_2 &= \phi(X_1, U_2) \\ &\vdots \end{aligned}$$

onde $\psi_{\mu^{(0)}}$ é uma função de iniciação válida para $\mu^{(0)}$, ϕ é uma função de atualização válida para P e $(U_0, U_1, \dots)$ é um $i.i.d.$ sequência de variáveis aleatórias uniforme em $[0, 1]$.

A seguir, apresentamos uma segunda cadeia de Markov $(X_0, X_1, \dots)$ permitindo ψ_π ser uma função de iniciação válida para a distribuição π, permitindo $(U_0, U_1, \dots)$ ser outra sequência $i.i.d.$ (independente de $(U_0, U_1, \dots)$) de variáveis aleatórias uniformes [0, 1], donde

$$\begin{aligned} X'_0 &= \psi_\pi(U_0) \\ X'_1 &= \phi(X'_0, U'_1) \\ X'_2 &= \phi(X'_1, U'_2) \\ &\vdots \end{aligned}$$

Como π é uma distribuição estacionária, temos que X'_n tem distribuição π para qualquer n. Além disso, as cadeias $(X_0, X_1, \dots)$ e $(X'_0, X'_1, \dots)$ são independentes de cada outro, pela suposição de que as sequências $(U_0, U_1, \dots)$ e $(U'_0, U_1, \dots)$ estão independentes um do outro.

Um passo fundamental na prova agora é mostrar que, com probabilidade 1, as cadeias se encontrarão, o que significa que existe um n tal que $X_n = X'_n$. Para mostrar isso, defina o "horário da primeira reunião"

$$T = min\{n : X_n = X'_n\}$$

com a convenção de que $T = \infty$ se as cadeias nunca se encontram. Desde o Markov cadeia $(X_0, X_1, \dots)$ é irredutível e aperiódica, podemos encontrar, usando o Corolário 1, um $M < \infty$ tal que

$$(P^M)_{ij} > 0 \text{ para todo } i, j \in \{1, \dots, k\}.$$

Defina

$$\alpha = min\{(P^M)_{ij} : i \in \{1, \dots, k\}\},$$

e observe que $\alpha > 0$. Nós entendemos que

$$\begin{aligned}
P(T \leq M) &\geq P(X_M = X'_M) \\
&\geq P(X_M = s_1, X'_M = s_1) \\
&= P(X_M = s_1) \cdot P(X'_M = s_1) \\
&= \left(\sum_{i=1}^{k} P(X_0 = s_i, X_M = s_1) \right) \cdot \left(\sum_{i=1}^{k} P(X'_0 = s_i, X'_M = s_1) \right) \\
&= \left(\sum_{i=1}^{k} P(X_0 = s_i) \cdot P(X_M = s_1 \mid X_0 = s_i) \right) \\
&\cdot \left(\sum_{i=1}^{k} P(X'_0 = s_i) \cdot P(X'_M = s_1 \mid X'_0 = s_i) \right) \\
&\geq \left(\alpha \sum_{i=1}^{k} P(X_0 = s_i) \right) \cdot \left(\alpha \sum_{i=1}^{k} P(X'_0 = s_i) \right) = \alpha^2
\end{aligned}$$

de modo que

$$P(T > M) \leq 1 - \alpha^2.$$

Da mesma forma, dado tudo o que aconteceu até o momento M, temos probabilidade condicional de pelo menos α^2 de ter $X_{2M} = X'_{2M} = s_1$, de modo que

$$P(X_{2M} \neq X'_{2M} \mid T > M) \leq 1 - \alpha^2.$$

Segue que

$$\begin{aligned}
P(T > 2M) &= P(T > M) \cdot P(T > 2M \mid T > M) \\
&\leq (1 - \alpha^2) P(T > 2M \mid T > M) \\
&\leq (1 - \alpha^2) P(X_{2M} \neq X'_{2M} \mid T > M) \\
&\leq (1 - \alpha^2)^2
\end{aligned}$$

Ao iterar este argumento, obtemos para qualquer l que

$$P(T > lM) \leq (1-\alpha^2)^l$$

que tende a 0 quando $l \to \infty$. Por isso,

$$\lim_{n\to\infty} P(T > n) = 0 \tag{6.12}$$

em outras palavras, mostramos que as duas cadeias se encontrarão com probabilidade 1.

O próximo passo da prova é construir uma terceira cadeia de Markov $(X_0'', X_1'', \dots)$, pela configuração

$$X_0'' = X_0 \tag{6.13}$$

e, para cada n,

$$X_{n+1}'' = \begin{cases} \phi(X_n'', U_{n+1}), & \text{se} \quad X_n'' \neq X_n' \\ \phi(X_n'', U_{n+1}'), & \text{se} \quad X_n'' = X_n'. \end{cases}$$

Em outras palavras, a cadeia $(X_0'', X_1'', \dots)$ evolui exatamente como a cadeia $(X_0, X_1, \dots)$ Até o momento T quando ela encontra a cadeia pela primeira vez $(X_0', X_1', \dots)$. Isto então muda para evoluir exatamente como a cadeia $(X_0', X_1', \dots)$. É importante para perceber que $(X_0'', X_1'', \dots)$ realmente é uma cadeia de Markov com matriz de transição P. Isso pode exigir uma pausa para reflexão, mas a razão básica pela qual é verdade é que a cada atualização, a função de atualização é exposta a uma nova variável uniforme em $[0,1]$, ou seja, uma que é independente de todas as variáveis aleatórias anteriores.

(Se a nova cadeia é exposta a U_{n+1} ou a U_{n+1}' depende do anterior valores das variáveis niformes [0, 1], mas isso não importa, pois U_{n+1} e U_{n+1}' têm a mesma distribuição e são independentes de tudo que aconteceu até o tempo n.) Por causa de (5.13), temos esse X_0'' tem distribuição $\mu^{(0)}$. Portanto, para qualquer n, X_n'' tem distribuição $\mu^{(n)}$. Agora, para qualquer $i \in \{1, \dots, k\}$ obtemos

$$\begin{aligned} \mu_i^{(n)} - \pi_i &= P(X_n'' = s_i) - P(X_n' = s_i) \\ &\leq P(X_n'' = s_i, X_n' \neq s_i) \\ &\leq P(X_n'' \neq X_n') \\ &= P(T > N) \end{aligned}$$

que tende a 0 quando $n \to \infty$, devido a (6.12). Usando o mesmo argumento (com o papéis de X_n'' e X_n' trocados), vemos que

$$\pi_i - \mu_i^{(n)} \leq P(T > n)$$

também, novamente tendendo a 0 quando $n \to \infty$. Por isso,

$$\lim_{n\to\infty} \mid \mu_i^{(n)} - \pi_i \mid = 0$$

Isso implica que

$$\lim_{n\to\infty} d_{TV}(\mu^{(n)}, \pi) = \lim_{n\to\infty} \left(\frac{1}{2} \sum_{i=1}^{k} \mid \mu_i^{(n)} - \pi_i \mid \right) = 0$$

Portanto, (6.11) é estabelecido. □

Teorema 9 (**Singularidade da distribuição estacionária**). *Qualquer irredutível e aperiódica cadeia de Markov tem exatamente uma distribuição estacionária.*

Demonstração. Seja $(X_0, X_1, \dots)$ Uma cadeia de Markov irredutível e aperiódica com matriz de transição P. Pelo Teorema 6, existe pelo menos uma distribuição estacionária de P, então só precisamos mostrar que há no máximo uma distribuição estacionária. Sejam π e π' dois (a priori possivelmente diferentes) distribuições estacionárias para P; nossa tarefa é mostrar que $\pi = \pi'$.

Suponha que a cadeia de Markov comece com a distribuição inicial $\mu^{(0)} = \pi'$. Então $\mu^{(n)} = \pi'$ para todo n, assumindo que π' é estacionário. No outro Por outro lado, o Teorema 7 nos diz que $\mu^{(n)} \overset{TV}{\to} \pi$, o que significa que

$$\lim_{n\to\infty} d_{TV}(\mu^{(n)}, \pi) = 0.$$

Dado que $\mu^{(n)} = \pi'$, este é o mesmo que

$$\lim_{n\to\infty} d_{TV}(\pi', \pi) = 0.$$

Mas $d_{TV}(\pi', \pi)$ não depende de n e, portanto, é igual a 0. Isso implica que $\pi = \pi'$, então a prova está completa. □

Para resumir os Teoremas 7 e 8: Se uma cadeia de Markov for irredutível e aperiódico, então ele tem uma distribuição estacionária única π, e a distribuição $\mu^{(n)}$ da cadeia no tempo n se aproxima de π quando $n \to \infty$, independentemente da distribuição $\mu^{(0)}$.

7 CADEIAS DE MARKOV REVERSÍVEIS

Neste capítulo, apresentamos uma classe especial de cadeias de Markov conhecidas como reversíveis. Eles são chamados assim porque, em certo sentido, parecem o mesmo, independentemente de o tempo correr para trás ou para frente.

Definição 9. *Seja* $(X_0, X_1, \dots)$ *uma cadeia de Markov com espaço de estado* $S = \{s_1, \dots, s_k\}$ *e matriz de transição P. Uma distribuição de probabilidade* π *em S é dito ser reversível para a cadeia (ou para a matriz de transição P) se para todos* $i, j \in \{1, \dots, k\}$ *nós temos*

$$\pi_i P_{i,j} = \pi_j P_{j,i} \tag{7.1}$$

A cadeia de Markov é considerada reversível se houver uma distribuição reversível para ela.

Teorema 10. *Seja* $(X_0, X_1, \dots)$ *uma cadeia de Markov com espaço de estado* $S = \{s_1, \dots, s_k\}$ *e a matriz de transição P. Se* π *for uma distribuição reversível para o cadeia, então também é uma distribuição estacionária para a cadeia.*

Demonstração. A propriedade $(1.)$ da definição 5 é imediata, então só resta mostrar que para qualquer $j \in \{1, \dots, k\}$, temos

$$\pi_j = \sum_{i=1}^{k} \pi_i P_{i,j}$$

nós temos

$$\pi_j = \pi_j \sum_{i=1}^{k} P_{j,i} = \sum_{i=1}^{k} \pi j P_{j,i} = \sum_{i=1}^{k} \pi_i P_{i,j}$$

onde na última igualdade usamos (7.1). □

Exemplo 9 (Passeios aleatórios em gráficos). *Este exemplo é uma generalização do exemplo de passeio aleatório na Figura 1. Um gráfico* $G = (V, E)$ *consiste em um conjunto de vertice* $V = \{v_1, \dots, v_k\}$*, junto com um conjunto de arestas* $E = \{e_1, \dots, e_l\}$*. Cada aresta conecta dois vértices; uma aresta conectando os vértices* v_i *e* v_j *é denotada* $\langle v_i, v_j \rangle$*. Duas arestas não são permitidas para conectar o mesmo par de vértices. Dois os vértices são considerados vizinhos se compartilham uma aresta. Por exemplo, o gráfico na Figura 4 tem conjunto de vértices* $V = \{v_1, \dots, v_8\}$ *e conjunto de arestas*

$$\begin{aligned} E = \{&\langle v_1, v_3 \rangle, \langle v_1, v_4 \rangle, \langle v_2, v_3 \rangle, \langle v_2, v_5 \rangle, \langle v_2, v_6 \rangle, \langle v_3, v_4 \rangle, \\ &\langle v_3, v_7 \rangle, \langle v_3, v_8 \rangle, \langle v_4, v_8 \rangle, \langle v_5, v_6 \rangle, \langle v_6, v_7 \rangle, \langle v_7, v_8 \rangle\}. \end{aligned}$$

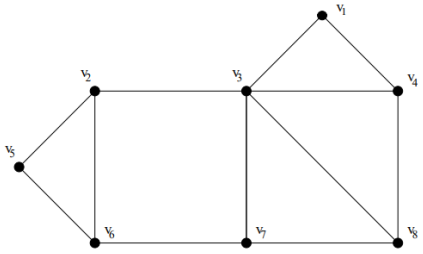


Figura 4

Um passeio aleatório em um gráfico $G = (V,E)$ é uma cadeia de Markov com espaço de estado $V = \{v_1, \ldots, v_k\}$ e o seguinte mecanismo de transição: se o caminhante aleatório ficar em um vértice v_i no tempo n, então ele se move no tempo $n+1$ para um dos vizinhos de v_i escolhido ao acaso, com probabilidade igual para cada um dos vizinhos. Assim, se denotarmos o número de vizinhos de um vértice v_i por d_i, então os elementos da matriz de transição é dada por

$$P_{i,j} = \begin{cases} \dfrac{1}{d_i}, & \text{se } v_i \text{ e } v_j \text{ são vizinhos,} \\ 0, & \text{caso contrário.} \end{cases}$$

Acontece que passeios aleatórios em gráficos são cadeias de Markov reversíveis, com distribuição reversível π dada por

$$\pi = \left(\frac{d_1}{d}, \frac{d_2}{d}, \ldots, \frac{d_k}{d}\right) \tag{7.2}$$

onde $d = \sum_{i=1}^{k} d_i$. Para ver que (7.1) vale para esta escolha de π, calculamos

$$\pi_i P_{ij} = \begin{cases} \dfrac{d_i}{d}\dfrac{1}{d_i} = \dfrac{1}{d} = \dfrac{d_j}{d}\dfrac{1}{d_j} = \pi_j P_{j,i}, & \text{se } v_i \text{ e } v_j \text{ são vizinhos} \\ 0 = \pi_j P_{ji}, & \text{caso contrário.} \end{cases}$$

Para o gráfico da Figura 4, (7.2) torna-se

$$\pi = \left(\frac{2}{24}, \frac{3}{24}, \frac{5}{24}, \frac{3}{24}, \frac{2}{24}, \frac{3}{24}, \frac{3}{24}, \frac{3}{24}\right)$$

de modo que, em equilíbrio, v_3 é o vértice mais provável para o caminhante aleatório, enquanto v_1 e v_5 são os menos prováveis.

Exemplo 10. *Seja $(X_0, X_1, \ldots)$ uma cadeia de Markov com espaço de estado $S = \{s_1, \ldots, s_k\}$ e matriz de transição P, e suponha que a matriz de transição tenha as propriedades que*

1. *$P_{i,j} > 0$ sempre que $\mid i - j \mid = 1$, e*
2. *$P_{i,j} = 0$ sempre que $\mid i - j \mid \geq 2$*

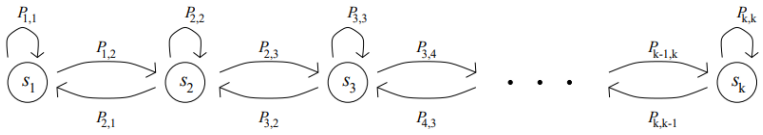


Figura 5

Essa cadeia de Markov é muitas vezes chamada de processo de nascimento e morte, e sua transição gráfico tem a forma delineada na Figura 5 *(com alguns ou todos os* $P_{i,i}$ *"loops"possivelmente ausente). Afirmamos que qualquer cadeia de Markov desse tipo é reversível. Para construir uma distribuição reversível* π *para a cadeia, começamos definindo* π_1^* *igual a algum número arbitrário estritamente positivo a. A condição* (7.1) *com* $i = 1$ *e* $j = 2$ *nos força a tomar*

$$\pi_2^* = a \cdot \frac{P_{1,2}}{P_{2,1}}$$

Aplicando (7.1) *novamente, agora com* $i = 2$ *e* $j = 3$*, obtemos*

$$\pi_3^* = \pi_2^* \cdot \frac{P_{2,3}}{P_{3,2}} = a \cdot \frac{P_{2,3}}{P_{3,2}} \cdot \frac{P_{1,2}}{P_{2,1}}$$

Podemos continuar desta forma e obter

$$\pi_i^* = a \cdot \frac{\prod_{l=1}^{i-1} P_{l,l+1}}{\prod_{l=1}^{i-1} P_{l+1,l}}$$

para cada i. Então $\pi = (\pi_1, \pi_2, \ldots, \pi_k)$ *satisfaça os requisitos de um reversível distribuição, exceto possivelmente que as entradas não somam* 1*, como é necessário para qualquer distribuição de probabilidade. Mas isso é facilmente resolvido dividindo todas as entradas por sua soma. É prontamente verificado que*

$$\pi = (\pi_1, \pi_2, \ldots, \pi_k) = \left(\frac{\pi_1^*}{\sum_{i=1}^k \pi_i^*}, \frac{\pi_2^*}{\sum_{i=1}^k \pi_i^*}, \ldots, \frac{\pi_k^*}{\sum_{i=1}^k \pi_i^*} \right)$$

é uma distribuição reversível.

Tendo chegado tão longe, pode-se ter a impressão de que a maioria das cadeias de Markov são reversíveis. Isso não é realmente verdade, no entanto, para compensar essa falsa impressão, consideremos também um exemplo de uma cadeia de Markov que é não reversível.

Exemplo 11 (Uma cadeia de Markov irreversível). *Vamos considerar uma modificação versão do passeio aleatório na Figura* 1*. Suponha que os lances de moeda usados por os caminhantes aleatórios na Figura* 1 *são tendenciosos, de tal forma que a cada tempo inteiro, ele se move um passo no sentido horário com probabilidade* $\frac{3}{4}$*, e um passo no sentido anti-horário com*

probabilidade $\frac{1}{4}$. *Isso produz uma cadeia de Markov com o gráfico de transição em Figura* 6. *É claro que* $\pi = \left(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right)$ *é uma distribuição estacionária para esta cadeia. Além disso, uma vez que a cadeia é irredutível, temos pelo Teorema* 8 *que esta é a única distribuição estacionária. Por causa do Teorema* 9, *portanto, precisamos que* π *seja reversível para que a cadeia de Markov para ser reversível.*

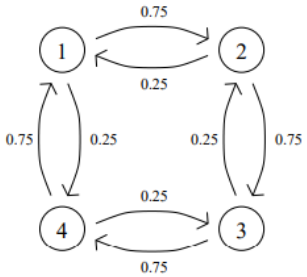


Figura 6

Mas se, por exemplo, tentarmos (7.1) *com* $i = 1$ *e* $j = 2$, *obteremos*

$$\pi_1 P_{1,2} = \frac{1}{4} \cdot \frac{3}{4} = \frac{3}{16} > \frac{1}{16} = \frac{1}{4} \cdot \frac{1}{4} = \pi_2 P_{2,1}$$

de modo que $\pi_1 P_{1,2} = \pi_2 P_{2,1}$ *e a reversibilidade falha. Intuitivamente, a razão pela qual essa cadeia não é reversível é que o andador tende a se mover no sentido horário. Se filmamos o andarilho e assistimos ao filme ao contrário, parecerá que ele preferiu mover-se no sentido anti-horário, de modo que em outras palavras a cadeia se comporta diferente no "tempo para trás"em comparação com o "tempo para a frente".*

8 CADEIA DE MARKOV MONTE CARLO

Neste capítulo e no próximo, consideramos o seguinte problema: Dada uma distribuição de probabilidade π em $S = \{s_1, \ldots, s_k\}$, como simulamos um objeto aleatório com distribuição π? Para motivar o problema, começamos com um exemplo.

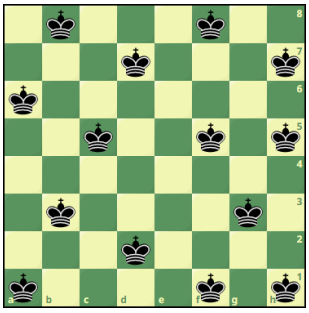


Figura 7

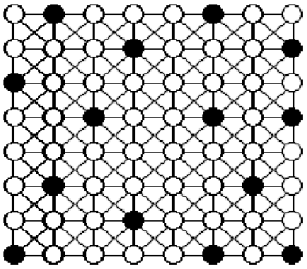


Figura 8

Exemplo 12 (O modelo hard-core). *Seja $G = (V,E)$ um grafo (lembre-se Exemplo 6.1 para a definição de um grafo) com conjunto de vértices $V = \{v_1, \ldots, v_k\}$ e conjunto de arestas $E = \{e_1, \ldots, e_l\}$. No chamado modelo hard-core em G, nós atribuimos aleatoriamente o valor 0 ou 1 a cada um dos vértices, de forma que não dois vértices adjacentes (ou seja, não há dois vértices que compartilhem uma aresta), ambos recebem o valor 1. Atribuições de 0 e 1 aos vértices são chamadas de configurações e podem ser pensados como elementos do conjunto $\{0,1\}^V$. Configurações em que não há dois 1's ocupando vértices adjacentes são chamados de viáveis. A maneira precisa em que escolhemos uma configuração aleatória é tomar cada uma das configurações viáveis com igual probabilidade. Escrevemos μ_G para a medida de probabilidade resultante em $\{0,1\}^V$. Portanto, para $\xi \in \{0,1\}^V$, temos*

$$\mu_G(\xi) = \begin{cases} \dfrac{1}{Z_G}, & \text{se } \xi \text{ é viável,} \\ 0, & \text{caso contrário.} \end{cases} \tag{8.1}$$

onde Z_G é o número total de configurações viáveis para G. Veja a Figura 7 para uma configuração aleatória escolhida de acordo com μ_G no caso em que G é um grafo de formato quadrado de

tamanho 8×8. *Este modelo (com o gráfico G sendo uma grade tridimensional) foi introduzido em física estatística para capturar parte do comportamento de um gás cujas partículas têm raios não negligenciáveis e não podem se sobrepor; aqui* 1*'s representam partículas e* 0*'s representam locais vazios. (O modelo também tem sido usado em telecomunicações para modelar situações onde um nó ocupado desativa todos os seus nós vizinhos.) Uma pergunta muito natural é: qual é o número esperado de* 1*'s de uma configuração aleatória escolhida de acordo com* μ_G*? Se escrevermos* $n(\xi)$ *para o número de* 1*'s na configuração* ξ*, e X para uma configuração aleatória escolhida de acordo com* μ_G*, então este valor esperado é dado por,*

$$E[n(X)] = \sum_{\xi \in \{0,1\}^V} n(\xi) \cdot \mu_G(\xi) = \frac{1}{Z_G} \cdot \sum_{\xi \in \{0,1\}^V} n(\xi) \cdot I_{\{\xi \text{ é viável}\}} \tag{8.2}$$

onde Z_G *é o número total de configurações viáveis para o gráfico G.*
Avaliar esta soma pode ser inviável a menos que o gráfico seja muito pequeno, uma vez que o número de configurações (e, portanto, o número de termos na soma) cresce exponencialmente no tamanho do gráfico (por exemplo, temos $2^{64} = 1,8 \cdot 10^{19}$ *diferentes configurações para o gráfico de tamanho moderado na Figura* 7*; em aplicações físicas geralmente se interessa por gráficos muito maiores). Pode ajudar um pouco que a maioria dos termos assume o valor* 0*, mas o número de termos diferentes de zero aumenta exponencialmente também. Observe também que o cálculo de* Z_G *é computacionalmente não trivial.*

Já que a expressão exata em (8.2) *está além de nossos recursos computacionais pode lidar, uma boa idéia pode ser reverter para as simulações. Se soubermos simular uma configuração aleatória X com distribuição* μ_G*, então podemos fazer muitas vezes, e estimar* $E[n(X)]$ *pelo número médio de* 1*'s em nossas simulações. Pela Lei dos Grandes Números (Teorema* 2*), esta estimativa converge para o verdadeiro valor de* $E[n(X)]$*, pois o número de simulações tende ao infinito, e podemos formar intervalos de confiança, usando procedimentos estatísticos padrão.*

Com este exemplo em mente, vamos discutir como podemos simular um variável X distribuída de acordo com uma dada distribuição de probabilidade π em um estado espaço S. Em princípio, é muito simples: apenas enumerar os elementos de S como $s_1, \ldots, s_k$, e então deixe

$$X = \psi(U)$$

onde U é uma variável aleatória uniforme $[0,1]$ e a função $\psi : [0,1] \to S$ é dado por

$$\psi(x) = \begin{cases} s_1, & \text{se} \quad x \in [0, \pi(s_1)) \\ s_2, & \text{se} \quad x \in [\pi(s_1), \pi(s_1) + \pi(s_2)) \\ \vdots & \\ s_i, & \text{se} \quad x \in \left[\sum_{j=1}^{i-1} \pi(s_j), \sum_{j=1}^{i} \pi(s_j) \right) \\ \vdots & \\ s_k, & \text{se} \quad x \in \left[\sum_{j=1}^{k-1} \pi(s_j), 1 \right] \end{cases} \tag{8.3}$$

como em (4.2). Argumentando como no Capítulo 4, vemos que isso dá a X o desejado distribuição π. Na prática, no entanto, essa abordagem é inviável, a menos que o espaço de estado S seja pequeno. Para o modelo de esferas duras em uma grade quadrada do tamanho de um tabuleiro de xadrez ou maior, a avaliação da função ψ em (8.2) torna-se muito demorado para este método ter alguma utilidade prática.

É precisamente neste tipo de situação que a cadeia de Markov Monte Carlo (MCMC) é útil. O método se origina na física, onde o os primeiros usos remontam à década de 1950. Posteriormente, teve grandes booms em outras áreas, especialmente na análise de imagens na década de 1980, e cada vez mais importante na área de estatísticas conhecida como estatísticas Bayesianas na década de 1990.

A ideia é a seguinte: Suponha que construímos uma cadeia de Markov aperiódica e irredutível $(X_0, X_1, \dots)$, cuja distribuição estacionária (única) é π. Se executarmos a cadeia com distribuição inicial arbitrária (por exemplo, começando em um estado fixo), então o teorema de convergência da cadeia de Markov (Teorema 7) garante que a distribuição da cadeia no tempo n converge para π, quando $n \to \infty$. Portanto, se executarmos a cadeia por um tempo n suficientemente longo, então a distribuição de X_n será muito próxima de π. Claro, isso é apenas um aproximação, mas o ponto é que a aproximação pode ser feita arbitrariamente boa escolhendo o tempo de execução n grande.

Uma objeção natural nesta fase é: Como pode ser mais fácil construir uma cadeia de Markov com a propriedade desejada do que construir uma variável com distribuição π direta-

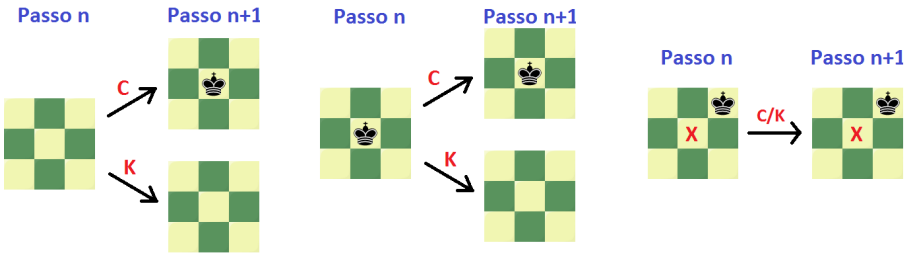
mente? Para responder a isso, vamos direto para um exemplo.

Exemplo 13 (Um algoritmo MCMC para o modelo hard-core). *Vamos considerar o modelo hard-core do Exemplo* 11 *em um gráfico* $G = (V,E)$ *(que para concretude pode ser considerado o da Figura* 7*) com* $V = \{v_1, \ldots, v_k\}$*. A fim de obter um algoritmo MCMC para este modelo, queremos construir uma cadeia de Markov cujo espaço de estado* S *é o conjunto de configurações viáveis para* G*, ou seja,*

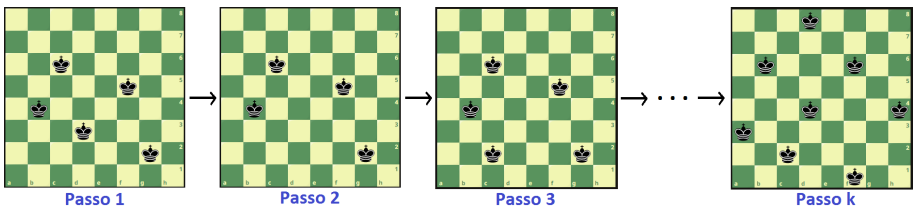
$$S = \{\xi \in \{0,1\}^V : \xi \text{ é viável}\}.$$

Além disso, queremos que a cadeia de Markov seja irredutível e aperiódica e tenha distribuição estacionária μ_G dada por (8.1). Uma cadeia de Markov $(X_0, X_1, \ldots)$ com as propriedades desejadas pode ser obtida usando o seguinte mecanismo de transição. A cada tempo inteiro $n+1$, fazemos o seguinte:

1. Escolha um vértice $v \in V$ aleatoriamente (uniformemente).
2. Jogue uma moeda justa.
3. Se a moeda der cara, e todos os vizinhos de v assumirem o valor 0 em X_n, então deixe $X_{n+1}(v) = 1$; caso contrário, deixe $X_{n+1}(v) = 0$.
4. Para todos os vértices w diferentes de v, deixe o valor em w inalterado, ou seja, deixe $X_{n+1}(w) = X_n(w)$.



Temos que $P_{\xi,\xi} > 0$, pois X_n e X_{n+1} diferem em um ou em nenhum vértice. Desse modo, a cadeia é aperiódica. Trocando um vértice de cada vez, é possível observar que $\xi \to \xi'$ e a cadeia é irredutível.



$$\xi = \xi_{n_1} \to \xi_{n_2} \to \cdots \to \xi_{n_k} = \xi'$$

Portanto, resta mostrar que μ_G é uma distribuição estacionária para a cadeia. Pelo Teorema 9, é suficiente mostrar que μ_G é reversível. $P_{\xi,\xi'}$ denota a probabilidade de transição do estado ξ para o estado ξ' (com transição mecanismo como acima), portanto, precisamos verificar se

$$\mu_G(\xi) \cdot P_{\xi,\xi'} = \mu_G(\xi') \cdot P_{\xi',\xi} \tag{8.4}$$

para quaisquer duas configurações viáveis ξ e ξ'. Vamos escrever $d = d(\xi, \xi')$ para o número de vértices em que ξ e ξ' diferem, e trata os três casos $d = 0$, $d = 1$ e $d \geq 2$ separadamente. Em primeiro lugar, o caso $d = 0$ significa que $\xi = \xi'$, nesse caso a relação (8.4) é completamente trivial. Em segundo lugar, o caso $d \geq 2$ é quase tão trivial, porque a cadeia nunca muda os valores em mais de um vértice de cada vez, tornando ambos os lados de (8.4) iguais a 0. Finalmente, considere o caso $d = 1$ onde ξ e ξ' diferem em exatamente um vértice v. Então, todos os vizinhos de v devem assumir o valor 0 em ambos ξ e ξ', pois de outra forma uma das configurações não seria viável. Portanto, obtemos

$$\mu_G(\xi) \cdot P_{\xi,\xi'} = \frac{1}{Z_G} \cdot \frac{1}{2k} = \mu_G(\xi') \cdot P_{\xi',\xi}$$

e (8.4) é verificado (lembre-se de que k é o número de vértices). Portanto, a cadeia tem μ_G como uma distribuição reversível (e portanto estacionária).

Agora podemos simular essa cadeia de Markov usando os métodos do Capítulo 4. A escolha conveniente da função de atualização ϕ é dividir o intervalo da unidade $[0,1]$ em $2k$ subintervalos de igual comprimento $1/2k$, representando as escolhas:

$$(v_1, \text{cara}), (v_1, \text{coroa}), (v_2, \text{cara}), \ldots, (v_k, \text{coroa})$$

na descrição acima do mecanismo de transição. Se agora executarmos a cadeia por um longo tempo n, começando com uma configuração inicial arbitrária viável, como a configuração de "todos os 0's"e saída X_n, então obtemos uma configuração aleatória cujo a distribuição é de aproximadamente μ_G.

O acima é um algoritmo MCMC típico em vários aspectos. Em primeiro lugar, observe que embora seja apenas necessário que a cadeia tenha a distribuição desejada como uma distribuição estacionária, encontramos uma cadeia com a propriedade mais forte que a distribuição é reversível. Este é o caso da grande maioria dos conhecidos Algoritmos MCMC.

A razão para isso é que, na maioria das situações não triviais, a maneira mais fácil de construir uma cadeia com uma dada distribuição estacionária π é que a condição de reversibilidade (7.1) se mantém.

Em segundo lugar, o algoritmo no Exemplo 12 é um exemplo de um comumente usado classe especial de algoritmos MCMC conhecidos como amostradores de Gibbs que são úteis para simular distribuições de probabilidade π em espaços de estado da forma S^V, onde S e V são conjuntos finitos. Em outras palavras, temos um conjunto finito V de vértices com um conjunto finito S de valores atingíveis em cada vértice, e π é a distribuição de alguma atribuição aleatória de valores em S aos vértices em V (no exemplo do modelo hard-core, temos $S = \{0,1\}$). O amostrador Gibbs é uma cadeia de Markov que a cada tempo inteiro $n+1$ faz o seguinte.

1. Escolha um vértice $v \in V$ aleatoriamente (uniformemente).
2. Escolha $X_{n+1}(v)$ de acordo com a distribuição π condicional do valor em v dado que todos os outros vértices assumem valores de acordo com X_n
3. Seja $X_{n+1}(w) = X_n(w)$ para todos os vértices $w \in V$ exceto v.

Não é difícil mostrar que esta cadeia de Markov é aperiódica, e que tem π como uma distribuição reversível (portanto estacionária). Se além disso a cadeia for irredutível (o que pode ou não ser o caso, dependendo de quais elementos de S^V têm probabilidade π diferente de zero), então esta cadeia de Markov é um algoritmo MCMC correto para simular variáveis aleatórias com distribuição π. Damos outro exemplo:

Exemplo 14 (**Um algoritmo MCMC para q-coloriveis aleatórios**). *Seja $G = (V,E)$ seja um gráfico e seja $q \geq 2$ um inteiro. Uma q-coloração do gráfico G é um atribuição de valores de $\{1,\ldots,q\}$ (considerado como q diferentes "cores") com a propriedade de que dois vértices adjacentes não tenham o mesmo valor (cor). Por coloração q aleatória para G, queremos dizer uma coloração q escolhida uniformemente a partir do conjunto de possíveis q-coloriveis para G, e escrevemos $\rho_{G,q}$ para a distribuição de probabilidade correspondente em S^V.*

Para um vértice $v \in V$ e uma atribuição ξ de cores aos vértices diferentes de v, a distribuição condicional $\rho_{G,q}$-distribuição da cor em v é uniforme sobre o conjunto de todos cores que não são obtidas em ξ em algum vizinho de v. Um amostrador Gibbs para q-coloriveis aleatórios é, portanto, uma cadeia de Markov avaliada em S^V onde em cada tempo $n+1$, as transições ocorrem da seguinte maneira.

1. *Escolha um vértice $v \in V$ aleatoriamente (uniformemente)*
2. *Escolha $X_{n+1}(v)$ de acordo com a distribuição uniforme sobre o conjunto de cores que não são alcançados em qualquer vizinho de v.*
3. *Deixe a cor inalterada em todos os outros vértices, ou seja, deixe $X_{n+1}(w) = X_n(w)$ para todos os vértices $w \in V$ exceto v.*

Esta cadeia é aperiódica e possui $\rho_{G,q}$ como distribuição estacionária. Se a cadeia é irredutível ou não depende de G e q, e não é trivial problema em geral para determinar isso. No caso, podemos mostrar que é irredutível, este amostrador de Gibbs torna-se um algoritmo MCMC útil.

Vamos também mencionar que uma variante comumente usada do amostrador de Gibbs é o Segue. Em vez de escolher os vértices para atualizar aleatoriamente, podemos circular sistematicamente através do conjunto de vértices. Por exemplo, se $V = \{v_1, \ldots, v_k\}$, podemos decidir atualizar o vértice

$$\begin{cases} v_1, & \text{nas vezes } 1, k+1, 2k+1 \ldots \\ v_2, & \text{nas vezes } 2, k+2, 2k+2 \ldots \\ \vdots & \\ v_i, & \text{nas vezes } i, k+i, 2k+i \ldots \\ \vdots & \\ v_k, & \text{nas vezes } k, 2k, 3k \ldots \end{cases} \tag{8.5}$$

Isso dá uma cadeia de Markov não homogênea (porque há k diferentes regras de atualização usadas em momentos diferentes) que é aperiódico e tem o desejado distribuição como uma distribuição reversível. Além disso, é irredutível se e somente se o amostrador de Gibbs de "vértice aleatório" original for irredutível. Provar essas afirmações são razoavelmente diretas, mas requerem uma extensão notacionalmente um tanto inconveniente da teoria nos Capítulos $5-7$ para o caso de cadeias de Markov não homogêneas; portanto, omitimos os detalhes. Esta variante do amostrador de Gibbs é referido como o amostrador de Gibbs de varredura sistemática.

Outro procedimento geral importante para projetar uma cadeia de Markov reversível para algoritmos MCMC é a construção de uma chamada Metrópole cadeia. Vamos descrever uma maneira (não a mais geral possível) de construir uma cadeia de Metrópolis para simular uma dada distribuição de probabilidade $\pi = (\pi_1, \ldots, \pi_k)$ em um conjunto $S = \{s_1, \ldots, s_k\}$. O

primeiro passo é construir alguns grafos G com conjunto de vértices S. O conjunto de arestas (estrutura de vizinhança) deste gráfico pode ser arbitrário, exceto que

1. o grafo deve ser conectado a fim de garantir a irredutibilidade da cadeia resultante, e
2. cada vértice não deve ser o ponto final de muitas arestas, caso contrário a cadeia torna-se computacionalmente muito pesada para simular na prática

Como de costume, dizemos que dois estados s_i e s_j são vizinhos se o grafo contém uma borda $\langle s_i, s_j \rangle$ ligando-os. Também escrevemos d_i para o número de vizinhos do estado s_i. A cadeia Metropolis correspondente a uma determinada escolha de G tem matriz de transição

$$P_{i,j} = \begin{cases} \frac{1}{d_i} \cdot \min\{\frac{\pi_j d_i}{\pi_i d_j}, 1\}, & \text{se} \quad s_i \text{ e } s_j \text{ são vizinhos} \\ 0, & \text{se} \quad s_i \neq s_j \text{ não são vizinhos} \\ 1 - \sum \frac{1}{d_i} \cdot \min\{\frac{\pi_j d_i}{\pi_i d_j}, 1\}, & \text{se} \quad i = j \end{cases}$$

onde a soma é sobre todos os estados s_l que são vizinhos de s_i. Esta transição matriz corresponde ao seguinte mecanismo de transição: Suponha que $X_n = s_i$. Primeiro escolha um estado s_j de acordo com a distribuição uniforme no conjunto de vizinhos de s_i (de modo que cada vizinho seja escolhido com probabilidade $1/d_i$) Então defina

$$X_{n+1} = \begin{cases} s_j, & \text{com probabilidade } \min\{\frac{\pi_j d_i}{\pi_i d_j}, 1\} \\ s_i, & \text{com probabilidade } 1 - \min\{\frac{\pi_j d_i}{\pi_i d_j}, 1\} \end{cases}$$

Para mostrar que esta cadeia de Markov tem π como sua distribuição estacionária, é suficiente para verificar se a condição de reversibilidade

$$\pi_i P_{i,j} = \pi_j P_{j,i} \tag{8.6}$$

vale para todos os i e j. Procedemos como no Exemplo 12, observando primeiro que (8.6) é trivial para $i = j$. Para o caso em que $i = j$ e s_i e s_j não são vizinhos, (8.6) é válido porque ambos os lados são 0. Finalmente, dividimos o caso em que s_i e s_j são vizinhos em dois subcasos de acordo com ou não $\frac{\pi_j d_i}{\pi_i d_j} \geq 1$. Se $\frac{\pi_j d_i}{\pi_i d_j} \geq 1$, então

$$\begin{cases} \pi_i P_{i,j} & = \pi_i \frac{1}{d_i} \\ \pi_j P_{j,i} & = \pi_j \frac{1}{d_j} \frac{\pi_i d_j}{\pi_j d_i} = \frac{\pi_i}{d_i} \end{cases}$$

de modo que (8.6) se mantenha. Da mesma forma, se $\frac{\pi_j d_i}{\pi_i d_j} < 1$, então

$$\begin{cases} \pi_i P_{i,j} & = \pi_i \frac{1}{d_i} \frac{\pi_j d_i}{\pi_i d_j} = \frac{\pi_j}{d_j} \\ \pi_j P_{j,i} & = \pi_j \frac{1}{d_j} \end{cases}$$

e novamente (8.6) se mantém. Portanto, π é uma distribuição reversível (portanto estacionária) para a cadeia Metropolis, que portanto pode ser usada para simulação MCMC de π.

9 CONVERGÊNCIA RÁPIDA DE ALGORITMOS MCMC

Embora a abordagem MCMC para simulação, descrita no capítulo anterior, seja altamente útil, vamos observar duas desvantagens do método:

1. A principal base teórica para o método MCMC é o Teorema 7, que garante que a distribuição $\mu^{(n)}$ no tempo n de uma cadeia de Markov irredutível e aperiódica iniciada em um estado fixo converge para a estacionária distribuição π como $n \to \infty$. Mas isso não significa que $\mu^{(n)}$ sempre se torna igual a π, só que chega muito perto. Na verdade, na maioria dos exemplos, temos $\mu^{(n)} \neq \pi$ para todo n. Portanto, não importa o quão grande seja n é considerado no algoritmo MCMC, há ainda haverá alguma discrepância entre a distribuição da saída e a distribuição desejada π.
2. A fim de tornar o erro devido a (1) pequeno, precisamos descobrir quão grande n precisa ser tomado para garantir que a discrepância entre $\mu^{(n)}$ e π (medido na distância de variação total $d_{TV}(\mu^{(n)}, \pi)$ é menor do que algum dado $\varepsilon > 0$. Em muitas situações, descobriu-se ser muito difícil obter limites superiores de quão grande n precisa ser tomadas, que são pequenas o suficiente para ter qualquer uso prático

O problema (1) acima em si não é um obstáculo particularmente sério. Na maioria das situações, podemos tolerar um pequeno erro na distribuição da saída, desde que pois temos uma ideia sobre o quão pequeno ele é. É apenas em combinação com (2) que se torna realmente incômodo. Uma cadeia de Markov $(X_0, X_1, \dots)$ cuja distribuição $\mu^{(n)}$ converge para a distribuição desejada π, pois o tempo de execução n tende a ∞, é construído. A cadeia é então executada por um tempo razoavelmente longo n (digamos, 10^4 ou 10^5, e X_n é a saída, na esperança de que a cadeia tenha chegado perto do equilíbrio por então.

Esta situação é claramente insatisfatória e uma quantidade substancial de esforço nos últimos anos tem tentado corrigi-lo. Neste capítulo, daremos uma olhada em duas abordagens diferentes. O que vamos considerar neste capítulo é tentar superar o problema mais sério (2) por estabelecer limites úteis para taxas de convergência de cadeias de Markov. Em geral, este continua sendo um problema aberto difícil, mas em uma série de situações específicas, resultados muito bons foram obtidos.

Para ilustrar o tipo de resultados de taxa de convergência que podem ser obtidos, e uma das principais técnicas de prova, neste capítulo iremos nos concentrar em um exemplo onde

a cadeia MCMC foi analisada com sucesso, ou seja, o q-colorivel aleatórios no Exemplo 13.

Uma variedade de técnicas diferentes (mas às vezes relacionadas) para provar a rápida convergência ao equilíbrio de cadeias de Markov foram desenvolvidas, incluindo limites de autovalor, argumentos de caminho e fluxo, várias comparações entre cadeias diferentes e o conceito de dualidade estacionária forte. Outra técnica importante, que já abordamos no Capítulo 6, é o uso de acoplamentos, e essa é a abordagem que faremos aqui.

Vamos considerar o exemplo q-colorivel. Fixe um grafo $G = (V,E)$ e um inteiro q, e lembre-se de que $\rho_{G,q}$ é a distribuição de probabilidade em $\{1,\dots,q\}^V$ que é uniforme em todos os $\xi \in \{1,\dots,q\}^V$ que são q cores válidas, ou seja, sobre todas as atribuições de cores $1,\dots,q$ aos vértices de G com a propriedade que não haja dois vértices compartilhando uma aresta com a mesma cor. Nós consideramos o Amostrador de Gibbs descrito no Exemplo 13, com a modificação de que o vértice a ser atualizado é escolhido como no amostrador de Gibbs de varredura sistemática definido em (8.5). Isso significa que em vez de escolher um vértice aleatoriamente de maneira uniforme a partir de $V = \{v_1,\dots,v_k\}$, varremos sistematicamente o conjunto de vértices atualizando vértice v_1 no tempo 1, v_2 no tempo 2,..., v_k no tempo k, v_1 novamente no tempo $k+1$, e assim por diante, como em (8.5).

É natural formular a pergunta sobre as taxas de convergência para este MCMC algoritmo (ou outros) da seguinte forma: Dado $\varepsilon > 0$ (como por exemplo $\varepsilon = 0,01$), de quantas iterações n do algoritmo precisamos para fazer o total distância de variação $d_{TV}(\mu^{(n)}, \rho_{G,q})$ menor que ε? Aqui $\mu^{(n)}$ é a distribuição da cadeia após n iterações.

Teorema 11. *Seja $G = (V,E)$ um grafo. Seja k o número de vértices em G, e suponha que qualquer vértice $v \in V$ tenha no máximo d vizinhos. Suponha além disso, $q > 2d^2$. Então, para qualquer $\varepsilon > 0$ fixo, o número de iterações necessário para o amostrador de Gibbs de varredura sistemática descrito acima (a partir de qualquer q-coloração fixa ξ) para entrar na distância de variação total ε do alvo distribuição $\rho_{G,q}$ é no máximo*

$$k \cdot \left(\frac{log(k) + log(\varepsilon^{-1}) - log(d)}{log(\frac{q}{2d^2})} + 1 \right). \tag{9.1}$$

Antes de ir para a prova desse resultado, alguns comentários cabem:

1. O aspecto mais importante do limite em (9.1) é que ele é limitado por

$$C \cdot k \cdot (log(k) + log(\varepsilon^{-1}))$$

para alguma constante $C < \infty$ que não depende de k ou de ε. Isso significa que o número de iterações necessárias para chegar à distância de variação total ε da distribuição alvo $_{G,q}$ não cresce terrivelmente rápido quando $k \to \infty$ como $\varepsilon \to 0$. É fácil ver que qualquer algoritmo para gerar q colorações aleatórias deve ter um tempo de execução que cresce pelo menos linearmente em k (porque leva cerca de tempo k até mesmo para imprimir o resultado). O log de fator extra (k) que chegamos aqui não é uma desaceleração particularmente grave.
2. Nosso limite $q > 2d^2$ para quando obtivermos convergência rápida é um ponto bastante bruto estimativa.
3. Se G fizer parte da rede quadrada (como, por exemplo, o gráfico da Figura 7), então $d = 4$, de modo que o Teorema 8.1 fornece convergência rápida do MCMC algoritmo para $q \geq 33$. O melhor limite de Jerrum dá convergência rápida para $q \geq 9$.
4. Pode parecer estranho que obtemos convergência rápida para grandes q apenas, como um pode intuitivamente pensar que seria mais difícil simular o maior q fica, devido ao fato de que o número de q-colorivel em G está aumentando em q. Isso é, no entanto, enganoso, e a intuição correta é, em vez disso, a seguir. Quanto maior q fica, menos dependente é a coloração de um vértice v se torna em seus vizinhos. Se q for muito grande, podemos escolher o cor em v uniformemente ao acaso, e tem muito pouco risco de que esta cor seja já levado por um de seus vizinhos. Portanto, a diferença entre $\rho_{G,q}$ e a distribuição uniforme sobre todos os elementos de $\{1,\dots,q\}^V$ torna-se muito pequena no limite quando $q \to \infty$ e a última distribuição é, naturalmente, fácil de simular: basta atribuir i.i.d. cores (uniformemente de $\{1,\dots,q\}$) aos vértices

Demonstração. Como na prova do Teorema 7, usaremos um argumento de acoplamento: Devemos executar duas cadeias de Markov com valor de $\{1,\dots,q\}^V$ $(X_0, X_1, \dots)$ e $(X'_0, X'_1, \dots)$ simultaneamente. Eles terão as mesmas matrizes de transição (ou seja, aqueles dados pelo amostrador de Gibbs de varredura sistemática para colorações q de G, conforme descrito acima). A diferença será que o primeiro cadeia é iniciada no estado fixo $X_0 = \xi$, enquanto a segunda é iniciada em um estado aleatório X'_0 escolhido de acordo com a distribuição estacionária $\rho_{G,q}$. Então X'_n tem distribuição $\rho_{G,q}$ para todo n, pela definição de estacionariedade. Também escrever $\mu^{(n)}$ para a distribuição da primeira cadeia $(X_0, X_1, \dots)$ no tempo n; Isto é o cadeia na qual esta-

mos principalmente interessados. Queremos limitar a variação total $d_{TV}(\mu^{(n)}, \rho_{G,q})$ entre $\mu^{(n)}$ e a distribuição estacionária, e nós deve ver que $d_{TV}(\mu^{(n)}, \rho_{G,q})$ é próximo de 0 se $P(X_n = X'_n)$ está próximo de 1.

Lembre-se do Exemplo 13 que sempre que um vértice v é escolhido para ser atualizado, escolher uma nova cor para v de acordo com a distribuição uniforme no conjunto de núcleos que não são alcançadas por nenhum vizinho de v. Uma maneira de implementar isso concretamente é escolher uma permutação aleatória

$$R = (R^1, \ldots, R^q)$$

do conjunto $\{1, \ldots, q\}$, escolhido uniformemente do $q!$ diferentes permutações possíveis e, em seguida, deixe v obter a primeira cor de a permutação que não é alcançada por nenhum vizinho de v.

Claro, precisamos escolher uma nova (e independente) permutação em cada atualização de uma cadeia. No entanto, nada nos impede de usar as mesmas permutações para a cadeia $(X'_0, X'_1, \ldots)$ quanto a $(X_0, X_1, \ldots)$, e isso é de fato o que nós faremos. Seja $R_0, R_1, \ldots$ um i.i.d. sequência de permutações aleatórias, cada deles uniformemente distribuídos no conjunto de permutações de $\{1, \ldots, q\}$. Em cada tempo n, as atualizações das duas cadeias usam a permutação

$$R_n = (R_n^1, \ldots, R_n^q)$$

e o vértice v a ser atualizado recebe o novo valor

$$X_{n+1}(v) = R_n^i$$

onde

$$i = min\{j : X_n(w) \neq R_n^j \text{ para todos os vizinhos } w \text{ de } v\}$$

na primeira cadeia. Na segunda cadeia, definimos de forma semelhante

$$X'_{n+1}(v) = R_n^{i'}$$

onde

$$i' = min\{j' : X'_n(w) \neq R'^{j'}_n \text{ para todos os vizinhos } w \text{ de } v\}.$$

Isso define nosso acoplamento de $(X_0, X_1, \dots)$ e $(X'_0, X'_1, \dots)$. O que esperamos pois é ter $X_T = X'_T$ em algum tempo (aleatório, mas não muito grande) T, no qual caso também teremos $X_n = X'_n$ para todo $n \geq T$ (porque o acoplamento é definido de forma que, uma vez que as duas cadeias coincidam, elas fiquem juntas para sempre). Para estimar a probabilidade de que as configurações X_n e X'_n sejam iguais, vamos primeiro consideremos a probabilidade de que eles coincidam em um determinado vértice, ou seja, que $X_n(v) = X'_n(v)$ para um determinado vértice v.

Considere a atualização das duas cadeias em um vértice v no tempo n, onde nós tome $n \leq k$, de modo que em outras palavras estamos na primeira varredura do Gibbs amostrador através do conjunto de vértices. Chamamos a atualização de sucesso se resultar em tendo $X_{n+1}(v) = X'_{n+1}(v)$; caso contrário, dizemos que a atualização falhou. o probabilidade de uma atualização bem-sucedida depende do número de cores que são alcançado na vizinhança de v em ambas as configurações X_n e X'_n, e em o número de cores que são alcançadas em cada uma delas. Defina

$B_0 =$ o número de cores $r \in \{1, \dots, q\}$ que são obtidas na vizinhança de v em nenhum de X_n e X'_n

$B_1 =$ o número de cores $r \in \{1, \dots, q\}$ que são obtidas na vizinhança de v em exatamente um de X_n e X'_n

$B_2 =$ o número de cores $r \in \{1, \dots, q\}$ que são obtidas na vizinhança de v de X_n e X'_n

e observe que $B_0 + B_1 + B_2 = q$. Observe também que se a primeira cor R_n^1 no permutação R_n está entre as cores B_2 alcançadas na vizinhança de v em ambas as configurações, então os amostradores Gibbs simplesmente descartam R_n^1 e olhe para R_n^2 em vez disso, e assim por diante. Portanto, a atualização é bem-sucedida se e somente se o primeiro cor em R_n que é atingida na vizinhança de v em nenhum de X_n e X'_n aparece mais cedo na permutação do que a primeira cor que é alcançada em a vizinhança de v em exatamente um de X_n e X'_n. Este evento (de ter um atualização bem-sucedida), portanto, tem probabilidade

$$\frac{B_0}{B_0 + B_1}$$

condicionada em B_0, B_1 e B_2. Em outras palavras, nós temos

$$P(\text{atualização falhada}) = \frac{B_1}{B_0 + B_1}. \tag{9.2}$$

Prosseguimos para estimar o lado direito em (9.2). Claramente, $0 \leq B_2 \leq d$. Além disso,

$$B_1 \leq 2d - 2B_2 \tag{9.3}$$

Argumentando da mesma forma para a terceira varredura e para a segunda varredura, nós temos

$$P(X_{3k}(v) \neq X'_{3k}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right)^2$$

e continuando da maneira óbvia, obtemos para $m = 4,5,\ldots$ que

$$P(X_{mk}(v) \neq X'_{mk}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right)^{m-1} \tag{9.7}$$

Após esta análise da probabilidade de que X_{mk} e X'_{mk} diferem em um dado vértice, a seguir queremos estimar a probabilidade $P(X_{mk} \neq X'_{mk})$ que o primeiro cadeia não consegue ter exatamente a mesma configuração que a segunda cadeia, no momento mk. Desde o evento $X_{mk} \neq X'_{mk}$ implica que $X_{mk}(v) \neq X'_{mk}(v)$ por pelo menos um vértice $v \in V$, temos

$$\begin{aligned} P(X_{mk} \neq X'_{mk}) &\leq \sum_{v \in V} P(X_{mk}(v) \neq X'_{mk}) \\ &\leq k\frac{2d}{q}\left(\frac{2d^2}{q}\right)^{m-1} \\ &= \frac{k}{d}\left(\frac{2d^2}{q}\right)^{m} \end{aligned} \tag{9.8}$$

onde a desigualdade em (9.8) é devida a (9.7) e a suposição de que o gráfico tem k vértices. Agora seja $A \subseteq \{1,\ldots,q\}^V$ qualquer subconjunto de $\{1,\ldots,q\}^V$. Por (6.10), temos que

$$\begin{aligned} d_{TV}(\mu^{(mk)}, \rho_{G,q}) &= \max_{A \subseteq \{1,\ldots,q\}^V} \mid \mu^{(mk)}(A) - \rho_{G,q(A)} \mid \\ &= \max_{A \subseteq \{1,\ldots,q\}^V} \mid P(X_{mk} \in A) - P(X'_{mk} \in A) \mid . \end{aligned} \tag{9.9}$$

Para qualquer A, temos

$$\begin{aligned} P(X_{mk} \in A) - P(X'_{mk} \in A) = & \\ &= P(X_{mk} \in A, X'_{mk} \in A) + P(X_{mk} \in A, X'_{mk} \notin A) \\ &- P(X'_{mk} \in A, X_{mk} \in A) - P(X'_{mk} \in A, X_{mk} \notin A) \\ &= P(X_{mk} \in A, X'_{mk} \notin A) - P(X'_{mk} \in A, X_{mk} \notin A) \\ &\leq P(X_{mk} \in A, X'_{mk} \notin A) \\ &\leq P(X_{mk} \neq X'_{mk}) \\ &\leq \frac{k}{d}\left(\frac{2d^2}{q}\right)^{m}. \end{aligned}$$

Da mesma forma, nós temos

$$P(X'_{mk} \in A) - P(X_{mk} \in A). \tag{9.10}$$

Segue que

$$| P(X_{mk} \in A) - P(X'_{mk} \in A) | \leq \frac{k}{d} \left(\frac{2d^2}{q} \right)^m \tag{9.11}$$

Tirando o máximo de todo $A \subseteq \{1, \ldots, q\}^V$, e inserindo em (9.9), nós temos

$$d_{TV}(\mu^{(mk)}, \rho_{G,q}) \leq \frac{k}{d} \left(\frac{2d^2}{q} \right)^m \tag{9.12}$$

que tende a 0 quando $m \to \infty$. Tendo estabelecido este limite, nosso próximo e final problema é:

Quão grande deve ser tirado para fazer o lado direito de (9.12) menor que ε?

Pela configuração,

$$\frac{k}{d} \left(\frac{2d^2}{q} \right)^m = \varepsilon$$

e resolvendo para m, descobrimos que

$$m = \frac{log(k) + log(\varepsilon^{-1}) - log(d)}{log\left(\frac{q}{d^2}\right)}$$

de modo que executar o amostrador de Gibbs por tempo suficiente para obter pelo menos esse número de varreduras através do conjunto de vértices dá $d_{TV}(^{(mk)}, \rho_{G,q}) \leq \varepsilon$. Para ir do número de verifica m para o número de etapas n da cadeia de Markov, temos que multiplicar por k, dando isso

$$n = k \cdot \frac{log(k) + log(\varepsilon^{-1}) - log(d)}{log\left(\frac{q}{d^2}\right)} \tag{9.13}$$

deve ser suficiente. No entanto, tomando n como em (9.13), não necessariamente obtemos um valor inteiro para $m = n/k$, então, para estar do lado seguro, devemos considerar n como pelo menos o menor número que é maior do que o lado direito de (9.13) e o que torna n/k um inteiro. Isso significa aumentar n em no máximo k em comparação com (9.13), de modo que nossa resposta final é que tomando

$$n = k \cdot \left(\frac{log(k) + log(\varepsilon^{-1}) - log(d)}{log\left(\frac{q}{d^2}\right)} + 1 \right)$$

é suficiente, e o Teorema 10 é estabelecido. □

10 DECIFRANDO CRIPTOGRAFIAS

A Criptografia é um conjunto de técnicas aplicadas a uma informação de modo que apenas o emissor e o recptor possam compreendê-las.

Figura 8

Um dos primeiros modelos de criptografia foi a cifra de César que consiste em transladar o alfabeto um número n de vezes. Por exemplo,

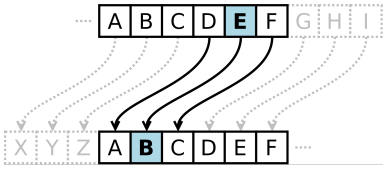


Figura 9

- Se $n = 3$, então **criptografia** é criptografada como **fulswrjudild**

Esse método é bem simples de decifrar, pois temos 26 configurações possíveis. Logo, surgiram métodos mais avançados como, por exemplo, a utilização de números primos que são ideiais para proteger informações de bancos, redes sociais, etc.

- Use um texto grande para base nas estastíticas, como por exemplo, um livro do Harry Potter.
- Denote $M(\alpha,\beta)$ a proporção que a letra β surge depois de α.
- Considere o texto criptografado como uma sequência de símbolos

$$\omega_1, \omega_2, \omega_3, \ldots, \omega_{k-1}, \omega_k$$

- Dada uma descriptografia $g : \{\text{códigos}\} \to \{\text{alfabeto}\}$, calculamos sua plausibilidade por

$$Pl(g) = \prod_{i}^{k-1} M(g(\omega_i), g(\omega_{i+1}))$$

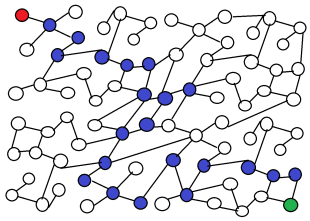


Figura 10

Agora, vamos utilizar o processo de otimização de Monte Carlo, seguindo os passos:

- Escolha uma $g : \{\text{códigos}\} \to \{\text{alfabeto}\}$ arbitrária
- Calcule $Pl(g)$
- Considere $g*$ transpondo aleatoriamente duas imagens de g
- Calcule $Pl(g*)$. Se $Pl(g*) > Pl(g)$, então aceite g*.
- Caso contrário, jogue uma moeda com probabilidade $\dfrac{Pl(g*)}{Pl(g)}$ de sair cara.
- Se sair cara, escolha g*. Caso contrário, escolha g.

Desse modo, vamos convergir para a maior plausibilidade e, consequentemente, para o texto original.

porque contando os vizinhos em ambas as configurações, há no máximo $2d$ delas, e cada cor que contribui para B_2 usa até duas delas. Nós temos

$$\begin{aligned} P(\text{atualização falhada}) &= \frac{B_1}{B_0+B_1} = \frac{B_1}{q-B_2} \\ &\leq \frac{2d-2B_2}{q-B_2} \leq \frac{2d-B_2}{q-B_2} \\ &= \frac{2d(1-\frac{B_2}{2d})}{q(1-\frac{B_2}{q})} \leq \frac{2d}{q} \end{aligned} \tag{9.4}$$

onde a primeira desigualdade é apenas (9.3), enquanto a desigualdade final é devido ao suposição $q > 2d^2$, o que implica $q > 2d$, o que por sua vez implica $(1-\frac{B_2}{q}) \geq (1-\frac{B_2}{2d})$.
Portanto, temos, após k etapas das cadeias de Markov (ou seja, após a primeira varredura dos amostradores de Gibbs através do conjunto de vértices), que, para cada vértice v

$$P(X_k(v) \neq X'_k(v)) \leq \frac{2d^2}{q}. \tag{9.5}$$

Agora, considere as atualizações durante a segunda varredura do amostrador de Gibbs, ou seja, entre os tempos k e $2k$. Para uma atualização no tempo n durante a segunda varredura para falham, as configurações X_n e X'_n precisa diferir em pelo menos um vizinho de v. Cada vizinho w tem $X_n(w) \neq X'_n(w)$ com probabilidade no máximo $\frac{2d}{q}$ (devido a (9.4), e somando no máximo d vizinhos, obtemos que

$$P(\text{discrepância}) \leq \frac{2d^2}{q} \tag{9.6}$$

onde "discrepância"é a abreviação para o evento de que existe um vizinho w de v com $X_n(w) \neq X'_n(w)$. Dado o evento em (9.6), temos, ao repetir os argumentos em (9.2) e (9.4), que a probabilidade condicional P(atualização com falha | discrepância) de uma atualização com falha é limitada por $\frac{2d}{q}$. Portanto,

$$\begin{aligned} P(\text{atualização com falha}) &= P(\text{discrepância}) \cdot P(\text{atualização com falha} \mid \text{discrepância}) \\ &\leq \frac{4d^3}{q^2} = \frac{2d}{q}\left(\frac{2d^2}{q}\right). \end{aligned}$$

Portanto, após $2k$ etapas das cadeias de Markov, cada vértice $v \in V$ tem diferentes cores nas duas cadeias com probabilidade no máximo

$$P(X_{2k}(v) \neq X'_{2k}(v)) \leq \frac{2d}{q}\left(\frac{2d^2}{q}\right).$$

11 REFERÊNCIAS

[1] HAGGSTROM, O.; Finite markov chains and algorithmic applications. Cambridge University Press, 2002.

[2] PERSI DIACONIS, Persi. The Markov Chain Monte Carlo Revolution. Departments of Mathematics and Statistics, Stanford University, 1-3.