

# Lições de Teoria Ergódica, Processos Estocásticos e Sistemas Dinâmicos

Nelson Luís Dias

28 de fevereiro de 2014

# Capítulo 1

## 2014-02-19: Aditividade finita

### Como conceitualizamos e formalizamos a propabilidade?

Existem várias abordagens possíveis:

1. Clássica (teórica ou “a priori”):

Consideramos um processo aleatório com  $n$  resultados igualmente prováveis, e um evento  $A$  que consiste em  $m$  desses resultados. A probabilidade desse evento é então definida por

$$P(A) \equiv \frac{m}{n}.$$

Crítica: no termo “igualmente prováveis”, já há a suposição de que nós “sabemos” o que é probabilidade antes de defini-la. Trata-se portanto de um argumento circular. (COMO PODEMOS MELHORAR ESSE TEXTO?)

2. Empírica (“a posteriori” ou frequentista):

Supõe-se que um determinado experimento é repetido  $n$  vezes “nas mesmas condições”. Se  $A$  é um evento identificável no experimento, a probabilidade de  $A$  é definida como o limite da razão entre número  $m$  de ocorrências de  $A$  e o número de repetições  $n$  quando  $n \rightarrow \infty$ :

$$P(A) \equiv \lim_{n \rightarrow \infty} \frac{m}{n}.$$

3. Subjetiva:

Aceita-se que podemos atribuir a diversos eventos uma “probabilidade” de ocorrência. Por exemplo, eu *acho* que a probabilidade de que eu encontre petróleo no terreno de minha casa é (ou deve ser)  $10^{-12}$ .

4. Axiomática (Kolmogorov, 1933).

Uma tripla de propabilidade é uma tripla formada por  $(\Omega, \mathcal{F}, P)$ , sendo  $\Omega$  um conjunto não vazio,  $\mathcal{F}$  um campo sigma (uma  $\sigma$ -álgebra) de subconjuntos de  $\Omega$  (PRECISAMOS USAR OS TERMOS CORRETOS), e  $P$  uma função, com

$$P : \mathcal{F} \rightarrow [0, 1],$$

$$A \in \mathcal{F} \mapsto P(A).$$

Axiomas:

$$P(A) \geq 0, \quad (1.1)$$

$$P(\Omega) = 1, \quad (1.2)$$

$$P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i), \quad \text{se} \quad A_i \cap A_j = \emptyset. \quad (1.3)$$

Os axiomas funcionam quando  $\Omega$  é finito. Contudo, há conjuntos maiores/infinitos (?) para os quais a noção de probabilidade não faz sentido. Assim, uma  $\sigma$ -álgebra será um subconjunto de  $2^\Omega$  com uma certa estrutura, para o qual deverá fazer sentido especificar probabilidades.

**Exemplo:** Sabendo que  $A_1 \cup A_2 \cup A_3 = (A_1 \cup A_2) \cup A_3$ , prove por indução que o axioma (1.3) vale para todo  $n$  se ele valer para  $n = 2$ .

Para  $n = 2$ ,

$$A_1 \cup A_2 = \emptyset \Rightarrow P(A_1 \cup A_2) = \sum_{i=1}^2 P(A_i). \quad (1.4)$$

Suponha agora que (1.3) valha para  $n$ , e que

$$A_{n+1} \cap \left[ \bigcup_{i=1}^n A_i \right] = \emptyset, \quad i = 1, \dots, n.$$

Então,

$$P(A_1 \cup \dots \cup A_n \cup A_{n+1}) = P(B \cup A_{n+1}), \quad (1.5)$$

fazendo-se

$$B = \bigcup_{i=1}^n A_i.$$

A partir de (1.4),

$$P(B \cup A_{n+1}) = P(B) + P(A_{n+1}). \quad (1.6)$$

Por sua vez, como supusemos a validade de (1.3),

$$P(B) = P\left(\bigcup_{i=1}^n A_i\right) = \sum_{i=1}^n P(A_i). \quad (1.7)$$

Logo,

$$P(A_1 \cup \dots \cup A_n \cup A_{n+1}) = P(A_{n+1}) + \sum_{i=1}^n P(A_i) = \sum_{i=1}^{n+1} P(A_i). \quad (1.8)$$

Note entretanto que, para que a prova seja válida, precisamos garantir que

$$A_{n+1} \cap \left[ \bigcup_{i=1}^n A_i \right] = \emptyset \Rightarrow A_{n+1} \cap A_i = \emptyset, \forall i = 1, \dots, n.$$

Faça  $C = A_{n+1}$ , e considere a igualdade:

$$C \cap \left[ \bigcup_{i=1}^n A_i \right] = \bigcup_{i=1}^n C \cap A_i. \quad (1.9)$$

Se ela for verdadeira, então:

$$\begin{aligned} A_{n+1} \cap \left[ \bigcup_{i=1}^n A_i \right] = \emptyset &\Rightarrow \bigcup_{i=1}^n C \cap A_i = \emptyset \\ &\Rightarrow A_{n+1} \cap A_i = \emptyset, \quad \forall i = 1, \dots, n. \end{aligned}$$

Portanto, se (1.9) for verdadeira, a questão está liquidada.

De fato,

$$\begin{aligned} x \in C \cap \left[ \bigcup_{i=1}^n A_i \right] &\Rightarrow (x \in C) \text{ e } \left( x \in \bigcup_{i=1}^n A_i \right), \\ &\Rightarrow \exists j \in \{1, \dots, n\} \mid (x \in C) \text{ e } (x \in A_j) \\ &\Rightarrow x \in C \cap A_j \\ &\Rightarrow x \in \bigcup_{i=1}^n C \cap A_i. \end{aligned}$$

Isso significa que

$$C \cap \left[ \bigcup_{i=1}^n A_i \right] \subseteq \bigcup_{i=1}^n C \cap A_i.$$

Por outro lado,

$$\begin{aligned} x \in \bigcup_{i=1}^n C \cap A_i &\Rightarrow \exists j \mid x \in C \cap A_j \\ &\Rightarrow x \in C \cap \bigcup_{i=1}^n A_i. \end{aligned}$$

Isso significa que

$$\bigcup_{i=1}^n C \cap A_i \subseteq C \cap \left[ \bigcup_{i=1}^n A_i \right].$$

Com isso, (1.9) está provada, e chegamos ao fim (desta prova).

## Notas de Aula Professor Paulo Cezar P. de Carvalho - Ailin

### Modelos elementares

$\Omega = \{\omega_1, \dots, \omega_n\} \rightarrow \text{espaço amostral}$

$\mathcal{F} = 2^\Omega$  é o conjunto potência e inclui todos os subconjuntos de  $\Omega$ , e, em particular, inclui  $\{\omega_1\}, \{\dots\}, \{\omega_n\}$ , os quais são chamados eventos complementares.

$$P(\{\omega_i\}) = P_i \in [0, 1] \mid \sum_{i=1}^n P_i = 1 \quad (1.10)$$

Caso equiprovável:  $P_i = 1/n, \forall i \in \{1, \dots, n\}$ .

**Exemplo:** 3 moedas são lançadas. Qual a probabilidade de saírem 2 caras?

Como defino  $\Omega$ ? Se considerarmos  $\Omega = \{0, 1, 2, 3\}$ , as probabilidades são  $1/8$  para 0 e 3, e  $3/8$  para 1 e 2. Para  $i = 0, 1, 2, 3$ , temos

$$P(i) = \left(\frac{1}{8}\right)^i \left(1 - \frac{1}{8}\right)^{3-i} \binom{3}{i}, \quad (1.11)$$

distribuição binomial herdada do modelo equiprovável.

**Exemplo:** Escolher um número no intervalo  $[0, 1]$  tal que  $P([a, b]) = b - a$  para qualquer intervalo  $[a, b] \subset [0, 1]$ .

$\Omega = [0, 1]$

A primeira tentativa seria atribuir  $P(\{a\})$ . Se for equiprovável com  $P \neq 0$  já estaria em contradição com a aditividade.

Com um conjunto enumerável (infinito) não é possível ter equiprobabilidade nem atribuindo probabilidade nula, porque não conseguiremos que a “soma” das  $P(\{\})$  seja 1.

## Capítulo 2

### 2014-02-24: Aditividade infinita

Passamos agora para casos em que o espaço amostral  $\Omega$  deixa de ser um conjunto finito. Um conjunto infinito pode ser enumerável ou não-enumerável. Um conjunto enumerável é um conjunto cujos elementos possam ser colocados em uma relação biunívoca com os naturais. Os racionais são um conjunto enumerável (Cantor). Os números reais no intervalo fechado  $[0, 1]$  são um conjunto não-enumerável.

Quando  $\Omega$  é finito, todos os elementos de  $2^\Omega$  são eventos: a todos e a cada um deles pode ser atribuída uma probabilidade, e os axiomas (1.1)–(1.3) se aplicam.

Antes de seguir para o infinito, considere o exemplo:  $n$  lançamentos de uma moeda, cujos resultados individuais podem ser “cara” (0) ou “coroa” (1). Os eventos elementares com os quais podemos construir um espaço amostral são  $n$ -uplas do tipo

$$\begin{aligned} &(0, 0, \dots, 0, 0) \\ &(0, 0, \dots, 0, 1) \\ &(0, 0, \dots, 1, 0) \\ &\vdots \\ &(1, 1, \dots, 1, 1). \end{aligned}$$

Existem  $2^n$  casos.

Suponha por exemplo que desejemos calcular a probabilidade de que ocorram  $k$  caras (e, conseqüentemente,  $n - k$  coroas). Um evento deste tipo (exatamente  $k$  caras e  $n - k$  coroas) pode ocorrer de  $n!$  maneiras. No entanto, a posição das  $k$  caras é imaterial: todos os  $k!$  casos aparecem da mesma forma. Idem para os  $(n - k)!$  casos de permuta das posições das coroas. Concluimos que há

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

possibilidades de ocorrência de  $k$  caras. A sua probabilidade é

$$\frac{\binom{n}{k}}{2^n} = \binom{n}{k} \left(\frac{1}{2}\right)^k \left(\frac{1}{2}\right)^{n-k}.$$

Isso é um caso particular da distribuição binomial. Se 0 tem probabilidade  $p$ , e 1 tem probabilidade  $1 - p$ , a probabilidade de  $k$  zeros em  $n$  lançamentos é

$$P(k) = \binom{n}{k} p^k (1 - p)^{n-k}.$$

**Exercício:** Mostre que

$$\sum_{k=0}^n P(k) = 1.$$

Prova:

$$\begin{aligned}(p + (1 - p))^n &= 1 \\ &= \sum_{k=0}^n \binom{n}{k} p^k (1 - p)^{n-k} \\ &= \sum_{k=0}^n P(k).\end{aligned}$$

Agora, se  $\Omega = \{x_1, x_2, x_3, \dots\}$  for enumerável, precisamos de

$$\sum_{i=1}^n P(x_i) = 1$$

e fica evidente que os  $P(x_i)$  não podem ser todos iguais. Entretanto, ainda é possível aproveitar os  $x_i$ 's desde que a soma acima funcione.

**Exemplo:** Em um jogo, dez bolas numeradas de 0 a 9 podem ser sorteadas. Cada jogador sorteia uma bola, mostra o resultado e retorna a bola. Ganha o primeiro jogador que sortear um 7. O jogo poderia durar para sempre?

Nossa opção para construção do espaço amostral é

$$\Omega = \{0, 1, 2, 3, 4, \dots\}$$

0 significa que o 7 *nunca* é sorteado; 1 significa que o 7 foi sorteado na primeira rodada; 2 na segunda; e assim por diante. As probabilidades desses eventos não são iguais:

$$\begin{aligned}P(0) &= ?, \\ P(1) &= \frac{1}{10}, \\ P(2) &= \frac{9}{10} \times \frac{1}{10}, \\ P(3) &= \frac{9}{10} \times \frac{9}{10} \times \frac{1}{10}, \\ &\vdots \\ P(n) &= \left(\frac{9}{10}\right)^{n-1} \times \frac{1}{10}\end{aligned}$$

É elementar verificar que  $P(n)$ ,  $n \geq 1$ , é uma série geométrica com soma 1. Portanto, o evento “o 7 nunca é sorteado”, indicado por 0, tem probabilidade complementar à  $P(1) + P(2) + \dots = 1$ , e sua probabilidade é zero.

Finalmente, considere o caso em que desejamos atribuir probabilidades dentro do conjunto não-enumerável  $\Omega = [0, 1]$ . Note que faz sentido atribuir probabilidade zero a um ponto qualquer:

$$P(X = a) = 0$$

e que é muito razoável atribuir probabilidades a intervalos:

$$P([a, b]) = b - a.$$

O problema é que se  $A$  é um evento, o seu complemento  $\overline{A}$  também tem que ser, com  $P(\overline{A}) = 1 - P(A)$ , pela propriedade de aditividade finita (1.3). Portanto, se  $(a, b] \in \mathcal{F}$ , devemos também ter  $\overline{(a, b]} \in \mathcal{F}$ , onde  $\mathcal{F}$  será a classe dos eventos cujas probabilidades podem ser quantificadas.

Entretanto, o complemento de um único intervalo  $(a, b]$  *não* é um único intervalo. Desconfiamos que uma criatura desse tipo,  $[0, a] \cup (b, 1]$ , precisa ser definida com as mesmas propriedades genéricas de  $(a, b]$ , de forma que ambos pertençam a  $\mathcal{F}$ . O caminho para  $\mathcal{F}$ , entretanto, é longo.

Uma extensão do que vimos para a binomial é a distribuição multinomial:

$$1 = (p_1 + \dots + p_n)^n = \sum_{l_1 + \dots + l_k = n} \binom{n}{l_1 \dots l_k} p_1^{l_1} \dots p_k^{l_k},$$

$$\binom{n}{l_1 \dots l_k} = \frac{n!}{l_1! \dots l_k!}.$$



# Capítulo 3

## 2014-02-26: Semi-anéis, anéis, e outros bichos

### Definição

Uma classe  $\mathcal{S}$  de conjuntos é um *semi-anel* quando:

$$\begin{aligned}\emptyset &\in \mathcal{S}, \\ A, B \in \mathcal{S} &\Rightarrow A \cap B \in \mathcal{S}, \\ A, B \in \mathcal{S} &\Rightarrow A - B = A \cap \overline{B} = \bigsqcup_{i=1}^n E_i,\end{aligned}$$

onde  $E_i \in \mathcal{S}$ . O símbolo  $\bigsqcup$  significa “uniões disjuntas”.

Seja  $\mathcal{S}$  a classe formada por *intervalos* do tipo

$$(a, b] \quad \text{ou} \quad \emptyset.$$

1.  $\emptyset \in \mathcal{S}$ ? Sim.
2. A interseção de dois elementos de  $\mathcal{S}$  pertence a  $\mathcal{S}$ ?

Sim: as possibilidades para interseção de  $(a, b]$  com  $(c, d]$  são

$$\begin{aligned}\emptyset &\in \mathcal{S}, \\ (c, b] &\in \mathcal{S}, \\ (c, d] &\in \mathcal{S}, \\ (a, d] &\in \mathcal{S}, \\ (a, b] &\in \mathcal{S}.\end{aligned}$$

Talvez seja possível resumir:

$$(a, b] \cap (c, d] = (\max(a, c), \min(b, d)) \quad \text{ou} \quad \emptyset?$$

3.  $A - B$  ( $A, B$  intervalos) é exprimível como uma união finita disjunta de intervalos?

Sim:

$$\begin{aligned}(a, b] \cap \overline{(c, d]} &= (a, b] \cap [(0, c] \cup (d, 1]] \\ &= \underbrace{(a, b] \cap (0, c]}_{\in \mathcal{S}} \cup \underbrace{(a, b] \cap (d, 1]}_{\in \mathcal{S}} \blacksquare\end{aligned}$$

Portanto, essa classe  $\mathcal{S}$  de intervalos é um semi-anel.

**Definição:**

$\mathcal{R} \subset 2^\Omega$  é um *anel* quando:

$$\begin{aligned}\emptyset &\in \mathcal{R}, \\ A, B \in \mathcal{R} &\Rightarrow A \cap B \in \mathcal{R}, \\ A, B \in \mathcal{R} &\Rightarrow A \Delta B \in \mathcal{R}.\end{aligned}$$

Lembre-se:

$$A \Delta B \equiv (A - B) \cup (B - A).$$

Tivemos uma discussão sobre o motivo de se usar a diferença simétrica nessas definições: alguém gostaria de resumir a discussão em L<sup>A</sup>T<sub>E</sub>X?

Anéis triviais são:

$$\{\emptyset, \Omega\} \quad \text{e} \quad 2^\Omega.$$

É possível mostrar as seguintes propriedades de anéis: se  $A, B \in \mathcal{R}$ , então:

$$\begin{aligned}A \cap B &\in \mathcal{R}, \\ A \Delta B &\in \mathcal{R}, \\ A \cup B &\in \mathcal{R}, \\ A - B &\in \mathcal{R}, \\ B - A &\in \mathcal{R}, \\ \emptyset &\in \mathcal{R}.\end{aligned}$$

Mas a última não faz parte da *definição* de  $\mathcal{R}$ ????

Note também que o complemento ainda não apareceu na jogada.

**Teorema**

A partir de um semi-anel  $\mathcal{S}$  é possível construir um anel  $\mathcal{R}$  por meio somente de uniões disjuntas finitas de elementos de  $\mathcal{S}$ , ou seja:

$$\mathcal{R} = \left\{ \bigcup_{i=1}^n A_i \right\}, \quad A_i \in \mathcal{S}.$$

**Definição**

Uma *álgebra* ou um *campo*  $\mathcal{A}$  é um anel que contém  $\Omega$ . Segue-se imediatamente que

$$A \in \mathcal{A} \Rightarrow \overline{A} \in \mathcal{A}.$$

**Definição** Um  $\sigma$ -anel é um anel fechado por uma união enumerável

Comentário: “fechado” significa que uniões enumeráveis de elementos do  $\sigma$ - $\mathcal{R}$  ainda pertencem a ele.

Segue-se imediatamente que o  $\sigma$ - $\mathcal{R}$  também é fechado por interseções enumeráveis.

**Definição** Uma  $\sigma$ -álgebra ou  $\sigma$ -campo ou campo de Borel é uma álgebra fechada por uniões enumeráveis.

Segue-se imediatamente que uma  $\sigma$ -álgebra também é fechada por interseções enumeráveis.

**Definição** Dada uma classe  $\mathcal{C} \subseteq 2^\Omega$ , uma sequência monótona de elementos  $E_i \in \mathcal{C}$ ,  $i \in \mathbb{N}$ , é definida por

$$E_i \subseteq E_{i+1}$$

ou

$$E_i \supseteq E_{i+1}.$$

**Definição** Uma classe  $\mathcal{M}$  é dita *monótona* quando todas as suas sequências monótonas atendem a:

$$E_i \subseteq E_{i+1} \Rightarrow \bigcup_{i=1}^n E_i \in \mathcal{M},$$

ou

$$E_i \supseteq E_{i+1} \Rightarrow \bigcap_{i=1}^n E_i \in \mathcal{M}.$$

A questão agora é como construir  $\sigma$ -álgebras a partir de álgebras, anéis ou semi-anéis.

**Teorema:** Para as famílias  $\mathcal{R}$ ,  $\mathcal{A}$ ,  $\sigma\text{-}\mathcal{R}$ ,  $\sigma\text{-}\mathcal{A}$ ,  $\mathcal{M}$  de anéis, álgebras, sigma-anéis, sigma-álgebras, e classes monótonas  $\mathcal{M}$ , interseções arbitrárias produzem famílias de mesmo tipo.

Em resumo: se  $\mathcal{F}_i$ ,  $i \in I$ , são classes de algum dos tipos acima, então

$$\bigcap_{i \in I} \mathcal{F}_i$$

também é.

Por exemplo: se

$$\mathcal{F}_i, i \in I$$

são  $\sigma$ -álgebras, então

$$\bigcap_{i \in I} \mathcal{F}_i$$

também é uma  $\sigma$ -álgebra.

### 3.1 Geração de $\sigma$ -álgebras

Seja  $\mathcal{S}$  um semi-anel que gera o anel  $\mathcal{R}$ . A *menor*  $\sigma$ -álgebra contendo  $\mathcal{S}$  ou gerada por  $\mathcal{R}$  é denominada “ $\sigma$ -álgebra de Borel”  $\mathcal{B}$ .

No caso de  $\Omega = [0, 1]$ , a  $\sigma$ -álgebra de Borel é a menor  $\sigma$ -álgebra que contém os intervalos  $(a, b]$ .

Para ela, é possível definir uma medida de probabilidade

$$\begin{aligned} P &: \mathcal{B} \rightarrow [0, 1], \\ A \in \mathcal{B} &\mapsto P(A) \in [0, 1], \end{aligned}$$

de tal forma que

$$P(\emptyset) = 0, \tag{3.1}$$

$$P(\Omega) = 1, \tag{3.2}$$

$$P\left(\bigsqcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} P(A_i). \tag{3.3}$$

# Referências Bibliográficas

Kolmogorov, A. N. (1933). *Grundbegriffe der Wahrscheinlichkeitsrechnung (Foundations of the theory of probability)*. Springer, Berlin.