Lições de Teoria Ergódica, Processos Estocásticos e Sistemas Dinâmicos

Nelson Luís Dias

11 de março 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 $n \to \infty$:
   $$P(A) \equiv \lim_{n\to\infty} \frac{m}{n}.$$

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 $(\Omega, \mathscr{F}, P)$, sendo Ω um conjunto não vazio, $\mathscr{F}$ um campo sigma (uma σ-álgebra) de subconjuntos de Ω (PRECISAMOS USAR OS TERMOS CORRETOS), e P uma função, com

$$P : \mathscr{F} \to [0,1],$$
$$A \in \mathscr{F} \mapsto P(A).$$

Axiomas:

$$P(A) \geq 0, \tag{1.1}$$
$$P(\Omega) = 1, \tag{1.2}$$
$$P\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i), \qquad \text{se} \qquad A_i \cap A_j = \emptyset. \tag{1.3}$$

Os axiomas funcionam quando Ω é finito. Contudo, há conjuntos maiores/infinitos (?) para os quais a noção de probabilidade não faz sentido. Assim, uma σ-álgebra será um subconjunto de 2^{Ω} 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 $n = 2$,

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

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

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

Então,

$$P\left(A_1 \cup ... \cup A_n \cup A_{n+1}\right) = P(B \cup A_{n+1}), \tag{1.5}$$

fazendo-se

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

A partir de (1.4),

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

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

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

Logo,

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

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

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

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

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

Se ela for verdadeira, então:

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

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

De fato,

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

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,

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

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

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

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

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

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

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

Como defino Ω? 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

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

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

(Ou σ–Aditividade)

Passamos agora para casos em que o espaço amostral Ω 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 Ω é finito, todos os elementos de 2^Ω 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

$$
\begin{gathered}
(0, 0, \ldots, 0, 0) \\
(0, 0, \ldots, 0, 1) \\
(0, 0, \ldots, 1, 0) \\
\vdots \\
(1, 1, \ldots, 1, 1).
\end{gathered}
$$

Existem 2^n casos.

Suponha por exemplo que desejemos calcular a probabilidade de que ocorram k caras (e, consequentemente, $n - k$ 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. Concluímos 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 $\Omega = \{x_1, x_2, x_3, \ldots\}$ 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

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

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 $P(1) + P(2) + \ldots = 1$, 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 $(a, b] \in \mathscr{F}$, devemos também ter $\overline{(a, b]} \in \mathscr{F}$, onde $\mathscr{F}$ 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 $\mathscr{F}$. O caminho para $\mathscr{F}$, entretanto, é longo.

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

$$1 = (p_1 + \ldots + p_n)^n = \sum_{l_1 + \ldots + l_k = n} \binom{n}{l_1 \ldots l_k} p_1^{l_1} \ldots p_k^{l_k},$$
$$\binom{n}{l_1 \ldots l_k} = \frac{n!}{l_1! \ldots l_k!}.$$

Capítulo 3

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

Definição

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

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

onde $E_i \in \mathscr{S}$. O símbolo $\bigsqcup$ significa "uniões disjuntas".

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

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

1. $\emptyset \in \mathscr{S}$? Sim.

2. A interseção de dois elementos de $\mathscr{S}$ pertence a $\mathscr{S}$?

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

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

   Talvez seja possível resumir:

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

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

   Sim:

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

Portanto, essa classe $\mathscr{S}$ de intervalos é um semi-anel.
Definição:
$\mathscr{R} \subset 2^\Omega$ é um *anel* quando:

$$\begin{gathered}
\emptyset \in \mathscr{R}, \\
A, B \in \mathscr{R} \Rightarrow A \cap B \in \mathscr{R}, \\
A, B \in \mathscr{R} \Rightarrow A \vartriangle B \in \mathscr{R}.
\end{gathered}$$

Lembre-se:

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

Tivemos uma discussão sobre o motivo de se usar a diferença simétrica nessas definições: alguém gostaria de resumir a discussão em LaTeX?
Anéis triviais são:

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

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

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

Mas a última não faz parte da *definição* de $\mathscr{R}$????
Note também que o complemento ainda não apareceu na jogada.
Teorema
A partir de um semi-anel $\mathscr{S}$ é possível construir um anel $\mathscr{R}$ por meio somente de uniões disjuntas finitas de elementos de $\mathscr{S}$, ou seja:

$$\mathscr{R} = \left\{ \bigsqcup_{i=1}^{n} A_i \right\}, \ A_i \in \mathscr{S}.$$

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

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

Definição Um σ-anel é um anel fechado por uma união enumerável
Comentário: "fechado" significa que uniões enumeráveis de elementos do σ-$\mathscr{R}$ ainda pertencem a ele.
Segue-se imediatamente que o σ-$\mathscr{R}$ também é fechado por interseções enumeráveis.
Definição Uma σ-álgebra ou σ-campo ou campo de Borel é uma álgebra fechada por uniões enumeráveis.
Segue-se imediatamente que uma σ-álgebra também é fechada por interseções enumeráveis.

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

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

ou

$$E_i \supseteq E_i.$$

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

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

ou

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

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

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

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

$$\bigsqcap_{i \in I} \mathscr{F}_i$$

também é.

Por exemplo: se

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

são σ-álgebras, então

$$\bigsqcap_{i \in I} \mathscr{F}_i$$

também é uma σ-álgebra.

3.1 Geração de σ-álgebras

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

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

Para ela, é possível definir uma medida de probabilidade

$$P : \mathscr{B} \to [0, 1],$$
$$A \in \mathscr{B} \mapsto P(A) \in [0, 1],$$

de tal forma que

$$
\begin{aligned}
P(\emptyset) &= 0, \\
P(\Omega) &= 1, \\
P\left(\bigsqcup_{i=1}^{\infty} A_i\right) &= \sum_{i=1}^{\infty} P(A_i).
\end{aligned}
$$

Capítulo 4

2014-03-10: Existe um conjunto não-mensurável em $(0, 1]$

Uma nova operação será usada *ad nauseam* nesta lição. Para $x, y \in (0, 1]$:

$$x \boxplus y \equiv \begin{cases} x + y, & x + y \le 1, \\ x + y - 1, & x + y > 1. \end{cases} \tag{4.1}$$

Seguem-se imediatamente os seguintes fatos: para $x, y, z \in (0, 1]$,

$$x \boxplus y = y \boxplus x, \tag{4.2}$$

$$z = x \boxplus y \Leftrightarrow \exists\, r \in (-1, +1] : z = x + r. \tag{4.3}$$

Agora, para *qualquer* subconjunto E de $(0, 1]$, defina um novo conjunto $E(x)$

$$E(x) \equiv \{x \boxplus y,\ y \in E\}. \tag{4.4}$$

$E(x)$ é a *translação* (de uma distância x) do conjunto E.

Dúvida: $E \subseteq (0, 1]$ ou $E \in \mathscr{B}$?

Dúvida: "translação *em x*" me soa estranho, pois todo $y \in E$ é transladado *de x*.

Suponha que exista uma coisa tal como uma medida "natural" em $(0, 1]$. Para o intervalo $(a, b]$ essa medida é

$$|(a, b]| \equiv b - a. \tag{4.5}$$

Vamos supor, sem entrar em muitos detalhes, que para todo $B \in \mathscr{B}$, existe uma $|B|$ compatível com (4.5), *i.e.*, redutível a (4.5) se B for um intervalo.

A notação $E(x)$ é a usada por Taylor (1973).

Agora, se $E \in \mathscr{B}$, então,

$$|E(x)| = |E|. \tag{4.6}$$

Agora, como sempre, $\mathbb{Q}$ é o conjunto dos racionais. Esse conjunto é enumerável. Consideremos os racionais contidos em $(0, 1]$. Esse segundo conjunto é

$$Q \equiv \mathbb{Q} \cap (0, 1]. \tag{4.7}$$

Valeria a pena provar que

Q é enumerável.

Com essas definições à mão, estudemos então as propriedades dos conjuntos do tipo $Q(x)$.

1.
$$x \in (0,1] \Rightarrow x \in Q(x). \tag{4.8}$$
Será verdade? Como provar?
$$Q(x) = \{x \boxplus y,\ y \in Q\}$$
Se 0 pertencesse a Q, (4.8) seria trivial. Mas é quase, porque $1 \in Q$. Faça $y = 1$ acima; então,
$$x = x + 1 - 1 = x \boxplus 1 \in Q(x) \blacksquare$$

2.
$$x \in Q \Rightarrow Q(x) = Q. \tag{4.9}$$
De fato: para começar, $x, y \in Q \Rightarrow x \boxplus y \in Q$. De fato, $x \boxplus y \in (0,1]$, e tanto $x + y$ quanto $x + y - 1$, conforme for o caso, são números racionais em $(0,1]$. Isso basta!, pois, *neste caso*, $Q(x) = \{x \boxplus y,\ y \in Q\} = Q \blacksquare$

3.
$$x_1 - x_2 \notin \mathbb{Q} \Rightarrow Q(x_1) \cap Q(x_2) = \emptyset, \tag{4.10}$$
$$x_1 - x_2 \in \mathbb{Q} \Rightarrow Q(x_1) = Q(x_2). \tag{4.11}$$
Dessa forma, os conjuntos $\{Q(x),\ x \in (0,1]\}$ (que constituem uma *classe*, ou *família*) particionam o intervalo $(0,1]$ em subconjuntos disjuntos cuja união é o próprio $(0,1]$. Há bastante material aqui. Antes das deduções, vamos escrever formalmente essa última observação:
$$\bigcup_{x \in (0,1]} Q(x) = (0,1].$$
Note também que os índices na expressão acima são demasiados, devido a (4.11). Queremos chegar a uma afirmação mais econômica:
$$\bigsqcup_{x \in T} Q(x) = (0,1]$$
(note a disjunção). Na sequência, precisamos provar (4.10)–(4.11) e prosseguir na obtenção do conjunto T. Esse último se revelará um conjunto interessante, e na verdade o ponto final desta lição: T se revelará um conjunto *não mensurável*.

Para provar (4.10): Vamos tentar *reductio ad absurdum*. Seja $z \in Q(x_1)$ e $z \in Q(x_2)$: nesse caso, a interseção $Q(x_1) \cap Q(x_2)$ não seria o conjunto vazio. Porém, debaixo dessa hipótese:
$$z = x_1 \boxplus y,\ y \in Q,$$
$$z = x_2 \boxplus y,\ y \in Q.$$

Agora,

$$\begin{aligned}(x_1 \boxplus y) - (x_2 \boxplus y) &= x_1 - x_2, \text{ ou} \\ &= x_1 - x_2 - 1 \text{ ou} \\ &= x_1 - x_2 + 1.\end{aligned}$$

Portanto, subtraindo (dessa forma) as duas expressões acima,

$$(-1 \text{ ou } 0 \text{ ou } +1) = x_1 - x_2.$$

mas $(-1, 0, +1)$ são racionais, o que contraria a hipótese original sobre $x_1 - x_2$ ■

Para provar (4.11): Volte acima e escreva a expressão geral:

$$(x_1 \boxplus y) - (x_2 \boxplus y) = x_1 - x_2 + s,$$

onde, como vimos, ou $s = 0$ ou $s = -1$ ou $s = +1$. Reescreva:

$$x_1 \boxplus y = x_2 \boxplus y + (x_1 - x_2) + s.$$

Note agora que é *sempre* possível escrever $x_2 \boxplus y = x_2 + r$ (veja (4.3)), *onde agora r é racional*, e não necessariamente está em Q. Substitua:

$$x_1 \boxplus y = x_2 + r + s + (x_1 - x_2).$$

O lado esquerdo é um número em Q. Portanto, o lado direito é um número em Q:

$$x_2 + p \in Q, \tag{4.12}$$

onde $p = (r + s + (x_1 - x_2))$ e portanto $p \in \mathbb{Q}$ (mas não necessariamente $p \in Q$). Agora, utilizando (4.3), vemos que é possível escrever o lado direito como $x_2 \boxplus z$, onde $z \in Q$. Disso se segue que

$$\{x_1 \boxplus y,\ y \in Q\} = \{x_2 \boxplus z,\ z \in Q\}$$

e portanto $Q(x_1) = Q(x_2)$ ■

Relembrando:

$$x \in Q \Rightarrow Q(x) = Q$$

significa, por exemplo:

$$Q(1/2) = Q(1/3) = Q(1).$$

$$x_1 - x_2 \in \mathbb{I} \Rightarrow Q(x_1) \cap Q(x_2) = \emptyset$$

significa, por exemplo:

$$Q(\sqrt{3}/2) \cap Q(3/2) = \emptyset.$$

$$x_1 - x_2 \in \mathbb{Q} \Rightarrow Q(x_1) = Q(x_2)$$

significa, por exemplo:

$$Q(\sqrt{2}/1000 + 1/8) = Q(\sqrt{2}/1000 + 3/8)$$

Ou seja: as criaturas estão ficando estranhas.

Para fechar esta parte bastante cansativa para a mente:

$$\bigcup_{x \in (0,1]} Q(x) = (0, 1]$$

pois $x \in Q(x)$.

4.1 O axioma da seleção e um conjunto estranho

Seja $\mathscr{C}$ a família dos conjuntos $Q(x)$, $x \in (0,1]$. Escolha um único ponto em $(0,1]$ pertencente a cada $Q(x)$. O conjunto dos pontos assim escolhidos será chamado T, e temos que $T \subset (0,1]$. O que fizemos significa que, *por definição*, não há dois pontos em T pertencendentes ao mesmo $Q(x)$. Segue-se que

$$\bigsqcup_{t \in T} Q(t) = (0,1].$$

Estudemos as propriedades dos conjuntos $T(r_i), r_i \in Q$.

1. $$\bigcup_{i=1}^{\infty} T(r_i) = (0,1]. \tag{4.13}$$

   Só precisamos provar que, se $x \in (0,1]$, $\exists i \in Q : x \in T(r_i)$. Mas, de (4.8), segue-se que $x \in (0,1] \Rightarrow x \in Q(x)$. Agora, portanto, se $x \in Q(x)$, escolha $t \in Q(x)$, onde t é o representante de $Q(x)$: $t \in T$.

   Veja:

   $$Q(x) = x \boxplus y, \ y \in Q,$$
   $$t \in Q(x) \Rightarrow t = x \boxplus y \text{ para algum } y \in Q.$$

   Logo, de (4.3), existe algum $q \in Q$ tal que $t = x + q$; pelo mesmo motivo agora deve existir algum $r \in Q$ tal que $x = t + r$. Mas Q é enumerável (não provamos!), portanto existe um índice i tal que $x = t + r_i$, $i \in \mathbb{N}$, e $Q = \bigsqcup_{i=1}^{\infty} r_i$. Logo, $x \in T(r_i)$. A união dos $T(r_i)$ gera o $(0,1]$.

2. Os $T(r_i)$ são disjuntos. Lembre-se de que T contém um único representante de cada $Q(x)$. Se houvesse $r_i \neq r_j$ com $y \in [T(r_i) \cap T(r_j)]$, então teríamos

   $$y = t_i \boxplus r_i \qquad \text{e}$$
   $$y = t_j \boxplus r_j.$$

   "Subtraia":

   $$0 = (t_i - t_j) + q$$

   onde q é racional (novamente, nós usamos (4.3)). Logo, $t_i - t_j$ é racional, donde $Q(t_i) = Q(t_j)$ (devido a (4.11)). Mas isso não é possível, porque $Q(t_i)$ possui um único representante em T. Portanto, a disjunção dos $T(r_i)$'s transforma (4.13) em

   $$\bigsqcup_{i=1}^{\infty} T(r_i) = (0,1]. \tag{4.14}$$

Finalmente: se T fosse mensurável, haveria $|T| = |T(r_i)|$ para todo i. Agora, pela sigma-aditividade:

$$\sum_{i=1}^{\infty} |T(r_i)| = |(0,1]| = 1.$$

Isso, nós também já vimos em outra lição, é impossível. T não pode ser mensurável ■

Referências Bibliográficas

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

Taylor, S. J. (1973). *Introduction to measure and integration*. Cambridge University Press.