6 Indução bem fundada

6.1 Relações bem fundadas

Definição 140. Uma relação $\prec$ sobre $A \neq \varnothing$ é dita **bem fundada** se todo subconjunto não vazio $S \subseteq A$ contém um elemento minimal com respeito $\prec$, ou seja, existe $m \in S$ tal que para qualquer $n \in S$ *não pode valer* $n \prec m$. Notemos que a relação deve ser irreflexiva, caso contrário teríamos $m \prec m$.

Equivalentemente, $\prec$ sobre $A \neq \varnothing$ é bem fundada se, e somente se, vale a **condição de cadeia descendente**: não existe uma sequência (x_n) de elementos de A tal que $x_{i+1} \prec x_i$ para todo i, ou seja, em A não há uma cadeia da forma $\cdots \prec x_2 \prec x_1 \prec x_0$.

Exercício 141. Verifique a equivalência das definições.

Toda ordem estrita de uma boa ordem é uma relação bem fundada. Isso decorre imediatamente das definições de cada um desses conceitos.

Exemplo 142. Em particular o $<$ sobre $\mathbb{N}$ é uma relação bem fundada, porém, o $\leqslant$ sobre $\mathbb{N}$ não é uma relação bem fundada.

Exemplo 143. A relação S sobre $\mathbb{N}$ dada por $n\ S\ m$ se e só se $m = n+1$ é bem fundada pois qualquer $A \subseteq \mathbb{N}$ não vazio tem mínimo m pro qual não existe $n \in A$ tal que $n\ S\ m$.

Os inteiros positivos com a relação definida por $x \mid y$ e $x \neq y$ é relação bem fundada.

A inclusão própria $\subsetneq$ sobre 2^X, o conjunto das partes de um conjunto X é bem fundada, uma vez que um dado subconjunto não vazio $S \subseteq 2^X$ contém pelo menos um conjunto $A \in S$ de modo que não seja um subconjunto próprio de qualquer outro conjunto $B \in S$.

A relação de pertinência $\in_X := \{(a,b) \in X \times X \colon a \in b\}$ definida em um conjunto X é bem fundada. Isso decorre do axioma da fundação (ou regularidade, página 23). O axioma da fundação garante que não há uma sequência (x_n) de elementos tal que ocorra $\cdots \ni x_2 \ni x_1 \ni x_0$.

Também é uma relação bem fundada sobre o conjunto de todas as palavras[2] sobre um alfabeto fixo e totalmente ordenado com a ordem definida por: $w \prec w'$, para palavras w e w', se w é mais curta (tem menos letras) que w' e no caso de empate w é lexicograficamente menor que w'.

A relação $\prec$ sobre $\mathbb{N} \times \mathbb{N}$ dada por $(a,b) \prec (x,y)$ se, e só se, $a < x$ e $b < y$ é uma relação bem fundada. Tome X_1 o conjunto das primeiras coordenadas dos elementos de X, que pelo PBO admite um mínimo m_1. Tome X_2 o conjunto das segundas coordenadas dos elementos de X_1, que pelo PBO admite um mínimo m_2. O par (m_1, m_2) é um elemento minimal de X. De fato, $(m_1, m_2) \in X$ e se $(x,y) \in X$ então $m_1 \leqslant x$ e $m_2 \leqslant y$, por definição de m_1 e m_2.

Uma razão importante pela qual as relações bem fundadas são interessantes é porque vale um princípio de indução nelas. Os princípios indutivos e definições recursivas que vimos são casos especiais de um princípio geral denominado indução bem fundada. Em essência, a indução estrutural, que ainda veremos, funciona porque decompor uma estrutura (e.g. conjunto, função, relação, estrutura de dados, linguagem) em subestruturas não pode continuar para sempre, eventualmente, chegamos em estruturas atômicas que não podem ser mais decompostas. Se uma propriedade falha em ser herdada por subestruturas então ela deve falhar em alguma estrutura mínimal que, quando quebrada, produz subestruturas que satisfazem a propriedade. A característica essencial compartilhada tanto pela relação de subestrutura quanto pela relação de predecessor nos números naturais é que eles não dão origem a cadeias descendentes infinitas.

6.1.1 Indução bem fundada

O seguinte resultado é conhecido como **indução noetheriana**.

Teorema 144 (Princípio de indução completo para relação bem fundada) *Sejam A um conjunto, $\prec$ uma relação bem fundada sobre A e P uma propriedade de elementos de A. Todos os elementos de A têm a propriedade P sempre que*

para todo $y \in A$, se $P(x)$ é verdadeiro para todo $x \prec y$, então $P(y)$ é verdadeiro.

Dizendo de outro modo, em símbolos, $P(a)$ é verdadeira para todo $a \in A$ se é verdadeira a sentença

$$\forall y \in A\big(\forall x \in A(x \prec y \to P(x)) \to P(y)\big) \tag{6.7}$$

Na utilização desse resultado, a base da indução é o caso quando y não tem predecessores por $\prec$ e nesse caso a sentença $\forall x \in A(x \prec y \to P(x))$ é verdadeira por vacuidade, portanto, temos que verificar que $P(y)$ vale nos elementos minimais de A com respeito a ordem. No caso da relação $<$ em $\mathbb{N}$ (exemplo 142) temos de (6.7) o PIFc e no caso da relação de sucessor em $\mathbb{N}$, exemplo 143, em (6.7) temos o PIF.

[2] Dado um alfabeto Σ, uma palavra é uma cadeia finita $\ell_1 \ell_2 \ldots \ell_t$ de elementos (as letras) do alfabeto, $\ell_i \in \Sigma$.

Demonstração do teorema 144. Sejam A um conjunto, $\prec$ uma relação bem fundada sobre A e P uma propriedade de elementos de A. A demonstração é por contradição. Suponhamos que exista $a \in A$ para o qual não vale $P(a)$. Seja $X := \{x \in A\colon \text{não-}P(x)\}$ o conjunto não vazio dos contraexemplos de P.

De $\prec$ bem fundada temos que X tem um elemento mimimal m e, por definição, para todo $x \in A$ tal que $x \prec m$ a propriedade P vale, isto é, $P(x)$ é verdadeiro. Portanto, de (6.7) (para $y = m$) temos que $P(m)$ é verdadeiro, uma contradição. □

Um exemplo de demonstração na ordem estrita e bem fundada $(\mathbb{N} \setminus \{0,1\}, <)$ foi dada na página 52 quando provamos o teorema fundamental da aritmética. Reveja: Seja $P(n)$ a sentença *n é primo ou pode ser escrito como produto de primos.* 2 é primo, portanto $P(2)$ é verdadeiro. Seja $y > 2$ um natural arbitrário. Se y é primo então o $P(y)$ é verdadeiro, senão y é composto. Se para qualquer $x < y$ no domínio vale $P(x)$, então, como $y = a \cdot b$, para $a < y$ e $b < y$, temos que y é produto de primos pois $P(a)$ e $P(b)$ são verdadeiros. Por indução $P(n)$ é verdadeiro para todo n.

Exemplo 145 (**função de Ackermann**). A função de Ackermann $A\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ definida recursivamente por

$$A(x,y) = \begin{cases} y+1 & \text{se } x = 0 \\ A(x-1,1) & \text{se } x > 0 \text{ e } y = 0 \\ A(x-1, A(x,y-1)) & \text{c.c.} \end{cases}$$

é conhecida pela extraordinária velocidade com que cresce, $A(0,y) = y+1$, $A(1,y) = y+2$, $A(2,y) = 2y+3$, $A(3,y) = 2^{y+3} - 3$, $A(4,1) = A(5,0) = 65533$, $A(4,2) = 2^{65536} - 3$ e

$$A(4,y) = 2^{2^{2^{\cdots^{2}}}} - 3$$

onde as potências formam uma torre com $y+3$ ocorrências de 2's. Mais que isso, essa função é um contraexemplo importante para a conjectura de que toda função computável é primitiva recursiva.

Nesse caso devemos ter uma relação sobre os pares (x,y) com condição de cadeia descendente para garantir a condição de parada da recorrência da definição de A.

A função de Ackermann está bem definida, ou seja, existe e é única a imagem de cada par de naturais (x,y) pela função A que satisfaz 145. Considere a ordem lexicográfica estrita $\lhd$ sobre $\mathbb{N} \times \mathbb{N}$ que é bem fundada. O valor $A(0,0)$ está definido e é 1. Seja $(x,y) \neq (0,0)$ arbitrário e assuma que $A(x_0,y_0)$ está definido para todo $(x_0,y_0) \lhd (x,y)$. Vamos mostrar que $A(x,y)$ está definido em três casos: (1) $x = 0$; (2) $x \neq 0$ e $y = 0$; (3) $x, y \neq 0$.

No caso (1), se $x = 0$, então $A(0,y)$ está definido e vale $y+1$. No caso (2), se $x \neq 0$ e $y = 0$, então em $(x-1,1) \lhd (x,0)$ a função está definida por indução, assim fica definido o valor $A(x,0) = A(x-1,1)$. No caso (3), se $x, y \neq 0$, então $(x,y-1) \lhd (x,y)$ de modo que $A(x,y-1)$ está definido por indução. Além disso, $(x-1, A(x,y-1)) \lhd (x,y)$, logo por indução $A(x-1, A(x,y-1)) = A(x,y)$ está definida. Portanto, a função está definida em todo par ordenado de números naturais.

Exemplo 146 (**teorema de Bachet–Bézout**). Vamos demostrar um teorema devido a Euclides (veja o exercício 79, página 42) usando indução bem fundada. O teorema enuncia que para todos os inteiros positivos m e n, existem inteiros x e y tais que $xm + yn = \text{mdc}(m,n)$. A prova é por indução em (m,n) usando a ordem lexicográfica estrita $\lhd$. Para o par $(1,1)$, mais geralmente (m,n) para $m = n$, temos $x = 1$ e $y = 0$. Seja (m,n) um par de inteiros positivos, podemos assumir que $m \neq n$. Assumamos que o enunciado é verdadeiro para todos os pares de inteiros positivos lexicograficamente menores que (m,n) e que $m > n$.

Como $(m-n,n) \lhd (m,n)$ existem inteiros x_0 e y_0 tais que $x_0(m-n) + y_0 n = \text{mdc}(m-n,n)$. Notemos que um divisor de m e de n também divide $m-n$, assim $x_0(m-n) + y_0 n = \text{mdc}(m,n)$. Ademais $x_0(m-n) + y_0 n = x_0 m + (y_0 - x_0)n$ de modo que para $x = x_0$ e $y = y_0 - x_0$ temos $xm + yn = \text{mdc}(m,n)$.

Exercício 147. Seja $I \subset \mathbb{N}$ o conjunto definido recursivamente no exemplo 114. Defina em $\mathbb{N}$ a relação bem fundada $\prec$ por $a \prec b$ se, e só se, b pode ser obtido a partir de a por somas sucessivas de 2. Por exemplo, $1 \prec 3$ e $3 \prec 131$, mas $1 \not\prec 2$, $1 \not\prec 20$ e $3 \not\prec 8$.

1. Verifique que a relação é bem fundada.
2. Prove usando a indução noetheriana que I é o conjuntos dos naturais ímpares.

Estruturas definidas recursivamente e indução estrutural

A indução estrutural é uma generalização do PIFc e um caso da indução noetheriana para uma estrutura definida recursivamente, é usada para provar que alguma propriedade vale para todo elemento dessa estrutura que tem uma ordem bem fundada subjacente. Tais estruturas como, por exemplo, fórmulas, listas ou árvores são comuns em disciplinas da matemática discreta como a lógica, linguagens formais, teoria da computação e a teoria de grafos.

Exemplo 148. As fórmulas boolenanas formam um conjunto $\mathscr{F}$ das cadeias finitas de símbolos tomados do conjunto

$$\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow, (,), p_0, p_1, p_2, p_3, \ldots\}$$

chamado de alfabeto. O conjunto $\mathscr{F}$ é definido recursivamente por

1. para todo $i \in \mathbb{N}$, $p_i \in \mathscr{F}$;
2. se $\alpha, \beta \in \mathscr{F}$ então $(\neg\alpha) \in \mathscr{F}$ e $(\alpha \vee \beta) \in \mathscr{F}$ e $(\alpha \wedge \beta) \in \mathscr{F}$ e $(\alpha \rightarrow \beta) \in \mathscr{F}$ e $(\alpha \leftrightarrow \beta) \in \mathscr{F}$;
3. não há outros elementos em $\mathscr{F}$ além dos obtido pelo uso das regras 1 e 2 um número finito de vezes.

São exemplos de fórmulas p_1, $(\neg p_2)$ e $(p_3 \rightarrow (p_1 \wedge (\neg p_1)))$.

Nesse caso, consideramos a relação $\prec$ sobre $\mathscr{F}$ dada por $\alpha \prec \beta$ se, e só se, β pode ser obtida de α por uma aplicação da regra 2 acima. Por exemplo, $p_3 \prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$, $(\neg p_1) \not\prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$ e $(p_1 \wedge (\neg p_1)) \prec (p_3 \rightarrow (p_1 \wedge (\neg p_1)))$. Claramente vale a condição da cadeia descendente.

A indução noetheriana pode ser reescrita para fórmulas e obtemos o seguinte princípio de indução para fórmulas booleanas.

TEOREMA 149 *Seja P uma propriedade de fórmulas*

(1) se P é verdadeira para toda fórmula atômica e

(2) se P é verdadeira para α e β então também é verdadeira para $(\neg\alpha)$, para $(\alpha \wedge \beta)$, para $(\alpha \vee \beta)$, para $(\alpha \rightarrow \beta)$ e para $(\alpha \leftrightarrow \beta)$.

Então então P é verdadeira para toda $\alpha \in \mathscr{F}$.

O seguinte exemplo ilustra uma prova por indução.

Exemplo 150. Vamos provar usando a indução que *toda fórmula bem formada tem um quantidade par de parênteses.* Cada fórmula atômica tem 0 parênteses. Para todo α que tem um número par, digamos $2n$, de parênteses, $(\neg\alpha)$ tem $2n+2 = 2(n+1)$ parênteses, portanto par. Suponha que α e β tenham, respectivamente, $2n$ e $2m$ parênteses, então $(\alpha \wedge \beta)$ tem $2n+2m+2 = 2(n+m+1)$ parênteses (os casos $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$ e $(\alpha \leftrightarrow \beta)$ são idênticos). Pelo Princípio de indução para fórmulas toda fórmula bem formada tem um quantidade par de parênteses.

O exemplo a seguir ilustra uma **definição recursiva** de uma função definida em $\mathscr{F}$. Pelo princípio de indução em fórmulas, precisamos defini-la para as fórmulas atômicas e, assumindo definida para α e β, escrever a definição para as fórmulas obtidas de α e β usando os conectivos.

Exemplo 151. As vezes é conveniente medir a complexidade de uma FBF pelo seu *grau* dado por:

1. $\text{grau}(\alpha) = 0$ se $\alpha = p_i$ para algum i;
2. $\text{grau}(\neg\alpha) = \text{grau}(\alpha) + 1$ e $\text{grau}(\alpha \square \beta) = \max\{\text{grau}(\alpha), \text{grau}(\beta)\} + 1$, onde $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

Pelo princípio de indução a função grau está definida para toda fórmula de $\mathscr{F}$.

Exercício 152. Demonstre que para toda fórmula α vale que $\text{grau}(\alpha)$ é no máximo o número de conectivos lógicos que aparecem em α. Demonstre também que $\text{grau}(\beta) < \text{grau}(\alpha)$ para toda subfórmula própria β da fórmula α.

Exemplo 153 (**Árvore binária com raiz**). Uma árvore binária sobre $\mathbb{N}$ com raiz é uma tripla definida recursivamente por

1. se $r \in \mathbb{N}$ então $(, r,)$ é uma árvore binária com raiz r;
2. se E e D são árvores binárias com raiz, então (E, r, D) é uma árvore binária com raiz r. Nesse caso chamamos E de *subárvore esquerda* e D de *subárvore direita.*

Só consideraremos árvores obtidas por uma aplicação dessas regras um número finito de vezes.

Se T é uma árvore binária, as subárvores (binárias) da forma $(, r,)$ que ocorrem em T são chamadas de *folhas* de T. Os outros nós são ditos *internos.*

Um exemplo de árvore binária com raiz é $\big(\big(, 1, \big), 3, \big(, 2, \big)\big), 5, \big(, 4, \big)\big)$ que pode ser mais facilmente entendida pelo diagrama da figura 6.6 a seguir. As folhas são $(, 1,)$, $(, 2,)$ e $(, 4,)$, as quais denotamos simplesmente por 1, 2 e 4.

Outro exemplo de árvore binária com raiz é dado por $\big(\big(, 1, \big), 5, \big(, 2, \big)\big), 7, \big(\big(, 3, \big), 6, \big(, 4, \big)\big)\big)$ representada na figura 6.7 As folhas são 1, 2, 3 e 4.

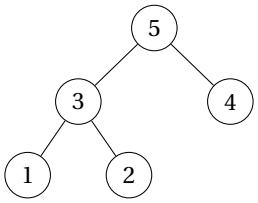

Figura 6.6: árvore binária

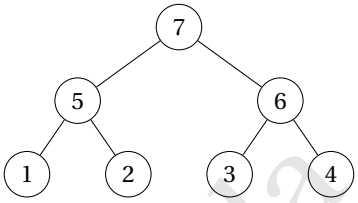

Figura 6.7: árvore binária

A *quantidade de nós* de uma árvore binária T é definida recursivamente por

$$n(T) = \begin{cases} 1 & \text{se } T = (,r,) \\ 1 + n(E) + n(D) & \text{se } T = (E,r,D), \end{cases}$$

e a *altura* de uma árvore binária T é definida recursivamente por

$$h(T) = \begin{cases} 0 & \text{se } T = (,r,) \\ 1 + \max\{h(E), h(D)\} & \text{se } T = (E,r,D). \end{cases} \tag{6.8}$$

As duas árvores dos exemplos anteriores, figuras 6.6 e 6.7, têm altura 2. Na figura 6.8 representamos uma árvore de altura 3. As folhas são $1,2,3,5,6$.

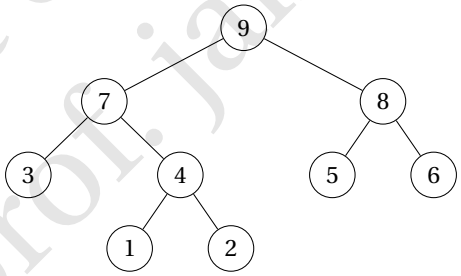

Figura 6.8: outra árvore binária

A relação $S \prec T$ definida por "S é a subárvore binária a esquerda ou a direita de T" é bem fundada, pela condição de cadeia descendente. Por exemplo,

$$\big(,1,\big),5,\big(,2,\big)\big) \prec \Big(\big(\big(,1,\big),5,\big(,2,\big)\big),7,\big(\big(,3,\big),6,\big(,4,\big)\big)\Big).$$

Agora, vamos provar usando indução que o número de nós numa árvore binária T de altura $h(T)$ é

$$n(T) \leqslant 2^{h(T)+1} - 1 \tag{6.9}$$

Se $T = (,r,)$ então $h(T) = 0$ e $n(T) = 1$, o que satisfaz (6.9). Seja $T = (E,r,D)$ uma árvore binária arbitrária e assuma que (6.9) é verdadeira para E para D. Por hipótese $n(E) \leqslant 2^{h(E)+1} - 1$ e $n(D) \leqslant 2^{h(D)+1} - 1$, logo

$$n(T) = 1 + n(E) + n(D) \leqslant 1 + 2^{h(E)+1} - 1 + 2^{h(D)+1} - 1 \leqslant 2 \cdot \max\{2^{h(E)+1}, 2^{h(D)+1}\} - 1$$

mas $\max\{2^{h(E)+1}, 2^{h(D)+1}\} = 2^{\max\{h(E),h(D)\}+1}$ que, por (6.8), é $2^{h(T)}$, portanto, $n(T) \leqslant 2 \cdot 2^{h(T)} - 1 = 2^{h(T)+1} - 1$. Pela indução noetheriana (6.9) vale para toda árvore binária.

Como no caso do PIF e PBO temos uma estratégia de prova por contradição: assumindo que no conjunto de todas as estruturas de um certo tipo há aquelas que não têm uma determinada propriedade, então o subconjunto de contraexemplos não é vazio, portanto, deve ter um elemento *minimal*. A partir desse contraexemplo mínimo derivamos uma contradição. Vejamos um exemplo.

Definimos árvore binária *plena* como árvore binária em que os nós internos têm, obrigatoriamente, dois descendentes, ou seja, na formação da árvore (E,r,D) não podemos ter E vazia nem D vazia, exceto nos casos base onde ambas são vazias.

PROPOSIÇÃO 154 *Em qualquer árvore binária plena o número de folhas é um a mais que o número de nós internos.*

DEMONSTRAÇÃO. Suponha que haja um contraexemplo para tal afirmação. Então deve existir um contraexemplo T com $i(T)$ nós internos e $f(T) \geqslant 1$ folhas onde $i(T) + 1 \neq f(T)$ e $\prec$-minimal.

O contraexemplo T não é da forma $(,r,)$ porque tal árvore tem 0 nós internos e 1 folha, portanto, $T = (E,r,D)$ com $E, D \neq \varnothing$. Pela minimalidade de T temos $i(E) + 1 = f(E)$ e $i(D) + 1 = f(D)$. Assim

$$f(T) = f(E) + f(D) = i(E) + i(D) + 2 = i(T) + 1$$

pois $i(E) + i(D) + 1 = i(T)$, contrariando o fato de T ser um contraexemplo. □

Uma demonstração alternativa da proposição acima usando o PBO é como segue. Suponha que haja um contraexemplo para tal afirmação. O contraexemplo T não é da forma $(,r,)$, logo tem pelo menos uma folha f cujo nó pai p é um nó interno. Exclua essa folha f e seu pai p da árvore, promovendo o nó irmão da folha f para a posição ocupada por seu pai (nó imediatamente acima no diagrama). Por exemplo, essa operação no nó 5 da árvore da figura 6.8 resulta na árvore da figura 6.9). O resultado dessa operação é uma árvore binária plena T' com uma folha e um nó interno a menos, portanto, $i(T') + 1 \neq f(T')$ e, portanto, é um contraexemplo menor, uma contradição.

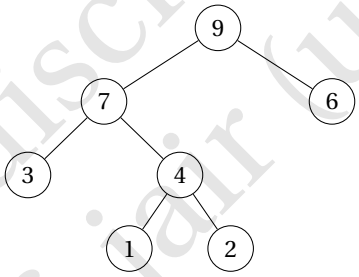

Figura 6.9: árvore binária plena obtida da árvore binária plena da figura 6.8 por remoção de uma folha (5) e seu pai (8).

Exercícios

1. Sejam $(A,\prec)$ e $(B,\sqsubset)$ duas ordens estritas. Tome em $A \times B$ a ordem lexicográfica estrita $\lhd$, isto é,

   $$(x,y) \lhd (a,b) \text{ se, e só se } x \prec a \text{ ou } (x = a \text{ e } y \sqsubset b).$$

   Prove que se $(A,\prec)$ e $(B,\sqsubset)$ são bem fundadas então $(A \times B, \lhd)$ é bem fundada.

2. Prove que a relação binária $\{(m,m+1) : m \in \mathbb{N}\}$ é uma ralação de ordem bem fundada sobre $\mathbb{N}$. Reescreva o princípio de indução para ordens bem fundadas para esse caso específico. É um resultado conhecido?

3. Prove que a relação de ordem estrita usual sobre $\mathbb{N}$ é bem fundada. Reescreva o princípio de indução para ordens bem fundadas para esse caso específico. É um resultado conhecido?

4. Prove que a relação de inclusão estrita de conjuntos é bem fundada se, e só se, o universo donde são tomados os subconjuntos é finito.

5. Prove que as três relações da seção 6.1.1, a saber $\alpha \prec \beta$ em fórmulas e "é uma subárvore binária própria de" e "tem menos nós" sobre árvores binárias, são relações bem fundadas.

6. **(Fechos de uma relação)** Seja $R \subseteq A \times A$ uma relação qualquer. Se S e T são duas relações reflexivas sobre A então $S \cap T$ também é uma relação reflexiva sobre A.

   (6.1) Demonstre que a interseção de duas relações reflexivas sore o mesmo conjunto é uma relação reflexiva.

   Ademais, se $R \subseteq S$ e $R \subseteq T$ então $R \subseteq S \cap T$. Podemos formar o conjunto $\mathscr{R}$ de todas as relações reflexivas que contêm R de modo que

   $$\bigcap \mathscr{R}$$

   é uma relação reflexiva que contém R, é a "menor" ($\subset$-minimal) relação com essa propriedade, chamada de **fecho reflexivo** de R. Por exemplo, o fecho reflexivo de $<$ sobre $\mathbb{N}$ é $\leqslant$.

   (6.2) Demonstre que não existe relação reflexiva S que contém R tal que $S \subsetneq \bigcap \mathscr{R}$.

   Analogamente, a interseção de relações transitivas sobre um conjunto A resulta numa relação transitiva, assim podemos formar o conjunto $\mathscr{T}$ de todas as relações transitivas que contêm R de modo que

   $$\bigcap \mathscr{T}$$

   é a "menor" ($\subset$-minimal) relação transitiva que contém R, chamada de **fecho transitivo** de R.

   (6.3) Demonstre os análogos de (6.1) e (6.2) para o fecho transitivo.

   Ainda, podemos formar o conjunto de todas as relações reflexivas e transitivas que contém R, tomar a interseção que resultada no fecho reflexivo e transitivo da relação R.

   (6.4) Demonstre os análogos de (6.1) e (6.2) para o fecho reflexivo e transitivo.

   (6.5) Seja $\prec$ uma relação bem fundada sobre um conjunto A. Demonstre que

   (a) o fecho transitivo de $\prec$ é uma relação bem fundada;

   (b) o fecho reflexivo e transitivo de $\prec$ é uma ordem parcial.

7. Prove usando indução que na linguagem livre de contexto S → ab | aSb | SS todas as palavras têm a mesma quantidade de símbolos a e b.

Construção dos Inteiros

Intuitivamente, digamos que queremos construir um conjunto de números onde $n-k$ faça sentido quaisquer que sejam os naturais n, k, por exemplo $4-11$. Façamos $-7 := 4-11$. Mas então há várias representações $-7 := 4-11 = 3-10 = 5-12 = \cdots$. Notemos que se $a-b = n-m$ então $a+m = b+n$ e se fizermos todas essas representações do -7 equivalentes temos uma relação de equivalência. Formalmente, considere a relação $\mathbf{Z} \subset \mathbb{N} \times \mathbb{N}$ definida por

$$(a,b)\mathbf{Z}(n,m) \text{ se, e só se } a+m = b+n$$

Z que é uma relação de equivalência.

Para cada (a,b), a *classe de equivalência de* (a,b) é o conjunto

$$[(a,b)] := \{(n,m) \in \mathbb{N} \times \mathbb{N} \colon (a,b)\mathbf{Z}(n,m)\}.$$

Por exemplo,

$$[(1,2)] = \{(0,1),(1,2),(2,3),(3,4),\ldots\}$$

$$[(5,2)] = \{(3,0),(4,1),(5,2),(6,3),\ldots\}$$

Notemos que $[(1,2)] = [(2,3)] = [(0,1)] \neq [(5,2)] = [(4,1)]$.

$\mathbb{Z}$ é o conjunto dessas classes de equivalência e seus elementos são chamados números inteiros.

Denotamos

$$0 := [(0,0)] = \{(n,n) : n \in \mathbb{N}\}$$
$$1 := [(1,0)] = \{(n+1,n) : n \in \mathbb{N}\}$$
$$-1 := [(0,1)] = \{(n,n+1) : n \in \mathbb{N}\}$$
$$-a := [(0,a)] = \{(n,n+a) : n \in \mathbb{N}\}$$

Se p é a classe $[(a,b)]$ e q a classe $[(n,m)]$, definimos $p+q$ como a classe de equivalência

$$p+q := [(a+n, b+m)]$$

Notemos que $[(1,2)] + [(5,2)] = [(0,1)] + [(3,0)]$. Definimos $p \cdot q$ como a classe de equivalência

$$p \cdot q := [(a \cdot n + b \cdot m, a \cdot m + b \cdot n)]$$

Definimos

$$p - q := p + (-q)$$

e definimos

$$p \leq q \Leftrightarrow q - p \in \mathbb{N}$$

para quaisquer inteiros p e q.

Números naturais e ordinais

No uso comum a palavra ordinal é um adjetivo para *ordem*, *posição* como primeiro, segundo, terceiro e assim por diante. Em teoria dos conjuntos são *tipos de ordem*, duas boas ordens são do mesmo tipo se são isomorfas (veja os exercícios 17 ao 28).

O conjunto $\mathcal{N}$ dos **ordinais finitos de Von Neumann** são dados pela definição recursiva

1. $\varnothing \in \mathcal{N}$
2. se $x \in \mathcal{N}$ então $x \cup \{x\} \in \mathcal{N}$.

Com isso os números naturais são definidos na teoria dos conjuntos ZF

$$0 = \varnothing$$
$$1 = \{\varnothing\} = \{0\}$$
$$2 = \{\varnothing, \{\varnothing\}\} = \{0,1\}$$
$$3 = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0,1,2\}$$

e assim por diante. Note que $0 \in 1 \in 2 \in 3$. De fato $\in$ é uma relação bem fundada em $\mathcal{N}$.

Tomando a função sucessor $S(n) = n \cup \{n\}$, a estrutura $(\mathcal{N}, 0, S)$ em que 0 é constante dada pelo conjunto vazio, satisfaz os axiomas de Peano:

1. Todo número natural possui um único sucessor, que também é um número natural.
2. Existe um único número natural, o 0, que não é sucessor de nenhum outro.
3. Números naturais diferentes possuem sucessores diferentes.
4. Se um conjunto de números naturais contém o número 0 e, além disso, contém o sucessor de cada um dos seus elementos, então esse conjunto coincide com o conjunto dos números naturais.

Podemos ir além dos ordinais finitos. O conjunto $\omega = \bigcup_{n \in \mathcal{N}} n$ não é sucessor de outro ordinal e é o primeiro ordinal infinito (ou, não finito). A partir da podemos tomar sucessores (agora escrito como +1)

$$\omega + 1 = \omega \cup \{\omega\} = \{0,1,2,\ldots,\omega\}$$
$$\omega + 2 = \omega + 1 \cup \{\omega + 1\} = \{0,1,2,\ldots,\omega,\{\omega\}\}$$

e assim por diante, usando a definição recursiva acima e, em seguida, temos o próximo ordinal que não é sucessor de outro ordinal $\omega + \omega = \bigcup_{\alpha \in \omega + \omega} \alpha$.

Cada ordinal de von Neumann é o conjunto bem ordenado dos ordinais menores e pode-se provar que todo conjunto bem ordenado é isomorfo a um ordinal von Neumann. Eles podem ser construídos da seguinte forma:

1. 0 é o conjunto vazio ;

2. se α é ordinal então $\alpha+1=\alpha\cup\{\alpha\}$ é ordinal;

3. se A é um conjunto de ordinais então $\bigcup A$ é ordinal.

Os $\alpha+1$ são **ordinais sucessores** e os $\bigcup A$ são **ordinais limites**, que não são sucessores de outro ordinal. Os ordinais de von Neumann têm a propriedade conveniente que, se $\alpha<\beta$ então $\alpha\in\beta$ e $\alpha\subsetneq\beta$.

Os números ordinais são $0,1,2,3,\ldots,\omega,\omega+1,\omega+2\omega+2,\ldots,\omega+\omega,\omega+\omega+1,\ldots$. Não há um maior ordinal, nem o conjunto de todos os ordinais.

Agora, podemos generalizar facilmente o conceito de sequência pois se α é um ordinal então uma **sequência transfinita** de elementos de X, denotado $(x_\beta)_{\beta\in\alpha}$ é uma função $x\colon \alpha\to X$. Uma indução similar ao PIF, ao invés do PIFc como vimos, pode ser escrita como: se $P(0)$ é verdadeiro; para todo $\beta\in\alpha$ sucessor, se $P(\beta)$ então $P(\beta+1)$ é verdadeiro; para todo β limite $P(\beta)$ é verdadeiro, então $P(\beta)$ é verdadeiro para todo $\beta\in\alpha$.

O teorema de Dilworth

O seguinte resultado é equivalente a vários teoremas importantes em combinatória, como o teorema de Hall[3] e o teorema de Birkhoff–Von Neumann[4], também é uma generalização do teorema de Erdős–Szekeres sobre subsequências monótonas[5].

Teorema 155 (Teorema de Dilworth) *Numa ordem parcial finita A, o menor número m de cadeias tal que todo elemento de A pertence a alguma dessas cadeias é igual ao número máximo de elementos M em uma anticadeia de A.*

Demonstração. Vamos provar que $m\leqslant M$. A prova é por indução completa em $n=|A|$.

Se $n=1$, então $m=M$. Seja $k\geqslant 1$ um natural arbitrário e assuma que para toda ordem parcial com $\leqslant k$ elementos o teorema é verdadeiro.

Tome $(A,\preccurlyeq)$ uma ordem parcial com $k+1$ elementos e considere C uma cadeia maximal (com respeito a inclusão) em A.

Se toda anticadeia em $A\setminus C$ tem no máximo $M-1$ elementos, então $A\setminus C$ pode ser escrito como união de no máximo $M-1$ cadeias, por hipótese da indução, que com a cadeia C formam no máximo M cadeias tal que todo elemento de A pertence a alguma dessas cadeias. Portanto $m\leqslant M$.

Agora suponha que X seja uma anticadeia em $A\setminus C$ com M elementos e defina os conjuntos

$$X^-=\{x\in A\colon x\preccurlyeq a \text{ para algum } a\in X\}$$
$$X^+=\{x\in A\colon a\preccurlyeq x \text{ para algum } a\in X\}$$

de $|X|=M$, o tamanho máximo de uma anticadeia, $A=X^-\cup X^+$, caso contrário haveria z incomparável como os elementos de X e $X\cup\{z\}$ seria uma anticadeia.

Se $|X^+|,|X^-|<|A|$ então, pela hipótese da indução, $|X^+|$ pode ser escrito como união de $\leqslant M$ cadeias cujos mínimos estão em X e $|X^-|$ pode ser escrito como união de $\leqslant M$ cadeias cujos máximos estão em X. Portanto P é união de $\leqslant M$ cadeias.

Resta verificar que $|X^+|,|X^-|<|A|$. Isso segue do fato de $\max(C)\notin X^-$ e $\min(C)\notin X^+$. Portanto, pelo PIFc, para todo natural n, o teorema vale para uma ordem parcial com n elementos. □

Exercício 156. Seja $a_1,a_2,\ldots,a_{n^2+1}$ uma sequência de números reais. Uma subsequência $i_1<i_2<\cdots<i_k$ é dita *monótona crescente* (respec., monótona decrescente) se $a_{i_1}\leqslant a_{i_2}\leqslant\cdots\leqslant a_{i_k}$ (resp. $a_{i_1}\geqslant a_{i_2}\geqslant\cdots\geqslant a_{i_k}$). A sequência é *monótona* se for monótona crescente ou monótona decrescente.

Use o teorema de Dilworth para provar a seguinte afirmação, o teorema de Erdős–Szekerés: toda sequência $a_1,a_2,\ldots,a_{n^2+1}$ de números reais contém uma subsequência monótona de comprimento $n+1$.

Lema de Zorn e teorema da boa ordem

> "The Axiom of Choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?" — Jerry Bona

Para encerrar essa seção enunciaremos dois resultados bem conhecidos e importantes para, por exemplo, provar que todo espaço vetorial tem base, o teorema de Hahn–Banach da análise funcional e o teorema de Tychonoff da topologia. O lema de Zorn é útil quando precisamos iterar algum tipo de operação "infinitamente muitas vezes" de maneira rigorosa.

[3] O teorema de Hall dá uma condição necessária e suficiente para poder selecionar elementos distintos de cada conjunto de uma família de conjuntos finitos.

[4] Toda matriz duplamente estocástica (cada linha e cada coluna somam 1) pode ser escrita como combinação convexa de matrizes de permutação (matriz quadrada 0-1 com um único 1 em cada linha e em cada coluna).

[5] Toda sequência de $mn+1$ números reais possui uma subsequência crescente de $m+1$ termos ou uma subsequência decrescente $n+1$ termos.

TEOREMA 157 (LEMA DE ZORN) *Seja $A \neq \varnothing$ um conjunto parcialmente ordenado tal que toda cadeia em A tem um limitante superior. Então A tem um elemento maximal.* □

TEOREMA 158 (TEOREMA DA BOA ORDEM) *Para todo conjunto A não vazio, existe uma ordem $\preccurlyeq$ tal que $(A, \preccurlyeq)$ é bem-ordenado.* □

O lema de Zorn e o Teorema da boa-ordem podem ser demonstrados na teoria ZFC de conjuntos usando o axioma da escolha. De fato, as três sentenças, Axioma da Escolha, Lema de Zorn e Teorema da Boa Ordem, são equivalentes no sentido que na teoria dos conjuntos assumindo os axiomas de ZF, se acrescentamos a boa-ordem aos axiomas, então provamos escolha e Zorn e se acrescentamos Zorn então provamos escolha e boa ordem . Por, exemplo, da boa ordem é fácil provar o "axioma" da escolha, a função escolha é $f(y) = \min(y)$.