Minicurso de Métodos de Prova

Renata de Freitas
e
Petrucio Viana

IME-UFF

II Colóquio de Matemática da Região Sul
24 a 28 de abril de 2012
Universidade Estadual de Londrina
Londrina, PR

Sumário

Capítulo 1

Introdução

Parte da dificuldade encontrada pelos alunos dos Cursos de Matemática não está na compreensão e utilização de conceitos matemáticos, mas no domínio da linguagem e dos raciocínios básicos, necessários para assimilar e expressar o conhecimento sobre esses conceitos.

Em particular, uma das principais características da Matemática é o uso de provas para justificar a veracidade das proposições. Em Matemática, uma prova serve tanto como um meio de assegurar quanto de comunicar a veracidade do teorema provado e, como é de conhecimento de todos, a inabilidade de um aluno em tratar com esta ferramenta fundamental pode prejudicar consideravelmente seu aprendizado.

Uma tentativa inicial de se resolver este problema seria o de elaborar processos sistemáticos para a prova de teoremas e processos didáticos que objetivassem ensinar estes processos aos alunos. Mas, da mesma maneira que não existe um método sistemático para provar teoremas [5], também parece não existir uma técnica universal para ensinar como os teoremas podem ser provados [7, 6]. Por outro lado, a experiência adquirida com o ensino de Matemática leva a crer que, muito embora nem todas as sutilezas da atividade matemática possam ser ensinadas, isto pode ser feito para uma quantidade razoável desta atividade [4, 11].

Uma das principais conquistas da Lógica Matemática [2, 5, 12] foi a determinação de que, embora não exista uma maneira sistemática de provar teoremas, existem certos métodos ou regras de prova que, quando utilizados de uma forma organizada, fornecem:

- Um método para se verificar que uma dada prova, feita de acordo com as regras, está correta.
- A elaboração de estratégias de prova que, embora possam não levar à

prova do teorema em questão, levam a uma melhor compreensão de quais passos podem ser efetuados para que o teorema seja provado.

Neste texto, apresentamos certas técnicas, desenvolvidas para que um estudante de matemática possa projetar estratégias de como provar um dado teorema. Em particular, utilizando as técnicas apresentadas, é possível aprender como escrever, ler e até mesmo fazer a prova de teoremas simples. Os exemplos iniciais servirão como um ingresso neste intrincado mundo que é a arte de provar teoremas.

Não é possível, em um texto com estas dimensões, abordar todos os métodos de prova. Não vamos, nem ao menos, citar todos os métodos básicos. Este texto apresenta apenas alguns métodos, para ilustrar as considerações gerais desenvolvidas nos primeiros capítulos. No entanto, para não deixar a falsa impressão de que os métodos de prova em matemática se resumem aos métodos básicos, no capítulo final apresentamos o *Princípio das Casas de Pombo*, um método de prova utilizado na justificativa de certos resultados em vários ramos da Matemática. Nosso objetivo, neste capítulo, é apresentar um exemplo de método de prova que não é, usualmente, utilizado para a justificativa de resultados nos cursos de graduação. Queremos deixar claro que não existe uma catalogação fechada de todos os métodos de prova e que a arte de provar teoremas, que é o coração da atividade matemática, está sempre sendo renovada. No instante em que você lê este parágrafo, grupos de matemáticos, pelo mundo, estão desenvolvendo novos métodos de prova.

É preciso enfatizar que este texto não foi escrito para o público em geral, mas apenas para estudantes de matemática.

Capítulo 2

Justificativas em Matemática

Neste capítulo, mostramos que a *evidência* não pode ser usada como um critério objetivo para a *justificativa* de enunciados matemáticos. Em Matemática, os enunciados devem ser *provados*.

2.1 Princípio da razão suficiente

A investigação científica é regida pelo **Princípio da Razão Suficiente**:

Em ciência, todo enunciado deve ser justificado.

Isto é, para que possa ser aceita como um fato científico, um enunciado deve vir acompanhado de uma justificativa.

Consideramos que as ciências se dividem em **empíricas** (tais como a Física) ou **formais** (tais como a Matemática).

Nas ciências empíricas, as justificativas são argumentações apoiadas em observações e experiências ou, caso essas observações e experiências não sejam viáveis, em indicações acerca da possibilidade de comprovação mediante observações e experiências.

Exemplo 2.1.1 Considere o enunciado: *a Terra não é plana.* Uma justificativa para este enunciado foi apresentada por Eratóstenes de Cirene, no século II a.C., e pode ser resumida na seguinte argumentação:

> *Na cidade de Siene existe um poço cujas águas, a cada 21 de junho, ao meio dia, refletem o Sol, quando este se encontra no ponto mais alto do céu. Em Alexandria, situada a 800 km de Siene, no mesmo dia e na mesma hora, existe um obelisco que projeta uma sombra bastante pronunciada. O Sol está tão distante no espaço que seus*

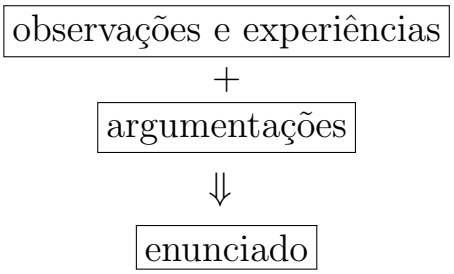
> *raios ao chegarem à superfície da Terra são praticamente paralelos. Assim, se a Terra fosse plana, no mesmo instante em que as águas do poço em Siene refletem o Sol, o obelisco em Alexandria não poderia projetar uma sombra tão pronunciada. Logo, a Terra não é plana.*

Para que seja aceita como uma justificativa de um fato científico, a argumentação apresentada por Eratóstenes deve estar apoiada em experiências que comprovem todos os fatos utilizados como apoio ao enunciado. Por exemplo, que os raios do Sol são praticamente paralelos quando chegam à superfície da Terra.

Assim, no caso das ciências empíricas, se queremos justificar um enunciado e, podemos fazer o seguinte:

1. Apresentar justificativas para e, apoiadas em observações e experiências.
2. Utilizar essas justificativas para argumentar em favor da verdade de e.

A figura a seguir resume como se dá a justificativa de enunciados no caso das ciências empíricas.



2.2 Enunciados evidentes e não-evidentes

Como a Matemática lida com entes abstratos, tais como números e figuras, a justificativa de enunciados matemáticos não pode ser apoiada em observações e experiências. Somos assim levados à questão:

Como justificar enunciados matemáticos?

Numa primeira tentativa de responder a esta questão, poderíamos classificar os enunciados matemáticos em **evidentes** e **não-evidentes**. Os enunciados evidentes não necessitariam de justificativa. Os não-evidentes seriam aqueles que deveriam ser justificados.

Exemplo 2.2.1 (a) Considere o enunciado: *2 é um número par.* À primeira vista, este enunciado poderia ser classificado como evidentemente verdadeiro e, portanto, pareceria não necessitar de justificativa.

(b) Considere o enunciado: *2 é um número ímpar.* À primeira vista, este enunciado poderia ser classificado como evidentemente falso e, portanto, pareceria não necessitar de justificativa.

Mas a evidência de um enunciado não pode ser considerada um bom critério para julgá-lo. Isso se dá por, pelo menos, três motivos:

1. Evidência é um conceito muito impreciso, isto é, dado um enunciado, pode ser muito difícil classificá-lo como evidente ou não-evidente.
2. Evidência é um conceito relativo, isto é, o que é evidente para algumas pessoas pode não ser evidentes para outras, e vice-versa.
3. Evidência é um conceito enganoso, isto é, alguns enunciados que à primeira vista parecem ser evidentemente verdadeiros (falsos), na verdade são falsos (verdadeiros).

Existem vários casos em que podemos nos deixar enganar pelo aspecto evidente de um enunciado.

Exemplo 2.2.2 Considere o enunciado: *o conjunto dos números pares e o conjunto dos números naturais têm a mesma quantidade de elementos.* Este enunciado parece evidentemente falso. Na verdade, ele contradiz um outro enunciado mais geral: *dado um conjunto qualquer, ele possui mais elementos que cada uma de suas partes próprias.* Assim, como o conjunto dos números pares é apenas uma parte do conjunto dos números naturais, aparentemente, existem mais números naturais que números pares e somos levados a concluir que o enunciado é falso.

Apesar de parecer evidentemente falso, podemos justificar que o enunciado acima é verdadeiro. Uma argumentação que justifica sua veracidade está baseada no conceito de bijeção.

Uma **bijeção** entre dois conjuntos A e B é uma maneira de associar os elementos de A e os elementos de B, de modo que cada elemento de A esteja associado a um único elemento de B e cada elemento de B esteja associado a um único elemento de A. Por exemplo, dados os conjuntos $A = \{1, 2, 3\}$ e $B = \{2, 4, 6\}$, uma bijeção entre seus elementos é dada na figura:

$$\begin{array}{ccc} 1 & \leftrightarrow & 2 \\ 2 & \leftrightarrow & 4 \\ 3 & \leftrightarrow & 6 \end{array}$$

A idéia de que, para definir uma bijeção entre os conjuntos A e B, devemos associar cada elemento de A a um elemento de B e um elemento de B a cada elemento de A, nos leva a considerar que quando existe uma bijeção entre dois conjuntos, eles possuem a mesma quantidade de elementos.

Podemos definir uma bijeção entre os elementos do conjunto dos números naturais e os elementos do conjunto dos números pares. Para isto basta associar cada número natural n ao seu dobro $2n$.

$$\begin{array}{ccc} 1 & \leftrightarrow & 2 \\ 2 & \leftrightarrow & 4 \\ 3 & \leftrightarrow & 6 \\ 4 & \leftrightarrow & 8 \\ \vdots & \vdots & \vdots \end{array}$$

De fato, como cada número natural possui um único dobro, que é um número par, e cada número par é o dobro de um único número natural, a associação acima é uma bijeção, o que mostra que existem tantos números naturais quanto números pares.

Exemplo 2.2.3 Um dos princípios básicos da Teoria dos Conjuntos, tal como é apresentada no Ensino Médio, é o **Princípio da Abstração**:

> *Dada uma propriedade qualquer $P(x)$, referente a objetos x, existe o conjunto $A = \{x : P(x)\}$, formado por todos os objetos que possuem a propriedade $P(x)$.*

Por exemplo, dada a propriedade *x é ser humano*, existe o conjunto

$$H = \{x : x \text{ é ser humano}\},$$

formado por todos os seres humanos. E dada a propriedade *x é ser abstrato*, existe o conjunto

$$A = \{x : x \text{ é ser abstrato}\},$$

formado por todos os seres abstratos.

Tal como é formulado e exemplificado no Ensino Médio, o Princípio da Abstração parece ser um enunciado evidentemente verdadeiro. Mas, apesar de parecer evidentemente verdadeiro, o Princípio da Abstração é falso.

Uma argumentação que justifica sua falsidade está baseada nos conceitos de conjuntos normal e anormal.

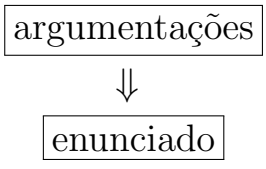
Um conjunto é **normal** se não possui a propriedade que o define. Por exemplo, o conjunto dos seres humanos é normal, já que não é um ser humano. Um conjunto é **anormal** se possui a propriedade que o define. Por exemplo, o conjunto dos seres abstratos é anormal, já que é abstrato. Observe que, dado um conjunto qualquer, ou ele é normal ou ele é anormal.

Considere agora a propriedade: *X é conjunto normal*. De acordo com o Princípio da Abstração, existe o conjunto $N = \{X : X \text{ é conjunto normal}\}$, formado pelos conjuntos normais. Assim, por exemplo, H é um elemento de N, já que é um conjunto normal. Por outro lado, A não é um elemento de N, já que é um conjunto anormal. Como todo conjunto ou é normal ou é anormal, dado um conjunto qualquer, ou ele é um elemento de N ou ele não é um elemento de N. Podemos agora fazer a seguinte pergunta: em qual das duas categorias acima o próprio conjunto N se enquadra? Ou seja, N é um elemento de si mesmo ou N não é um elemento de si mesmo? Veremos que nem uma coisa nem outra, já que as duas possibilidades resultam em contradições.

De fato, se admitimos que N é um elemento de si mesmo, temos, pela definição do conjunto N, que N é um conjunto normal, ou seja, que N não é um elemento de si mesmo; e chegamos a uma contradição. Se admitimos que N não é um elemento de si mesmo, temos, pela definição de conjunto anormal, que N é um conjunto anormal, ou seja, que N é um elemento de si mesmo; e chegamos a outra contradição.

Assim, o conjunto N não pode existir, já que ele não pode ser classificado nem como normal, nem como anormal.

No Exemplo 2.2.2 e no Exemplo 2.2.3 mostramos que enunciados aparentemente falsos podem ser verdadeiros e enunciados aparentemente verdadeiros podem ser falsos. Além disso, em cada caso, apresentamos uma justificativa tanto para a veracidade de um enunciado aparentemente falso quanto para a falsidade de um enunciado aparentemente verdadeiro, por meio de argumentações.



De uma maneira geral, consideramos que, como na Matemática a justificativa de enunciados não pode se apoiar em observações e experiências, para justificar a verdade ou a falsidade de um enunciado matemático, podemos apenas *argumentar* em favor da verdade ou falsidade deste enunciado. A figura anterior resume como se dá a justificativa de enunciados no caso da Matemática.

Capítulo 3

O que é uma prova

Neste capítulo, discutimos o que é uma *prova* e apresentamos algumas propriedades que as provas devem ter. Em particular, mostramos que existe uma *estrutura comum a todas as provas.*

3.1 Enunciados e provas

Para descrever como os matemáticos justificam enunciados usando apenas argumentações, vamos fixar alguns conceitos e apresentar algumas propriedades dos conceitos fixados.

Um **enunciado** é uma expressão da linguagem matemática, que pode ser classificada como *verdadeira* ou *falsa*, de maneira exclusiva, em um dado *contexto.*

Exemplo 3.1.1 São exemplos de enunciados:

(*a*) 0 *é par.*

(*b*) $0 = 1$.

(*c*) x *é positivo.*

(*d*) *Se* x *é natural, então* x^2 *é natural.*

(*e*) *Se* x *é real, então* $x^2 < 0$.

(*f*) *Se* x *é natural, então* x *é natural.*

(*g*) x *é natural e* x *não é natural.*

Vamos considerar apenas a justificativa da veracidade dos enunciados.

Dentre os enunciados anteriores, (a) é verdadeiro; (b) é falso; (c) pode ser verdadeiro ou falso, dependendo do valor de x; (d) é verdadeiro e (e) é falso, independentemente do valor de x; finalmente, (f) é verdadeiro e (g) é falso, independentemente até do significado do vocábulo "natural".

Uma **prova** de um enunciado verdadeiro é uma argumentação na linguagem matemática que justifica sua veracidade.

Toda investigação matemática é regulada pelo **Princípio da Razão Suficiente, para a Matemática**:

Em Matemática, todo enunciado deve ser provado.

Isto é, para que possa ser aceito como um fato matemático, um enunciado deve vir acompanhado de uma prova.

Exemplo 3.1.2 (a) Uma prova do enunciado: 2 *é um número par* pode ser a seguinte:

Todo número que é divisível por 2 *é par.* 2 *é divisível por* 2. *Logo,* 2 *é um número par.*

(b) Uma prova do enunciado: *o conjunto dos números pares e o conjunto dos números naturais têm a mesma quantidade de elementos*, que já mostramos no Capítulo 2 (Exemplo 2.2.2) ser verdadeiro, pode ser a seguinte:

Se existe uma correspondência um a um entre os elementos de dois conjuntos, então esses conjuntos possuem a mesma quantidade de elementos. A associação de cada número natural ao seu dobro estabelece uma correspondência um a um entre os elementos do conjunto dos números pares e os elementos do conjunto dos números naturais. Assim, esses conjuntos possuem a mesma quantidade de elementos.

Provas são argumentações, explicações detalhadas de por que um enunciado é verdadeiro. Nem toda argumentação é uma prova. É difícil caracterizar as provas. Mas existem características das provas que são evidentes.

Nas próximas seções, vamos apresentar algumas das características que uma argumentação deve possuir para que seja considerada uma prova. Posteriormente, vamos discutir como podemos fazer para elaborar argumentações que possuem as propriedades apresentadas.

3.2 Riqueza de detalhes

Para que possa ser aceita como uma prova de um enunciado, uma argumentação deve conter uma certa *riqueza de detalhes*. Estes detalhes devem ser suficientes para convencer à(s) pessoa(s) a quem a prova se destina, da verdade do enunciado.

Exemplo 3.2.1 Considere a seguinte proposição:

Proposição 3.2.1 *Todo espaço vetorial tem uma base.*

Para uma pessoa que possui uma certa familiaridade com a linguagem e os raciocínios utilizados em Matemática, a seguinte argumentação pode ser considerada como uma prova da Proposição 3.2.1:

> *Seja V um espaço vetorial. Um conjunto B de vetores de V é uma base se, e somente se, é um conjunto linearmente independente maximal. Seja C uma cadeia de conjuntos linearmente independentes de vetores de V. É fácil verificar que $\bigcup C$ é linearmente independente. Assim, pelo Lema de Zorn, V tem uma base.*

Mas a riqueza de detalhes contida na prova de um enunciado deve variar, de acordo com a(s) pessoa(s) a quem a prova se destina.

Exemplo 3.2.2 Considere a seguinte proposição:

Proposição 3.2.2 *Se $f : [a, b] \to \mathbb{R}$ é uma função contínua com $f(a) < 0 < f(b)$, então existe $c \in [a, b]$, tal que $f(c) = 0$.*

Para um aluno de um curso de Análise Matemática, uma prova da Proposição 3.2.2 pode ser uma argumentação envolvendo a definição de função contínua e algumas propriedades das funções contínuas. Para um aluno de um curso de Cálculo, uma prova desta mesma proposição pode ser um diagrama como o da Figura 3.1.

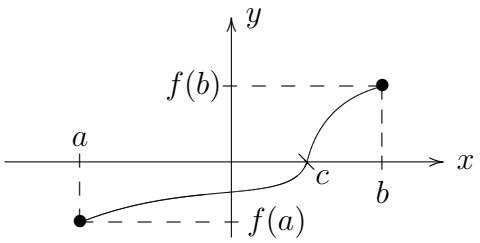


Figura 3.1: Zero de função contínua.

Embora a riqueza de detalhes seja uma propriedade desejável de uma prova, é difícil especificar o que este conceito significa e utilizá-lo como um critério objetivo na elaboração de provas. Mas, como os exemplos apresentados sugerem, toda prova pressupõe algum *conhecimento prévio* e uma *liguagem comum* e, para que possa ser usada na divulgação de uma verdade matemática, é necessário que a(s) pessoa(s) a quem a prova se destina dominem esse conhecimento e essa linguagem.

3.3 Premissas e conclusão

O conhecimento prévio pressuposto em uma prova, usualmente, é expresso na forma de enunciados que são utilizadas na elaboração da argumentação.

Exemplo 3.3.1 Considere a seguinte proposição:

Proposição 3.3.1 *A soma dos ângulos internos de um triângulo é* 180°.

Uma prova desta proposição pode ser a seguinte:
Prova: Seja um triângulo de vértices A, B e C e ângulos respectivos α, β e δ (Figura 3.2).

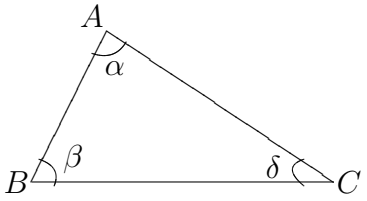


Figura 3.2: Triângulo ABC.

Seja r a reta que passa pelos vértices B e C e que contém o lado BC do triângulo (Figura 3.3).

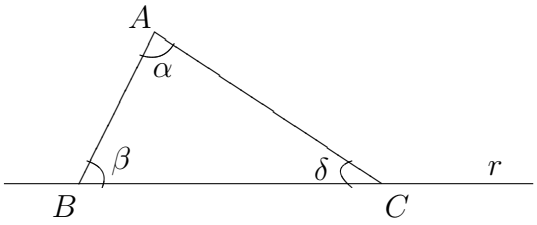


Figura 3.3: Reta que contém BC.

Traçamos pelo vértice A uma reta s paralela r. Sejam x e y os ângulos adjacentes a α (Figura 3.4).

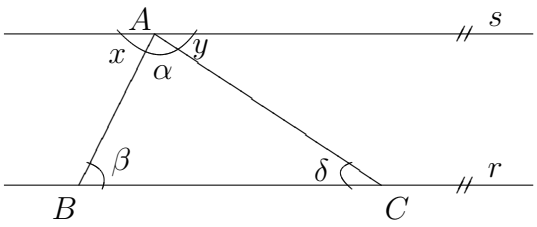


Figura 3.4: Reta paralela a BC, passando por A.

Como os ângulos x e β são alternos internos, pelo Teorema de Tales, eles são iguais. Analogamente, como os ângulos y e δ são alternos internos, pelo Teorema de Tales, eles são iguais. Como $x + \alpha + y = 180°$, então $\alpha + \beta + \delta = 180°$. E a proposição está provada. ∎

Os principais enunciados utilizados nesta prova, como enunciados que justificam a verdade do enunciado provado, são:

1. Dado um segmento de reta BC, existe uma reta que passa por B e C e que contém todos os pontos de BC.
2. Axioma das paralelas: Dada uma reta r e um ponto A fora de r, existe uma única reta s que passa por A e é paralela a r.
3. Teorema de Tales: Dadas duas retas paralelas r e s que passam, respectivamente, pelas extremidades de um segmento AB, os ângulos formados pelo segmento AB com as retas r e s e que estão em lados opostos em relação ao segmento AB são iguais.
4. O ângulo raso mede 180°.

A princípio, podemos considerar que, além dos enunciados apresentados, um dos elementos utilizados essecialmente na prova anterior foram os diagramas que acompanham cada parte da prova. Mas deve-se ter em mente

que cada diagrama é considerado apenas como *meio auxiliar* para a prova da proposição. Isto é, os diagramas são utilizados apenas para facilitar a apresentação da prova e esta deve poder ser apresentada, apenas com uma notação mais elaborada, sem o uso de diagramas. A posição tradicional quanto ao uso de diagramas em provas é que diagramas não devem ser essenciais. No entanto, diagramas têm sido utilizados seriamente, inclusive como a parte principal das provas, na justificativa de enunciados matemáticos. Mas este é um assunto que está fora do escopo deste texto.

Alguns dos enunciados que compõem uma prova P recebem uma denominação especial.

1. **Premissas**: são os enunciados que são utilizados na elaboração de P mas cuja justificativa não faz parte de P.
2. **Enunciados intermediários**: são os enunciados que são utilizados na elaboração de P e cuja justificativa faz parte de P.
3. **Conclusão**: é o enunciado do qual P é uma prova.

Exemplo 3.3.2 Consideremos a prova apresentada no Exemplo 3.3.1.

(a) Dentre as premissas utilizadas nesta prova, podemos citar o Axioma das Paralelas e o Teorema de Tales.

(b) Dentre os enunciados intermediários utilizados nesta prova, podemos citar os enunciados *os ângulos x e β são iguais* e $x + \alpha + y = 180°$.

(c) A conclusão desta prova é o enunciado *a soma dos ângulos internos de um triângulo é* $180°$.

3.4 Regresso infinito e círculo vicioso

Como vimos na Seção 3.3, a prova de um enunciado φ é baseada na verdade de enunciados $\varphi_1, \varphi_2, \ldots, \varphi_m$, utilizados como premissas. Aplicando o Princípio da Razão Suficiente, para aceitar a verdade dos enunciados φ_1, φ_2 , $\ldots$, φ_m e considerar que o enunciado φ foi provado, devemos ter as provas das premissas $\varphi_1, \varphi_2, \ldots, \varphi_m$. Mas, da mesma forma que na prova de φ, a prova de cada um dos enunciados $\varphi_1, \varphi_2, \ldots, \varphi_m$, será baseada na verdade de outros enunciados, utilizadas como premissas (Figura 3.5).

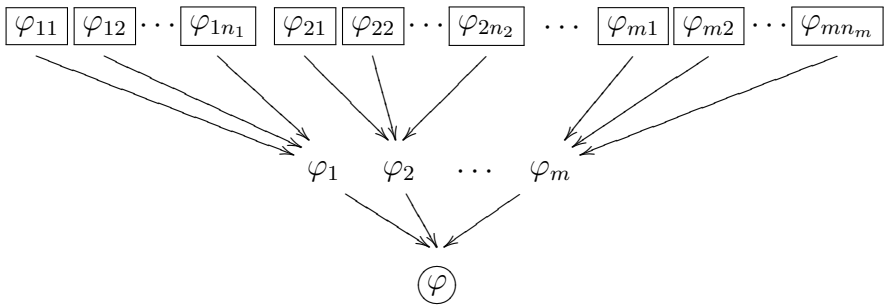


Figura 3.5: Prova de φ, baseada na verdade de $\varphi_{11}, \ldots, \varphi_{mn_m}$.

Aplicando novamente o Princípio da Razão Suficiente, para que possamos aceitar a verdade dos enunciados φ_{11} , . . . , φ_{1n_1}, φ_{11} , . . . , φ_{1n_2} , . . . , φ_{m1} , . . . , φ_{mn_m} e considerar que o enunciado φ foi provada, devemos ter provas destes enunciados e estas provas também serão baseadas na verdade de outros enunciados utilizados como premissas.

Se estendêssemos o processo esboçado acima, duas coisas poderiam acontecer, um *regresso infinito* ou um *círculo vicioso*.

1. Regreso Infinito: estaríamos diante de um *regresso infinito* na prova de um enunciado φ se tentássemos provar cada premissa utilizada na prova de φ, cada premissa utilizada na prova de cada premissa de φ, cada premissa utilizada na prova de cada premissa utilizada na prova de cada premissa de φ e etc. (Figura 3.6).

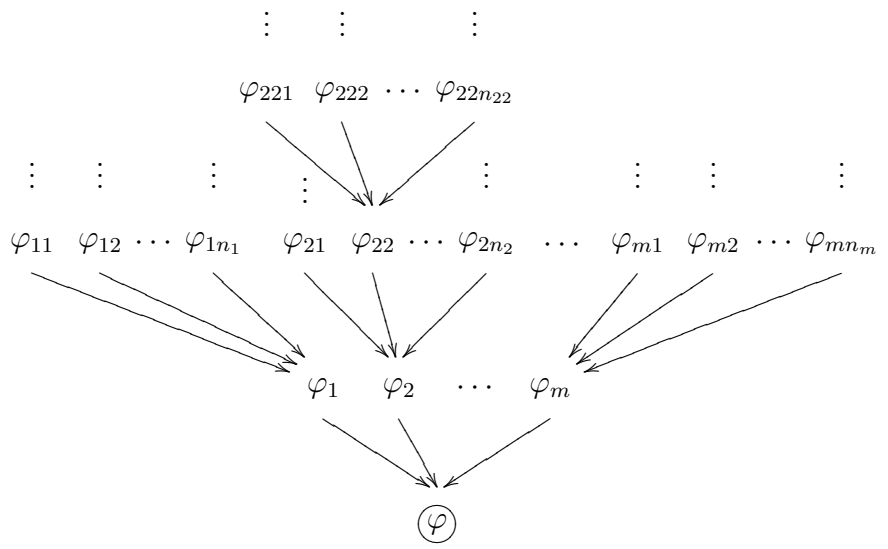


Figura 3.6: Regresso infinito.

2. Círculo Vicioso: estaríamos diante de um *círculo vicioso* na prova de um enunciado φ se em algum momento do processo esboçado acima uti-

lizássemos como premissa na prova de um enunciado φ_j um dos enunciados φ_i que já foram provados. Observe que, como φ_j é uma das premissas das premissas ... das premissas utilizadas na prova de φ_i, estaríamos provando φ_i utilizando φ_j e provando φ_j utilizando φ_i (Figura 3.7).

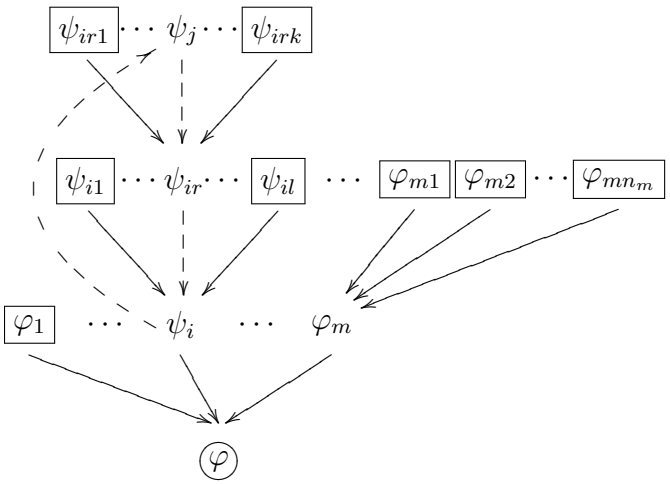


Figura 3.7: Círculo Vicioso.

Obviamente, para que seja aceita como uma prova, uma argumentação não pode conter nem um regresso infinito nem um círculo vicioso. Mas, embora evitar regressos infinitos não seja difícil, pois para isto basta que o processo esboçado acima seja interrompido em algum momento, nem sempre é fácil perceber que estamos diante de um círculo vicioso.

Exemplo 3.4.1 Como um caso limite de círculo vicioso, um erro comum na prova de enunciados é utilizar o próprio enunciado que estamos querendo provar como premissa, em sua própria prova. Vejamos um exemplo.

Proposição 3.4.1 *Todo número natural maior ou igual a* 2 *possui um fator primo.*

Prova: Sendo m um natural maior ou igual a 2, temos dois casos a considerar:
Caso 1 Se m é primo, como m é um fator de si mesmo, ele possui um fator primo.
Caso 2 Se m não é primo, então ele pode ser fatorado em um produto ab, onde a e b são números naturais maiores ou iguais a 2. Como a possui um fator primo e todo fator de a é também fator de m, temos que m possui um fator primo. ∎

A argumentação anterior não é uma prova da Proposição 3.4.1. De fato, argumentamos que m possui um fator primo, usando como premissa que a tem um fator primo. Como a também é um número natural maior ou igual a 2, usamos como premissa a própria proposição que estamos querendo provar.

Para evitar regressos infinitos e dificultar a ocorrência de círculos viciosos na prova de enunciados, devemos admitir o seguinte critério fundamental sobre a estrutura das provas:

Toda prova é baseada em um certo número de enunciados aceitos sem justificativa, ou seja, aceitos sem prova.

Assim, toda prova possui a estrutura apresentada na Figura 3.8, onde φ é a conclusão e $\varphi_1, \varphi_2, \ldots, \varphi_m$ são as premissas.

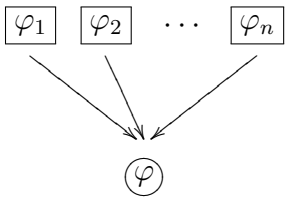


Figura 3.8: Estrutura das provas.

Toda prova pode ser vista como uma justificativa do fato de que, se suas premissas são verdadeiras, então sua conclusão também é verdadeira.

O que parece à primeira vista uma característica negativa das provas, pode ser visto como um fator positivo. De fato, suponhamos que estejamos diante de um enunciado φ, que não sabemos se é verdadeiro ou não, mas que por uma razão ou outra estamos tentando provar. Suponhamos que conhecemos enunciados $\varphi_1, \varphi_2, \ldots, \varphi_m$ que, por uma razão ou outra, sabemos serem verdadeiros. Suponhamos por fim que sabemos fazer uma prova de φ baseada na verdade dos enunciados $\varphi_1, \varphi_2, \ldots, \varphi_m$. Podemos então concluir com toda segurança que φ também é verdadeiro.

3.5 Axioma, teorema, lema, corolário

Chamamos de **enunciados básicos** de uma prova P os enunciados que são premissas de P e dos quais não se tem uma prova.

Observe que todo enunciado básico de uma prova é uma premissa desta prova, mas estas noções são distintas.

Uma premissa é um enunciado que ocorre na prova mas que não foi justificado na prova. Isto não quer dizer que ele não possa ter sido justificado em algum outro lugar. Tal é o caso do Teorema de Tales, no Exemplo 3.3.1. Ele não é justificado naquela prova mas existe uma prova do Teorema de Tales no desenvolvimento usual da Geometria Euclidiana.

Um enunciado básico é um enunciado que ocorre na prova, que não foi justificado na prova e que não foi justificado em nenhum outro lugar. Tal é o caso do Axioma das Paralelas no Exemplo 3.3.1. Ele não é justificado naquela prova e nem existe uma prova do Axioma das Paralelas no desenvolvimento usual da Geometria Euclidiana.

É importante distinguir, também, entre *enunciados básicos* e *axiomas*.

Quando classificamos um enunciado como *básico*, isto é feito com relação a uma determinada *prova*, considerando-se o desenvolvimento usual das várias áreas da matemática. Quando classificamos um enunciado como *axioma*, isto é feito com relação a uma determinada *teoria*.

Chamamos **teoria** a uma organização de um certo ramo de conhecimento, na qual alguns enunciados, chamados **axiomas** da teoria são escolhidos como base para a justificativa de todos os outros enunciados (verdadeiros) deste ramo de conhecimento. Isto deve ser feito de modo que seja possível justificar todos os outros enunciados com provas nas quais apenas os axiomas da teoria sejam enunciados básicos. Quando um certo ramo de conhecimento é organizado desta maneira, dizemos também que temos uma **apresentação axiomática** deste ramo de conhecimento.

Assim, a classificação de um enunciado como *axioma* diz respeito à estrutura de uma *teoria* e a classificação como *enunciado básico* diz respeito à estrutura de uma *prova* específica.

Um mesmo enunciado pode ser um axioma em uma teoria e um ser teorema em outra. Por exemplo, não existe uma prova do Axioma das Paralelas no desenvolvimento usual da Geometria Euclidiana. No entanto, existem outras apresentações axiomáticas da Geometria Euclidiana nas quais o Axioma das Paralelas é um enunciado justificado (um teorema), e não um axioma. Por exemplo, é possível desenvolver a Geometria Euclidiana tomando o Teorema de Pitágoras como axioma e apresentando uma prova do Axioma das Paralelas na qual o Teorema de Pitágoras é uma das premissas. As palavras "axioma" e "teorema" que aparecem nas expressões "Axioma das Parale-

las" e "Teorema de Pitágoras" referem-se à classificação destes enunciados como axioma e teorema, respectivamente, na apresentação axiomática usual da Geometria Euclidiana.

É importante salientar também que, em geral, o conhecimento matemático não se dá no corpo de uma teoria. Como é natural, o que acontece primeiro é o desenvolvimento do conhecimento, nos vários ramos da matemática. A prova de enunciados é uma atividade central neste desenvolvimento. Um passo posterior é a organização deste conhecimento em teorias.

Os enunciados matemáticos justificados são normalmente chamados de *teorema* ou *proposição*. Mas os nomes *lema* e *corolário* também são usados para fazer referência a enunciados para os quais apresentamos uma prova. **Teoremas** são os enunciados matemáticos justificados que são considerados importantes, segundo algum critério. **Proposições** são os enunciados matemáticos justificados que não são considerados tão importantes. **Lemas** são os enunciados matemáticos justificados que são apresentados apenas como um passo para a prova de um teorema, que não tem importância em si mesmos. **Corolários** são os enunciados matemáticos justificados que são consequência imediata da prova de outro enunciado e cuja prova, portanto, fica bastante simplificada ao considerarmos dada a prova deste outro enunciado.

A Figure 3.9 apresenta uma classificação dos enunciados, de acordo com o que dissemos anteriormente.

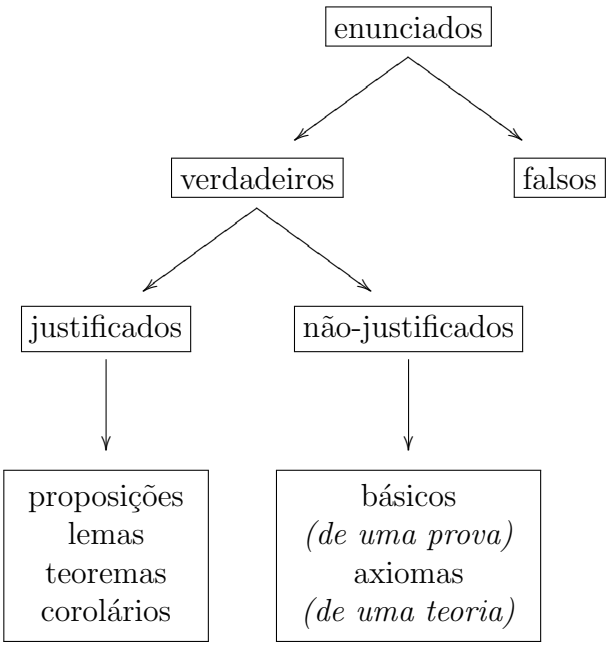


Figura 3.9: Classificação de enunciados.

Capítulo 4

Definições

Neste capítulo, discutimos o que é uma *definição* e apresentamos algumas propriedades que as definições devem ter. Em particular, mostramos que existe uma *estrutura comum a todas as definições.*

4.1 Definições

Como dissemos no Capítulo 3, a prova de um enunciado pressupõe conhecimento prévio e linguagem comum. O conhecimento prévio é expresso na forma de premissas, que são utilizadas na prova do enunciado. A linguagem comum usualmente é fixada na forma de definições, que são utilizadas na elaboração da argumentação. Ou seja, em Matemática, as definições são utilizadas com o objetivo de fixar o significado de determinados vocábulos.

Uma **definição** é uma parte de um texto que introduz um novo vocábulo, fixando o seu significado.

Exemplo 4.1.1 (a) Uma relação fundamental entre conjuntos é a relação de inclusão, cujo significado pode ser fixado pela seguinte definição:

Definição Se cada elemento de um conjunto A é também um elemento de um conjunto B, dizemos que A é um *subconjunto* de B.

(b) Uma função importante da Trigonometria é a função seno, cujo significado pode ser fixado pela seguinte definição:

Definição Dado um ângulo agudo x, por um ponto pertencente a um de seus lados, tracemos uma perpendicular ao outro lado (Figura 4.1).

Vamos definir

$$sen(x) = seno\ de\ x = \frac{cateto\ oposto\ a\ x}{hipotenusa} = \frac{AB}{BC} = \frac{c}{a}.$$

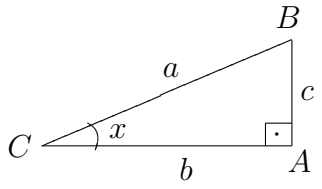


Figura 4.1: $sen(x) = \dfrac{c}{a}$

(c) Um conceito fundamental sobre números naturais é a propriedade de ser par, cujo significado pode ser fixado pela seguinte definição:

Definição Um número natural é *par* se é o dobro de algum número natural.

(d) Um conceito importante da Teoria dos Grafos é a noção de grafo euleriano (lê-se *óileriano*), cujo significado pode ser fixado pela seguinte definição:

Definição Um grafo é *euleriano* se possui uma trilha fechada que contém cada aresta exatamente uma vez.

Como o Exemplo 4.1.1 sugere, o significado do vocábulo que está sendo definido é fixado a partir do significado de outros vocábulos.

Exemplo 4.1.2 (a) No item (a) do Exemplo 4.1.1, definimos *subconjunto* a partir de noções como *elemento*, *conjunto* e *pertinência*.

(b) No item (b) do Exemplo 4.1.1, definimos *seno* a partir de noções como *cateto oposto*, *hipotenusa* e *quociente de dois números reais*.

(c) No item (c) do Exemplo 4.1.1, definimos *número par* a partir de noções como *número natural* e *dobro*.

(*d*) No item (*d*) do Exemplo 4.1.1, definimos *grafo euleriano* a partir de noções como *grafo*, *trilha fechada* e *aresta*.

Uma outra maneira de se utilizar uma definição, em Matemática, é com o objetivo de verificar se um dado objeto corresponde, ou não, ao conceito definido.

Uma **definição** é uma parte de um texto que estabelece o significado de um conceito, dando condições para sua verificação ou determinação.

Exemplo 4.1.3 (*a*) Segundo a definição de inclusão, dados dois conjuntos A e B, para verificar se A é ou não um subconjunto de B, basta verificar se cada elemento de A é também um elemento de B.

(*b*) Segundo a definição de seno, dado um ângulo agudo x, para calcular o seno de x basta fazer um desenho como na Figura 4.1, determinar as medidas a e c e calcular o quociente $\frac{c}{a}$.

(*c*) Segundo a definição de número par, dado um número natural n, para verificar se n é par, basta calcular sua metade e verificar se esta é um número natural.

Observação. É importante salientar que, em Matemática, as definições não ocorrem ao acaso. Usualmente, são motivadas pela presença de um conceito que aparece com frequência. Por exemplo, a ocorrência frequente do conceito *número natural positivo maior do que* 1 *que não possui fatores diferentes de* 1 *e de si mesmo* levou à necessidade de se definir o conceito de número primo. Neste sentido, uma definição pode ser vista como uma *convenção* que diz qual o significado de um conceito e que estabelece condições para sua verificação ou determinação.

4.2 Forma normal das definições

Como veremos no Capítulo 6, por transmitirem significados e apresentarem condições de verificação, as definições desempenham um papel importante na prova de enunciados. Mas, para que possam ser utilizadas de maneira sistemática, nas provas, as definições devem estar escritas de modo adequado. Assim, somos levados a considerar uma maneira especial de escrever as definições. Esta maneira decorre da análise a seguir.

4.2.1 Tipos de objetos

Em primeiro lugar, uma definição só faz sentido quando aplicada a um certo *tipo* de objeto.

Exemplo 4.2.1 (*a*) A relação de inclusão (como está definida no item (a) do Exemplo 4.1.1) diz respeito a conjuntos.

(*b*) A função seno (como está definida no item (b) do Exemplo 4.1.1) é aplicada a ângulos agudos.

(*c*) A propriedade ser par (como está definida no item (c) do Exemplo 4.1.1) é aplicada a números naturais.

Esta observação simples nos afasta de aplicações indevidas das definições.

Exemplo 4.2.2 Se aplicarmos a definição de número par, formulada para números naturais, a números reais, teremos

> *Um número real é par, se é o dobro de algum número real. Como todo número real pode ser dividido por dois, deste fato concluímos que todo número real é par, o que é um absurdo.*

Para evitar que apliquemos uma definição formulada para um certo tipo de objeto a objetos de um outro tipo, ao escrevermos as definições vamos exigir que o tipo de objeto ao qual ela se aplica esteja explicitamente determinado.

Maneiras mais adequadas de escrever as definições apresentadas no Exemplo 4.1.1 são as seguintes:

Exemplo 4.2.3 (*a*) Sejam A e B conjuntos. Se cada elemento de A é também um elemento de B, dizemos que A é um subconjunto de B.

(*b*) Seja x um ângulo agudo como o da Figura 4.1. Definimos

$$\textit{seno de } x = \textit{sen}(x) = \frac{\textit{cateto oposto a } x}{\textit{hipotenusa}} = \frac{AB}{BC} = \frac{c}{a}.$$

(*c*) Seja a um número natural. Dizemos que a é par se é o dobro de algum número natural.

4.2.2 Conceitos definidos e primitivos

Em segundo lugar, uma definição só introduz um conceito a partir de conceitos já conhecidos. Assim, os conceitos que ocorrem em uma definição podem ser classificados em duas categorias:

1. **Conceito definido**: é o conceito cujo significado está sendo fixado na definição.
2. **Conceitos primitivos**: são os conceitos utilizados na definição, mas cujos significados não estão expressos na definição.

Exemplo 4.2.4 (*a*) Em relação ao item (a) do Exemplo 4.2.3, temos que o conceito definido é *subconjunto* e entre os conceitos primitivos estão *elemento*, *conjunto* e *pertinência*.

(*b*) Em relação ao item (b) do Exemplo 4.2.3, temos que o conceito definido é *seno* e entre os conceitos primitivos estão *cateto oposto*, *hipotenusa* e *quociente de números reais*.

(*c*) Em relação ao item (c) do Exemplo 4.2.3, temos que o conceito definido é *número par* e entre os conceitos primitivos estão *número natural* e *dobro*.

Podemos, então, dizer que uma definição de um conceito c é baseada no conhecimento dos conceitos $c_1, c_2, \ldots, c_m$, utilizados como conceitos primitivos na definição de c.

$$\underbrace{c_1, c_2, \ldots, c_m}_{\Downarrow}$$
$$c$$

Agora, como o significado dos conceitos devem ser fixados por suas definições, analogamente ao que acontece no caso da prova de enunciados, para que possamos aceitar $c_1, c_2, \ldots, c_m$ como conhecidos e considerar que c foi definido, devemos ter as definições dos conceitos primitivos $c_1, c_2, \ldots, c_m$. Mas, da mesma forma que na definição de c, a definição de cada um dos conceitos $c_1, c_2, \ldots, c_m$, será baseada no conhecimento de outros conceitos, utilizados como conceitos primitivos nas definições de $c_1, c_2, \ldots, c_m$.

$$\underbrace{c_{11}, \ldots, c_{1n_1}}_{\Downarrow} \quad \underbrace{c_{21}, \ldots, c_{2n_2}}_{\Downarrow} \quad \ldots \quad \underbrace{c_{m1}, \ldots, c_{mn_k}}_{\Downarrow}$$
$$c_1 \qquad\qquad c_2 \qquad\qquad \ldots \qquad\qquad c_m$$

Se levarmos adiante o processo esboçado acima, também no caso das definições, correremos o risco de encontrar regressos infinitos e/ou círculos viciosos e, obviamente, uma definição correta deve excluir essas duas possibilidades. Assim, devemos admitir o seguinte critério fundamental sobre a estrutura das definições:

Toda definição é baseada em um certo número de conceitos previamente conhecidos, ou seja, aceitos sem definição.

Para evitar que façamos confusão sobre qual é o conceito que está sendo definido e quais são os conceitos que estão sendo considerados como primitivos, quando escrevermos a definição, vamos exigir que essa classificação dos conceitos esteja bem determinada. Faremos isto estipulando que o conceito definido esteja escrito sempre antes dos conceitos primitivos que estão sendo utilizados na definição.

Exemplo 4.2.5 (*a*) Uma maneira mais adequada de escrever a definição de inclusão, apresentada no item (a) do Exemplo 4.2.3, é:

Sejam A e B conjuntos. Dizemos que A é um *subconjunto* de B se cada elemento de A é também um elemento de B.

(*b*) Uma maneira mais adequada de escrever a definição de seno, apresentada no item (b) do Exemplo 4.2.3, é:

Seja x um ângulo agudo como o da Figura 4.1. O *seno de* x é definido como

$$sen(x) = \frac{cateto\ oposto\ a\ x}{hipotenusa} = \frac{AB}{BC} = \frac{c}{a}.$$

(*c*) Uma maneira mais adequada de escrever a definição de número par, apresentada no item (c) do Exemplo 4.2.3, é:

Seja a um número natural. Dizemos que a é *par* se é o dobro de algum número natural.

4.2.3 Forma normal

Segue do que foi dito que toda definição consiste de três partes:

1. **Atribuição**: é a parte da definição que especifica a que tipo de objetos a definição se aplica.

2. **O que é definido (*definiendum*)**: é a parte da definição que especifica qual o conceito que está sendo definido.

3. **O que define (*definiens*)**: é a parte da definição que consiste de um enunciado que expressa o significado do conceito definido a partir do significado dos conceitos primitivos.

Todas as definições devem ser escritas (ou reescritas) de acordo com a especificação abaixo, onde cada uma das partes aparece em destaque e na ordem em que deve ser escrita, para uma melhor entendimento dos conceitos definidos.

FORMA NORMAL DE DEFINIÇÕES.

Uma definição está em *forma normal*, se possui a seguinte forma:

atribuição
+
o que é definido
+
o que define

1. Inicialmente, a especificação do tipo de objetos aos quais definição se aplica.

2. Em seguida, a especificação do conceito que está sendo definido.

3. Por fim, um enunciado que expressa o significado do conceito definido a partir do significado dos conceitos primitivos, onde o que é definido aparece em *destaque* no texto da definição e o que define aparece escrito com *uma certa quantidade de rigor matemático*.

Exemplo 4.2.6 (*a*) Uma definição em forma normal de inclusão é a seguinte:

Definição Sejam A e B conjuntos. Dizemos que A é um *subconjunto* de B se todo elemento de A é também um elemento de B.

(b) Uma definição de seno em forma normal é a seguinte:

Definição Seja x um ângulo agudo como o da Figura 4.1. O *seno* de x é o número $sen(x) = \frac{c}{a}$.

(c) Uma definição de número par em forma normal é a seguinte:

Definição Seja a um número natural. Dizemos que a é *par* se existe um número natural b, tal que $a = 2b$.

Observação. Um dos critérios para que uma definição esteja em forma normal é que o que define deve estar escrito com uma certa quantidade de rigor matemático. Embora rigor matemático seja uma propriedade desejável das definições, é difícil especificar o que este conceito significa e utilizá-lo como um critério objetivo na elaboração de definições. No próximo capítulo, vamos mostrar que enunciados podem ser considerados como formadas a partir de outros enunciados e apresentar uma classificação dos enunciados, de acordo com a maneira como são formados. Estipularemos uma maneira de escrever os enunciados que pertencem a cada uma das classes definidas e mostraremos como essa maneira de escrever os enunciados pode ser utilizada como um critério para o rigor com que as definições devem ser apresentadas.

Capítulo 5

Estrutura de enunciados

Enunciados podem ser combinados para formar novos enunciados. Neste capítulo, apresentamos uma classificação inicial dos enunciados, de acordo com a maneira como são formados. Um refinamento dessa classificação levará à elaboração dos *métodos de prova* que serão apresentados.

5.1 Combinando enunciados

No Capítulo 3 discutimos o valor de verdade (verdadeiro ou falso) dos enunciados. Outra característica essencial a todos os enunciados é que, além de poderem ser classificados como verdadeiros ou falsos, eles também podem ser combinados para formar novos enunciados. Isto é feito com o auxílio de certas expressões especialmente reservadas para este fim.

Enunciados podem ser combinados para formar novos enunciados por meio de expressões como *e* e *se...então*.

Exemplo 5.1.1 Por exemplo, considere os enunciados:

(*a*) 2 *é par.*

(*b*) 2 *é primo.*

(*c*) x *é par.*

(*d*) x^2 *é par.*

(*e*) *O número natural da forma* $2^n + 1$ *é primo.*

Por aplicações sucessivas das expressões *e* e *se...então* podemos formar novos enunciados a partir dos enunciados dados:

(f) *2 é par e 2 é primo.*

(g) *Se x é par, então x^2 é par.*

(h) *Se 2 é par e 2 é primo, então o número da forma $2^n + 1$ é primo.*

Também podemos formar novos enunciados por aplicação de expressões como *não* e *existe*, que são aplicadas a um único enunciado.

Exemplo 5.1.2 Dados os enunciados (d) e (e) do Exemplo 5.1.1, podemos obter:

(i) *x^2 não é par.*

(j) *Existe um número natural da forma $2^n + 1$ que é primo.*

5.2 Conectivos e quantificadores

Neste texto, trataremos exclusivamente de enunciados formados por aplicação das expressões *não*, *e*, *ou*, *se...então*, *se e somente se*, *para todo* e *existe*. Embora essas expressões não possuam todas a mesma classificação gramatical, do ponto de vista da linguagem matemática todas possuem a mesma função, a saber, a de formar novos enunciados a partir de um ou mais enunciados previamente dados.

Exemplo 5.2.1 Dados os enunciados *2 é par* e $3 < x$, da linguagem matemática, podemos formar, por exemplo, os seguintes enunciados:

(a) *2 é par e $3 < x$.*

(b) *2 é par ou $3 < x$.*

(c) *Se 2 é par, então $3 < x$.*

(d) *2 é par se, e somente se, $3 < x$.*

(e) *2 não é par.*

(f) *Para todo $x \in \mathbb{N}$, temos que $3 < x$.*

(g) *Existe $x \in \mathbb{R}$ tal que $3 < x$.*

Um modo adequado de se considerar as expressões *não*, *e*, *ou*, *se...então*, *se e somente se*, *para todo* e *existe* é pensar nelas como operações. Uma *operação* é uma maneira de combinar elementos para formar novos elementos. Por exemplo, a operação de adição que associa aos números 1 e 2 o número 3. No caso das expressões *não*, *e*, *ou*, *se...então* e *se e somente se*, os elementos operados são enunciados e o resultado obtido é um novo enunciado. No caso das expressões *para todo* e *existe*, os elementos operados são: uma variável, um conjunto onde essa variável toma valores e um enunciado onde a variável ocorre; e o resultado obtido é um novo enunciado.

Exemplo 5.2.2 Em relação ao Exemplo 5.2.1, temos:

(*a*) Operando os enunciados 2 *é par* e $3 < x$ por intermédio do *se...então*, obtemos o enunciado *se* 2 *é par, então* $3 < x$.

(*b*) Operando o enunciado 2 *é par* por intermédio do *não*, obtemos o enunciado: 2 *não é par*.

(*c*) Operando a variável x, o conjunto $\mathbb{N}$, onde x toma valores, e o enunciado $3 < x$, que possui ocorrência de x, por intermédio do *para todo*, obtemos o enunciado *para todo* $x \in \mathbb{N}$, *temos que* $3 < x$.

5.3 Enunciados atômicos e moleculares

Um **conectivo** é uma das expressões *não*, *e*, *ou*, *se...então* e *se e somente se*. Um **quantificador** é uma das expressões *para todo* e *existe*.

Podemos agora classificar os enunciados de acordo com o fato de terem sido ou não formados a partir de enunciados anteriores, por aplicação dos conectivos e/ou quantificadores.

Um enunciado é **atômico** se nele não ocorrem conectivos nem quantificadores.

Os enunciados atômicos são considerados os enunciados mais simples e aqueles a partir dos quais todos os outros enunciados podem ser formados.

Exemplo 5.3.1 São exemplos de enunciados atômicos:

(*a*) 5 *é primo*.

(*b*) x *é um quadrado perfeito*.

Os enunciados acima são atômicos, pois em nenhum deles ocorre *não*, *e*, *ou*, *se...então* e *se e somente se* , como conectivos, nem *para todo* e *existe*, como quantificadores.

Um enunciado é **molecular** se não é atômico, isto é, se nele ocorre pelo menos um conectivo ou quantificador.

Exemplo 5.3.2 Temos, então, que:

(*a*) O enunciado *5 não é primo* é molecular pois nele ocorre o conectivo *não*.

(*b*) O enunciado *Se x e y são pares, então x + y é par* é molecular pois nele ocorrem os conectivos *e* e *se...então*.

(*c*) O enunciado *Existe um número natural da forma* $991n^2 + 1$ *que não é um quadrado perfeito* é molecular, pois nele ocorre o quantificador *existe*.

Vamos considerar que a classe de todos os enunciados se encontra particionada, segundo a classificação acima, em duas subclasses, a classe dos enunciados atômicos e a classe dos enunciados moleculares (Figura 5.1).

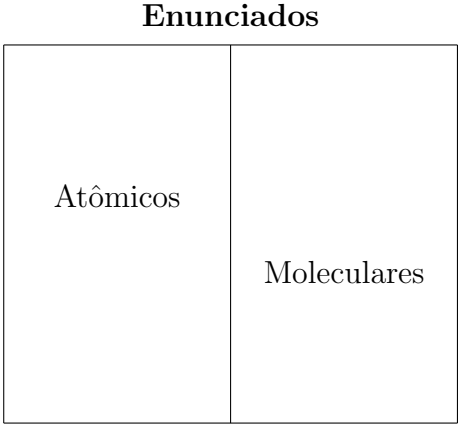


Figura 5.1: Partição da classe dos enunciados.

Nosso objetivo, daqui por diante, é particionar a classe dos enunciados moleculares em subclasses, de modo que possamos associar a cada uma das subclasses obtidas, um método de prova que pode ser aplicado na tentativa de provar enunciados que pertencem a essa subclasse.

5.4 Conjunções

Um enunciado é uma **conjunção** se é formado a partir de dois outros enunciados, por aplicação do conectivo *e*.

Exemplo 5.4.1 O enunciado *x e y são pares* pode ser reescrito como *x é par e y é par*. Portanto, é a conjunção do enunciado *x é par* com o enunciado *y é par*.

Podemos dizer que um enunciado é uma conjunção se pode ser reescrito na forma

$$\varphi \ e \ \psi,$$

onde φ e ψ são enunciados. Observe que, para se obter uma conjunção, o *e* deve ser aplicado a dois enunciados. Os enunciados utilizados na formação de uma conjunção são chamados as **componentes** da conjunção.

Exemplo 5.4.2 O enunciado *X e Y são colineares* não é uma conjunção, mas um enunciado atômico.

Embora a partícula *e* ocorra no enunciado *X e Y são colineares*, não podemos analisar este enunciado como tendo sido obtido a partir de outros enunciados usando o conectivo *e*. No enunciado *X e Y são colineares*, a partícula *e* é utilizada para formar o sujeito composto *X e Y*. Neste enunciado, a partícula *e* não ocorre como conectivo, juntando enunciados para formar enunciados novos. Portanto temos, de fato, uma enunciado atômico.

5.5 Implicações

Um enunciado é uma **implicação** se é formado a partir de dois outros enunciados, por aplicação do conectivo *se...então*.

Exemplo 5.5.1 O enunciado *o triângulo será isósceles, caso seja retângulo* pode ser reescrito como *se o triângulo é retângulo, então é isósceles*. Portanto, é a implicação do enunciado *o triângulo é isósceles* pelo enunciado *o triângulo é retângulo*.

Podemos dizer que um enunciado é uma implicação se pode ser reescrito na forma

Se φ, então ψ,

onde φ e ψ são enunciados. Observe que, para se obter uma implicação, o *se...então* deve ser aplicado a dois enunciados. Os enunciados utilizados na formação de uma implicação são chamados **componentes** da implicação.

Exemplo 5.5.2 O enunciado *as retas r e s são paralelas pois não possuem pontos em comum* é uma implicação, pois pode ser reescrito como *se as retas r e s não possuem pontos em comum, então elas são paralelas*, o que mostra que ele foi obtido a partir dos enunciados componentes *as retas r e s não possuem pontos em comum* e *as retas r e s são paralelas*, por aplicação do conectivo *se...então*.

Dizemos ainda que o enunciado *as retas r e s não possuem ponto em comum* é o antecedente da implicação e o enunciado *as retas r e s são paralelas* é o consequente da implicação.

De uma maneira geral, chamamos φ de **antecedente** e ψ de **consequente** da implicação *se φ, então ψ*.

5.6 Generalizações

Um enunciado é uma **generalização** se é formado a partir de um outro enunciado, por aplicação do quantificador *para todo,* em relação a uma certa variável e a um certo conjunto.

Exemplo 5.6.1 Vejamos alguns exemplos:

a) O enunciado *todo elemento de A também é elemento de C* pode ser reescrito como *para todo $x \in A$, temos que $x \in C$.* Portanto, é a generalização do enunciado $x \in C$ em relação à variável x e ao conjunto A.

b) O enunciado $sen^2x + cos^2x = 1$ *sempre que* $x \in \mathbb{R}$ pode ser reescrito como *para todo $x \in \mathbb{R}$, temos que $sen^2x + cos^2x = 1$.* Portanto, é a generalização do enunciado $sen^2x + cos^2x = 1$ em relação à variável x e ao conjunto dos números reais.

Podemos dizer que um enunciado é uma generalização se pode ser reescrito na forma

Para todo $x \in A$, temos que $\varphi(x)$,

onde x é uma variável, A é um conjunto e $\varphi(x)$ é um enunciado onde ocorre a variável x. Observe que, para se obter uma generalização, o *para todo* deve ser aplicado a um único enunciado. O enunciado utilizado na formação de uma generalização é chamado de **componente** da generalização.

Exemplo 5.6.2 O enunciado *quando n é um número natural par, n^2 também é par* é uma generalização, pois pode ser reescrito como *para todo $n \in \mathbb{N}$ temos que, se n é par, então n^2 é par*, o que mostra que ele foi obtido a partir do enunciado componente *se n é par, então n^2 é par*, por aplicação do quantificador *para todo*, em relação à variável n e ao conjunto dos números naturais.

Dizemos ainda que a variável n é a variável de generalização, o conjunto $\mathbb{N}$ é o domínio de generalização e o enunciado *se n é par, então n^2 é par* é o enunciado generalizado.

De uma maneira geral, dada uma generalização *para todo $x \in A$, temos que $\varphi(x)$*, chamamos x de **variável de generalização**, A de **domínio de generalização** e $\varphi(x)$ de **enunciado generalizado**.

5.7 Existencializações

Um enunciado é uma **existencialização** se é formado a partir de um outro enunciado, por aplicação do quantificador *existe* em relação a uma certa variável e a um certo conjunto.

Exemplo 5.7.1 A definição de número par, em forma normal, dada no Capítulo 4, é a seguinte:

Definição Seja $n \in \mathbb{N}$. Dizemos que n é *par* se existe um número natural k tal que $n = 2k$.

A partir desta definição, o enunciado *n é par* pode ser reescrito como *existe $k \in \mathbb{N}$ tal que $n = 2k$*, e portanto é a existencialização do enunciado $n = 2k$ com relação à variável k e ao conjunto $\mathbb{N}$.

Assim, podemos dizer que um enunciado é uma *existencialização* se pode ser reescrito na forma

Existe ao menos um $x \in A$ *tal que* $\varphi(x)$,

onde x é uma variável, A é um conjunto e $\varphi(x)$ é um enunciado onde ocorre a variável x. Observe que, para se obter uma existencialização, o *existe* deve ser aplicado a um único enunciado. O enunciado utilizado na formação de uma existencialização é chamado de **componente** da existencialização.

Exemplo 5.7.2 O enunciado $\mathbb{N}$ *possui um menor elemento* é uma existencialização, pois pode ser reescrito como *existe um número natural n que é menor que qualquer outro número natural*, o que mostra que ele foi obtido a partir do enunciado componente *n é menor que qualquer outro número natural*, pelo uso do quantificador *existe* aplicado à variável n e ao conjunto $\mathbb{N}$.

Dizemos ainda que a variável n é a variável de existencialização, o conjunto $\mathbb{N}$ é o domínio de existencialização e o enunciado *n é menor que qualquer outro número natural* é o enunciado existencializado.

De uma maneira geral, dada uma existencialização *existe* $x \in A$ *tal que* $\varphi(x)$, chamamos x a **variável de existencialização**, A o **domínio de existencialização** e $\varphi(x)$ o **enunciado existencializado**.

5.8 Negações

Um enunciado é uma **negação** se pode ser considerado como obtido a partir de um outro enunciado, por intermédio do conectivo *não*.

Exemplo 5.8.1 O enunciado $\sqrt{2}$ *não é um número racional* pode ser reescrito como *não é o caso que* $\sqrt{2}$ *é um número racional*. Portanto, é a negação do enunciado 2 *é um número racional*.

Podemos dizer que um enunciado é uma negação se pode ser escrito na forma

Não é o caso que φ,

ou, simplesmente,

Não φ,

onde φ é um enunciado. Observe que, para se obter uma negação, o *não* deve ser aplicado a um único enunciado. O enunciado utilizado na formação de uma negação é chamado de **componente** da negação.

Exemplo 5.8.2 O enunciado *não existe um maior número natural* é uma negação, pois pode ser reescrito como *não é o caso que existe um maior número natural*, o que mostra que ele foi obtido a partir do enunciado componente *existe um maior número natural* pelo uso do conectivo *não*.

Dizemos ainda que o enunciado *existe uma maior número natural* é o enunciado negado.

Muitas vezes, a negação de um enunciado é indicada pelo uso de prefixos de negação.

Exemplo 5.8.3 O enunciado *o conjunto dos números primos é infinito* é uma negação, pois pode ser reescrito como *não é o caso que o conjunto dos números primos é finito*, o que mostra que ele foi obtido a partir do enunciado componente *o conjunto dos números primos é finito* pelo uso do conectivo *não*.

O enunciado *o conjunto dos números primos é finito* é o enunciado negado.

De uma maneira geral, chamamos φ o **enunciado negado** da negação *não* φ.

5.9 Disjunções

Um enunciado é uma **disjunção** se é formado a partir de dois outros enunciados, por aplicação do conectivo *ou*.

Exemplo 5.9.1 O enunciado 2 *é par ou não é natural*, ou seja, 2 *é par ou* 2 *não é natural*, é a disjunção do enunciado 2 *é par* com o enunciado 2 *não é natural*.

Observe que, para se obter uma disjunção, o *ou* deve ser aplicado a dois enunciados. Os enunciados utilizadas na formação de uma disjunção são chamadas *componentes* da disjunção. De uma maneira geral, se φ e ψ são enunciados quaisquer, dizemos que φ é a *primeira componente* e que ψ é a *segunda componente* da disjunção φ *ou* ψ.

Exemplo 5.9.2 O enunciado *2 é um número par ou eu como o meu chapéu* é uma disjunção, pois foi obtido a partir dos enunciados componentes *2 é um número par* e *eu vou comer o meu chapéu* pelo uso do conectivo *ou*. Dizemos ainda que o enunciado *2 é um número par* é a *primeira componente* da disjunção e o enunciado *eu vou comer o meu chapéu* é a segunda componente da disjunção.

5.10 Biimplicações

Um enunciado é uma **biimplicação** se é formado a partir de dois outros enunciados, por aplicação do conectivo *se e somente se*.

Exemplo 5.10.1 O enunciado *David Hilbert está errado se, e somente se, há um problema que não possui solução* é a bimplicação dos enunciados *David Hilbert está errado* e *há um problema que não possui solução*.

Observe que, para se obter uma biimplicação, o *se, e somente se* deve ser aplicado a dois enunciados. Os enunciados utilizados na formação de uma biimplicação são chamados *componentes* da biimplicação. De uma maneira geral, se φ e ψ são enunciados quaisquer, dizemos que φ é a *primeira componente* e que ψ é a *segunda componente* da biimplicação *φ se, e somente se, ψ*.

Exemplo 5.10.2 O enunciado *o número de átomos no universo é primo se, e somente se, não possui divisores próprios* é uma biimplicação, pois foi obtido a partir dos enunciados componentes *o número de átomos no univeros é primo* e *o número de átomos no universo não possui divisores próprios* pelo uso do conectivo *se, e somente se*. Dizemos ainda que o enunciado *o número de átomos no univeros é primo* é a primeira componente da biimplicação e o enunciado *o número de átomos no universo não possui divisores próprios* é a segunda componente da biimplicação.

Vamos considerar que a classe de todos os enunciados moleculares se encontra particionada em sete subclasses, a classe das conjunções, das implicações, das generalizações, das existencializações, das negações, das disjunções e das biimplicações. Assim, consideramos que a classe de todos os enunciados está particionada como na Figura 5.2.

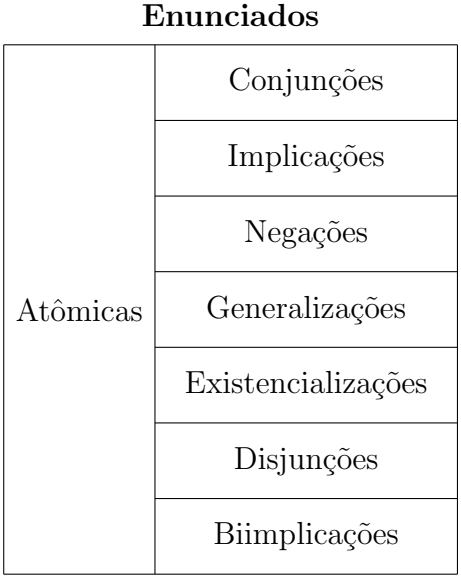


Figura 5.2: Partição da classe dos enunciados.

Capítulo 6

Prova de implicações

Neste capítulo, tratamos do *problema de provar implicações*. Em particular, apresentamos o *Método da Suposição*, para a prova de implicações.

6.1 O problema de provar implicações

Inicialmente, vamos considerar a justificativa da veracidade de enunciados obtidos por aplicação do conectivo *se...então*. Isto é, vamos considerar o problema de provar implicações verdadeiras.

Problema: Prova de Implicações.

Dada: Uma implicação verdadeira *se φ, então ψ*.

Questão: Apresentar uma prova de *se φ, então ψ*, ou seja, uma argumentação que justifica que a implicação é, de fato, verdadeira.

6.2 Provando implicações

De acordo com o que foi dito sobre a estrutura das provas no Capítulo 3, uma solução para o problema da prova de implicações seria uma argumentação da forma mostrada na Figura 6.4, onde *se φ, então ψ* é a conclusão e $\varphi_1, \varphi_2, \ldots, \varphi_n$ são premissas utilizadas na prova de *se φ, então ψ*. Mas, analisando o significado das implicações, observamos o seguinte:

Uma implicação é verdadeira quando a verdade do seu antecedente acarreta a verdade do seu consequente.

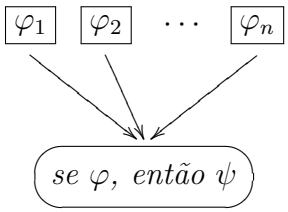


Figura 6.1: O problema da prova de implicações.

Exemplo 6.2.1 A implicação *se chove, então a rua está molhada* é verdadeira, pois caso admitamos que está chovendo somos obrigados a admitir que a rua está molhada.

Observe que a implicação não afirma nem que está chovendo nem que a rua está molhada, mas que existe uma certa relação de causa e efeito entre chover e a rua estar molhada. Assim:

> Quando sabemos que uma implicação é verdadeira, não podemos concluir que seu antecedente é verdadeiro nem que seu consequente é verdadeiro, mas que não podemos considerar seu antecedente verdadeiro e seu consequente falso.

Exemplo 6.2.2 A implicação *se a rua está molhada, então chove* é falsa, pois a rua pode estar molhada sem que, necessariamente, esteja chovendo. Por exemplo, a válvula de abertura de um hidrante pode estar arrebentada.

Essa análise da relação entre o antecendente e o consequente de uma implicação verdadeira nos leva a considerar que, para provar implicações, podemos utilizar o seguinte método:

> MÉTODO DA SUPOSIÇÃO, MS.
>
> Para provar uma implicação *se φ, então ψ*, é suficiente fazer o seguinte:
>
> 1. Supor que o antecedente φ é verdadeiro.
> 2. Provar que o consequente ψ é verdadeiro, usando φ como premissa.

Em termos de justificativas por meio de argumentações, o Método da Suposição afirma que, para justificar que uma implicação é verdadeira, basta supor que o antecedente está justificado e apresentar uma justificativa do consequente, que depende do antecedente.

Vejamos alguns exemplos de aplicação do Método da Suposição:

Exemplo 6.2.3 Sejam A, B e C conjuntos quaisquer. Queremos provar a proposição:

Proposição 6.2.1 *Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.*

que afirma que a inclusão de conjuntos é transitiva. Considerando que a Proposição 6.2.1 é uma implicação com antecedente $A \subseteq B$ *e* $B \subseteq C$ e consequente $A \subseteq C$, segundo o Método da Suposição, para prová-la, é suficiente fazer o seguinte (cf. Figura 6.2):

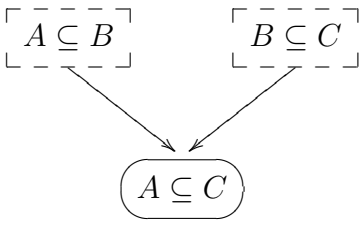


Figura 6.2: Estrutura da prova de *se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.*

1. Supor que $A \subseteq B$ e $B \subseteq C$.
2. Provar que $A \subseteq C$, usando como hipótese que $A \subseteq B$ e $B \subseteq C$.

Exemplo 6.2.4 Seja x um número natural qualquer. Queremos provar a proposição:

Proposição 6.2.2 *Se x é múltiplo de 4, então x é múltiplo de 2.*

que afirma que um múltiplo de 4 é também um múltiplo de 2. Considerando que a Proposição 6.2.2 é uma implicação com antecedente *x é múltiplo de* 4 e consequente *x é múltiplo de* 2, segundo o Método de Suposição, para prová-la basta fazer o seguinte (Figura 6.3):

1. Supor que x é múltiplo de 4.

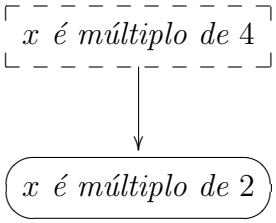


Figura 6.3: Estrutura da prova de *se x é múltiplo de 4, então x é múltiplo de 2*.

2. Provar que x é múltiplo de 2, usando como hipótese que x é múltiplo de 4.

Em resumo, o Método da Suposição afirma que, para provar uma implicação *se φ, então ψ*, ao invés de apresentar uma prova de *se φ, então ψ*, com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m$, como na Figura 6.1, podemos apresentar uma prova de ψ com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \varphi$, como na Figura 6.4. Ou seja, o MS estabelece o seguinte critério fundamental sobre a prova de implicações:

Para provar uma implicação verdadeira *se φ, então ψ*, ao invés de apresentar uma argumentação que justifique *se φ, então ψ*, basta apresentar uma argumentação que justifica ψ, na qual φ ocorre como um enunciado que não foi justificado.

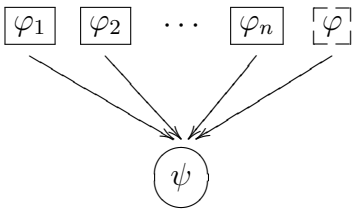


Figura 6.4: Estrutura das provas de implicações *se φ, então ψ*.

Capítulo 7

Prova de generalizações

Neste capítulo, tratamos do *problema de provar generalizações*. Em particular, apresentamos o *Método da Generalização*, para a prova de generalizações. Um erro muito comum na prova de generalizações também é discutido.

7.1 O problema de provar generalizações

Voltemos agora à prova da proposição que afirma que a inclusão de conjuntos é transitiva, apresentada no Capítulo 6:

Proposição 7.1.1 *Se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$.*

Como essa proposição é uma implicação, o Método da Suposição nos diz que para prová-la podemos fazer o seguinte:

1. Supor que $A \subseteq B$ e $B \subseteq C$.
2. Provar que $A \subseteq C$, usando como hipótese que $A \subseteq B$ e $B \subseteq C$.

Ou seja, o método afirma que podemos provar a Proposição 7.1.1 provando apenas a proposição $A \subseteq C$ (mas, como está especificado em 2, isto deve ser feito de uma maneira adequada). Aplicando, então, o Método da Suposição à Proposição 7.1.1, somos levados a considerar o seguinte problema:

Problema: Prova de Inclusões.

Dada: Uma inclusão entre dois conjuntos A e B.

Questão: Apresentar uma prova de $A \subseteq B$, ou seja, uma argumentação que justifica que a inclusão é verdadeira.

Mas como podemos provar uma inclusão? Ou seja, como podemos, dados dois conjuntos, provar que um está contido no outro? Como já dissemos no Capítulo 4, uma das características de uma definição é que ela estabelece o significado de um conceito, dando condições para a sua verificação. Assim, para responder a esta pergunta, vamos examinar a definição de inclusão, em forma normal, dada no Capítulo 4:

Definição Sejam A e B conjuntos. Dizemos que A é um *subconjunto* de B se todo elemento de A é também um elemento de B.

A definição nos diz que, para provar que um conjunto A é subconjunto de um conjunto B, basta provar que *todo elemento de A é também elemento de B*. Observe agora que a proposição *todo elemento de A é também elemento de B* inicia com uma ocorrência de *todo*. Assim, para provar que $A \subseteq B$, devemos saber como provar uma proposição que começa com uma ocorrência do quantificador *para todo*.

7.1.1 Justificativa de generalizações

Vamos considerar agora a justificativa da veracidade de proposições obtidas por aplicação do quantificador *para todo*. Isto é, vamos considerar o problema de provar generalizações verdadeiras:

Problema: Prova de Generalizações.

Dada: Uma generalização verdadeira *para todo $x \in A$, temos que $\varphi(x)$*.

Questão: Apresentar uma prova de que *para todo $x \in A$, temos que $\varphi(x)$*, ou seja, uma argumentação que justifica que a generalização é, de fato, verdadeira.

De acordo com o que foi dito sobre a estrutura das provas no Capítulo 4, uma solução para o problema da prova de generalizações seria uma argumentação da forma mostrada na Figura 7.1, onde *para todo $x \in A$, temos que $\varphi(x)$* é a conclusão e $\varphi_1, \varphi_2, \ldots, \varphi_m$ são premissas utilizadas na prova de *para todo $x \in A$, temos que $\varphi(x)$*. Vamos agora analisar o significado das generalizações, de modo a obter um método que nos permita elaborar argumentações adequadas para a prova de generalizações.

Exemplo 7.1.1 Considere o conjunto $A = \{4, 8, 12, 16\}$.

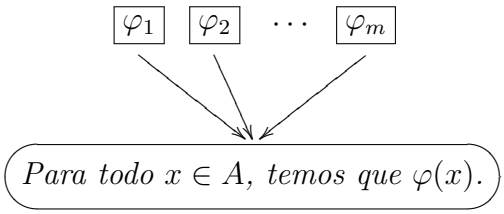


Figura 7.1: O problema da prova de generalizações.

a) Sobre A, fazemos a afirmação *todos os elementos de A são números pares*. Este enunciado é uma generalização verdadeira. De fato, pode ser reescrito como *para todo $x \in A$, temos que x é par*, e examinando cada um dos enunciados:

$$4 \text{ é par},$$
$$8 \text{ é par},$$
$$12 \text{ é par},$$
$$16 \text{ é par},$$

obtidos a partir do enunciado generalizado *x é par*, pela substituição de x pelos elementos de A, verificamos que todos são verdadeiros. Como $4, 8, 12$ e 16 são os únicos elementos de A, temos que a generalização é verdadeira.

b) Agora, sobre A, fazemos a afirmação *todos os elementos de A são menores do que* 15. Este enunciado é uma generalização falsa. De fato, pode ser reescrito como *para todo $x \in A$, temos que $x < 15$*, e examinando cada um dos enunciados:

$$4 < 15,$$
$$8 < 15,$$
$$12 < 15,$$
$$16 < 15.$$

obtidos a partir do enunciado generalizado $x < 15$, pela substituição de x pelos elementos de A, verificamos que as três primeiras são verdadeiras e a última é falsa. Como $4, 8, 12$ e 16 são os únicos elementos de A, temos que a generalização é falsa.

De uma maneira geral, quando A é finito, dada uma generalização *para todo* $x \in A$, *temos que* $\varphi(x)$, temos o seguinte critério sobre a verdade/falsidade de generalizações:

1. A generalização é verdadeira se, e somente se, quando x assume como valores cada um dos elementos a de A, obtemos sempre enunciados $\varphi(a)$ que são verdadeiros.
2. A generalização é falsa se, e somente se, quando x assume como valores cada um dos elementos a de A, obtemos enunciados $\varphi(a)$ dos quais pelo menos um é falso.

Assim, caso A seja finito, temos que a justificativa da verdade de uma generalização *para todo* $x \in A$, *temos que* $\varphi(x)$, fica reduzida a justificativa da verdade de uma quantidade finita de enunciados, obtidos a partir de $\varphi(x)$ pela substituição de x pelos elementos de A. Logo, se podemos justificar que cada enunciado $\varphi(a)$ obtido é verdadeiro, podemos justificar que a generalização *para todo* $x \in A$, *temos que* $\varphi(x)$ também é verdadeira.

Exemplo 7.1.2 Dado o conjunto $A = \{4, 8, 12, 16\}$, podemos justificar que a generalização *para todo* $x \in A$, *temos que* x *é par* é verdadeira, justificando cada um dos enunciados:

$$4 \text{ } \textit{é par},$$
$$8 \text{ } \textit{é par},$$
$$12 \text{ } \textit{é par},$$
$$16 \text{ } \textit{é par}.$$

Cada um destes enunciados afirma que um dado número natural é par. Assim, podemos justificá-los apresentando argumentações que provam que números naturais são pares. O leitor deve se convencer que cada uma das argumentações abaixo prova, respectivamente, que um dos elementos de A é par:

ARGUMENTAÇÃO 1 (prova de que 4 é par) Sabemos que $4 = 2+2$. Sabemos também que a soma de dois números pares é um número par. Logo, 4 é par.

ARGUMENTAÇÃO 2 (prova de que 8 é par) Sabemos que a soma de dois números ímpares é um número par. Temos que $8 = 1 + 7$. Logo, 8 é par.

ARGUMENTAÇÃO 3 (prova de que 12 é par) Podemos concluir que 12 é par. De fato, $12 = 2 \times 6$. E temos que o dobro de um número natural é um número par.

ARGUMENTAÇÃO 4 (prova de que 16 é par) Temos que $16 = 4 \times k_1$, onde k_1 é um número natural. Por outro lado, $4 \times k_1 = (2 \times 2) \times k_1 = 2 \times (2 \times k_1)$. Assim, concluimos que $16 = 2 \times k_2$, onde k_2 é um número natural. Mas sabemos que um número natural da forma $2 \times k_2$, onde k_2 é um número natural, é um número par. Logo, 16 é par.

As argumentações acima formam, em conjunto, uma prova de que todos os elementos de $A = \{4, 8, 12, 16\}$ são pares.

Vejamos agora o que acontece quando A é infinito.

Exemplo 7.1.3 Considere o conjunto $B = \{4n : n \in \mathbb{N}\}$.

a) Sobre B, fazemos a afirmação *todos os elementos de B são pares.* Afirmar que todos os elementos de B são pares é o mesmo que afirmar que *para todo $n \in \mathbb{N}$, temos que $4n$ é par.* Assim, este enunciado é uma generalização.

Aplicando agora o critério sobre a verdade/falsidade de generalizações formulado para generalizações sobre domínios finitos a esta afirmação, temos que a verdade de *todos os elementos de B são pares* se reduz à verdade dos enunciados:

$$\begin{gathered} 4 \text{ } \textit{é par}, \\ 8 \text{ } \textit{é par}, \\ 12 \text{ } \textit{é par}, \\ 16 \text{ } \textit{é par}, \\ \vdots \end{gathered}$$

obtidos a partir do enunciado generalizado *$4n$ é par*, pela substituição de n pelos elementos de $\mathbb{N}$. Sendo que a generalização *para todo $n \in \mathbb{N}$, temos que $4n$ é par* deve ser verdadeira se, e somente se, quando n assume como valores cada um dos elementos de $\mathbb{N}$, obtemos sempre enunciados *$4n$ é par* que são verdadeiros.

b) Agora, sobre B fazemos a afirmação *todos os elementos de B são menores do que* 1999. Afirmar que todos os elementos de B são menores do que 1999 é o mesmo que afirmar que *para todo $n \in \mathbb{N}$, temos que* $4n < 1999$. E, aplicando o mesmo critério sobre a verdade/falsidade de generalizações, formulado para generalizações sobre domínios finitos, a este enunciado, temos que a falsidade de *todos os elementos de B são menores que* 1999 se reduz à falsidade dos enunciados:

$$\begin{aligned} 4 &< 1999, \\ 8 &< 1999, \\ 12 &< 1999, \\ 16 &< 1999, \\ &\vdots \end{aligned}$$

obtidos a partir do enunciado generalizado $4n < 1999$, pela substituição de n pelos elementos de $\mathbb{N}$. Sendo que a generalização *para todo $n \in \mathbb{N}$, temos que* $4n < 1999$ deve ser falsa se, e somente se, quando n assume como valores cada um dos elementos de $\mathbb{N}$, obtemos enunciados $4n < 1999$ dos quais pelo menos um é falso.

Até o momento temos um critério para verdade/falsidade de generalizações. E este nos fornece um critério para *justificativas* da verdade/falsidade de generalizações sobre domínios finitos. Vamos agora tratar de *justificativas* da verdade/falsidade de generalizações sobre domínios infinitos.

Aplicando de maneira direta o critério de justificativa do caso finito quando A é infinito, vamos considerar que a justificativa da verdade ou falsidade da generalização *para todo $x \in A$, temos que $\varphi(x)$* fica reduzida à justificativa da verdade ou falsidade de uma quantidade infinita de enunciados obtidos a partir de $\varphi(x)$ pela substituição de x pelos elementos de A. Em particular, vamos considerar que, se podemos justificar que todos os enunciados obtidos são verdadeiros, podemos justificar que a generalização é verdadeira.

7.1.2 Contra-exemplos

Vejamos o que acontece quando aplicamos estes critérios à justificativa das generalizações apresentadas no Exemplo 7.1.3.

Exemplo 7.1.4 No item (b) do Exemplo 7.1.3, temos um conjunto infinito B sobre o qual fazemos a afirmação *todos os elementos de B são menores do que* 1999. Como os elementos de B são da forma $4n$, onde $n \in \mathbb{N}$, isto é o mesmo que afirmar que *para todo $n \in \mathbb{N}$, temos que* $4n < 1999$.

Segundo o que foi dito acima, este enunciado é verdadeiro se cada um dos infinitos enunciados $4 < 1999$, $8 < 1999$, $12 < 1999$, $16 < 1999$, ... é verdadeiro. Em contrapartida, este enunciado é falso caso exista um valor de n em $\mathbb{N}$ para o qual o enunciado $4n < 1999$ é falso. Ou seja, o enunciado é falso se, tomando sucessivos valores de n a partir do 1, encontrarmos um valor de n para o qual $4n$ seja um número maior ou igual a 1999.

Se calcularmos sucessivamente o valor de $4n$ para $n = 1, 2, 3, \ldots, 499$ encontraremos sempre valores menores do que 1999. Mas para $n = 500$, teremos: $4n = 2000 > 1999$. Assim, o enunciado é falso.

Observe que, em última análise, mostrar que o enunciado *para todo $n \in \mathbb{N}$, temos que* $4n < 1999$ é falso consiste em exibir um valor de $n \in \mathbb{N}$ para o qual o enunciado $4n < 1999$ é falso.

Um valor de $x \in A$ para o qual o enunciado $\varphi(x)$ é falso é chamado um **contra-exemplo** para a generalização *para todo $x \in A$, temos que $\varphi(x)$*. Por exemplo, $n = 20$ é um contra-exemplo para a Proposição *para todo $n \in \mathbb{N}$, temos que* $4n < 1999$.

Nem sempre é fácil exibir um contra-exemplo para uma generalização falsa. Isto acontece usualmente por dois motivos.

Em primeiro lugar, o primeiro valor que não possui a propriedade generalizada pode ser difícil de determinar.

Exemplo 7.1.5 Considere os números da forma $F_n = 2^{2^n} + 1$, onde $n \in \mathbb{N} \cup \{0\}$. Calculando F_n para valores iniciais de n, temos:

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3 \\ F_1 &= 2^{2^1} + 1 = 5 \\ F_2 &= 2^{2^2} + 1 = 17 \\ F_3 &= 2^{2^3} + 1 = 257 \\ F_4 &= 2^{2^4} + 1 = 65.537 \end{aligned}$$

No século XVII, o matemático francês Pierre de Fermat (1601–1665), verificou que todos os números obtidos acima são primos e *conjecturou* a seguinte proposição:

Proposição 7.1.2 *Para todo $n \in \mathbb{N}$, temos que $F_n = 2^{2^n} + 1$ é primo.*

Somente um século depois, o matemático suiço Leonard Euler (1707–1783) desenvolveu algumas técnicas de fatoração que lhe permitiram mostrar que a conjectura de Fermat era falsa. Na verdade, tomando $n = 5$, temos que $F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \times 6.700.417$ e 5 é um contra-exemplo para a Proposição 7.1.2.

Em segundo lugar, o primeiro valor que não possui a propriedade generalizada pode ser muito grande.

Exemplo 7.1.6 Dizemos que um número natural é **não-quadrado** se ele não é um quadrado perfeito. Por exemplo, $2, 3, 5, 6, 7, 8$ e 10 são não-quadrados.

Considere a expressão $991n^2 + 1$, onde n é um número natural. Já foi mostrado que tomando valores sucessivos a partir do 1 e calculando o valor da expressão acima para muitos valores de n, encontramos somente números não-quadrados. Baseados, então, numa grande quantidade de casos, pode-se julgar que a generalização *para todo $n \in \mathbb{N}$, temos que $991n^2 + 1$ é não-quadrado* é verdadeira. Mas este enunciado é falso. De fato, pode-se mostrar que se

$$n = 12.055.735.790.331.359.447.442.538.767,$$

então $991n^2 + 1$ é um quadrado perfeito. Este é o menor valor de n que é um contra-exemplo para a Proposição 7.1.2.

7.1.3 O problema dos domínios infinitos

Voltemos ao item (a) do Exemplo 7.1.3. Temos um conjunto infinito B sobre o qual fazemos a afirmação *todos os elementos de B são pares*. Como os elementos de B são da forma $4n$, onde $n \in \mathbb{N}$, isto é o mesmo que afirmar que *para todo $n \in \mathbb{N}$, temos que $4n$ é par*.

Segundo o critério de verdade/falsidade de generalizações, esse enunciado é verdadeiro se, e somente se, cada um dos infinitos enunciados *4 é par*, *8 é par*, *12 é par*, *16 é par*, ... é verdadeiro.

Aplicando o mesmo critério de justificativa formulado para o caso em que os domínios de generalização são finitos, podemos mostrar que esse enunciado é verdadeiro mostrando que cada enunciados *$4n$ é par* é verdadeiro. Mas como $\mathbb{N}$ é infinito isto não pode ser feito da mesma maneira que para domínios

finitos, ou seja, tomando-se valores sucessivos de n a partir do 1 e justificando que cada um dos enunciados obtidos é verdadeiro. De fato, se A é infinito, este processo de justificativa nunca terá fim.

Em resumo, caso A seja finito, temos um método para justificar que uma generalização *para todo* $x \in A$, *temos que* $\varphi(x)$ é verdadeira. Este consiste na justificativa de que cada um dos enunciados $\varphi(x)$, obtidos pela substituição de x por elementos de A, é verdadeiro. Mas, no caso infinito, este processo não pode ser executado, já que levaria a um processo de justificativa que nunca teria fim. Surge, então, a seguinte questão:

> Como podemos justificar a verdade de generalizações, quando os domínios de generalização são conjuntos infinitos?

Na verdade, este problema surge mesmo para certos domínios finitos. No caso de termos um domínio A finito mas "muito grande" e querermos justificar a veracidade de um enunciado *para todo* $x \in A$, *temos que* $\varphi(x)$, teríamos que justificar uma quantidade "muito grande" de enunciados, todos os que são obtidos a partir do enunciado $\varphi(x)$, pela substituição de x por cada um dos elementos de A.

7.2 Provando generalizações

Para responder a questão levantada no final da Seção 7.1.3, vamos examinar as Argumentações 1 e 4 apresentadas no Exemplo 7.1.2.

A Argumentação 1 justifica que 4 *é par* utilizando como premissas que $4 = 2 + 2$ e que *a soma de dois números pares é um número par*. Observe que fazendo pequenas modificações na Argumentação 1, podemos produzir argumentações análogas à Argumentação 1, para justificar que cada um dos elementos de $A = \{4, 8, 12, 16\}$ é par. De fato, para justificar, por exemplo, que 8 *é par* utilizando uma argumentação análoga à Argumentação 1, basta executar os seguintes passos:

1. Parcelar o número 8 como uma soma de dois números pares.
2. Aplicar a propriedade que diz que a soma de dois números pares é par ao parcelamento obtido.

Assim, podemos apresentar, por exemplo, a seguinte argumentação que prova que 8 é par.

ARGUMENTAÇÃO 5 (prova de que 8 é par) Sabemos que $8 = 2+6$. Sabemos também que a soma de dois números pares é um número par. Logo, 8 é par.

As únicas diferenças entre a Argumentação 5 e a Argumentação 1 são a ocorrência do 8 no lugar do 4 e a premissa que afirma que $8 = 2+6$ no lugar da premissa que afirma que $4 = 2 + 2$.

Já a Argumentação 4 justifica que 16 *é par* utilizando como premissas que $16 = 4 \times k_1$, *onde* k_1 *é um número natural*, que $4 \times k_1 = 2 \times (2 \times k_1)$, que $16 = 2 \times k_2$, *onde* k_2 *é um número natural* e, finalmente, que *um número natural da forma* $2 \times k_2$, *onde* k_2 *é um número natural, é um número par.*

Observe que, fazendo pequenas modificações na Argumentação 4, também podemos produzir argumentações análogas à Argumentação 4, para justificar que cada um dos elementos de A é par. De fato, para justificar, por exemplo, que 12 *é par* utilizando uma argumentação análoga à Argumentação 4, basta executar os seguintes passos:

1. Afirmar que $12 = 4 \times k_1$, onde k_1 é um número natural.
2. Observar que $4 \times k_1 = 2 \times (2 \times k_1)$.
3. Concluir que $12 = 2 \times k_2$, onde k_2 é um número natural.
4. E aplicar a propriedade que diz que *um número natural da forma* $2 \times k_2$, *onde* k_2 *é um número natural, é um número par* à igualdade obtida.

Assim, podemos apresentar, por exemplo, a seguinte argumentação que prova que 12 é par.

ARGUMENTAÇÃO 6 (prova de que 12 é par) Temos que $12 = 4 \times k_1$, onde k_1 é um número natural. Por outro lado, $4 \times k_1 = (2 \times 2) \times k_1 = 2 \times (2 \times k_1)$. Assim, concluimos que $12 = 2 \times k_2$, onde k_2 é um número natural. Mas sabemos que um número natural da forma $2 \times k_2$, onde k_2 é um número natural, é um número par. Logo, 12 é par.

A única diferença entre a Argumentação 6 e a Argumentação 4 é que na Argumentação 6 há ocorrências do número 12 em todos os lugares onde na Argumentação 4 ocorre o número 16.

Concluímos, então, que não é difícil apresentar argumentações análogas à Argumentação 1 e nem argumentações análogas à Argumentação 4, para justificar que cada um dos elementos do conjunto $A = \{4, 8, 12, 16\}$ é par.

Vejamos agora o que acontece quando tentamos apresentar argumentações análogas à Argumentação 1 para justificar que cada uma dos elementos do conjunto infinito $B = \{4, 8, 12, 16, \ldots\}$ é par.

Segundo o que foi dito acima, dado um número $b \in B$, para provar que x é par apresentando uma argumentação análoga à Argumentação 1, temos que fazer duas pequenas modificações na Argumentação 1:

1. substituir a ocorrência do 4 pelo número b,
2. substituir o parcelamento dado, do 4, por um parcelamento adequado do número b.

Como o conjunto B é infinito e cada elemento de B deve ser parcelado de uma maneira diferente, temos que fazer uma modificação adequada para cada elemento de B e, portanto, temos que fazer uma infinidade de modificações e esse processo de justificativa nunca terá fim.

Por outro lado, vejamos o que acontece quando utilizamos argumentações análogas à Argumentação 4 para justificar que cada uma dos elementos do conjunto infinito $B = \{4, 8, 12, 16, \ldots\}$ é par.

Segundo o que foi dito, se vamos apresentar argumentações análogas à Argumentação 4 para justificar que cada um dos elementos do conjunto infinito $B = \{4, 8, 12, 16, \ldots\}$ é par, a única modificação que temos que fazer na Argumentação 6 é a substituição das ocorrências do número 16 pelo número que estamos provando que é par. Como o conjunto B é infinito e temos que fazer uma substituição para cada elemento de B, esse processo de justificativa, também não terá fim.

Mas, como vimos acima, a modificação que temos que fazer na Argumentação 1 é a de mudar uma das premissas por uma outra premissa adequada. Sendo que para cada número do conjunto B devemos utilizar uma premissa diferente, mostrando como podemos parcelar o número considerado em uma soma de dois números pares. Um mesmo número pode ter mais de um parcelamento em números pares, mas para cada número esses parcelamentos são diferentes. Enquanto que na Argumentação 4 não temos que mudar uma das premissas mas apenas um dos valores que ocorre em algumas das premissas. Em outras palavras, a Argumentação 4 fornece a seguinte *estrutura* que pode ser utilizada para gerar cada uma das novas argumentações pela simples substituição da variável x pelo elemento que estamos querendo provar que é par:

ARGUMENTAÇÃO 7 (prova de que um elemento x de $B = \{4, 8, 12, 16, \ldots\}$ é par) Temos que $x = 4 \times k_1$, onde k_1 é um número natural. Por outro lado, $4 \times k_1 = (2 \times 2) \times k_1 = 2 \times (2 \times k_1)$. Assim, concluimos que $x = 2 \times k_2$, onde k_2 é um número natural. Mas sabemos que um número natural da forma $2 \times k_2$, onde k_2 é um número natural, é um número par. Logo, x é par.

Os exemplo acima sugerem que ao tentar modificar uma justificativa, dada para um elemento a de um conjunto A, para obter justificativas para os outros elementos de A, deparamos com duas situações:

1. Ao fazer a modificação, temos que mudar um ou mais enunciados que valem para a em outros enunciados que valem para o elemento que estamos tentando justificar.

2. Ao fazer a modificação, temos que mudar somente o valor do elemento em alguns enunciados que ocorrem na justificativa feita para a.

No primeiro caso, estamos utilizando na justificativa dada uma propriedade de a que a não compartilha com os outros elementos de A. No segundo caso, estamos utilizando na justificativa dada somente propriedades de a que a compartilha com todos os outros elementos de A.

Uma propriedade de um elemento x, pertencente a um conjunto A, é *genérica* em A se todos os elementos de A possuem a propriedade.

Exemplo 7.2.1 A propriedade *existe* $k_1 \in \mathbb{N}$, *tal que* $x = 4k_1$, do elemento 4 de B, é genérica em $B = \{4, 8, 12, 16, \ldots\}$.

A idéia então é a seguinte: já que uma justificativa para um dado elemento de A, formada por propriedades genéricas de a, fornece uma estrutura que gera cada uma das argumentações que estamos procurando para os outros elementos, porque não aceitar essa estrutura como a justificativa para todos os elementos de A?

Exemplo 7.2.2 A Argumentação 7 dada acima é a justificativa de que todos os elementos de B são pares.

Essa é a idéia expressa no método de provas de generalizações.

Para provar generalizações podemos usar o seguinte método:

MÉTODO DA GENERALIZAÇÃO, MG.

Para provar uma generalização *para todo $x \in A$, temos que $\varphi(x)$* basta fazer o seguinte:

1. Supor que a variável de generalização x assume como valor um elemento qualquer no domínio de generalização A.
2. Provar que o enunciado generalizado $\varphi(x)$ é verdadeiro, usando somente propriedades de x que são genéricas em A, ou seja, usando como propriedades de x somente propriedades que valem para todos os elementos de A.

Em termos de justificativas por meio de argumentações, o Método da Generalização afirma que, para justificar que uma generalização é verdadeira, basta que escolhamos um elemento qualquer do domínio de generalização e apresentemos uma justificativa do enunciado generalizado aplicado ao elemento escolhido, onde todas as afirmações feitas sobre o elemento escolhido possam ser feitas também sobre os outros elementos do domínio de generalização (Figura 7.2).

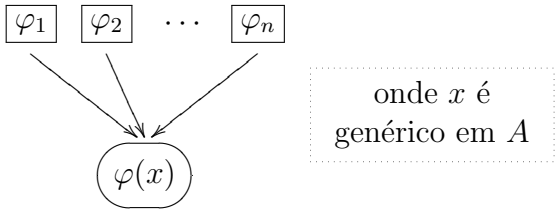


Figura 7.2: Estrutura das provas de generalizações *para todo $x \in A$, temos que $\varphi(x)$*.

Voltemos, então, à prova do enunciado *se $A \subseteq B$ e $B \subseteq C$, então $A \subseteq C$*, que foi reduzida à prova do enunciado *para todo $x \in A$, temos que $x \in C$*, a partir de *$A \subseteq B$ e $B \subseteq C$*.

Como a proposição que queremos provar é uma generalização, segundo o Método de Generalização, basta fazer o seguinte:

1. Supor que a variável x assume como valor um elemento qualquer de A.

2. Provar que $x \in C$, usando como propriedades de x somente propriedades que valem para todos os elementos de A.

Vejamos como isso pode ser feito:

ARGUMENTAÇÃO 8 (prova de que a inclusão é transitiva)

Em primeiro lugar, de acordo com MG, supomos que $x \in A$, ou seja, que x assume como valor um elemento qualquer de A.

Agora, de acordo com MS, na prova de que $A \subseteq C$ podemos usar como premissa que $A \subseteq B$.

Mas, de acordo com a definição de inclusão, $A \subseteq B$ quer dizer que *todo elemento de A também é elemento de B*. E como este enunciado se refere a todos os elementos de A, ela se refere também a x, já que supomos que x é um elemento de A.

Podemos concluir então que $x \in B$.

Agora, de acordo com MS, na prova de que $A \subseteq C$ também podemos usar como premissa que $B \subseteq C$.

Mas, de acordo com a definição de inclusão, $B \subseteq C$ quer dizer que *todo elemento de B também é elemento de C*. E como este enunciado se refere a todos os elementos de B, ela se refere também a x, já que provamos que x é um elemento de B.

Podemos concluir então que $x \in C$.

Assim, provamos que *se $x \in A$ então $x \in C$*, ou seja que *se x é um elemento de A, então x é um elemento de C*.

Em relação ao uso do Método da Generalização, dois aspectos são importantes na argumentação acima:

1. Provamos que um dado elemento de A está em C.

2. As únicas propriedades utilizadas sobre x foram $x \in B$, que valia para todos os elementos de A, já que tinhamos como premissa que $A \subseteq B$, e *se $x \in B$, então $x \in C$*, que valia para todos os elementos de A, já que tínhamos provado que todos os elementos de A estão em B.

Como as únicas propriedades de x que foram utilizadas na argumentação são genéricas em A, o Método da Generalização permite concluir que o que foi provado, ou seja, que *se x é um elemento de A, então x é um elemento de C*, vale para todos os elementos de A. Assim, temos que todo elemento e A também é elemento de C, ou seja $A \subseteq C$.

Esta é uma maneira muito sutil de provar generalizações e a não observação das restrições apresentadas no método pode levar a erros consideráveis.

7.3 Um erro frequente

Um erro que frequentemente é cometido ao tentarmos provar uma generalização *para todo $x \in A$, temos que $\varphi(x)$*, é utilizar, na justificativa de $\varphi(x)$ para um elemento genérico x, uma ou mais propriedades de x que não são genéricas em A, mas que x compartilha apenas com alguns elementos de A.

Exemplo 7.3.1 Considere a seguinte proposição:

Proposição 7.3.1 *Para todo $x \in \mathbb{R}$, $sen^2(x) + cos^2(x) = 1$.*

A Proposição 7.3.1 é a generalização de $sen^2(x) + cos^2(x) = 1$ em relação à variável x e ao conjunto $\mathbb{R}$ dos números reais. Assim, segundo o Método de Generalização, para prová-la basta fazer o seguinte:

1. Supor que x assume como valor um número real qualquer.
2. Provar que $sen^2(x) + cos^2(x) = 1$, usando como propriedades de x somente propriedades que x compartilha com todos os números reais.

Considere agora a seguinte argumentação que é, pretensamente, uma prova da Proposição 7.3.1.

Pretensa prova:
Seja $x \in \mathbb{R}$. Associamos a x triângulo retângulo da Figura 7.3. Pela definição

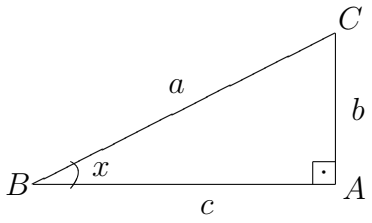


Figura 7.3: Triângulo retângulo.

de seno, temos que $sen(x) = \dfrac{b}{a}$. Pela definição de coseno, temos que $cos(x) =$

$\frac{c}{a}$. Assim, $sen^2(x) + cos^2(x) = \left(\frac{b}{a}\right)^2 + \left(\frac{c}{a}\right)^2 = \frac{b^2}{a^2} + \frac{c^2}{a^2} = \frac{b^2 + c^2}{a^2}$. Mas, pelo Teorema de Pitágoras, temos que $a^2 = b^2 + c^2$. Logo,

$$sen^2(x) + cos^2(x) = \frac{b^2 + c^2}{a^2} = \frac{a^2}{a^2} = 1. \quad \boxed{?}$$

A argumentação acima não é uma prova da Proposição 7.3.1, pois utiliza como premissa o enunciado que afirma que podemos associar a x um triângulo retângulo como o da Figura 7.3. Mas, segundo os conceitos básicos da Trigonometria, somente os números reais que estão no primeiro quadrante do ciclo trigonométrico possuem um círculo associado, da maneira descrita na argumentação. Por exemplo, se x está no segundo quadrante, o triângulo associado deveria ser como mostrado na Figura 7.4. Assim, ao formularmos a

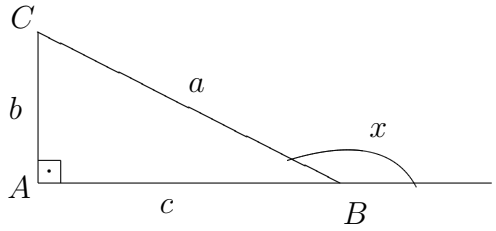


Figura 7.4: Triângulo retângulo para x no segundo quadrante.

argumentação, utilizamos uma propriedade que x não compartilha com todos os números reais, mas somente com aqueles que estão no primeiro quadrante do ciclo trigonométrico e a generalização não está provada.

Na verdade, o enunciado que está provado é o seguinte:

$$\textit{para todo } x \in \mathbb{R}, \textit{ se } 0 < x < \pi/2, \textit{ então } sen^2(x) + cos^2(x) = 1.$$

Vejamos um outro exemplo.

Exemplo 7.3.2 Considere a seguinte proposição:

Proposição 7.3.2 *Dados os pontos $P = (a, b)$ e $Q = (c, d)$ do plano cartesiano, a distância do ponto P ao ponto Q é dada por*

$$d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}.$$

A Proposição 7.3.2 é uma generalização, pois pode ser reescrita como:

Para todos $P = (a, b), Q = (c, d) \in \mathbb{R}^2$, *temos que*
$d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}$.

Assim, a Proposição 7.3.2 é a generalização do enunciado

$$d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}$$

em relação às variáveis P e Q e ao conjunto $\mathbb{R}^2$. Segundo o Método de Generalização, para prová-la basta fazer o seguinte:

1. Supor que $P = (a, b)$ e $Q = (c, d)$ são pontos quaisquer do plano cartesiano.
2. Provar que $d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}$, usando como propriedades de P e Q somente propriedades que P e Q compartilham com todos os pontos do plano cartesiano.

Considere agora a seguinte argumentação que é, pretensamente, uma prova da Proposição 7.3.2.

Pretensa prova:
Sejam $P = (a, b), Q = (c, d) \in \mathbb{R}^2$. Associamos a P e Q a Figura 7.5.

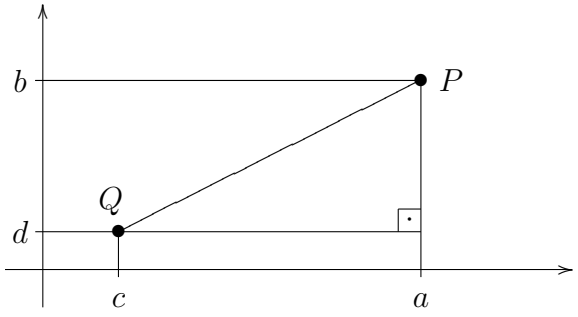


Figura 7.5: Distância entre P e Q.

Observe que o segmento PQ é a hipotenusa de um triângulo retângulo e que as medidas dos catetos deste triângulo são $a - c$ e $b - d$. Assim, pelo Teorema de Pitágoras, temos que $d(P, Q)^2 = (a - c)^2 + (b - d)^2$. Daí,

$$d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}. \quad \boxed{?}$$

A argumentação acima não é uma prova da Proposição 7.3.2, pois utiliza como premissa a proposição que afirma que podemos associar a P e Q um

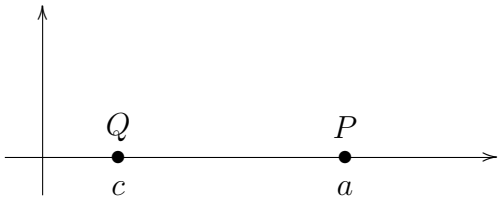


Figura 7.6: Distância entre P e Q, quando ambos estão sobre o eixo horizontal.

triângulo retângulo como o da figura. Por exemplo, se P e Q estão ambos sobre o eixo horizontal, deveríamos associar a Figura 7.6. Assim, ao formularmos a argumentação, utilizamos uma propriedade que P e Q não compartilham com todos os pontos do plano cartesiano, mas somente com aqueles que estão simultaneamente no primeiro quadrante dos eixos cartesianos. E a generalização não está provada.

Na verdade, o enunciado que está provado é o seguinte:

$$\begin{array}{c} \textit{para todos } P = (a, b), Q = (c, d) \in \mathbb{R}^2, \\ \textit{se } a, b, c, d > 0, \textit{ então } d(P, Q) = \sqrt{(a - c)^2 + (b - d)^2}. \end{array}$$

Capítulo 8

Prova de induções

O conjunto dos números naturais possui uma certa estrutura que decorre da maneira como os naturais são formados, a partir do zero, por aplicações sucessivas da operação de somar uma unidade. Levando isto em conta, apresentamos um novo método para a prova de generalizações para os casos em que o domínio de generalização é $\mathbb{N}$. Discutimos alguns erros frequentes na utilização deste método e algumas formas mais elaboradas em que o método pode ser apresentando.

8.1 O problema de provar induções

Em certas situações, existem alternativas, além de MG, para a prova de generalizações. Neste capítulo, apresentaremos um exemplo importante de tal situação. Para especificá-lo de maneira precisa, vamos introduzir uma distinção entre generalizações e enunciados particulares.

Exemplo 8.1.1 O enunciado *10 é múltiplo de cinco* é um enunciado particular. Já o enunciado *todos os números que terminam em zero são múltiplos de cinco* é uma generalização.

Um **enunciado particular**, em sua forma mais simples, afirma que um elemento a de um dado conjunto A possui uma propriedade P e pode ser escrito na forma:

$$a \text{ é } P$$

Já uma generalização, em sua forma mais simples, afirma que todos os elementos de um dado conjunto A possuem uma propriedade P e pode ser escrita na forma:

para todo $x \in A$, temos que x é P

onde x é uma variável que assume como valores elementos de A.

A aplicação do novo método de prova para generalizações está associada ao problema de justificar um enunciado obtido como conclusão a partir de outros enunciados tomadas como premissas, nos casos em que algumas das premissas são enunciados particulares e a conclusão é uma generalização.

A inferência de uma generalização a partir de um conjunto de enunciados particulares é chamada **indução**.

Exemplo 8.1.2 Considere o trinômio $n^2 + n + 41$, onde n é um número natural. Tomando alguns valores consecutivos para n, teremos a seguinte tabela:

n	$n^2 + n + 41$
1	43
2	47
3	53
4	61
5	71
6	83
7	97
8	113
9	131
10	151

Observando os valores obtidos, podemos efetuar induções, passando de enunciados particulares para generalizações. Dentre estas, duas são imediatas:

(*i*) Observando que os enunciados particulares 1^2+1+41 *é ímpar*, 2^2+2+41 *é ímpar*, ... , $10^2 + 10 + 41$ *é ímpar* são verdadeiros, podemos formular a generalização *para todo $n \in \mathbb{N}$, temos que $n^2 + n + 41$ é ímpar.*

(*ii*) Observando que os enunciados particulares 1^2+1+41 *é primo*, 2^2+2+41 *é primo*, ... , $10^2 + 10 + 41$ *é primo* são verdadeiros, podemos formular a generalização *para todo $n \in \mathbb{N}$, temos que $n^2 + n + 41$ é primo.*

As induções acima possuem uma forma bastante específica. Em ambos os exemplos tomamos uma propriedade $P(n)$, envolvendo um número natural

n, e observamos que enunciados particulares da forma $P(n)$ são verdadeiros, quando a variável n assume alguns valores iniciais em $\mathbb{N}$. Baseados nesta observação, formulamos a generalização *para todo* $n \in \mathbb{N}$*, temos que* $P(n)$.

Considere agora o problema de provar generalizações verdadeiras, obtidas quando efetuamos induções sobre números naturais.

PROBLEMA: PROVA DA INDUÇÃO.

Dado: Uma generalização verdadeira *para todo* $n \in \mathbb{N}$*, temos que* $P(n)$, obtida por uma indução sobre números naturais.

Questão: Provar que a generalização é, de fato, verdadeira.

Este é o problema ao qual o novo método de prova pode ser aplicado.

Como vimos no Capítulo 7, podemos utilizar o Método da Generalização para resolver o problema da prova de induções. Isto foi o que fizemos no caso do item (i) acima. A questão é que, para utilizar o método de generalização, devemos efetuar uma argumentação que não pode depender de nenhum valor particular da variável de generalização e isto, usualmente, depende de um pouco de inspiração.

Exemplo 8.1.3 Seja $S_n = 1 + 2 + 3 + \cdots + n$, onde n é um número natural.

Efetuando a soma acima para alguns valores de n, a partir do 1, teremos:

$$\begin{aligned} S_1 &= 1 \\ S_2 &= 1 + 2 = 3 \\ S_3 &= 1 + 2 + 3 = 6 \\ S_4 &= 1 + 2 + 3 + 4 = 10 \\ S_5 &= 1 + 2 + 3 + 4 + 5 = 15 \end{aligned}$$

Observando os valores obtidos, aparentemente não encontramos nenhum padrão que nos leve a formular uma generalização a partir destes enunciados

particulares, para uma indução. Mas reescrevendo cada soma, temos:

$$S_1 = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2}$$

$$S_2 = 1 + 2 = 3 = \frac{6}{2} = \frac{2 \cdot 3}{2} = \frac{2(2+1)}{2}$$

$$S_3 = 1 + 2 + 3 = 6 = \frac{12}{2} = \frac{3 \cdot 4}{2} = \frac{3(3+1)}{2}$$

$$S_4 = 1 + 2 + 3 + 4 = 10 = \frac{20}{2} = \frac{4 \cdot 5}{2} = \frac{4(4+1)}{2}$$

$$S_5 = 1 + 2 + 3 + 4 + 5 = 15 = \frac{30}{2} = \frac{5 \cdot 6}{2} = \frac{5(5+1)}{2}$$

Observando agora os valores reescritos, podemos efetuar uma indução, passando dos enunciados particulares

$$S_1 = \frac{1(1+1)}{2}$$

$$S_2 = \frac{2(2+1)}{2}$$

$$S_3 = \frac{3(3+1)}{2}$$

$$S_4 = \frac{4(4+1)}{2}$$

$$S_5 = \frac{5(5+1)}{2}$$

para a generalização *para todo* $n \in \mathbb{N}$*, temos que* $S_n = \dfrac{n(n+1)}{2}$.

Queremos justificar que a indução está correta. Ou seja, queremos provar que a generalização obtida é verdadeira. Para isto, podemos utilizar o Método de Generalização.

Proposição 8.1.1 *Para todo* $n \in \mathbb{N}$*, temos que* $S_n = 1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

Prova:
(Atribuída a C.F. Gauss, ±1780) Seja $n \in \mathbb{N}$. Temos que $S_n = 1 + 2 + \cdots + (n-1) + n$. Invertendo a ordem das parcelas, temos também que $S_n = n + (n-1) + \cdots + 2 + 1$. Somando as duas igualdades, membro a membro, temos $2S_n = (n+1) + (n+1) + \cdots + (n+1) + (n+1)$, onde a parcela $(n+1)$ aparece n vezes. Assim, $2S_n = n(n+1)$, e daí, temos que $S_n = \dfrac{n(n+1)}{2}$. ∎

Na prova da Proposição 8.1.1, tomamos a variável n, assumimos que ela denota um número natural e apresentamos uma argumentação que não depende de nenhum valor específico de n. Esse é um tipo de resposta que consideramos satisfatória para o problema de provar induções, já que as proposições obtidas por indução são generalizações. A única dificuldade da prova é perceber que, invertendo a ordem das parcelas de S_n e somando a expressão invertida com a soma original, temos duas expressões que quando somadas e manipuladas algebricamente nos levam ao resultado desejado.

Mas como a generalização é efetuada sobre números naturais, o Método de Indução matemática garante que podemos obter uma outra solução satisfatória por um caminho um pouco diferente. É o que veremos a seguir.

8.2 Provando induções

Para provar generalizações sobre números naturais, obtidas ou não por indução, podemos utilizar o seguinte método:

MÉTODO DE INDUÇÃO MATEMÁTICA, MI.

Seja $P(n)$ uma propriedade sobre números naturais. Para provar uma generalização *para todo* $n \in \mathbb{N}$, *temos que* $P(n)$, é suficiente fazer o seguinte:

1. Provar que o número natural 1 possui a propriedade. Ou seja, provar que $P(1)$.
2. Provar a generalização

   para todo $n \in \mathbb{N}$, *se* $P(n)$, *então* $P(n+1)$.

   Ou seja, provar que, para um natural genérico n, o fato de n possuir a propriedade acarreta que o número natural $n+1$ também possui a propriedade.

Em termos de justificativas por meio de argumentações, o Método de Indução Matemática afirma que, para justificar que uma generalização sobre números naturais é verdadeira, basta que façamos duas coisas. Em primeiro lugar, que apresentemos uma justificativa do enunciado generalizado aplicado ao número 1. Em segundo lugar, que escolhamos um natural qualquer e apresentemos uma justificativa para a generalização da implicação cujo antecendente é o enunciado generalizado aplicado à variável n e cujo consequente é o enunciado generalizado aplicado a $n+1$.

Exemplo 8.2.1 Vamos utilizar o Método de Indução Matemática para provar a generalização no item (i) do Exemplo 8.1.2 e a Proposição 8.1.1, já provadas pelo Método de Generalização.

(a) No caso da generalização no item (i) do Exemplo 8.1.2, temos:

Proposição 8.2.1 *Para todo* $n \in \mathbb{N}$, *temos que* n^2+n+41 *é ímpar.*

Segundo o método de indução, a prova consiste de duas etapas:

1. A prova de que 1 possui a propriedade.
2. A prova de que *para todo* $n \in \mathbb{N}$, *se* n^2+n+41 *possui a propriedade, então* $(n+1)^2+(n+1)+41$ *possui a propriedade.*

Neste caso, a propriedade considerada é *ser ímpar*. Assim, temos a seguinte prova para a Proposição 8.2.1:

Prova:
Se $n = 1$, então $n^2 + n + 41 = 1^2 + 1 + 42 = 43$, que é um número ímpar.

Seja $n \in \mathbb{N}$. Suponhamos que $n^2 + n + 41$ é ímpar.

Daí, $(n+1)^2+(n+1)+41 = n^2+2n+1+n+1+41 = n^2+n+41+2n+1+1 = n^2 + n + 41 + 2n + 2 = n^2 + n + 41 + 2(n + 1)$.

Por hipótese, $n^2 + n + 41$ é ímpar e como $2(n + 1)$ é par, temos que $n^2 + n + 41 + 2(n + 1)$ é ímpar, que é o que queríamos provar. ∎

(*b*) No caso da Proposição 8.1.1, temos:

Proposição 8.1.1 Para todo $n \in \mathbb{N}$, temos que

$$S_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Neste caso, a propriedade considerada é $S_n = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$. Assim, segundo o método de indução, a prova consiste de duas etapas:

1. A prova de que $S_1 = \frac{1(1+1)}{2}$.
2. A prova de que *para todo* $n \in \mathbb{N}$, *se* $S_n = \frac{n(n+1)}{2}$, *então* $S_{n+1} = \frac{(n+1)(n+1)+1}{2}$.

Assim, temos a seguinte prova da Proposição 8.1.1:

Prova:
Se $n = 1$, temos que $S_1 = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2}$.

Seja $n \in \mathbb{N}$. Suponhamos que $S_n = \frac{n(n+1)}{2}$.

Temos que $S_{n+1} = 1+2+\cdots+n+(n+1) = (1+2+\cdots+n)+(n+1) = S_n + (n+1)$. Como, por hipótese, $S_n = \frac{n(n+1)}{2}$, temos que $S_n + (n +$

$1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$, que é o que queríamos provar. ∎

8.3 Estrutura das provas por indução

Uma prova de uma generalização *para todo $n \in \mathbb{N}$, temos que $P(n)$*, obtida pelo Método de Indução, é chamada uma *prova por indução*. Toda prova por indução possui duas etapas.

1. Provar que o enunciado $P(1)$ é verdadeiro.
2. Provar que a generalização sobre números naturais *para todo $n \in \mathbb{N}$, se $P(n)$, então $P(n+1)$,* é verdadeira.

Exemplo 8.3.1 Considere o enunciado

$$\textit{para todo } n \in \mathbb{N}\textit{, temos que } 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2.$$

Este enunciado é da forma *para todo $n \in \mathbb{N}$, temos que $P(n)$,* onde $P(n)$ é o enunciado $2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$.

Para apresentar uma prova deste enunciado usando o Método de Indução, devemos cumprir as duas etapas a seguir.

1. Provar que o enunciado $P(1)$ é verdadeiro, isto é, provar que $2^1 = 2^1 - 1$, o que é imediato.
2. Provar que, *para todo $n \in \mathbb{N}$, se $P(n)$, então $P(n+1)$,* é verdadeiro. Isto é, provar que

$$\begin{array}{l}\textit{para todo } n \in \mathbb{N}\textit{, se } 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 2,\\ \textit{então } 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = 2^{(n+1)+1} - 2.\end{array}$$

Como a segunda etapa de uma prova por indução é a prova de uma generalização, podemos executá-la aplicando o Método de Generalização. Logo, para executar esta segunda etapa da prova por indução basta fazer o seguinte:

a. Supor que $P(n)$ é verdadeiro.

b. Provar que $P(n+1)$ é verdadeiro, usando $P(n)$ como premissa.

Ou seja, a segunda etapa de uma prova por indução pode ser subdivida em duas.

Exemplo 8.3.2 Assim, para concluir a prova do enunciado do exemplo anterior, basta fazer como segue.

2a. Suponhamos que $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

2b. Devemos mostrar que $2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = 2^{(n+1)+1} - 1$.

Como, por hipótese, $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$, temos que $2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$. Logo, $2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = 2 \cdot 2^{n+1} - 1$. Logo, $2^0 + 2^1 + 2^2 + \cdots + 2^n + 2^{n+1} = 2^{(n+1)+1} - 1$.

Assim, toda prova por indução de uma generalização sobre números naturais *para todo $n \in \mathbb{N}$, temos que $P(n)$,* possui três etapas:

1. Provar $P(1)$.
2. Supor $P(n)$.
3. Provar $P(n+1)$, utilizando $P(n)$ como premissa.

As três etapas acima são chamadas, respectivamente, a **base**, a **hipótese** e o **passo** de indução.

Exemplo 8.3.3 *Para todo $n \in \mathbb{N}$, temos que $n^2 + n$ é divisível por 2.*

Prova (por indução em n):

Base. Temos que $1^2 + 1 = 2$ é divisível por 2.

Hipótese. Suponhamos que $n^2 + n$ é divisível por 2.

Passo. Devemos mostrar que $(n+1)^2+(n+1)$ é divisível por 2. Pela hipótese de indução, temos que n^2+n é divisível por 2. Além disso, sabemos que $2n+2$ é divisível por 2. Logo, $(n^2+n)+(2n+2) = n^2+2n+1+n+1 = (n+1)^2+(n+1)$ é divisível por 2. ∎

Duas observações são importantes, sobre a estrutura específica de uma prova por indução. A primeira é que, se ao fazermos corretamente uma prova de uma generalização sobre números naturais, não cumprirmos cada uma das etapas acima, embora tenhamos uma prova correta, não podemos dizer que temos uma prova por indução. A segunda é que, às vezes, ao executarmos tanto a base quanto o passo de uma prova por indução, pode ser necessário que executemos as três etapas de provas por indução de outras generalizações.

Exemplo 8.3.4 (*a*) *Para todo $n \in \mathbb{N}$, se $n \neq 1$, então n é obtido a partir de um outro número natural, pela adição de uma unidade.*

Prova (por indução em n):

Base. Devemos mostrar que, se $1 \neq 1$, então 1 é obtido a partir de um outro número natural, pela adição de uma unidade.

Como $1 = 1$, o enunciado que devemos mostrar é verdadeiro, trivialmente.

Hipótese. Suponhamos que, se $n \neq 1$, então n é obtido a partir de um outro número natural, pela adição de uma unidade.

"Passo". Suponhamos que $n+1 \neq 1$. Daí temos que $(n+1)-1$ é um número natural. Como $n+1 = ((n+1)-1)+1$, temos que $n+1$ é obtido a partir de um outro número natural, pela adição de uma unidade. ∎

Observe que, no "passo de indução" desta prova, a hipótese de indução não foi utilizada. Por isto esta prova não é considerada uma prova por indução.

(*b*) *Para todos $m, n \in \mathbb{N}$, temos que $m + n = n + m$.*

Prova (por indução em n):

Base (1). Devemos mostrar que, *para todo $m \in \mathbb{N}$, temos que* $m + 1 = 1 + m$.

Por indução em m:

Base (2). Devemos mostrar que $1 + 1 = 1 + 1$, o que é trivial.

Hipótese (2). Suponhamos que $m + 1 = 1 + m$.

Passo (2). Devemos mostrar que $(m + 1) + 1 = 1 + (m + 1)$.

Pela hipótese de indução (2), temos que $m + 1 = 1 + m$.

Logo, $(m + 1) + 1 = (1 + m) + 1$.

Daí, pela associatividade da adição, $(m + 1) + 1 = 1 + (m + 1)$.

Hipótese (1). Suponhamos que, *para todo $m \in \mathbb{N}$, temos que* $m+n = n + m$.

Passo (1). Devemos mostrar que *para todo $m \in \mathbb{N}$, temos que* $m + (n + 1) = (n + 1) + m$.

Por indução em m:

BASE (3). Devemos mostrar que $1 + (n + 1) = (n + 1) + 1$.

Pela **Hipótese de indução (1)**, temos que $1 + n = n + 1$.

Logo, $(n + 1) + 1 = (1 + n) + 1$.

Daí, pela associatividade da adição, $1 + (n + 1) = (n + 1) + 1$.

HIPÓTESE (3). Suponhamos que $m + (n + 1) = (n + 1) + m$.

PASSO (3). Devemos mostrar que $(m + 1) + (n + 1) = (n + 1) + (m + 1)$.

Pela HIPÓTESE DE INDUÇÃO (3), temos que $m+(n+1) = (n+1)+m$.

Logo, $(m + (n + 1)) + 1 = ((n + 1) + m) + 1$.

Mas, pela **Hipótese de indução (1)**, temos que $n + 1 = 1 + n$.

Logo, $m + ((1 + n) + 1) = ((n + 1) + m) + 1$.

Finalmente, pela associatividade da adição, temos que $(m + 1) + (n + 1) = (n + 1) + (m + 1)$. ∎

Capítulo 9

Prova de existencializações

Neste capítulo, tratamos do problema de provar existencializações. Em particular, apresentamos o Método da Existencialização, para a prova de existencializações.

9.1 O problema de provar existencializações

Voltemos agora à prova do enunciado que afirma que o quadrado de um número par é par, apresentada no Capítulo 7:

Proposição 9.1.1 *Para todo $n \in \mathbb{N}$, se n é par, então n^2 é par.*

Como esse enunciado é uma generalização, o Método da Generalização nos diz que, para prová-lo, podemos fazer o seguinte:

1. Supor que n assume como valor um elemento qualquer de $\mathbb{N}$.
2. Provar que *se n é par, então n^2 é par*, usando somente propriedades de n que são genéricas em $\mathbb{N}$.

Ou seja, o método afirma que podemos provar a Proposição 9.1.1 provando apenas o enunciado *se n é par, então n^2 é par*, (mas, como está especificado em 2, isto deve ser feito de uma maneira adequada). Aplicando, então, o Método da Generalização à Proposição 9.1.1, somos levados ao problema de apresentar uma prova do seguinte enunciado:

Proposição 9.1.2 *Se n é par, então n^2 é par.*

Mas, como esse enunciado é uma implicação, o Método da Suposição nos diz que, para prová-lo, podemos fazer o seguinte:

1. Supor que n é par.

2. Provar que n^2 *é par*, usando como premissa que n *é par*.

Aplicando, então, o Método da Suposição ao enunciado acima, somos levados ao problema de apresentar uma prova do enunciado n^2 *é par*.

Mas como podemos provar que um número natural é par? Como já dissemos no Capítulo 7, uma das características de uma definição é que ela estabelece o significado de um conceito dando condições para sua verificação. Assim, para responder a esta pergunta, vamos examinar a definição de número par, em forma normal, dada no Capítulo 4:

Definição Seja $n \in \mathbb{N}$. Dizemos que n é *par* se existe um número natural k, tal que $n = 2k$.

A definição nos diz que, para provar que um número natural n é par, devemos mostrar que *existe um natural* k *tal que* $n = 2k$. Observe agora que o enunciado *existe um natural* k *tal que* $n = 2k$ inicia com uma ocorrência de *existe*. Assim, para provar que n^2 *é par*, devemos saber como provar um enunciado que começa com uma ocorrência do *existe*.

9.2 Provando existencializações

Consideramos que, para provar a existência de um objeto com determinadas propriedades, devemos exibir um objeto que possua estas propriedades e provar que, de fato, ele possui estas propriedades. Assim, para provar existencializações podemos usar o seguinte método:

MÉTODO DA EXISTENCIALIZAÇÃO, ME.

Para provar uma existencialização *existe* $x \in A$ *tal que* $\varphi(x)$ é suficiente fazer o seguinte:

1. Exibir um elemento específico a do domínio de existencialização A.
2. Provar que o enunciado existencializado $\varphi(x)$ é verdadeiro, quando a variável de existencialização x assume o elemento a como valor, ou seja, provar que $\varphi(a)$ é um enunciado verdadeiro.

Isto quer dizer que, para que consideremos que uma existencialização *existe* $x \in A$ *tal que* $\varphi(x)$ tenha sido provada, basta que apresentemos uma prova de $\varphi(a)$, para algum elemento $a \in A$. (Figura 9.1).

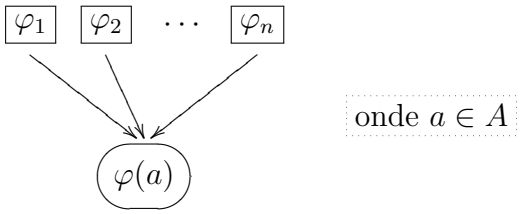


Figura 9.1: Estrutura das provas de generalizações *existe* $x \in A$ *tal que* $\varphi(x)$.

Exemplo 9.2.1 (a) Supondo que n é par, se queremos provar a existencialização *existe um natural* k *tal que* $n^2 = 2k$, basta fazer o seguinte:

1. Exibir um elemento apropriado $a \in \mathbb{N}$.
2. Provar que o enunciado $n^2 = 2a$ é verdadeiro.

Como n é par, sabemos que existe $m \in \mathbb{N}$ tal que $n = 2m$.

Logo, $n^2 = (2m)^2 = 2 \cdot 2m^2$.

Tomando $a = 2m^2$, temos que $n^2 = 2a$.

Assim, podemos concluir que n^2 é par, quando n é par. ∎

(b) Se queremos provar a existencialização *existe um menor número natural*, basta fazer o seguinte:

1. Exibir um elemento apropriado $a \in \mathbb{N}$.
2. Provar que o enunciado *a é menor ou igual a qualquer número natural* é verdadeiro.

Tomemos $1 \in \mathbb{N}$.

Sabemos que $1 \leq n$, para qualquer $n \in \mathbb{N}$.

Assim, podemos concluir que existe um menor número natural. ∎

(*c*) Se queremos provar a existencialização *existem n naturais consecutivos que não são primos*, basta fazer o seguinte:

1. Exibir n elementos apropriados $a_1, a_2, \ldots, a_n \in \mathbb{N}$.
2. Provar que o enunciado $a_1, a_2, \ldots, a_n$ *são naturais consecutivos que não são primos* é verdadeiro.

Tomando $a_1 = (n+1)! + 2, a_2 = (n+1)! + 3, \ldots, a_n = (n+1)! + (n+1)$, temos naturais consecutivos.

Para mostrar que cada $(n+1)! + i$ não é primo, quando $2 \leq i \leq n+1$, basta observar que i divide $(n+1)!$ e divide i e, portanto, divide $(n+1)! + i$. ∎

Capítulo 10

Prova de negações

Neste capítulo, tratamos do problema de provar negações. Em particular, apresentamos o Método de Redução ao Absurdo, para a prova de negações.

Consideramos que uma negação é verdadeira quando o enunciado negado é falso. Essa idéia nos leva a considerar que, para provar negações podemos usar o seguinte método:

> Método de Redução ao Absurdo, MRA.
>
> Para provar uma negação *não* φ, é suficiente fazer o seguinte:
>
> 1. Supor que o enunciado negado φ é verdadeiro.
> 2. Provar algum enunciado ψ que contradiga um enunciado θ, já conhecido, usando φ como premissa.

Exemplo 10.0.2 Vejamos alguns exemplos de aplicação do método.

(a) Um exemplo clássico do uso do Método de Redução ao Absurdo na prova de uma proposição matemática é a prova, apresentada pela escola pitagórica em II A. C., de que $\sqrt{2}$ não é um número racional.

A prova se baseia nos seguintes fatos:

(i) Todo número racional positivo pode ser escrito como uma fração de dois números naturais a e b, com $b \neq 0$. Por exemplo, o número racional $0,5$ pode ser escrito como a fração $5/10$.

(*ii*) Toda fração a/b de dois números naturais pode ser simplificada até uma fração c/d, pela eliminação de todos os fatores comuns aos números a e b. Por exemplo, $5/10$ pode ser simplificada até a fração $1/2$, onde 1 e 2 não possuem fatores comuns.

(*iii*) Todo número natural é par ou ímpar, de maneira exclusiva. Os números pares podem ser escritos na forma $2m$, onde m é um número natural. Os números ímpares podem ser escritos na forma $2n + 1$, onde n é um número natural.

(*iv*) O quadrado de um número ímpar é ímpar. De fato, se $a = 2n + 1$ é um número ímpar, então $a^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$ também é um número ímpar. Assim, se o quadrado de um número é par, então este número é par.

Podemos agora provar o seguinte resultado:

Proposição 10.0.1 *$\sqrt{2}$ não é um número racional.*

Prova:
Como o enunciado a ser provado é a negação do enunciado *$\sqrt{2}$ é um número racional*, segundo o Método de Redução ao Absurdo devemos fazer o seguinte:

1. Supor o enunciado negado, ou seja, supor que $\sqrt{2}$ é um número racional.
2. Provar um enunciado que contradiga um outro já conhecido, usando o enunciado negado como premissa.

Mas se $\sqrt{2}$ não é um número racional, existem números racionais a e b, com $b \neq 0$, tais que $\sqrt{2} = a/b$.

Simplificando a fração a/b, temos que $\sqrt{2} = c/d$, onde c e d não possuem fatores comuns (*).

Elevando ambos os membros da igualdade ao quadrado, temos que $2 = c^2/d^2$, ou seja, $c^2 = 2d^2$ (1) e daí, concluímos que c^2 é par. Como c^2 é par, temos que c também é par. Logo, $c = 2m$ (2).

Substituindo (2) em (1), temos: $(2m)^2 = 2d^2$ e, daí, $4m^2 = 2d^2$, ou seja, $2m^2 = d^2$ e concluímos que d^2 é par.

Como d^2 é par, podemos garantir que d é par e , daí, $d = 2n$, onde n é um número natural.

Assim, $c = 2m$ e $d = 2n$, acarretando que c e d possuem 2 como um fator comum, contradizendo (*). ∎

(b) Outro exemplo do uso do Método de Redução ao Absurdo na prova de uma proposição matemática é a prova de que existem infinitos números primos.

A prova se baseia nos seguintes fatos:

(i) Todo número natural maior que 1 pode ser escrito com um produto de números primos. Por exemplo, o número natural 18 pode ser escrito como o produto de primos $2 \cdot 3 \cdot 3$.

(ii) Se um número natural a divide os números naturais b e c, então a divide $b - c$.

(iii) O número 1 não possui divisores primos.

Podemos agora provar o seguinte resultado:

Proposição 10.0.2 *O conjunto dos números primos é infinito.*

Prova:
Como o enunciado a ser provado é a negação do enunciado *o conjunto dos números primos é finito*, segundo o Método de Redução ao Absurdo devemos fazer o seguinte:

1. Supor o enunciado negado, ou seja, supor que o conjunto dos números primos é infinito.
2. Provar um enunciado que contradiga um outro já conhecido, usando o enunciado negado como premissa.

Mas, se o conjunto dos números primos é finito, podemos considerar que $n \in \mathbb{N}$ é a quantidade de números primos e denotá-los por $p_1, p_2, \ldots, p_n$.

Consideremos o número $p = p_1 p_2 \cdots p_n + 1$. Como todo natural pode ser escrito como um produto de primos, temos que p possui um fator primo, digamos p_i. Temos, então, que p_i divide p e que p_i também divide $p_1 p_2 \cdots p_n$. Logo, p_i divide $p - p_1 p_2 \cdots p_n$. Mas $p - p_1 p_2 \cdots p_n = 1$. Logo,

p_i divide 1, uma contradição com o fato de que 1 não possui divisores primos. ∎

De uma maneira geral, o Método de Redução ao Absurdo afirma que, para provar uma negação *não* φ, ao invés de apresentar uma prova direta de *não* φ, com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m$ (Figura 10.1), podemos apresentar

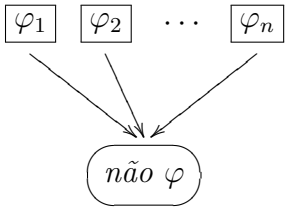


Figura 10.1: O problema da prova de negações.

uma prova de um enunciado que contradiz um outro enunciado já conhecido, com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \varphi$ (Figura 10.2). Ou seja, afirma que, para

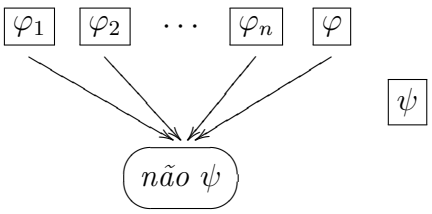


Figura 10.2: Estrutura das provas de negações, versão 1.

provar uma negação *não* φ, basta que apresentemos uma prova de dois enunciados que se contradizem, na qual φ ocorre como um enunciado que não foi justificado (Figura 10.3).

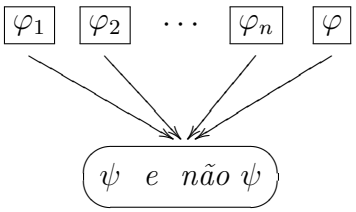


Figura 10.3: Estrutura das provas de negações, versão 2.

Capítulo 11

Método da Contraposição

Neste capítulo, apresentamos o *Método da Contraposição*, uma alternativa para a prova de implicações.

De acordo com o que foi dito sobre a estrutura das provas obtidas pela aplicação do Método da Suposição, no Capítulo 6, uma solução para o problema da prova de implicações seria uma argumentação da forma mostrada na Figura 11.1, onde ψ é a conclusão, e $\varphi_1, \varphi_2, \ldots, \varphi_n$ e φ são premissas utilizadas na prova de ψ.

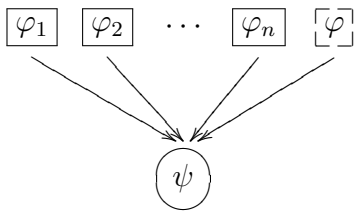


Figura 11.1: Estrutura das provas de implicações *se* φ*, então* ψ, usando MS.

Vamos tentar aplicar esta estratégia para provar o enunciado seguinte.

Exemplo 11.0.3 Seja x um número natural qualquer. Queremos provar a proposição:

Proposição 11.0.3 *Se* x^2 *é par, então* x *é par.*

Considerando que a Proposição 11.0.3 é uma implicação com antecedente x^2 *é par* e consequente x *é par*, segundo o Método da Suposição, para prová-la basta fazer o seguinte (Figura 11.2):

1. Supor que x^2 é par.

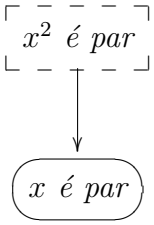


Figura 11.2: Estrutura da prova de *se x^2 é par, então x é par*, pelo Método da Suposição.

2. Provar que x é par, usando como hipótese que x^2 é par.

Vejamos como isto poderia ser feito:

Tentativa de prova: Suponhamos que x^2 é par. Daí, temos que $x^2 = 2n + 1$, com $n \in \mathbb{N}$.

Como poderemos usar esta informação mostrar que x é par?

Como já discutimos no Capítulo 6, quando sabemos que uma implicação *se φ, então ψ* é verdadeira, sabemos apenas que a verdade do seu antecedente φ acarreta a verdade do seu consequente ψ. Não podemos concluir que φ é verdadeiro nem que ψ é verdadeiro, mas apenas que não podemos considerar φ verdadeiro e ψ falso.

Essa análise da relação entre o antecendente e o consequente de uma implicação verdadeira nos levou a considerar o Método da Suposição, para a prova de implicações verdadeiras. Se lembramos que uma negação é verdadeira quando a sentença negada é falsa e que uma negação é falsa quando a sentença negada é verdadeira, podemos dar um outro enfoque para a análise da relação entre o antecendente e o consequente de uma implicação verdadeira.

> Quando sabemos que uma implicação é verdadeira, não podemos concluir que seu antecedente é verdadeiro nem que seu consequente é verdadeiro, mas que não podemos considerar a negação de seu consequente verdadeira e a negação de seu antecedente falsa.

Este outro enfoque nos leva a considerar o seguinte método alternativo para provar implicações:

Método da Contraposição, MC.

Para provar uma implicação *se φ, então ψ*, é suficiente fazer o seguinte:

1. Supor que a negação do consequente, *não ψ*, é verdadeira.
2. Provar que negação do antecedente, *não φ*, é verdadeira, usando *não ψ* como premissa.

Em termos de justificativas por meio de argumentações, o Método da Contraposição afirma que, para justificar que uma implicação é verdadeira, basta supor que a negação do consequente está justificada e apresentar uma justificativa da negação do antecedente, que depende da negação do consequente.

Como um exemplo de aplicação do Método da Contraposição, vejamos como podemos obter facilmente uma prova da Proposição 11.0.3, usando MC.

Exemplo 11.0.4 Seja x um número natural qualquer. Queremos provar o enunciado:

Se x^2 é par, então x é par.

Considerando que este enunciado é uma implicação com antecedente *x^2 é par* e consequente *x é par*, segundo o Método de Contraposição, para prová-lo basta fazer o seguinte (Figura 11.3):

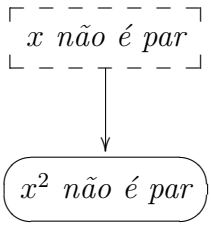


Figura 11.3: Estrutura da prova de *se x^2 é par, então x é par.*

1. Supor que x não é par, isto é, que x é ímpar.
2. Provar que x^2 não é par, isto é, que x^2 é ímpar, usando como hipótese que x é ímpar.

Vejamos como isto pode ser feito:

Prova:
Suponhamos que x não é par. Daí, temos que x é ímpar, ou seja, $x = 2n+1$, com $n \in \mathbb{N}$. Logo, $x^2 = (2n+1)^2 = 4n^2 + 2n + 1 = 2(2n^2 + n) + 1$, com $2n^2 + n \in \mathbb{N}$. Assim, x^2 é ímpar, ou seja, x^2 não é par. ∎

Em resumo, o Método da Contraposição afirma que, para provar uma implicação *se* φ, *então* ψ, ao invés de apresentar uma prova de ψ, com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \varphi$, como na Figura 11.1, podemos apresentar uma prova de *não* φ com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m$, *não* ψ, como na Figura 11.4. Ou seja, o MC estabelece o seguinte critério alternativo sobre a prova de implicações:

Para provar uma implicação verdadeira *se* φ, *então* ψ, ao invés de apresentar uma argumentação que justifique *se* φ, *então* ψ, basta apresentar uma argumentação que justifica *não* φ, na qual *não* ψ ocorre como um enunciado que não foi justificado.

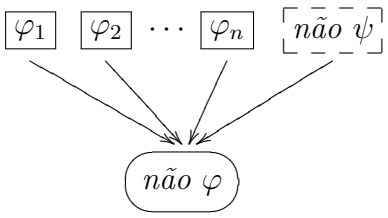


Figura 11.4: Estrutura das provas de implicações *se* φ, *então* ψ, usando MC.

Capítulo 12

Método da Prova por Casos

Neste capítulo, apresentamos o *Método da Prova por Casos*, MPC. Diferentemente dos métodos discutidos até agora, o MPC não se distingue por ser indicado para a justificativa de enunciados de determinados tipos. O MPC é um método adequado para o problema da prova de enunciados (quaisquer) quando uma das *premissas* consideradas é uma ψ_1 *ou* ψ_2 (Figura 12.1).

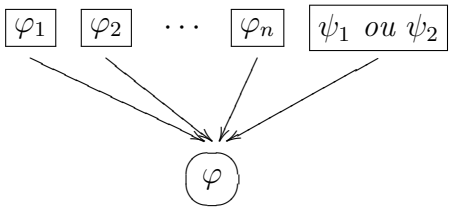


Figura 12.1: Problema da prova de enunciados a partir de premissas ψ_1 *ou* ψ_2.

Quando sabemos que uma disjunção ψ_1 *ou* ψ_2 é verdadeira, sabemos apenas que a verdade de uma das duas componentes (talvez das duas) está garantida. Não podemos concluir que o enunciado ψ_1 é verdadeiro nem que o enunciado ψ_2 é verdadeiro. Sabemos que um dos dois é verdadeiro, mas não sabemos qual.

Essa análise nos leva a considerar o seguinte método para provar enunciados a partir de premissas que são disjunções:

MÉTODO DA PROVA POR CASOS, MPC.

Para provar um enunciado φ a partir de uma premissa ψ_1 *ou* ψ_2, é suficiente fazer o seguinte:

1. Provar que φ é verdadeiro, usando ψ_1 como premissa (e não usando ψ_2).
2. De maneira independente, provar que φ é verdadeiro, usando ψ_2 como premissa (e não usando ψ_1).

Em termos de justificativas por meio de argumentações, o Método da Prova por Casos afirma que, para justificar que um enunciado é verdadeiro, usando uma disjunção como premissa, basta supor que a primeira componente da disjunção está justificada e apresentar uma justificativa do enunciado, que depende da primeira componente, e fazer o mesmo considerando a segunda componente, de maneira independente.

Vejamos um exemplo de aplicação do Método da Prova por Casos.

Exemplo 12.0.5 Seja x um número natural qualquer. Queremos provar o enunciado *x e x^2 possuem a mesma paridade.*

Na prova deste enunciado, vamos considerar que, quando x é um número natural qualquer, temos que *x é par ou x é ímpar.* Considerando esta premissa, segundo o Método da Prova por Casos, para provar que *x e x^2 possuem a mesma paridade*, basta fazer o seguinte (Figura 12.2):

1. Supor que x é par.
2. Provar que x e x^2 possuem a mesma paridade, o que, neste caso, significa provar que x^2 também é par, usando como hipótese que x é par.
3. Supor que x é ímpar.
4. Provar que x e x^2 possuem a mesma paridade, o que, neste caso, significa provar que x^2 também é ímpar, usando como hipótese que x é ímpar.

Vejamos como isto pode ser feito:

Prova:
Caso 1 Suponhamos que x é par. Daí, temos que $x = 2n$, com $n \in \mathbb{N}$. Logo,

$x^2 = (2n)^2 = 4n^2 = 2(2n^2)$, com $2n^2 \in \mathbb{N}$. Assim, x^2 também é par, ou seja, x e x^2 possuem a mesma paridade.
Caso 2 Suponhamos que x é ímpar. Daí, temos que $x = 2n+1$, com $n \in \mathbb{N}$. Logo, $x^2 = (2n+1)^2 = 4n^2 + 2n + 1 = 2(2n^2 + n) + 1$, com $2n^2 + n \in \mathbb{N}$. Assim, x^2 também é ímpar, ou seja, x e x^2 possuem a mesma paridade. ∎

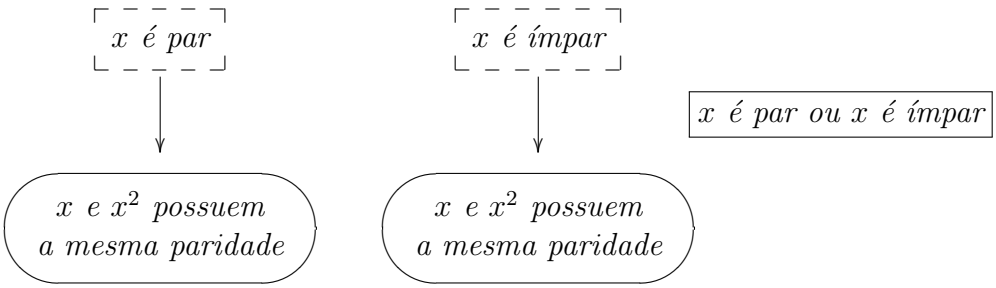


Figura 12.2: Estrutura da prova de *x e x^2 possuem a mesma paridade.*

Em resumo, o Método da Prova por Casos afirma que, para provar um enunciado φ a partir de premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \psi_1$ *ou* ψ_2, podemos apresentar uma prova de φ com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \psi_1$ e uma prova de φ com premissas $\varphi_1, \varphi_2, \ldots, \varphi_m, \psi_2$, como na Figura 12.3. Ou seja, o MPC estabelece o seguinte critério sobre a prova de enunciados a partir de disjunções:

Para provar um enunciado verdadeiro φ usando uma disjunção ψ_1 *ou* ψ_2 como premissa, basta apresentar uma argumentação que justifica φ, na qual ψ_1 ocorre como um enunciado que não foi justificado, e, de maneira independente, apresentar uma argumentação que justifica φ, na qual ψ_2 ocorre como um enunciado que não foi justificado.

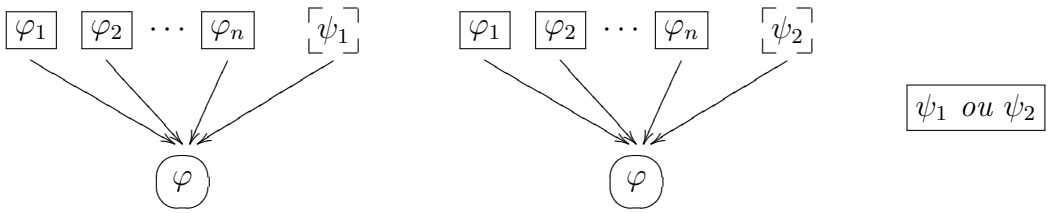


Figura 12.3: Estrutura das provas de φ a partir de ψ_1 *ou* ψ_2, usando MPC.

Capítulo 13

Princípio das casas de pombo

Neste capítulo[1], apresentamos e exemplificamos o Princípio das Casas de Pombo, PCP, tanto como um *resultado matemático*, quanto como um *método de prova*.

Como um resultado matemático, o PCP é bastante simples e intuitivo e parece, à primeira vista, ser de pouca aplicabilidade. Mas, como veremos através de alguns exemplos, quando usado como um método de prova, o PCP se torna uma ferramenta extremamente poderosa na resolução de problemas cujo objetivo é justificar a existência de configurações de objetos satisfazendo a certas propriedades.

Como vimos no Capítulo 9, para provar uma existencialização *existe* $x \in A$ *tal que* $\varphi(x)$, basta exibir um elemento específico a do domínio de existencialização A e provar que o enunciado existencializado $\varphi(x)$ é verdadeiro, quando a variável de existencialização x assume o elemento a como valor, Usando o PCP, podemos provar existencializações *existe* $x \in A$ *tal que* $\varphi(x)$, sem precisar exibir um objeto $a \in A$. Usando o PCP podemos garantir a existência de um elemento $a \in A$ para o qual o enunciado $\varphi(a)$ é verdadeiro de maneira indireta, sem exibir este elemento.

Este capítulo está estruturado como segue. Na Seção 13.1 e na Seção 13.2, motivamos e enunciamos o PCP. Na Seção 13.3 e na Seção 13.4, apresentamos alguns exemplos de aplicação do PCP na resolução de problemas. Na Seção 13.5, apresentamos alguns exemplos clássicos de aplicação do PCP na prova de teoremas.

[1]Este capítulo foi escrito em co-autoria com a Profa. Márcia Cerioli.

13.1 A ideia do PCP

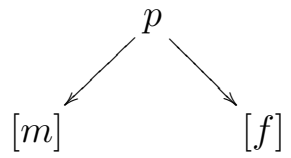
Considere o seguinte enunciado:

Em um conjunto de 3 pombos, existem pelo menos 2 do mesmo sexo.

Este enunciado é, obviamente, verdadeiro e nem carece de justificativa. Mas, uma justificativa detalhada para ele pode ser a seguinte:

Prova:
Em primeiro lugar, observe que queremos provar a existência de um certo subconjunto dos pombos dados (2 pombos), cujos elementos satisfazem a uma certa propriedade (são do mesmo sexo).

Para isto, consideramos os 3 pombos dados e duas casas de pombo, uma rotulada m (macho) e a outra rotulada f (fêmea). Vamos agora colocar os pombos nas casas de pombo, de acordo com o sexo. Isto é, cada pombo vai para uma das casas, de acordo com o seguinte critério: se o pombo é macho, ele vai para a casa m; se o pombo é fêmea (uma pomba, na verdade), ela vai para a casa f.



Como temos 3 pombos e 2 casas de pombo para colocá-los, uma das casas deverá conter mais do que $\frac{3}{2} = 1,5$ pombos. Mais especificamente, uma das casas deverá conter 2 pombos. Ou seja, ou temos 2 pombos machos ou temos 2 pombos fêmeas. ∎

A resolução deste problema simples ilustra a ideia principal associada ao PCP: o PCP dá origem a um método que pode ser usado na prova de que uma certa configuração (objetos que possuem uma certa propriedade) existe. Para isto, alguns objetos são considerados como pombos, outros como casas de pombo, e os pombos são colocados nas casas de pombo. O PCP, simplesmente, garante que existe uma casa de pombos que contém mais do que um certo número de pombos. Esta casa de pombos, obtida pelo PCP, usualmente nos leva à configuração procurada.

Para formalizar esta ideia, usamos as noções de *função* e de *imagem inversa de um elemento por uma função*.

13.2 Enunciado do PCP

Sejam P e C conjuntos finitos e não vazios. Uma *função* de P em C relaciona elementos de P a elementos de C, de maneira que:

- cada elemento de P está associado a algum elemento de C;
- nenhum elemento de P está associado a mais do que um elemento de C.

Assim, f é uma função de P em C, quando cada elemento de P está associado a um e exatamente um elemento de C por f. Funções são, usualmente, dadas por *conjuntos de pares ordenados* ou *leis algébricas*.

Dados os conjuntos P e C, escrevemos $f : P \to C$ para dizer que f é uma função de P em C. Além disso, dados $f : P \to C$, $p \in P$ e $c \in C$, escrevemos $f(p) = c$ para dizer que c é o único elemento de C associado a p por f.

Sejam P e C conjuntos, $f : P \to C$ e $c \in C$. A *imagem inversa* de c por f é o conjunto de todos os elementos de P que f associa a c, ou seja, é o conjunto

$$\{p \in P : f(p) = c\}.$$

Dados $f : P \to C$ e $c \in C$, escrevemos $f^{-1}(c)$ para denotar a imagem inversa de c por f. Observe que $f^{-1}(c)$ é um subconjunto de P.

A ideia central na formulação do PCP é a de que, se estabelecemos uma função de um conjunto P em um conjunto C, mesmo que tenhamos feito uma distribuição equitativa dos elementos de P entre os elementos de C, há um elemento de C que é o correspondente de, no mínimo, uma quantidade igual a divisão de $|P|$ (o número de elementos de P) por $|C|$ (o número de elementos de C).

Mais formalmente temos:

Princípio das Casas de Pombo:
Seja P um conjunto finito e não vazio (de pombos) e C um conjunto finito e não vazio (de casas de pombo).
Se $f : P \to C$ é uma função (que coloca os pombos nas casas de pombo), então existe c em C (uma casa de pombo), tal que

$$|f^{-1}(c)| \geq \frac{|P|}{|C|}$$

(a casa c possui ao menos $\frac{|P|}{|C|}$ pombos).

Antes de mais nada, observe que:

– O PCP garante que existe uma casa de pombo c que possui ao menos $\frac{|P|}{|C|}$ pombos, mas não mostra qual é a casa e nem quais são os pombos que estão nela.

– Usualmente, o PCP é enunciado com a restrição de que $|P| > |C|$, ou seja, de que existem mais pombos do que casas de pombo.

Embora estes sejam os casos que interessam na maioria das vezes, esta restrição não é necessária. De fato, se temos menos pombos do que casas, ou seja, se $|P| < |C|$, o PCP afirma que existe uma casa que possui pelo menos $1 > \frac{|P|}{|C|} > 0$ pombo e, portanto, está correto. Além disso, se temos tantos pombos quanto casas, ou seja, se $|P| = |C|$, o PCP também está correto, pois afirma que existe uma casa que possui pelo menos $1 = \frac{|P|}{|C|}$ pombo.

13.3 Primeiras aplicações do PCP

Nos exemplos mais diretos de aplicação, o PCP dá origem a um método de prova, da seguinte maneira:

1. Queremos provar a existência de uma certa configuração cuja existência não é fácil provar, à primeira vista.

2. Analisamos o problema de modo a determinar um certo conjunto de objetos P (pombos) e um outro conjunto de C (casas de pombo).

3. Determinamos o número $|P|$ de pombos e o número $|C|$ de casas de pombo.

4. Aplicamos o PCP e concluímos que existe uma casa de pombos c que possui ao menos $\frac{|P|}{|C|}$ pombos.

5. A partir da casa de pombos c, determinamos a configuração procurada.

Como um exemplo imediato da aplicação desta estratégia, vamos justificar os seguintes enunciados.

Exemplo 13.3.1 *Em um grupo de* 40 *pessoas, existem ao menos* 4 *que fazem aniversário no mesmo mês.*

Prova:
Observe que queremos provar a existência de um certo subconjunto das pessoas (4 pessoas) cujos elementos possuem uma certa propriedade (fazem aniversário no mesmo mês).

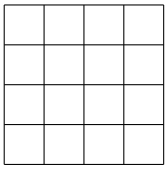
Vamos considerar P como sendo o conjunto das pessoas e C como sendo o conjunto dos meses do ano. Sabemos que $|P| = 40$ e $|C| = 12$. Consideremos também a função $f : P \to C$ tal que $f(p)$ é o mês de aniversário da pessoa p.

Assim, pelo PCP, existe uma casa c que possui ao menos $4 > 3,333\ldots = \frac{40}{12} = \frac{|P|}{|C|}$ pombos. Ou seja, temos ao menos 4 pessoas que fazem aniversário no mesmo mês. ∎

Exemplo 13.3.2 *Se escolhemos* 17 *pontos aleatoriamente dentro de um quadrado de área* 16*, então existem ao menos* 2 *pontos cuja distância de um para o outro é menor ou igual a* $\sqrt{2}$*.*

Prova:
Observe que queremos provar a existência de um certo subconjunto dos pontos (2 pontos) cujos elementos estão em uma certa relação (distam um do outro de no máximo $\sqrt{2}$).

Vamos considerar P como sendo o conjunto dos pontos e C como sendo o conjunto dos quadrados unitários desenhados dentro de um quadrado de área 16.



Sabemos que $|P| = 17$ e $|C| = 16$. Consideremos também a função $f : P \to C$ tal que $f(p)$ é o quadrado unitário ao qual o ponto p pertence.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 > 1,0625 = \frac{17}{16} = \frac{|P|}{|C|}$ pombos.

Como a diagonal do quadrado unitário mede $\sqrt{2}$, os pombos em c estão a uma distância menor ou igual a $\sqrt{2}$, um do outro. ∎

13.4 Segundas aplicações do PCP

Os exemplos da Seção 13.3 sugerem que a parte mais difícil na aplicação do PCP é determinar, de acordo com os dados do problema, qual é o conjunto de pombos e qual é o conjunto de casas de pombo. Nesta seção vamos considerar alguns exemplos mais complexos nos quais determinar P e C não é uma tarefa tão direta e exige alguma esperteza por parte de quem está aplicando o PCP.

Exemplo 13.4.1 *Considere um conjunto X contendo 10 números naturais não nulos menores que 100. Ou seja, $X \subseteq \{1, 2, 3, \ldots, 99\}$ e $|X| = 10$. Temos que existem dois subconjuntos Y e Z de X tais que $Y \neq \emptyset$, $Z \neq \emptyset$, $Y \cap Z = \emptyset$ e $\sum_{y \in Y} y = \sum_{z \in Z} z$.*

Prova:
Considere P como sendo o conjunto dos subconjuntos não vazios de X, e C como sendo o conjunto dos resultados possíveis dos somatórios dos subconjuntos não vazios de X, isto é, $C = \{\sum_{a \in A} a : A \subseteq X \text{ e } A \neq \emptyset\}$. Sabemos que $|P| = 2^{10} - 1$, pois $|X| = 10$ mas o conjunto vazio não pertence a P. Não temos informação suficiente para calcular $|C|$ com precisão. Mas uma cota superior para o valor de $|C|$ será suficiente para os nossos propósitos. Para calcular esta cota, observe que, como todos os 10 elementos de X são menores ou iguais a 99, temos que $\sum_{x \in X} x < 990$. Logo, se $A \subseteq X$, então $\sum_{a \in A} a < 990$. Ou seja, os resultados possíveis dos somatórios dos subconjuntos não vazios de X são valores entre 1 e 990, isto é, $|C| < 990$.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 \geq \dfrac{1023}{990} = \dfrac{|P|}{|C|}$ pombos. Isto é, existem dois subconjuntos não vazios A e B de X tais que $\sum_{a \in A} a = \sum_{b \in B} b$.

Não podemos garantir que $A \cap B = \emptyset$ mas, a partir destes conjuntos, é fácil obter dois subconjuntos não vazios Y e Z de A com todas as propriedades desejadas. Basta considerar $Y = A - (A \cap B)$ e $Z = B - (A \cap B)$. Temos então que $Y \cap Z = \emptyset$ e $\sum_{y \in Y} y = \sum_{z \in Z} z$. ∎

Exemplo 13.4.2 *Seja A um conjunto finito e não vazio de números naturais, com m elementos. Temos que existe um subconjunto B de A tal que m divide a soma dos elementos de B.*

Prova:
Seja $A = \{a_1, a_2, \ldots, a_m\}$. Observe que queremos provar a existência de um certo subconjunto $B = \{b_1, b_2, \ldots, b_n\}$ de A, $n \leq m$, cuja soma dos elementos $b_1 + b_2 + \ldots + b_n$ é um múltiplo de m. Para isto, vamos considerar as somas

$$a_1$$

$$a_1 + a_2$$

$$a_1 + a_2 + a_3$$

$$a_1 + a_2 + a_3 + a_4$$

$$\vdots$$

$$a_1 + a_2 + a_3 + a_4 + \cdots + a_m$$

Temos dois casos.

Se m divide uma das somas $a_1 + a_2 + a_3 + \cdots + a_i$, $1 \leq i \leq m$, basta considerar o conjunto $B = \{a_1, a_2, a_3, \ldots, a_i\}$.

Se nenhuma das somas $a_1 + a_2 + a_3 + \cdots + a_i$, $1 \leq i \leq m$ é um múltiplo de m, consideramos P como sendo o conjunto das somas e C como sendo o conjunto $\{1, 2, 3, \ldots, m-1\}$ dos possíveis restos quando dividimos as somas por m. Sabemos que $|P| = m$ e $|C| = m - 1$.

Assim, pelo PCP, existe uma casa c que possui ao menos $2 > \dfrac{m}{m-1} = \dfrac{|P|}{|C|}$ pombos.

Sejam $a_1 + a_2 + a_3 + \cdots + a_i$ e $a_1 + a_2 + a_3 + \cdots + a_j$, com $i < j$, estas somas. Temos que $a_1 + a_2 + a_3 + \cdots + a_i$ e $a_1 + a_2 + a_3 + \cdots + a_j$ deixam o mesmo resto na divisão por m.

Ora, se dois números a e b, com $a > b$ deixam o mesmo resto na divisão por m, então m divide a diferença $a - b$.

De fato, se $a = q_1m + r$ e $b = q_2m + r$, com $q_1 > q_2$, então $a - b = (q_1m + r) - (q_2m + r) = q_1m - q_2m = (q_1 - q_2)m$, que é um múltiplo de m.

Assim, temos que m divide $a_{i+1} + a_{i+2} + \cdots + a_j = (a_1 + a_2 + a_3 + \cdots + a_j) - (a_1 + a_2 + a_3 + \cdots + a_i)$.

Basta, então, considerar o conjunto $B = \{a_{i+1}, a_{i+2}, \ldots, a_j\}$. ∎

Exemplo 13.4.3 *Seja $s = (a_1, a_2, \ldots, a_{2n+1})$ uma sequência de $2n + 1$ números inteiros, $n \in \mathbb{N}$, e $(a_{i1}, a_{i2}, \ldots, a_{i(2n+1)})$ uma permutação de s. Temos que o produto*

$$(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{i(2n+1)} - a_{2n+1})$$

é um número par.

Prova:
Observe que

o produto $(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{in} - a_{2n+1})$ é par
se, e somente se,
existe um fator $a_{ij} - a_j$, $1 \leq j \leq 2n + 1$, que é um número par
se, e somente se,
existe um número j, $1 \leq j \leq 2n + 1$, tal que os números a_{ij} e a_j
são ambos pares ou ambos ímpares.

Para isto, vamos considerar P como sendo o conjunto cujos elementos são os números $a_1, a_2, \ldots, a_{2n+1}$ e C como sendo o conjunto cujos elementos são as palavras 'par' e 'ímpar'.

Sabemos que $|P| = 2n + 1$ e $|C| = 2$.

Assim, pelo PCP, existe uma casa c que possui ao menos $n+1 > \dfrac{2n+1}{2} = \dfrac{|P|}{|C|}$ pombos.

Sejam $b_1, b_2, \ldots, b_{n+1}$ estes números. Temos que $b_1, b_2, \ldots, b_{n+1}$ são todos pares ou todos ímpares.

Sejam, também, $c_1, c_2, \ldots, c_{n+1}$ os elementos que correspondem aos elementos $b_1, b_2, \ldots, b_{n+1}$, segundo p.

Observe que $\{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\} \neq \emptyset$. De fato, se fosse $\{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\} = \emptyset$, então a interseção $\{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\}$ teria $(n+1)+(n+1) = 2n+2 > 2n+1$ elementos, uma contradição.

Agora, seja $d \in \{b_1, b_2, \ldots, b_{n+1}\} \cap \{c_1, c_2, \ldots, c_{n+1}\}$. Ou seja, $d = b_k = c_l$, onde $1 \leq k, l \leq n+1$.

Temos que, $c_l - b_l = b_k - b_l$ é par, pois b_k e b_l são ambos pares ou ambos ímpares.

Como $c_l - b_l$ é um fator de $(a_{i1} - a_1)(a_{i2} - a_2)(a_{i3} - a_3) \ldots (a_{i(2n+1)} - a_{2n+1})$, temos que este último produto é par. ∎

13.5 Algumas aplicações clássicas do PCP

Uma das razões pelas quais o PCP merece destaque é que ele é, usualmente, empregado como método de prova na justificativa de vários teoremas importantes. Vamos deixar para o leitor a tarefa de procurar na bibliografia especializada de combinatória, os vários exemplos de uso do PCP neste contexto. Para uma leitura inicial, sugerimos os livros [1] e [8] e os artigos [3] e [10].

Nesta seção, apresentamos três exemplos clássicos de aplicação do PCP na prova de teoremas. Apresentamos a prova do Teorema de Erdös-Szekeres sobre subsequências monotônicas, a prova do Lema de Dilworth sobre ordens parciais e a prova do Teorema de Ramsey sobre subgrafos monocromáticos, seguindo [3].

13.5.1 O PCP e a prova do Teorema de Erdös-Szekeres

Para enunciar o Teorema de Erdös-Szekeres, utilizamos os conceitos a seguir.

Seja $s = (x_1, \ldots, x_n)$ uma sequência de números reais.

1. s é *monotônica crescente* se $x_1 \leq \cdots \leq x_n$.
2. s é *monotônica decrescente* se $x_1 \geq \cdots \geq x_n$.
3. s é *monotônica* se é monotônica crescente ou monotônica decrescente.

4. $s' = (y_1, \ldots, y_m)$ é uma *subsequência* de s se $m \leq n$ e, para todos y_i, y_j em s' tais que $i < j$, temos que existem x_k, x_l em s tais que $y_i = x_k$, $y_j = x_l$ e $k < l$.

Teorema 13.5.1 (Erdös-Szekeres) *Se $s = (x_1, \cdots, x_n)$ é uma sequência de números reais, então s contém uma subsequência monotônica com $\sqrt{n}$ termos.*

Prova:
Seja $s = (x_1, \cdots, x_n)$ uma sequência de números reais.

Suponhamos, para uma contradição, que toda subsequência monotônica de s possui no máximo $\sqrt{n} - 1$ termos.

Podemos então definir uma função

$$f : \{1, \ldots, n\} \to \{1, \ldots, \sqrt{n} - 1\} \times \{1, \ldots, \sqrt{n} - 1\}$$

tal que $f(i) = (c_i, d_i)$, onde c_i é o tamanho da maior subsequência monotônica crescente iniciada em x_i e d_i é o tamanho da maior subsequência monotônica decrescente iniciada em x_i.

Para a aplicação do PCP, consideramos

$$P = \{1, \ldots, n\} \text{ e } C = \{1, \ldots, \sqrt{n} - 1\} \times \{1, \ldots, \sqrt{n} - 1\},$$

donde $|P| = n$ e $|C| = (\sqrt{n} - 1)^2$. Pelo PCP, temos que existe $(c, d) \in C$ tal que

$$|f^{-1}(c, d)| \geq \frac{|P|}{|C|} = \frac{n}{(\sqrt{n} - 1)^2} = \frac{n}{n - 2\sqrt{n} + 1} > 1.$$

Assim, existem dois termos x_j e x_k da sequência s tais que $c_j = c_k = c$ e $d_j = d_k = d$.

Temos duas possibilidades: $x_j < x_k$ ou $x_j > x_k$. Se $x_j < x_k$, então a maior subsequência monotônica crescente iniciada em x_j possui ao menos um termo a mais do que a maior subsequência monotônica crescente iniciada em x_j. Ou seja, $c_j > c_k$, o que é uma contradição. Se $x_j > x_k$, então a maior subsequência monotônica decrescente iniciada em x_j possui ao menos um termo a mais do que a maior subsequência monotônica decrescente iniciada em x_j. Ou seja, $d_j > d_k$, o que também é uma contradição.

Assim, s contém uma subsequência monotônica com $\sqrt{n}$ termos. ∎

13.5.2 O PCP e a prova do Lema de Dilworth

Para enunciar o Lema de Dilworth, utilizamos os conceitos de ordem, cadeia e anticadeia.

Dizemos que $\leq$ é uma *relação de ordem* em um conjunto A se $\leq$ é uma relação binária em A que é reflexiva, antissimétrica e transitiva. Se, ao contrário, todos os elementos de A são incomparáveis segundo $\leq$, isto é, dados $a, b \in A$, temos que $a \not\leq b$ e $b \not\leq a$, dizemos que $\leq$ é uma *anticadeia*.

Lema 13.5.1 (Dilworth) *Seja A um conjunto finito e $\leq$ uma relação de ordem em A. Se $|A| = n$, com $n \geq 2$, então existe um subconjunto $B \subseteq A$ tal que $|B| = \sqrt{n}$ e B é uma cadeia ou uma anticadeia.*

Prova:
Suponhamos que A não contém nenhuma cadeia de tamanho $\sqrt{n}$. Para a aplicação do PCP, consideramos $P = A$ e $C = \{1, 2, \ldots, \sqrt{n} - 1\}$. Temos que $|P| = n$ e $|C| = \sqrt{n} - 1$.

Podemos definir uma função $f : P \to C$ tal que $f(x) = m$ se m é o tamanho da maior cadeia em A que tem x como último elemento.

Pelo PCP, existe $c \in C$ tal que

$$|f^{-1}(c)| \geq \frac{n}{\sqrt{n} - 1}.$$

Como $n \geq 2$, temos que $|f^{-1}(c)| \geq \sqrt{n}$. De fato, se $|f^{-1}(c)| \leq \sqrt{n} - 1$, teríamos que

$$\sqrt{n} - 1 \geq |f^{-1}(c)| \geq \frac{n}{\sqrt{n} - 1},$$

donde $n - 2\sqrt{n} + 1 \geq n$, uma contradição. Logo, $|f^{-1}(c)| > \sqrt{n} - 1$, isto é, $|f^{-1}(c)| \geq \sqrt{n}$. Agora vamos mostrar que $B = f^{-1}(c)$ é uma anticadeia. Suponhamos, para uma contradição, que existem $x, y \in B$ tais que $x \leq y$. Daí teríamos $f(x) > f(y)$, ou seja, $f(x) \neq f(y)$, uma contradição, pois, se $x, y \in f^{-1}(c)$, então $f(x) = f(y) = c$. Assim, $f^{-1}(c)$ é uma anticadeia de tamanho mínimo $\sqrt{n}$. ∎

13.5.3 O PCP e a prova do Teorema de Ramsey

O Teorema de Ramsey trata de coloração de grafos.

Um *grafo* é um conjunto finito de vértices ligados por arestas, de modo que:

- não haja laços, isto é, um vértice nunca está ligado a si mesmo por uma aresta, e
- não haja arestas múltiplas, isto é, um mesmo par de vértices está ligado por no máximo uma aresta.

Dado um grafo G, denotamos por $V(G)$ o conjunto de vértices de G e por $A(G)$ o conjunto de arestas de G. As arestas de G são representadas por pares de vértices de G. Dizemos que um grafo G é *completo* se existe uma aresta entre cada par de vértices, isto é, para todos $u, v \in V(G)$, temos que $(u, v) \in A(G)$. Um grafo completo com n vértices é denominado K_n. Dizemos que um grafo H é *subgrafo* de um grafo G se $V(H) \subseteq V(G)$ e $A(H) \subseteq A(G)$.

Uma *bicoloração* de um grafo G é uma assinalação de cores às arestas de G com uma ou duas cores. Uma bicoloração pode ser vista como uma função

$$f : A(G) \to \{\mathsf{vermelho}, \mathsf{amarelo}\},$$

onde $A(G)$ é o conjunto das arestas de G. Um subgrafo H de G é *monocromático* segundo uma bicoloração f se f é constante em $A(H)$. Se H é monocromático, dizemos que H é *vermelho* ou *amarelo*.

Dados $a, b \in \mathbb{N}$ tais que $a, b \geq 2$, o *número de Ramsey* para a e b, denotado por $R(a, b)$, é o menor natural tal que, para qualquer bicoloração f de $K_{R(a,b)}$, temos um subgrafo K_a vermelho segundo f ou um subgrafo K_b amarelo segundo f.

Vejamos o caso em que $a = b = 3$. O número de Ramsey para estes valores é $R(3, 3) = 6$. Em geral, a prova de que $R(a, b) = n$ é feita em duas partes: (1) prova-se que $R(a, b) \geq n$, exibindo uma bicoloração de K_{n-1} segundo a qual nenhum subgrafo K_a é vermelho e nenhum subgrafo K_b é amarelo, e (2) prova-se que $R(a, b) \leq n$, usando-se argumentos de contagem, como o PCP, por exemplo.

Proposição 13.5.1 $R(3, 3) \geq 6$.

Prova:
A Figura 13.1 apresenta uma bicoloração de K_5 segundo a qual nenhum subgrafo K_3 é vermelho e nenhum subgrafo K_3 é amarelo, isto é, nenhum subgrafo K_3 é monocromático. ∎

Proposição 13.5.2 $R(3, 3) \geq 6$.

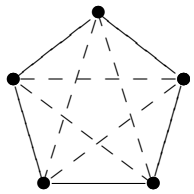


Figura 13.1: $R(3,3) \geq 6$

Prova:
Considere uma bicoloração para K_6. Seja v um vértice em K_6. Considere os conjuntos $P = V(K_6) \setminus \{v\}$ e $C = \{\mathsf{vermelho}, \mathsf{amarelo}\}$, e a função $f : P \to C$ tal que $f(u)$ é a cor da aresta que liga o vértice u ao vértice v. Temos que $|P| = 5$ e $|C| = 2$. Logo, pelo PCP, temos que existe uma cor $c \in C$ tal que

$$|f^{-1}(c)| \geq \frac{|P|}{|C|} = \frac{5}{2},$$

ou seja, existem pelo menos 3 vértices de K_6 ligados a v por vértices da mesma cor c, digamos vermelho. Agora temos dois casos a considerar.
Caso 1. Se estes 3 vértices estiverem ligados entre si por arestas amarelas, então temos um subgrafo K_3 amarelo.
Caso 2. Caso contrário, ou seja, se existir uma aresta vermelha entre dois destes vértices, então estes dois vértices, juntamente com v, formam um subgrafo K_3 vermelho.

Em qualquer caso, temos um subgrafo K_3 vermelho ou um subgrafo K_3 amarelo. Logo, $R(3,3) \leq 6$. ∎

O Teorema de Ramsey afirma que, no caso geral, sempre existe um natural n tal que $R(a,b) \leq n$. Em outras palavras, para todos $a, b \geq 2$, existe um valor mínimo $R(a,b)$.

Teorema 13.5.2 (Ramsey) *Se $a, b \in \mathbb{N}$ e $a, b \geq 2$, então $R(a,b)$ existe.*

Prova:
Por indução em a.

base. Vamos mostrar que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(2,b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(2,b)}$, temos um subgrafo vermelho K_2 ou um subgrafo amarelo K_b.

Seja $b \geq 2$. Vamos mostrar que $R(2, b) = b$. Considere uma bicoloração de K_b. Se K_b for amarelo segundo esta coloração, temos um subgrafo amarelo K_b. Se não, existem pelo menos uma aresta vermelha ligando dois vértices em K_b. Estes dois vértices constituem um subgrafo vermelho K_2.

HIPÓTESE. Seja $a \geq 2$ tal que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(a, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a,b)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_b.

PASSO. Vamos mostrar que, qualquer que seja $b \geq 2$, existe um valor mínimo $R(a + 1, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b. Apresentamos uma prova por indução em b.

Base. É fácil ver que $R(a, b) = R(b, a)$, para todos $a, b \in \mathbb{N}$. Além disso, como foi mostrado na BASE, temos que $R(2, a + 1) = a + 1$. Assim, $R(a + 1, 2) = R(2, a + 1) = a + 1$.

Hipótese. Seja $b \geq 2$ para o qual existe um valor mínimo $R(a + 1, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b.

Passo. Vamos mostrar que existe um valor mínimo $R(a + 1, b + 1) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a+1,b+1)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_{b+1}.

Pela HIPÓTESE, existe um valor mínimo $R(a, b+1)$ tal que, para qualquer bicoloração de $K_{R(a,b+1)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_{b+1}.

Pela Hipótese, existe um valor mínimo $R(a + 1, b)$ tal que, para qualquer bicoloração de $K_{R(a+1,b)}$, temos um subgrafo vermelho K_{a+1} ou um subgrafo amarelo K_b.

Vamos mostrar que $R(a + 1, b + 1) \leq R(a + 1, b) + R(a, b + 1)$.

Consideremos $n = R(a + 1, b) + R(a, b + 1)$ e uma bicoloração para o grafo completo K_n. Seja v um vértice em K_n, k o número de vértices ligados a v por arestas vermelhas e l o número de vértices ligados a v por arestas amarelas. Assim, $k+l = n-1 = R(a, b+1)+R(a+1, b)-1$.

Agora vamos analisar dois casos.

Caso 1. $k \geq R(a, b+1)$. Neste caso, pela HIPÓTESE, o (sub)grafo K_k de K_n constituído pelos k vértices ligados a v por arestas vermelhas possui um subgrafo K_a vermelho ou um subgrafo K_{b+1} amarelo. Se acrescentarmos v aos vértices que compõem o subgrafo K_a vermelho, teremos um subgrafo K_{a+1} vermelho.

Caso 2. $k < R(a, b+1)$. Neste caso, como

$$k + l = R(a, b+1) + R(a+1, b) - 1,$$

temos que $l > R(a+1, b)-1$, donde $l \geq R(a+1, b)$. Daí, pela Hipótese, o (sub)grafo K_l de K_n constituído pelos k vértices ligados a v por arestas amarelas possui um subgrafo K_{a+1} vermelho ou um subgrafo K_b amarelo. Se acrescentarmos v aos vértices que compõem o subgrafo K_b amarelo, teremos um subgrafo K_{b+1} amarelo.

Assim, para quaisquer $a, b \in \mathbb{N}$ tais que $a, b \geq 2$, existe um valor mínimo $R(a, b) \in \mathbb{N}$ tal que, para qualquer bicoloração de $K_{R(a,b)}$, temos um subgrafo vermelho K_a ou um subgrafo amarelo K_b. Além disso, quando $a, b \geq 3$, temos que $R(a, b) \leq R(a, b-1) + R(a-1, b)$. ∎

Referências Bibliográficas

[1] M. Aigner e G. M. Ziegler. *A Provas estão n'O Livro*. Segunda Edição. Edgard Blucher, São Paulo, 2002.

[2] N. Bourbaki. *Théorie des Ensembles*. Hermann, Paris, 1966.

[3] M. Erickson. An Introduction to Combinatorial Existence Theorems. *Mathematics Magazine*, 67(1994), 118–123.

[4] A. I. Fetissov. *A Demonstração em Geometria*. Atual, São Paulo, 1995.

[5] A. Fisher. *Formal Number Theory and Computability: a Workbook*. Clarendon, Oxford, 1982.

[6] L. Lamport. How to write a proof. *The American Mathematical Monthly* 120(1995), 600bib–608.

[7] U. Leron. Structuring mathematical proofs. *The American Mathematical Monthly* 90(1983), 174–185.

[8] L. Lovász, J. Pelikán e K. Vesztergombi. *Matemática Discreta*. Coleção Textos Universitários. SBM, Rio de Janeiro, 2003.

[9] J. Rubin. *Mathematical Logic: Applications and Theory*. Saunders College Publishing, Orlando, 1990.

[10] K. R. Rebman. The Pigeonhole Principle (What It Is, How It Works, and How It Applies to Map Coloring. *The Two-Year College Mathematics Journal*, 10(1979), 3–13.

[11] D. Solow. *How to Read and Do Proofs: an introduction to mathematical thought processes*. John Wiley & Sons, New York, 1990.

[12] R. L. Wilder. *Introduction to the Foundations of Mathematica*. John Wiley & Sons, New York, 1965.