Técnicas para Demonstrar Teoremas
Matemática Discreta I

Rodrigo Geraldo Ribeiro[1]

[1]Departamento de Ciências Exatas e Aplicadas – Universidade Federal de Ouro Preto

{rodrigogribeiro}@decea.ufop.br

1. Introdução

Matemáticos são pessoas céticas. Eles usam muitos métodos, incluindo experimentação com exemplos e tentativa e erro para tentar encontrar respostas para questões matemáticas, mas eles não são convencidos que esta resposta está correta a menos que eles consigam prová-la. Antes de iniciar o curso de *Matemática Discreta I*, você, com certeza, já deve ter se deparado com diversas provas matemáticas, porém, é possível que você não tenha experiência em escrever provas[1]. O objetivo deste texto é mostrar como construir suas próprias provas.

Pode-se fazer uma analogia do processo de construção de uma prova, com a montagem de um quebra-cabeças muito grande. Não existe uma regra para montar um quebra-cabeça grande. A única regra diz respeito ao resultado: Todas as peças devem se encaixar para formar a figura do quebra-cabeças corretamente. O mesmo vale para provas. Em uma demonstração, muitas vezes tentamos encaixar peças que não nos levam a lugar algum...

Apesar de não existirem regras de como quebra-cabeças devam ser resolvidos, algumas técnicas para resolvê-los paracem funcionar melhor que outras. Por exemplo, geralmente, você monta um quebra-cabeças preenchendo as bordas primeiro, e, gradativamente, preenche o interior deste. Algumas vezes, você pode tentar encaixar peças em lugares incorretos e depois de algum tempo percebe que não está fazendo nenhum progresso. A medida que as peças se encaixam, você percebe que a solução está mais próxima, e, aos poucos a figura final começa a surgir do emaranhado de peças aparentemente sem sentido.

Durante o processo de construção de uma prova, muitas vezes, *encaixamos peças* nos lugares errados. A medida que encaixamos uma peça no lugar correto, percebemos que a solução final, está próxima...

Matemáticos formalizam suas respostas a suas dúvidas por meio de um *teorema* que diz que se certas suposições chamadas *hipóteses* do teorema forem verdadeiras, então a *conclusão* também deve ser. Muitas vezes, as hipóteses e a conclusão contém variáveis livres[2], e neste caso, fica sub-entendido que estas variáveis podem ser quaisquer elementos do universo de discurso. Uma atribuição de valores particulares a estas variáveis é chamada de *instância* do teorema, e para que um teorema seja correto, este deve ser verdadeiro para todas as instâncias possíveis, sempre que as hipóteses deste toerema forem verdadeiras. Caso exista alguma instância que faça a conclusão ser falsa quando

[1]A partir deste ponto do texto, a palavra prova irá significar prova matemática, a menos que seja especificado o contrário.

[2]variáveis que não estão associadas a nenhum $\exists$ e $\forall$

as hipóteses forem verdadeiras, então diz-se que este teorema é *incorreto*. Esta instância que invalida um teorema é chamada de *contra-exemplo*.

2. Um primeiro exemplo...

Teorema. *Suponha* $x > 3$ *e* $y < 2$. *Então* $x^2 - 2y > 5$.

Este teorema é correto (A demostração deste teorema fica como exercício!). As hipóteses deste teorema são $x > 3$ e $y < 2$, e a conclusão é $x^2 - 2y > 5$. Como uma possível instância para este teorema, pode-se atribuir o valor 5 para x e 1 para y. Evidentemente, estes valores tornam verdadeiras as hipóteses $x > 3$ e $y < 2$, então o teorema nos diz que a conclusão também deve ser verdadeira. Atribuindo estes valores de x e y na conclusão temos que: $x^2 - 2y = 5^2 - 2 \cdot 1 = 25 - 2 = 23$ e, é evidente que $23 > 5$. Observe que este cálculo **não constitui** a prova deste teorema, pois uma prova deve mostrar que o teorema é válido para todas as suas instâncias.

Considere o mesmo teorema mostrado acima. Se removermos a segunda hipótese, o teorma fica *incorreto:*

Teorema Incorreto: *Suponha* $x > 3$. *Então* $x^2 - 2y > 5$.

Para mostrar que um teorema qualquer é incorreto, basta encontrar um *contra-exemplo*. Por exemplo, suponha $x = 4$ e $y = 6$. Então a única hipótese, $x > 3$, é verdadeira, mas $x^2 - 2y > 5 = 16 - 12 = 4$, então a conclusão $x^2 - 2y > 5$ é falsa.

Sempre que você encontrar um contra-exemplo para um teorema, então você pode afirmar com certeza que o teorema é incorreto, mas a única maneira de saber que o teorema é correto é provando-o. A prova de um teorema é simplesmente um argumento dedutivo em que as hipóteses são as premissas e a conclusão é a conclusão do teorema; ou seja, o primeiro passo para demonstrar um teorema é expressar suas hipóteses e sua conclusão utilizando sentenças lógicas.

Todas as técnicas de demonstração de teoremas apresentadas neste texto, são baseadas na forma lógica da conclusão e de suas hipóteses. Durante o processo de demonstração, deve-se aplicar, sobre as hipóteses, equivalências, regras de inferência para que a partir destas, chegue-se a conclusão; demonstrando assim a validade do teorema. Apesar das técnicas de demonstração, oferecerem um *caminho*, estas não funcionam como uma receita de bolo, nem sempre, uma técnica é a mais adquada para a demonstração de um teorema, e, somente com um pouco deexperiência em demonstrações você será capaz de dizer quando uma técnica é mais adequada que outra. Porém, existe a mais importante (na minha opinião...) regra para demonstração de teoremas, e, esta é mostrada abaixo:

2.1. Uma regra de ouro

Nunca utilize algo em uma demonstração que você não possa justificar completamente.

Isto quer dizer: *não invente*! Apenas utilize regras dedutivas ou equivalências já apresentadas em sala de aula, e, principalmente: *Uma prova deve ser construída passo a passo*, ou seja, *fazer direto* muitas vezes pode levar a erros durante o processo de dedução ou dificultar a escrita do texto correspondente a dedução lógica.

3. Técnicas de Demonstração

As técnicas de demonstração podem ser divididas em: provar uma conclusão que possui uma determinada forma ou utilizar uma hipótese com uma determinada forma. Durante o restante deste texto, serão apresentadas técnicas para provar conclusões e utilizar hipóteses que possuem uma determinada forma lógica.

A primeira técnica apresentada já foi mostrada em sala de aula, e, é conhecida em textos de matemática discreta como *prova direta*.

3.1. Para provar uma conclusão que possui a forma $P \to Q$:

Assuma que P é verdadeiro e então prove Q

Exemplo: *Suponha que a e b são números reais. Prove que se* $0 < a < b$ *então* $a^2 < b^2$

Antes de demonstrar este teorema, vamos dividir o processo de demonstrar um teorema em duas partes:

- Rascunho: Esta parte é utilizada para que você realize as deduções necessárias para a demonstração deste teorema. O resultado final da demonstração, não deve incluir o rascunho.
- O teorema: Este consiste em um texto em português usando alguns símbolos matemáticos que resumem o processo dedutivo realizado no rascunho. Este texto que é encontrado em livros e representa o resultado final de uma demonstração.

Então para demonstrar este exemplo, vamos considerar primeiro o rascunho.

Rascunho

Suponha que a e b são números reais. Prove que se $0 < a < b$ *então* $a^2 < b^2$

A partir do texto deste exemplo, pode-se ver facilmente que a única hipótese de que dispomos é que a e b são números reais[3]. Porém a conclusão possui a forma $P \to Q$, onde P é a proposição $0 < a < b$ e Q é $a^2 < b^2$. Assim nós começamos com as seguinte rascunho:

Hipóteses	Provar
$a, b \in \mathbb{R}$	$(0 < a < b) \to (a^2 < b^2)$

De acordo com nossa técnica de prova, nós podemos assumir que $0 < a < b$ e tentar usar essa suposição para provar que $a^2 < b^2$. Em outras palavras, nós tranformaremos o problema de provar $(0 < a < b) \to (a^2 < b^2)$ em provar $a^2 < b^2$ supondo que $0 < a < b$. Assim o rascunho ficaria:

Hipóteses	Provar
$a, b \in \mathbb{R}$	$(a^2 < b^2)$
$(0 < a < b)$	

Observando as desigualdades $a < b$ e $a^2 < b^2$ fica claro que devemos multiplicar ambos os lados da desigualdade $a < b$ por a ou por b para que fiquemos mais próximos de nosso objetivo. Como a e b são positivos (uma vez que $(0 < a < b)$), não há a necessidade

[3]Palavras como suponha e assuma em um texto denotam as hipóteses que podem ser utilizadas em uma demonstração

de inverter a direção da desigualdade caso multipliquemos ambos os lados de $a < b$ por a ou por b. Multiplicando $a < b$ por a temos que $a^2 < ab$, e multiplicando $a < b$ por b temos que $ab < b^2$. Assim temos que $a^2 < ab < b^2$, portanto $a^2 < b^2$.

Teorema: *Suponha que a e b são números reais. Se* $0 < a < b$ *então* $a^2 < b^2$

Prova: Suponha que $0 < a < b$. Multiplicando ambos os lados da desigualdade $a < b$ pelo número positivo a nós podemos concluir que $a^2 < ab$, e similarmente multiplicando por b obtemos $ab < b^2$. Assim, temos que $a^2 < ab < b^2$, e disto segue que $a^2 < b^2$. Portanto, se $0 < a < b$ então $a^2 < b^2$.

Como você pode ver no exemplo anterior, existe uma diferença entre o raciocínio que você usa durante uma demonstração e a versão final desta. Quando matemáticos escrevem provas, eles usualmente descrevem apenas os passos necessários para justificar suas conclusões, sem explicar como eles pensaram nelas[4]. Alguns destes passos serão sentenças indicando que o problema utiliza uma determinada técnica de demonstração; alguns passos serão justificados por regras de inferência aplicadas as hipóteses. Mais uma vez, convém ressaltar, que usualmente não existe explicação de como o matemático pensou nestes passos. A prova do exemplo anterior inicia-se com a frase *Suponha que* $0 < a < b$, indicando que você está adicionando a proposição $0 < a < b$ ao seu conjunto de hipóteses; e, o texto prosegue com uma seqüência de inferências que levam a conclusão $a^2 < b^2$.

Para manter claro como fica a estrutura de uma demonstração, para cada estratégia apresentada neste texto, serão apresentadas a estrutura do *rascunho* e do texto da *prova*. Abaixo é mostrado a estrutura de como realizar um rascunho e escrever uma prova quando uma conclusão possui a forma $P \to Q$.

3.1.1. Para provar uma conclusão que possui a forma $P \to Q$:

Assuma que P é verdadeiro e então prove Q

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
H_1	$P \to Q$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	Q
$\vdots$	
H_n	
P	

[4]No rascunho do exemplo anterior, houve a justificativa completa porquê podíamos multiplicar ambos os lados da desigualdade $a < b$ sem alterar sua direção, o que não ocorre na versão final desta prova.

Forma final da prova

Suponha P.
[Prova de Q]
Portanto, se P então Q. ($P \rightarrow Q$)

Note que a forma sugerida para a prova final mostra apenas o começo e o fim da prova; os passos do *meio* deverão ser preenchidos com as inferências realizadas para obter-se a conclusão.

Existe um segundo método para provar conclusões da forma $P \rightarrow Q$. Como $P \rightarrow Q \equiv \neg Q \rightarrow \neg P$, pode-se provar $P \rightarrow Q$ provando $\neg Q \rightarrow \neg P$. Ou seja:

3.2. Para provar uma conclusão que possui a forma $P \rightarrow Q$:

Assuma que Q é falso e prove que P é falso.

Cabe ressaltar que, assumir Q como falso significa adicionar $\neg Q$ as hipóteses e provar que P é falso, significa provar $\neg P$. Abaixo é mostrada a estrutura do rascunho e da prova final.

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
H_1	$P \rightarrow Q$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	$\neg P$
$\vdots$	
H_n	
$\neg Q$	

Forma final da prova

Suponha que Q é falso.
[Prova de $\neg P$]
Portanto, se P então Q. ($P \rightarrow Q$)

Esta estratégia de prova, é chamada de *prova pela contrapositiva*. Para exemplificar o seu uso, considere o seguinte exemplo:

Exemplo: Suponha que a, b e c são números reais e que $a > b$. Prove que se $ac \leq bc$ então $c \leq 0$.

Rascunho

Hipóteses	Provar
$a, b, c \in \mathbb{R}$	$(ac \leq bc) \rightarrow (c \leq 0)$
$a > b$	

A contrapositiva da conclusão é $\neg(c \leq 0) \rightarrow \neg(ac \leq bc)$, ou em outras palavras $(c > 0) \rightarrow (ac > bc)$, então pode-se provar esta conclusão adicionando $(c > 0)$ às hipóteses e fazendo $ac > bc$ a nova conclusão.

Hipóteses	Provar
$a, b, c \in \mathbb{R}$	$(ac > bc)$
$a > b$	
$c > 0$	

Agora, nós podemos escrever a primeira e a última sentença da prova. De acordo com a estratégia, a prova deve ter a seguinte forma:

Suponha que $c > 0$.
[Prova de $ac > bc$]
Portanto, se $ac \leq bc$ então $c \leq 0$.

Usando a nova hipótese $c > 0$, pode-se ver que a conclusão $ac > bc$ segue imediatamente multiplicando ambos os lados da desigualdade $a > b$ por c. Inserindo este passo entre a primeira e última sentença completa a prova.

Teorema: *Suponha* $a, b, c \in \mathbb{R}$ *e* $a > b$. *Se* $ac \leq bc$ *então* $c \leq 0$.

Prova: Esta prova será pela contrapositiva. Suponha $c > 0$. Então nós podemos multiplicar ambos os lados de $a > b$ por c e concluir que $ac > bc$. Portanto, se $ac \leq bc$ então $c \leq 0$.

3.3. Provas envolvendo negações e condicionais

Usualmente é mais fácil provar uma proposição *positiva*[5] que uma negativa, então é muitas vezes útil reexpressar uma conclusão da forma $\neg P$ antes de prová-la. Ao invés de usar uma conclusão que diz que *algo não pode ser verdadeiro*, observe se você rescrever esta como *algo que pode ser verdadeiro*[6]. Assim, nossa primeira estratégia de prova para conclusões da forma $\neg P$ é:

3.4. Para provar uma conclusão que possui a forma $\neg P$:

Tente reexpressar a conclusão em uma forma positiva, usando equivalências lógicas.

Exemplo: *Suponha que* $A \cap C \subseteq B$ *e que* $a \in C$. *Prove que* $a \notin A/B$

Rascunho

Hipóteses	Provar
$A \cap C \subseteq B$	$a \notin A/B \; a \in C$

Como a conclusão está em uma forma negativa, nós iremos reexpressá-la como uma sentença positiva:

$a \notin A/B \equiv \neg(a \in A \wedge a \notin B)$ (definição de A/B)
Mas isto é equivalente a $(a \notin A \vee a \in B)$ (pela lei de DeMorgan)
Mas isto é equivalente a $a \in A \rightarrow a \in B$.

[5] Isto é, uma proposição que não envolve o conectivo $\neg$

[6] isto pode ser facilmente feito utilizando equivalências lógicas já vistas.

Reescrevendo a conclusão desta maneira temos:

Hipóteses	Provar
$A \cap C \subseteq B$	$a \in A \rightarrow a \in B$
$a \in C$	

Agora podemos provar a conclusão utilizando uma estratégia para provar uma conclusão de forma $P \rightarrow Q$.

Hipóteses	Provar
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

O restante da prova é simples. Como $a \in A$ e $a \in C$ então $a \in A \cap C$, e como, $A \cap C \subseteq B$, segue que $a \in B$.

Teorema:*Suponha $A \cap C \subseteq B$ e $a \in C$. Então $a \notin A/B$.*

Prova: Suponha $a \in A$. Como $a \in C$, segue que $a \in A \cap C$. Mas como $A \cap C \subseteq B$ e $a \in A \cap C$, então $a \in B$. Assim não pode ser verdade que a é um elemento de A e não de B, isto é, $a \notin A/B$.

Algumas vezes não é possivel reexpressar uma conclusão da forma $\neg P$ como uma proposição positiva; o que impossibilita utilizar esta estratégia de prova. Nestes casos pode-se tentar construir uma prova por *contradição*, que será apresentada a seguir.

3.5. Para provar uma conclusão que possui a forma $\neg P$:

Assuma que P é verdadeiro e tente obter uma contradição. Uma vez obtida esta contradição, pode-se afirmar que P deve ser falso.

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
H_1	$\neg P$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	$\bot$
$\vdots$	
H_n	
P	

Forma final da prova

Suponha que P é verdadeiro.
[Prova de $\bot$]
Assim segue que P é falso.

Exemplo: Prove que se $x^2 + y = 13$ e $y \neq 4$ então $x \neq 3$.

Rascunho:

Observe que esta prova não possui hipóteses e sua conclusão é da forma $P \rightarrow Q$ (tente expressar você mesmo esta conclusão). Então, utilizando a estratégia de prova direta, temos que:

Hipóteses	Provar
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

Pelo que já foi visto até agora, a estrutura final da prova será semelhante a:

Suponha que $x^2 + y = 13$ e $y \neq 4$.
    [Prova de $x \neq 3$]
Assim segue que se $x^2 + y = 13$ e $y \neq 4$ então $x \neq 3$.

Em outras palavras, a primeira e última sentença da prova já estão determinadas, falta preencher a parte relativa a provar que $x \neq 3$. Provar $x \neq 3$ é o mesmo que provar $\neg(x = 3)$, como a proposição $x = 3$ não pode ser expressada usando conectivos lógicos, não é possível expressar esta conclusão em uma forma positiva. Para demonstrar este teorema, uma solução é tentar uma prova por contradição, resultando em:

Hipóteses	Provar
$x^2 + y = 13$	$\perp$
$y \neq 4$	
$x = 3$	

Novamente, a técnica de prova utilizada sugere como preencher as partes que estão faltando no texto final da prova:

Suponha que $x^2 + y = 13$ e $y \neq 4$.
    Suponha que $x = 3$
        [Prova de $\perp$]
    Portanto $x \neq 3$.
Assim segue que se $x^2 + y = 13$ e $y \neq 4$ então $x \neq 3$.

Recomenda-se que você termine o rascunho desta prova, que será omitido. Abaixo é mostrada a versão final do texto desta.

Teorema: *Se* $x^2 + y = 13$ *e* $y \neq 4$ *então* $x \neq 3$

Prova: Suponha que $x^2 + y = 13$ e $y \neq 4$. Suponha que $x = 3$. Substituindo este valor de x na equação $x^2 + y = 13$, obtém-se que $9 + y = 13$, então $y = 4$. Mas isto contradiz o fato que $y \neq 4$. Portanto $x \neq 3$. Assim segue que se $x^2 + y = 13$ e $y \neq 4$ então $x \neq 3$.

3.6. Para usar uma hipótese que possui a forma $\neg P$:

Se você está fazendo uma prova por contradição, torne P a conclusão a ser provada. Se você provar P, então a prova estará completa, uma vez que P contradiz a hipótese $\neg P$.

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
$\neg P$	$\bot$
H_1	
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
$\neg P$	P
H_1	
$\vdots$	
H_n	

Forma final da prova

[Prova de P]
Como sabe-se que $\neg P$, então isto é uma contradição.

Exemplo: Suponha que A, B e C são conjuntos, $A/B \subseteq C$. Prove que se $x \in A/C$ então $x \in B$.

Pode-se ver que temos como hipótese que $A/B \subseteq C$ e que nossa conclusão é $x \in A/C \rightarrow x \in B$. Como nossa conclusão é da forma $P \rightarrow Q$ temos que:

Hipóteses	Provar
$A/B \subseteq C$	$x \in B$
$x \in A/C$	

Como estamos utilizando nesta prova a técnica de demonstração direta, temos que a forma final do texto da prova será:

Suponha que $A/B \subseteq C$
[Prova de $x \in B$]
Assim, se $A/B \subseteq C$ então $x \in B$.

Observe que a proposição $x \in B$ não pode ser expressa utilizando conectivos lógicos, sendo assim, nenhuma das técnicas vistas até o momento podem ser utilizadas, exceto a prova por contradição. Sendo assim:

Hipóteses	Provar
$A/B \subseteq C$	$\bot$
$x \in A/C$	
$x \notin B$	

Após aplicar a técnica da prova por contradição, temos que a estrutura final da prova será:

Suponha que $A/B \subseteq C$
Suponha que $x \notin B$
[Prova de $\bot$]
Todavia $x \in B$
Assim, se $A/B \subseteq C$ então $x \in B$.

Como estamos fazendo uma prova por contradição e nossa última hipótese é uma proposição negativa, podemos usar a estratégia para hipóteses da forma $\neg P$. Infelizmente, esta estratégia, sugere que tornemos $x \in B$ como nossa nova conclusão, que nos leva para onde começamos. Devemos olhar as outra hipóteses para tentar encontrar uma contradição.

Analizando a hipótese $x \in A/C$ parece ser a melhor saída. Escrevendo a definição de $x \in A/C$ temos que $x \in A/C \equiv x \in A \wedge x \notin C$. Substituindo isto nas hipóteses temos que:

Hipóteses	Provar
$A/B \subseteq C$	$\bot$
$x \in A$	
$x \notin C$	
$x \notin B$	

Agora sim! Temos uma hipótese da forma $\neg P$, onde $P = x \in C$, então podemos aplicar a estratégia para usar hipóteses da forma $\neg P$ fazendo $x \in C$ nossa conclusão. Mostrando que $x \in C$ completa a prova porque contradiz a hipótese $x \notin C$. O rascunho, então, ficaria:

Hipóteses	Provar
$A/B \subseteq C$	$x \in C$
$x \in A$	
$x \notin C$	
$x \notin B$	

Novamente, podemos preencher um pouco mais o esqueleto do texto da prova:

Suponha que $A/B \subseteq C$
    Suponha que $x \notin B$
        [Prova de $x \in C$]
        Mas isto contradiz o fato que $x \notin C$
    Todavia $x \in B$
Assim, se $A/B \subseteq C$ então $x \in B$.

Finalmente chega-se a um ponto onde a conclusão segue facilmente das hipóteses. Como $x \in A$ e $x \notin B$ pode-se concluir que $x \in A/B$. Como $A/B \subseteq C$ e $x \in A/B$, segue que $x \in C$. O texto final deste teorema fica como exercício.

Esta estratégia apresentada para usar hipóteses da forma $\neg P$ é somente aplicável se estamos fazendo uma prova por contradição. Para outros tipos de prova, a estratégia seguinte pode ser usada. Esta nova estratégia é baseada no fato que uma proposição negativa pode ser escrita como uma positiva, utilizando regras de equivalência.

3.7. Para usar uma hipótese que possui a forma $\neg P$:

Se possível reexpresse esta hipótese de outra forma utilizando regras de equivalência.

Já foram apresentadas estratégias para hipóteses e conclusões da forma $\neg P$, mas somente foram apresentadas estratégias para conclusões da forma $P \rightarrow Q$. Agora serão apresentadas estratégias para utilizar hipóteses da forma $P \rightarrow Q$.

3.8. Para usar uma hipótese que possui a forma $P \rightarrow Q$:

Se você possuir P como hipótese, ou puder provar P, você pode concluir Q, usando a regra de inferência *modus ponens*. De maneira análoga, se você possuir como hipótese $\neq Q$ você pode concluir $\neg P$, uma vez que $P \rightarrow Q \equiv \neg Q \rightarrow \neg P$.

3.9. Para provar uma conclusão da forma $\forall x \cdot P(x)$

Assuma que x é um objeto arbitrário e então prove $P(x)$. A letra x deve corresponder a uma nova variável na prova. Se x já estiver sendo utilizada na prova, então escolha um novo nome de variável y, e prove $P(y)$.

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
H_1	$\forall x \cdot P(x)$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	$P(x)$
$\vdots$	
H_n	

Forma final da prova

Seja x arbitrário
    [Prova de $P(x)$]
Como x é arbitrário, pode-se concluir que $\forall x \cdot P(x)$.

Exemplo: Suponha que A, B e C sejam conjuntos quaisquer e que $A/B \subseteq C$. Prove que $A/C \subseteq B$.

Hipóteses	Provar
$A/B \subseteq C$	$A/C \subseteq B$

Como usual, iniciamos por representar a conclusão como uma expressão lógica:

Hipóteses	Provar
$A/B \subseteq C$	$\forall x(x \in A/C \rightarrow x \in B)$

Como a conclusão possui a forma $\forall x \cdot P(x)$, onde $P(x)$ é $(x \in A/C \rightarrow x \in B)$, iremos introduzir uma nova variável x na prova para representar um objeto arbitrário e então tentamos provar $x \in A/C \rightarrow x \in B$. Note que x é uma nova variável livre na prova[7]. Para garantir que x é um valor arbitrário nós não devemos fazer qualquer outra suposição a seu respeito. Após estes passos, o rascunho toma a seguinte forma:

Hipóteses	Provar
$A/B \subseteq C$	$(x \in A/C \rightarrow x \in B)$

[7] x aparece anteriormente na prova como uma variável ligada, devemos escolhar nomes diferentes para variáveis livres, uma vez que, variáveis ligadas não representam nada em particular

De acordo com nossa estratégia, a prova final deve ser semelhante a:

Seja x arbitrário
    [Prova de $(x \in A/C \rightarrow x \in B)$]
Como x é arbitrário, pode-se concluir que $\forall x \cdot (x \in A/C \rightarrow x \in B)$ então $A/C \subseteq B$.

O restante da prova é similar ao um exemplo apresentado na seção 3.6. Abaixo é mostrado o texto final da prova:

Teorema: *Suponha que A, B e C sejam conjuntos e que $A/B \subseteq C$. Então $A/C \subseteq B$.*

Prova: Seja x arbitrário. Suponha que $x \in A/C$. Isto significa que $x \in A$ e $x \notin C$. Suponha que $x \notin B$. Então $x \in A/B$, como $A/B \subseteq C$, $x \in C$. Mas isto contradiz o fato que $x \notin C$. Portanto $x \in B$. Assim, se $x \in A/C$ então $x \in B$. Como x é arbitrário, pode-se concluir que $\forall x \cdot (x \in A/C \rightarrow x \in B)$ então $A/C \subseteq B$.

Note que esta prova mostra que todo elemento de A/C é também um elemento de B, porém ela não faz nenhuma referência do tipo *todos os elementos de* A/C. Nesta prova nós simplesmente pensamos sobre x, que é tratado como um único elemento de A/C. Porém no decorrer da prova, nós tomamos o cuidado de não fazer nenhuma suposição sobre qual elemento de A/C, x deve ser. Somente no final da demonstração, é feita a observação de que x é um valor arbitrário, e portanto, nossas conclusões podem se aplicar a qualquer valor de $x \in A/C$. Esta é a principal vantagem de se provar uma conclusão da forma $\forall x \cdot P(x)$, pois, esta estratégia permite que você trate todo um conjunto de objetos como se fosse um *único*, enquanto este objeto for arbitário.

3.10. Para provar uma conclusão da forma $\exists x \cdot P(x)$

Tente encontrar um valor de x para o qual $P(x)$ é verdadeiro. Então comece sua prova com *Seja x = o valor que você escolheu* e prove $P(x)$ para este valor de x. Novamente, x deve ser uma nova variável livre.

Rascunho

Antes de usar a estratégia ($H_1 \ldots H_n$ são hipóteses com $n \geq 0$.):

Hipóteses	Provar
H_1	$\exists x \cdot P(x)$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	$P(x)$
$\vdots$	
H_n	

Forma final da prova

Seja x = (o valor que você escolher)
    [Prova de $P(x)$]

Assim, $\exists x \cdot P(x)$.

Encontrar o valor certo para x pode ser difícil em alguns casos. Uma possível maneira de encontrar este valor é assumir que $P(x)$ seja verdadeiro e então obtém-se o valor de x, a partir desta suposição. Se $P(x)$ for uma equação envolvendo x, o processo de encontrar x resume-se em resolver esta equação para x. Caso $P(x)$ não seja uma equação, você tem total liberdade para utilizar o método que quiser para descobrir este valor de x. A razão desta liberdade é que não há a necessidade de *especificar o raciocínio utilizado para obter o valor de* x no texto final da prova.

Exemplo: Prove que para todo número real x, se $x > 0$ então existe um número real y tal que $y(y + 1) = x$.

Rascunho

A conclusão a ser provada é $\forall x(x > 0 \rightarrow \exists y[y(y + 1) = x])$, onde as variáveis x e y abrangem quaisquer valores do conjunto $\mathbb{R}$. Conforme já visto, devemos iniciar nossa prova, assumindo que x seja um valor arbitrário e então tentamos provar que $\exists y[y(y+1) = x]$. Assim temos que nosso rascunho possui a forma[8]:

Hipóteses	Provar
$x > 0$	$\exists y[y(y + 1) = x]$

Como nossa conclusão possui a forma $\exists y P(y)$, onde $P(y) = y(y + 1) = x$, de acordo com nossa estratégia, devemos tentar achar um valor de y que torne $P(y)$ verdadeiro. Como $y(y + 1) = x$ é uma equação quadrática sobre y, resolvendo-a temos que $y = \frac{-1 \pm \sqrt{1+4x}}{2}$. Observe que $\sqrt{1 + 4x}$ é definido uma vez que $x > 0$. Como encontramos um valor para y tal que $P(y)$ é verdadeiro, então temos que $\exists y P(y)$, concluindo assim a prova. O esqueleto desta prova juntamente com seu texto seguem abaixo:

Seja x um número real arbitário.
  Suponha $x > 0$
    Seja $y = \frac{-1 \pm \sqrt{1+4x}}{2}$
      [Prova de $y(y + 1) = x$]
    Assim, $\exists y[y(y + 1) = x]$
  Portanto $x > 0 \rightarrow \exists y[y(y + 1) = x]$.
Desde que x é arbitrário, pode-se concluir que $\forall x(x > 0 \rightarrow \exists y[y(y + 1) = x])$.

Teorema Para todo número real x, se $x > 0$ então existe um número real y tal que $y(y + 1) = x$.

Prova Seja x um número real arbitrário e suponha $x > 0$. Seja $y = \frac{-1 \pm \sqrt{1+4x}}{2}$ que é um valor definido desde que $x > 0$. Então:

$$
\begin{aligned}
y(y + 1) = & \qquad (1)\\
\left(\frac{-1 \pm \sqrt{1 + 4x}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{1 + 4x}}{2} + 1\right) = & \\
\left(\frac{-1 \pm \sqrt{1 + 4x}}{2}\right) \cdot \left(\frac{-1 \pm \sqrt{1 + 4x} + 1}{2}\right) = & \\
\frac{1 + 4x - 1}{4} = \frac{4x}{4} = x. &
\end{aligned}
$$

[8] Alguns passos já vistos em seções anteriores foram omitidos.

Como x é arbitrário e existe um número real $y = \frac{-1 \pm \sqrt{1+4x}}{2}$ pode-se concluir que para todo número real $x > 0$ existe um valor y tal que $y(y+1) = x$.

3.11. Para usar uma hipótese da forma $\exists x P(x)$

Introduza uma nova variável livre x_0 na prova para representar um objeto para o qual $P(x_0)$ é verdadeiro. Isto significa que você pode assumir que $P(x_0)$ é verdadeiro. Note que usar uma hipótese da forma $\exists x P(x)$ é muito diferente de provar uma conclusão com a forma $\exists x P(x)$, porque quando você usa uma hipótese desta forma, você não tem que escolher um valor específico para x. Você pode assumir que x_0 é algum objeto para o qual $P(x_0)$ é verdadeiro, mas, você não pode fazer nenhuma suposição adicional sobre x_0.

3.12. Para usar uma hipótese da forma $\forall x P(x)$

Você pode introduzir uma variável livre a e afirmar que $P(a)$ é verdadeiro.

3.13. Para provar uma conclusão da forma $P \wedge Q$

Prove P e Q separadamente utilizando quaisquer técnicas de prova apresentadas.

3.14. Para usar uma hipótese da forma $P \wedge Q$

Considere-a como duas hipóteses separadas: P e Q.

Exemplo: Suponha que $A \subseteq B$, e que A e C são disjuntos. Prove que $A \subseteq B/C$.

Rascunho

Hipóteses	Provar
$A \subseteq B$	$A \subseteq B/C$
$A \cap C = \emptyset$	

Analisando a forma lógica da conclusão, pode-se ver que ela tem a forma $\forall x \cdot x \in A \rightarrow x \in B/C$, então podemos considerar x como um valor arbitário e assumir $x \in A$, e tentar provar que $x \in B/C$. A nova conclusão $x \in B/C$ significa $x \in B \wedge x \notin C$. Portanto de acordo com nossa estratégia para uma conclusão da forma $P \wedge Q$, nós podemos dividir esta conclusão em duas e prová-las separadamente. Sendo assim, o rascunho terá a seguinte forma, após utilizar esta estratégia:

Hipóteses	Provar
$A \subseteq B$	$x \in B$
$A \cap C = \emptyset$	$x \notin C$
$x \in A$	

Seja x arbitrário

Suponha $x \in A$

[Prova de $x \in B$]

[Prova de $x \notin C$]

Assim, $x \in B \wedge x \notin C$, então $x \in B/C$

Portanto $x \in A \rightarrow x \in B/C$

Como x é arbitrário, pode-se concluir que $\forall x \cdot x \in A \rightarrow x \in B/C$, então $A \subseteq B\, C$.

O texto final desta prova, bem como a prova de que $x \in B$ e $x \notin C$ são deixadas como exercício[9].

A partir das técnicas utilizadas para demonstrar conclusões e utilizar hipóteses para $P \to Q$ e $P \wedge Q$, pode-se desenvolver técnicas para $P \leftrightarrow Q$, uma vez que $P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$.

3.15. Para provar uma conclusão da forma $P \leftrightarrow Q$

Prove $P \to Q$ e $Q \to P$ separadamente.

3.16. Para usar uma hipótese da forma $P \leftrightarrow Q$

Trate esta hipótese como duas hipóteses separadas: $P \to Q$ e $Q \to P$.

Exemplo: Suponha que x é um número inteiro. Prove que x é par se e somente se x^2 é par.

Rascunho:

Como nossa conclusão é (x é par) $\leftrightarrow$ (x^2 é par), nós devemos dividir esta prova em duas conclusões, a saber: (x é par) $\to$ (x^2 é par) e (x^2 é par) $\to$ (x é par). Para a primeira conclusão, assume-se que x é par e prova-se que x^2 é par:

Hipóteses	Provar
$x \in \mathbb{Z}$	x^2 é par
x é par	

Escrevendo as definições de x é par e x^2 é par em sua forma lógica temos:

Hipóteses	Provar
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z} \cdot x^2 = 2k$
$\exists k \in \mathbb{Z} \cdot x = 2k$	

Como a segunda hipótese inicia com o quantificador existencial $\exists$, imediatamente consideramos k como sendo um inteiro tal que $x = 2k$. Portanto, agora temos mais duas hipóteses:

Hipóteses	Provar
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z} \cdot x^2 = 2k$
$k \in \mathbb{Z}$	
$x = 2k$	

Como a conclusão inicia com $\exists k$ e k já é uma variável livre usada na prova para representar um número inteiro em particular, nós não podemos atribuir um novo valor k para terminar esta demonstração. Todavia, podemos trocar k por outra letra, por exemplo j e reescrever a conclusão de maneira equivalente.

Hipóteses	Provar
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z} \cdot x^2 = 2j$
$k \in \mathbb{Z}$	
$x = 2k$	

Para provar esta conclusão nós precisamos selecionar um valor para j que satisfaça

[9]Dica: $A \cap C = \emptyset \equiv \neg\exists y \cdot y \in A \wedge y \in C$

a equação $x^2 = 2j$. Usando a hipótese $x = 2k$, temos que: $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Portanto parece que a escolha razoável para j é $j = 2k^2$.

Para provar a segunda conclusão (x^2 é par) $\rightarrow$ (x é par), nós iremos provar a contrapositiva, ou seja, (x não é par) $\rightarrow$ (x^2 não é par). Mas como todo inteiro é um número par ou ímpar, isto é equivalente a (x é ímpar) $\rightarrow$ (x^2 é ímpar).

Hipóteses	Provar
$x \in \mathbb{Z}$	x^2 é ímpar
x é ímpar	

Agora escrevemos a definição de x é ímpar e x^2 é ímpar como sentenças lógicas:

Hipóteses	Provar
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z} \cdot x^2 = 2j + 1$
$\exists k \in \mathbb{Z} \cdot x = 2k + 1$	

No próximo passo selecionamos um inteiro k específico, tal que $x = 2k + 1$, e o aplicamos as hipóteses:

Hipóteses	Provar
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z} \cdot x^2 = 2j + 1$
$k \in \mathbb{Z}$	
$x = 2k + 1$	

Agora para encerrar a demonstração, devemos encontrar um valor j tal que $x^2 = 2j + 1$. Substuindo para x o valor $2k + 1$ temos: $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. A partir deste desenvolvimento algébrico, temos que o valor de j deve ser igual a $2k^2 + 2k$.

Antes de escrever o formato final da prova, deve-se apresentar alguns comentários. As duas implicações provadas podem ser pensadas como as duas direções ($\leftarrow$ e $\rightarrow$) do conectivo $\leftrightarrow$. Estas duas partes da prova são usualmente marcadas com os símbolos $\leftarrow$ e $\rightarrow$.

Teorema: Suponha que x seja um número inteiro. Então x é par se e somente se x^2 é par.

Prova:

($\rightarrow$) Suponha que x seja par. Então para algum inteiro k, $x = 2k$. Porém, $x^2 = 4k^2 = 2(2k^2)$. Como $2k^2$ é um número inteiro, x^2 também é um número inteiro. Assim, se x é par então x^2 é par.

($\leftarrow$) Esta prova será feita pela contrapositiva. Suponha que x é ímpar. Então $x = 2k+1$ para algum inteiro k. Porém, $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$, então como $2k^2 + 2k$ é um inteiro, x^2 é ímpar. Assim, se x^2 é par então x é par.

3.17. Para usar uma hipótese da forma $P \vee Q$

Divida sua prova em casos. Para o caso 1, assuma que P é verdadeiro e use este fato para provar a conclusão. Para o caso 2, assuma que Q é verdadeiro e prove a conclusão usando este fato.

Rascunho

Antes de usar a estratégia: $H_1 \ldots H_n$ são hipóteses com $n \geq 0$ e C é a conclusão a ser demonstrada.

Hipóteses	Provar
H_1	C
$\vdots$	
H_n	
$P \vee Q$	

Depois de usar a estratégia:

Caso 1:

Hipóteses	Provar
H_1	C
$\vdots$	
H_n	
P	

Caso 2:

Hipóteses	Provar
H_1	C
$\vdots$	
H_n	
Q	

Forma final da prova:

Caso 1: P é verdadeiro.

[Prova da conclusão C]

Caso 2: Q é verdadeiro.

[Prova da conclusão C]

Exemplo: Suponha que A, B e C são conjuntos. Prove que se $A \subseteq C$ e $B \subseteq C$ então $(A \cup B) \subseteq C$.

Rascunho

Inicialmente, assumimos como hipóteses que $A \subseteq C$ e $B \subseteq C$ e escrevemos a conclusão em sua forma lógica.

Hipóteses	Provar
$A \subseteq C$	$\forall x \cdot x \in A \cup B \rightarrow x \in C$
$B \subseteq C$	

Para provar a conclusão fazemos x ser um número arbitrário e supomos que $x \in A \cup B$ e tentamos provar que $x \in C$. Como $x \in A \cup B \equiv x \in A \vee x \in B$ então o rascunho fica:

Hipóteses	Provar
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A \vee x \in B$	

Neste exemplo, vemos que uma das hipóteses possui a forma $P \vee Q$, portanto, segundo nossa técnica para usar este tipo de hipóteses, devemos dividir esta prova em casos. Para o primeiro caso, assumimos que $x \in A$ e para o segundo que $x \in B$. No primeiro caso temos o seguinte rascunho:

Hipóteses	Provar
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A$	

Desenvolvendo a hipótese $A \subseteq C$ temos que:

Hipóteses	Provar
$\forall x \cdot x \in A \rightarrow x \in C$	$x \in C$
$B \subseteq C$	
$x \in A$	

Usando a estratégia para hipóteses da forma $\forall x \cdot P(x)$ temos:

Hipóteses	Provar
$x \in A \rightarrow x \in C$	$x \in C$
$B \subseteq C$	
$x \in A$	

Finalmente, aplicando *modus ponens* entre $x \in A$ e $x \in A \rightarrow x \in C$, provamos a conclusão para este caso.

A demonstração para o caso correspondente a $x \in B$ é similar a esta demonstração e será omitida. Seguindo o esquema para escrever o texto de provas que utilizam esta estratégia temos que o texto final será:

Teorema: Suponha que A, B e C são conjuntos quaisquer. Se $A \subseteq C$ e $B \subseteq C$ então $A \cup B \subseteq C$.

Prova: Suponha que $A \subseteq C$ e $B \subseteq C$. Seja x um elemento arbitrário de $A \cup B$. Então temos que $x \in A$ ou $x \in B$.

Caso 1 -$x \in A$: Então como $A \subseteq C$ e $x \in A$ segue que $x \in C$.
Caso 2 -$x \in B$: Então como $B \subseteq C$ e $x \in B$ segue que $x \in C$.

Como sabemos que $x \in A$ ou $x \in B$, e estes casos cobrem todas as possibilidades possíveis para este elemento, podemos concluir que $x \in C$. Como x é um elemento arbitrário de $A \cup B$, isto significa que $A \cup B \subseteq C$.

Note que estes casos na demonstração **não** são exclusivos. Em outras palavras, é possível que $x \in A$ e que $x \in B$, assim como algum valor de x pertença apenas a um dos dois conjuntos. O que torna esta demonstração correta é o fato de cobrirmos todas as possibilidades para x. Ou seja, os casos devem ser exaustivos, isto é, cobrir todas as possibilidades; mas estes não necessariamente tem que ser exclusivos.

3.18. Para provar uma conclusão da forma $P \vee Q$

Divida sua prova em casos. Em um caso prove que P é verdadeiro, em outro prove que Q é verdadeiro.

Exemplo: Prove que para todo inteiro x, o resto de $\frac{x^2}{4}$ é 0 ou 1.

Hipóteses	Provar
$x \in \mathbb{Z}$	($\frac{x^2}{4}$ tem resto 0) $\vee$ ($\frac{x^2}{4}$ tem resto 1)

Como a conclusão tem a forma $P \vee Q$, podemos usar a estratégia de dividir esta em dois casos. Porém quais casos usar? Se fizermos uma pequena tabela com alguns valores para x pode ajudar a desvendar quais casos usar:

x	x^2	quociente de $\frac{x^2}{4}$	resto de $\frac{x^2}{4}$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1

Olha só... Parece que sempre que x é par o resto de $\frac{x^2}{4}$ é 0 e 1 quando x é ímpar. Portanto, para o caso 1, vamos assumir que x é par e provar que o resto de $\frac{x^2}{4}$ é 0 e para o caso 2, assumimos que x é ímpar e provamos que o resto de $\frac{x^2}{4}$ é 1. Para o caso 1, o rascunho assume a seguinte forma:

Hipóteses	Provar
$x \in \mathbb{Z}$	($\frac{x^2}{4}$ tem resto 0)
$\exists k \in \mathbb{Z} \cdot (x = 2k)$	

Imediatamente aplicamos a segunda hipótese escolhendo um valor k_0 que coresponde a um inteiro particular para o qual $x = 2k_0$. Sendo assim: $x^2 = (2k_0)^2 = 4{k_0}^2$. Como $x^2 = 4{k_0}^2$ é evidente que o quociente de $\frac{x^2}{4}$ é ${k_0}^2$ e o resto é 0.

A prova para o caso 2 é similar e é deixada como exercício. O texto final da demonstração segue abaixo:

Teorema: Para todo inteiro x, o resto de $\frac{x^2}{4}$ é 0 ou 1.

Prova: Suponha que x é um número inteiro arbitrário. Considere agora os seguintes casos:

Caso 1: x é par. Então $x = 2k$ para algum inteiro k, portanto, $x^2 = 4k^2$. Claramente o resto de $\frac{x^2}{4}$ é 0.
Caso 2: x é ímpar. Então $x = 2k+1$ para algum inteiro k, então $x^2 = 4k^2+4k+1$. Evidentemente, o resto de $4k^2 + 4k + 1$ dividido por 4 é 1.

3.19. Para provar uma conclusão da forma $P \vee Q$

Evidentemente que se P é verdadeiro, então $P \vee Q$ é verdadeiro. Portanto temos que nos preocupar apenas com o caso em que P é falso e provar que nesta situação, Q deve ser verdadeiro.

Rascunho

Antes de usar a estratégia: $H_1 \ldots H_n$ são hipóteses com $n \geq 0$.

Hipóteses	Provar
H_1	$P \vee Q$
$\vdots$	
H_n	

Depois de usar a estratégia:

Hipóteses	Provar
H_1	Q
$\vdots$	
H_n	
$\neg P$	

Forma final da prova:

Se P é verdadeiro, é evidente que $P \vee Q$ é verdadeiro. Agora suponha que P é falso.

[Prova de Q]

Assim pode concluir que $P \vee Q$ é verdadeiro.

Esta estratégia de demonstração nos diz que para provar $P \vee Q$, supomos $\neg P$ e provamos Q. Esta estratégia é baseada no fato de que $P \vee Q \equiv \neg P \rightarrow Q$. Cabe ressaltar que como o conectivo $\vee$ é comutativo[10] podemos supor $\neg Q$ e provar P.

3.20. Para usar uma hipótese da forma $P \vee Q$

Se você possuir $\neg P$ em seu conjunto de hipóteses ou você puder provar que P é falso, então você pode usar $P \vee Q$ para concluir que Q é verdadeiro. De maneira análoga se você possuir $\neg Q$ or puder provar que Q é falso, você poderá concluir que P é verdadeiro.

4. Indução Matemática

Até agora, neste texto, foram apresentadas técnicas de provas que podem ser usadas para demonstrar qualquer tópico da matemática. Nesta seção, será apresentada mais uma técnica de prova, chamada indução matemática, que é projetada para demonstrar predicados cujo universo de discurso é o conjunto dos números naturais.

Suponha que você deseja provar que todo número natural tem alguma propriedade P. Em outras palavras, você deseja mostrar que $0, 1, 2, \ldots$ têm a propriedade P. Claro, que existem infinitos números naturais, portanto, você não pode verificar um a um com respeito a propriedade P. A idéia por trás da indução matemática é que todo o conjunto dos números naturais é formado por um único elemento inicial e uma função:

- $0 \in \mathbb{N}$
- $n \in \mathbb{N} \rightarrow succ(n) \in \mathbb{N}$. Onde $succ(n) : \mathbb{N} \rightarrow \mathbb{N}$ e $succ(n) = n + 1$.

Provar que todo número natural tem uma propriedade P basta mostrar que esta propriedade é válida para 0, e que, para todo sucessor de um número natural, esta propriedade é válida.

4.1. Para provar uma conclusão da forma $\forall n \in \mathbb{N} \cdot P(n)$

Primeiro, prove que $P(0)$ é verdadeiro e então prove $\forall n \in \mathbb{N} \cdot P(n) \rightarrow P(n+1)$. A primeira destas duas provas é usualmente chamada de *caso base* e a segunda de *passo indutivo*.

[10] isto é: $P \vee Q \equiv Q \vee P$.

Forma final da prova:

Caso Base: [Prova de P(0)].

Passo Indutivo: [Prova de $\forall n \in \mathbb{N} \cdot P(n) \rightarrow P(n+1)$]

Exemplo: Prove que para todo $n \in \mathbb{N}$, $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$

Rascunho

Como pode ser facilmente observado, nossa conclusão a ser provada tem a forma $\forall n \in \mathbb{N} \cdot P(n)$, onde $P(n)$ é $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$. De acordo com a estratégia, podemos provar $\forall n \in \mathbb{N} \cdot P(n)$ provando $P(0) \wedge \forall n \in \mathbb{N} \cdot P(n) \rightarrow P(n+1)$.

Fazendo $n = 0$ e substituindo temos que $2^0 = 2^1 - 1 = 2^{0+1} - 1$, que corresponde a provar que $P(0)$ é verdadeiro.

Para o passo indutivo, devemos provar $\forall n \in \mathbb{N} \cdot P(n) \rightarrow P(n+1)$. Para isto, podemos utilizar todas as técnicas vistas anteriormente. Portanto, para esta parte da demonstração, assumimos que n é um número natural arbitrário e, suponhos que $P(n)$ é verdadeiro e provamos que $P(n+1)$ é verdadeiro. Em outras palavras, nós iremos fazer n um número natural arbitrário, supomos que $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ e provamos que $2^0 + 2^1 + 2^2 + \ldots + 2^{n+1} = 2^{(n+1)+1} - 1$. Sendo assim, teríamos o seguinte rascunho:

Hipóteses	Provar
$n \in \mathbb{N}$	$2^0 + 2^1 + 2^2 + \ldots + 2^{n+1} = 2^{(n+1)+1} - 1$
$2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$	

Evidentemente a segunda hipótese é similar a conclusão. Seria possível partirmos da hipótese de alguma maneira para chegarmos à conclusão usando operações algébricas? A resposta para isto é sim, e, a chave para isto é perceber que o lado esquerdo da equação na conclusão é exatamente igual ao lado esquerdo da segunda hipótese com o termo extra 2^{n+1}. Então parece que devemos tentar somar 2^{n+1} em ambos os lados da equação da hipótese.

$$(2^0 + 2^1 + 2^2 + \ldots + 2^n) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1}$$

Reescrevendo o lado direito temos:

$$(2^0 + 2^1 + 2^2 + \ldots + 2^n) + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1$$

Que é exatamente a conclusão! Abaixo é mostrado o texto final da demonstração.

Teorema: Para todo $n \in \mathbb{N}$, $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$

Prova: Esta prova usará indução matemática.

Caso base: Considerando $n = 0$, temos que $2^0 = 2^{0+1} - 1$, como requerido.
Passo indutivo: Seja n um número natural arbitrário e suponha que $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ então:

$$(2^0 + 2^1 + 2^2 + \ldots + 2^n) + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{(n+1)+1} - 1$$

Aparentemente, esta prova não convence muito, não é mesmo? Porém olhando com mais atenção para a estrutura desta prova podemos ficar convencidos de que ela realmente funciona. No caso base, nós provamos que $P(0)$ é verdadeiro. No passo indutivo, provamos que $\forall n \in \mathbb{N} \cdot P(n) \rightarrow P(n+1)$ então sabemos que para qualquer número natural n, $P(n) \rightarrow P(n+1)$. Por exemplo, fazendo $n = 0$ nós podemos concluir que $P(0) \rightarrow P(1)$, como no caso base provamos que $P(0)$ é verdadeiro, podemos aplicar *modus ponens* concluindo que $P(1)$ também é verdadeiro. De maneira análoga se fizermos $n = 1$ obtemos $P(1) \rightarrow P(2)$ e por conseqüência que $P(2)$ é verdadeiro. Continuando desta maneira, somos capazes de ver que aplicando repetidamente o passo indutivo, provamos que $P(n)$ é verdadeiro para qualquer número natural, ou seja, $\forall n \in \mathbb{N} \cdot P(n)$.

Exemplo: Prove que $\forall n \in \mathbb{N} \cdot (n^3 - n) \bmod 3 = 0$

Rascunho

Como usual, o caso base é fácil de se demonstrar[11]. Para o passo indutivo, consideremos n um número natural arbitrário e supomos que $(n^3 - n) \bmod 3 = 0$. Para provar que $((n+1)^3 - (n+1)) \bmod 3 = 0$ devemos primeiro escrever o significado da conclusão como uma sentença lógica. Observe que $((n+1)^3 - (n+1)) \bmod 3 = 0$ é o mesmo que dizer que $((n+1)^3 - (n+1))$ é um múltiplo de 3. Portanto, deve existir um número natural j tal que $3j = ((n+1)^3 - (n+1))$. Sendo assim, teremos o seguinte rascunho:

Hipóteses	Provar
$n \in \mathbb{N}$	$\exists j \in \mathbb{Z} \cdot 3j = ((n+1)^3 - (n+1))$
$\exists k \cdot 3k = (n^3 - n)$	

De acordo com nossas técnicas para utilizar hipóteses com o quantificador existencial, selecionamos um valor k_0 para o qual $3k_0 = (n^3 - n)$ é verdadeiro. Para completar esta prova, devemos encontrar um inteiro j, tal que $3j = ((n+1)^3 - (n+1))$, que esteja relacionado com k_0 de alguma maneira. Se expandirmos a expressão presente na conclusão temos que:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n - n - 1 = (n^3 - n) + 3n^2 + 3n$$

Desenvolvendo a expressão, obtemos, em uma parte desta, o valor $n^3 - n$. De acordo com nossas hipóteses, este valor é igual a $3k_0$.

$$3k_0 + 3n^2 + 3n = 3(k_0 + n^2 + n).$$

Evidentemente que o valor procurado para j é $j = k_0 + n^2 + n$.

Teorema: Para todo número natural n, $(n^3 - n) \bmod 3 = 0$.

Prova: Esta prova usará indução matemática.

Caso base: Se $n = 0$, então $n^3 - n = 0 = 3.0$, portanto $(n^3 - n) \bmod 3 = 0$.

[11] A operação mod retorna o resto da divisão entre dois números inteiros.

Passo Indutivo: Seja n um número natural arbitrário e suponha que $(n^3 - n) \bmod 3 = 0$. Então nós podemos escolher algum número k_0 tal que $3k_0 = n^3 - n$ Assim:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n - n - 1 = (n^3 - n) + 3n^2 + 3n =$$

$$3k_0 + 3n^2 + 3n = 3(k_0 + n^2 + n).$$

Portanto, $(n^3 - n) \bmod 3 = 0$ como requerido.

5. Indução forte

No passo indutivo de uma prova por indução matemática, nós provamos que um número natural tem alguma propriedade supondo que esta é válida para seu predecessor. Porém em alguns casos esta suposição não é suficiente. Algumas situações exigem que suponhamos que esta propriedade seja válida não apenas para um predecessor de um número natural, mas sim para *todos* os seus predecessores. Esta idéia fundamenta o princípio de prova conhecido como *indução forte*.

5.1. Para provar uma conclusão da forma $\forall n \in \mathbb{N} \cdot P(n)$

Prove que $\forall n \in \mathbb{N}[(\forall k < n \cdot P(k)) \rightarrow P(n)]$. Claro que a maneira mais direta de se provar isto é assumir que n seja um número natural arbitrário, supor que $(\forall k < n \cdot P(k))$ e provar $P(n)$.

Note que nem sempre há necessidade de um caso base em uma prova por indução forte. Tudo que precisamos é uma variante do passo indutivo no qual provaremos que se todo número $k < n$ tem uma propriedade, então n também a possui.

Exemplo: Prove que todo número inteiro $n > 1$ é primo ou um produto de primos.

Rascunho:

Inicialmente, antes de utilizar indução forte, vamos tentar demonstrar este teorema usando indução comum. Evidentemente que para demonstrar este teorema, usando indução comum, devemos considerar $n = 2$ em nosso caso base. Como 2 é um número primo, temos que o caso base é verdadeiro. Agora, como de costume, suporemos que este teorema seja válido para um número n arbitrário e tentaremos provar esta propriedade para o sucessor deste número. Sendo $n + 1$ um número primo, é evidente que não há com o que se preocupar. Porém, quando $n + 1$ for não um número primo, então ele pode ser escrito da forma $n + 1 = ab$ onde $a \neq 1, a \neq (n + 1), b \neq 1, b \neq (n + 1)$. Ao tentarmos escrever $(n + 1)$ como um produto de dois inteiros diferentes de 1 e $(n + 1)$ pode ser que os fatores obtidos não possuam o termo n, o que inviabiliza a utilização de nossa hipótese que esta propriedade é válida para um número natural n arbitrário, uma vez que, os valores destes fatores podem ser *menores* que n. Observe que para demonstrar este teorema, a técnica de indução comum parece não possuir *poder* suficiente. Veja que neste exemplo, a suposição de que esta propriedade é válida para um número natural n arbitrário não é suficiente. Para demonstrar, devemos supor que esta propriedade é válida para todo número natural k menor que n, e então provar que esta propriedade é válida para n, ou seja, devemos usar indução forte.

Pode-se perceber facilmente que a conclusão a ser provada é $\forall n \in \mathbb{N}[\forall k < nP(k)] \rightarrow P(n)]$ onde $P(n) = n > 1 \rightarrow$ n é primo $\vee$ n é um produto de primos.

Utilizando a estratégia de indução forte temos o seguinte rascunho:

Hipóteses	Provar
	$\forall n \in \mathbb{N}[\forall k < nP(k)] \rightarrow P(n)]$

Como de costume, consideramos $n \in \mathbb{N}$ arbitrário e supomos $\forall k < nP(k)$. Isto leva ao seguinte rascunho:

Hipóteses	Provar
$n \in \mathbb{N}$	$n > 1 \rightarrow$ n é primo $\vee$ n é produto de primos
$\forall k < n$ k é primo $\vee$ k é produto de primos	

Agora, supomos $n > 1$ e resta provar: n é primo $\vee$ n é produto de primos.

Hipóteses	Provar
$n \in \mathbb{N}$	n é primo $\vee$ n é produto de primos
$\forall k < n[$ k é primo $\vee$ k é produto de primos]	
$n > 1$	

Como nossa conclusão possui a forma $P \vee Q$, podemos supor $\neg P$ e provar Q. Sendo assim, vamos adicionar as hipóteses que n não é primo e provar que n deve ser um produto de primos. Porém dizer que um número não é primo significa que $\exists a \exists b(n = ab \wedge a < n \wedge b < n)$. Portanto:

Hipóteses	Provar
$n \in \mathbb{N}$	n é produto de primos
$\forall k < n[$ k é primo $\vee$ k é produto de primos]	
$n > 1$	
$\exists a \exists b(n = ab \wedge a < n \wedge b < n)$	

Imediatamente selecionamos novas variáveis a e b para representar números inteiros tais que $n = ab \wedge a < n \wedge b < n$. Como neste caso, garantimos que $a > 1 \wedge b > 1$, temos necessariamente que $1 < a, b < n$. Pela hipótese $\forall k < n[$ k é primo $\vee$ k é produto de primos], temos que a e b são primos ou produto de primos. Mas como $n = ab$, temos que n é um produto de primos, completando a demonstração. Abaixo é mostrado o resultado final desta demonstração:

Teorema: Todo número inteiro maior que um é primo ou um produto de primos.

Prova: Esta prova utilizará indução forte. Suponha $n \in \mathbb{N}$ arbitrário e que para todo inteiro k, se $1 < k < n$ então k é primo ou um produto de primos. Suponha que $n > 1$. Evidentemente que se n é primo nada resta a provar, portanto suponha que n não seja primo. Então devem existir números inteiros a e b tais que $n = ab$, $a < n$ e $b < n$. Note que se $a < n$ e $b < n$ então $a > 1$ e $b > 1$. Portanto temos que $1 < a < n$ e $1 < b < n$. Como supomos que para todo inteiro $k < n$, k é primo ou um produto de primos, temos que a e b são primos ou um produto de primos. Uma vez que $n = ab$, temos que necessariamente n é um produto de primos.