Aula 05

Teoremas e Demonstrações

Técnicas de demonstração

- Técnicas de demonstração
  - Teoremas e Demonstrações Informais
    - Os argumentos lógicos formais tem a forma $P \rightarrow Q$, onde P e Q podem representar proposições compostas.
    - Temos que demonstrar a validade do argumento.
    - As vezes temos que provar argumentos que não são universalmente verdadeiros, sendo apenas em certos contextos.

Técnicas de demonstração

- Temos que provar que, se P é verdadeiro nesse contexto, Q também o é.
- Se pudermos provar essa condição, então $P \rightarrow Q$ torna-se um teorema sobre aquele assunto.
- Os teoremas podem ser enunciados e demonstrados de maneira menos formal do que usando argumentos da lógica formal.

Técnicas de demonstração

- Um teorema é uma proposição que é garantida por uma prova.
- Um axioma é uma proposição que se assume como verdadeira e que não precisa de prova.
- Uma conjectura é uma proposição que ainda não foi provada e nem refutada.

Técnicas de demonstração

Provar ou Não Provar

- Raciocínio indutivo – Algo que se conclui baseado na Experiência.
  - Por exemplo, observando que, em diversos casos nos quais sempre P é verdade, Q também o é, formula-se uma conjectura: Quanto mais verifica-se que Q segue de P, mais confiante que a conjectura é verdadeira.

Técnicas de demonstração

- Raciocínio dedutivo – Verificação de fato se a conjectura é verdadeira.
  - Produzir uma demonstração que $P \to Q$, transformando a conjectura em um teorema.
  - Ou encontrando um contra-exemplo, mostrando que a conjectura está errada, com um caso onde P é verdadeiro e Q é falso.

Obs: Não é simples a decisão de qual a abordagem: provar ou buscar um contra-exemplo.

- Ex. 01: Para um inteiro positivo n, n! é definido com sendo n(n-1)(n-2)...1. Prove ou encontre um contra-exemplo para a conjectura “para todo inteiro positivo n, $n! \leq n^2$.

Demonstração exaustiva

- Encontrar um contra-exemplo pode não ser simples. Então o caminho para provar uma conjectura é usar métodos para demonstrá-la.
- Quando temos uma conjectura sobre uma coleção finita, ela pode ser provada verificando se ela é válida para cada elemento da coleção.
- Uma demonstração por exaustão significa que foram exauridos todos os casos possíveis.

- Ex.02: Provar a conjectura: “Se um inteiro entre 1 e 20 é divisível por 6, então também é divisível por 3.”

  Como existe um número finito de casos, a conjectura pode ser provada mostrando que é verdadeira para todos os inteiros de 1 a 20, por exemplo, usando uma tabela.

Demonstração exaustiva

- Ex.03: Provar a conjectura: “Para qualquer inteiro positivo menor ou igual a 5, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro.”

- Ex.04: Dê um contra-exemplo para a conjectura: “Para qualquer inteiro positivo, o quadrado do inteiro é menor ou igual à soma de 10 mais 5 vezes o inteiro.”

Demonstração Direta

- Uma demonstração ou prova é dita direta quando pressupões verdadeira a hipótese e, a partir desta, prova ser verdadeira a tese.

- Ex.05: Considere a seguinte conjectura: “A soma de dois números pares é um número par”.

- Podemos efetuar a demonstração direta a partir dos seguintes passos:

  1. Reescrevendo na forma $P \rightarrow Q$: Se n e m são dois números pares quaisquer, então n+m é um número par.

- Podemos efetuar a demonstração direta a partir dos seguintes passos:

  1. Reescrevendo na forma $P \to Q$: Se n e m são dois números pares quaisquer, então n+m é um número par.

  2. Lembrando que um numero par n pode ser definido por n=2r, onde r é um numero inteiro qualquer.

- Podemos efetuar a demonstração direta a partir dos seguintes passos:

  1. Reescrevendo na forma $P \rightarrow Q$: Se n e m são dois números pares quaisquer, então n+m é um número par.

  2. Lembrando que um numero par n pode ser definido por n=2r, onde r é um numero inteiro qualquer.

  3. Se n e m são pares, então existem r, s tais que: n=2r e m=2s, então: n+m=2r+2s => 2(r+s), como r+ s é um número inteiro, logo, n+m é um número par.

- Ex.06: Considere a seguinte conjectura: “O produto de dois números inteiros pares é um número par”. Faça a demonstração direta (informal) da mesma.

Contraposição

- Se a demonstração direta $P \rightarrow Q$, não foi atingida, pode-se tentar algumas variantes da técnica de demonstração direta.
- Se puder provar o teorema $Q' \rightarrow P'$, pode-se concluir que $P \rightarrow Q$, usando a tautologia $(Q' \rightarrow P') \rightarrow (P \rightarrow Q)$.
  - $Q' \rightarrow P'$ é a contrapositiva de $P \rightarrow Q$

- A técnica de provar $P \rightarrow Q$ através de uma demonstração direta de $Q' \rightarrow P'$ é chamada de demonstração por contraposição.
- A tautologia $(Q' \rightarrow P') \rightarrow (P \rightarrow Q)$ vem da regra de inferência onde $P \rightarrow Q$ pode ser deduzida de $Q' \rightarrow P'$.

- Ex. 07: Prove o seguinte teorema n pertence ao conjunto dos números reais:
  - $n! > (n+1) \rightarrow n>2$

- Por equivalência, pode-se demonstrar por contraposição, que:
  - $n \leq 2 \rightarrow n! \leq (n+1)$

- Ex.08: Mostre que se n + 1 senhas diferentes foram distribuídas para n alunos, então algum aluno recebe ≥ 2 senhas.

  - A contrapositiva é “Se todo aluno recebe < 2 senhas, então não foram distribuídas n + 1 senhas”.

Demonstração por absurdo

- Quando a demonstração de $P \rightarrow Q$, consiste em supor a hipótese P, supor a negação de Q e concluir uma contradição (em geral $Q \wedge Q'$), a demonstração é chamada de por absurdo.
  - Lembrando que uma contradição é uma fbf cujo valor lógico é sempre Falso. Ela pode se denotada por 0.
  - Para provar $P \rightarrow Q$, podemos levar em conta a seguinte fbf: $(P \wedge Q' \rightarrow 0) \rightarrow (P \rightarrow Q)$.
  - Construindo a tabela verdade, concluímos a que a fbf é uma tautologia.
  - Então se provarmos que $P \wedge Q' \rightarrow 0$, isto implicará em $P \rightarrow Q$.

Demonstração por Absurdo

- Portanto, na demonstração por absurdo, assumese o oposto do que se quer provar, ao chegar a uma contradição, a prova é finalizada.

- Ex.10: Demonstrar por absurdo a proposição: “Se um número somado a ele mesmo é igual a ele mesmo, então esse número é 0”.

- Ex.10: Demonstrar por absurdo a proposição: “Se um número somado a ele mesmo é igual a ele mesmo, então esse número é 0”.
  - Representando x por um numero qualquer.
  - A hipótese é $x+x=x$ e a conclusão é $x=0$.
  - Para demonstrar por absurdo, supomos que $x+x=x$ e $x\neq0$. Então $2x=x$ e $x\neq0$.
  - Dividindo ambos os lados da eq. $2x=x$ por x, obtém-se $2=1$, uma contradição, que buscamos.
  - Portanto, $(x+x=x)\rightarrow(x=0)$

- Ex.11: Demonstrar por absurdo que o produto de inteiros ímpares não é par.

Técnica	Abordagem para provar $P \rightarrow Q$	Observações
Exaustão	Demonstre $P \rightarrow Q$ para todos os casos possíveis	Pode ser usada para provar um número finito de casos.
Direta	Suponha P, deduza Q	Abordagem padrão – o que se deve tentar em geral.
Contraposição	Suponha Q’, deduza P’	Use a técnica se Q’ parece dar mais munição que P.
Por Absurdo	Suponha P ^ Q’, deduza uma contradição	Use essa técnica quando Q disser que alguma coisa não é verdade.

Aula 06

Indução

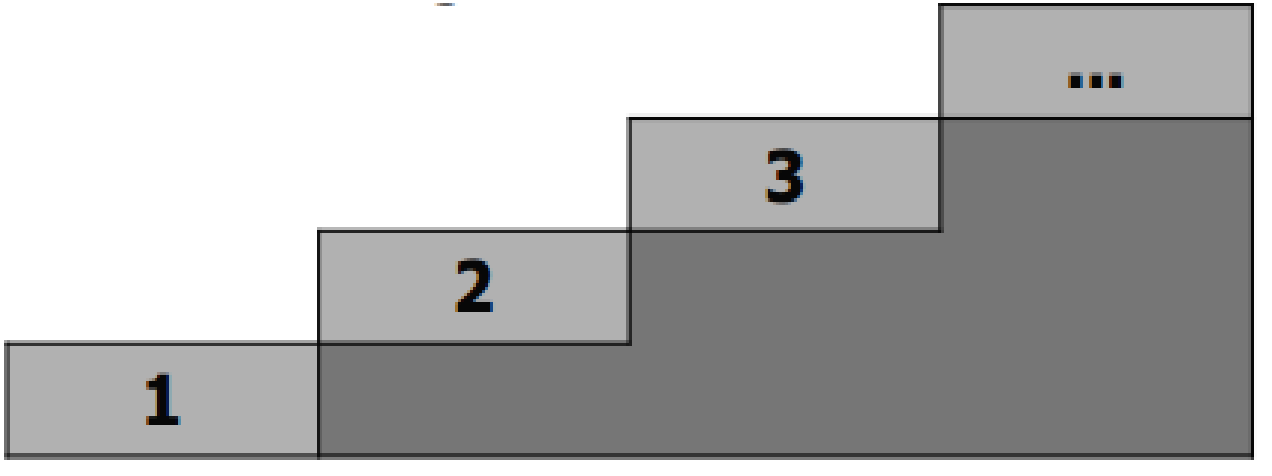
Indução - Primeiro Princípio de Indução

- Imagine que você está subindo uma escada infinitamente alta. Como você será capaz de saber se será capaz de chegar a um degrau arbitrariamente alto?
  - Você pode inicialmente fazer as seguintes hipóteses sobre a sua capacidade de subir:
    1. Você consegue alcançar o primeiro degrau.
    2. Uma vez chegado a um degrau, você sempre será capaz de chegar ao próximo.

- Se a proposição 1 e o condicional 2 são verdadeiros, então, pela proposição 1, você consegue chegar no primeiro degrau e, portanto, pela 2, consegue chegar no segundo.
- Novamente pela 2, consegue chegar no terceiro.
- Mais uma vez, pela 2, chega no quarto degrau e assim por diante.
- Você poderá subir tão alto quanto quiser.

- Nesse caso, ambas as hipóteses são necessárias. Se apenas a primeira fosse V, não teríamos a garantia de passar do primeiro degrau.
- Se apenas a 2ª fosse V, poderíamos não ser capazes de começar nunca.

• Numerando os degraus...



- Seja uma propriedade de que cada número que identifica o degrau possa ter.
- Ao invés de chegar a um degrau arbitrário, podemos buscar um número inteiro positivo que tenha essa propriedade.
- Usando a notação P(n) para dizer que o inteiro positivo n tem a propriedade P.
- Por analogia, vamos usar a mesma “técnica” usada para subir a escada, para provar que, qualquer que seja o inteiro positivo n, temos P(n).

- Precisamos provar as proposições:
  - 1. $P(1)$ - (1 tem a propriedade P)
  - 2. Para qualquer inteiro positivo k, $P(k) \rightarrow P(k+1)$ – Se qualquer número tem a propriedade P, o próximo também tem.
- Se pudermos provar ambas as proposições 1 e 2, então $P(n)$ é válida para qualquer inteiro positivo n.
- O fundamento para argumentos desse tipo é o primeiro princípio de indução matemática.

Primeiro Princípio de Indução

1. $P(1)$
2. $(\forall k)\ [P(k) \text{ verdade} \rightarrow P(k+1) \text{ verdade}]$

Primeiro Princípio de Indução

1. P(1)
2. $(\forall k)$ [P(k) verdade $\rightarrow$ P(k+1) verdade]

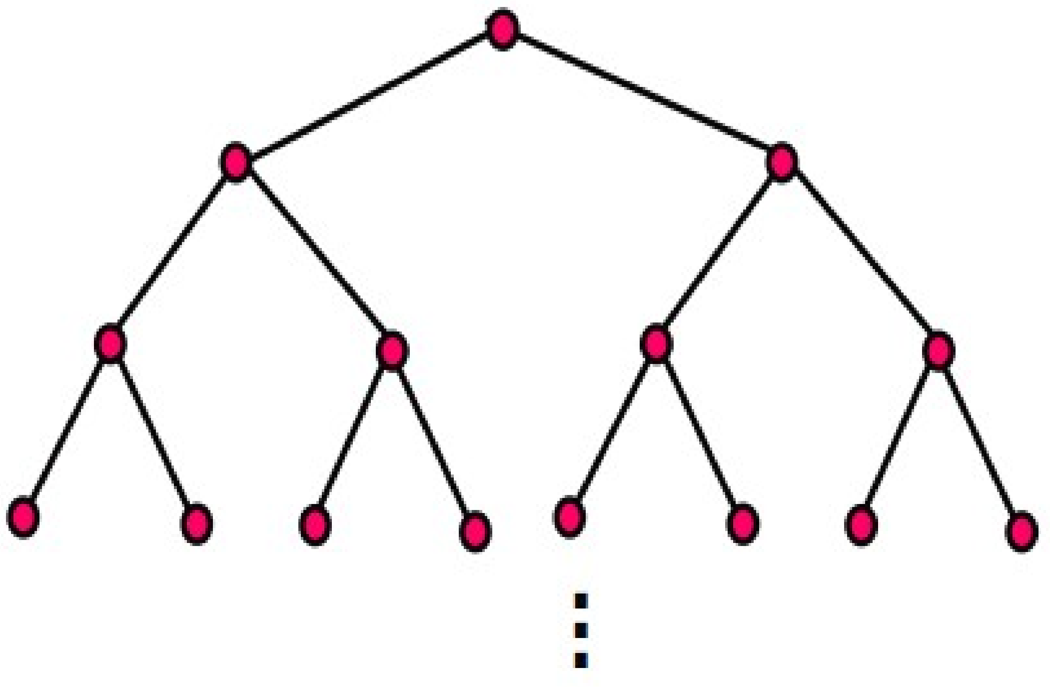
- O primeiro princípio de indução matemática é um condicional, com uma conclusão na forma “P(n) é verdade para todo inteiro positivo n”.
  - A técnica da indução se mostra mais apropriada para provarmos que alguma coisa é verdade para todo inteiro positivo n (conjunto dos números naturais).

- 1. P(1)
- 2. $(\forall k)$ [P(k) verdade $\rightarrow$ P(k+1) verdade]
  - Para mostrar que a conclusão dessa condicional é verdadeira, precisamos provar que as hipóteses 1 e 2 são.
  - Para provar a proposição 1, basta mostrar que o número 1 tem a propriedade P, (Base da Indução).
  - A proposição 2 é um condicional que tem que ser válido para todo k (Passo da Indução).

- Resumo

1. Passo 1 – Prove a base da indução P(1) (ou o menor inteiro positivo em questão.
2. Passo 2 – Suponha P(k)
3. Passo 3 – Prove P(k+1)

- Ex. 01:Suponha a árvore genealógica de uma família cuja característica fundamental é que cada casal tem sempre dois filhos e que cada um desses filhos também tem dois filhos. A árvore é ilustrada abaixo:



Geração	Descendentes
1	$2^1=2$
2	$2^2=4$
3	$2^3=8$
...	...

- Há de se perceber que a geração n contém 2^n descendentes. Precisamos demonstrar essa propriedade.
- Formalmente, se denotarmos por P(n) o número de descendentes em cada geração, nossa conjectura é que:

$$P(n) = 2^n$$

- Vamos usar a indução para provar que a conjectura está correta.

  1. O passo básico é estabelecer P(1), que é a equação:

$$P(1) = 2^1 = 2$$

- Vamos usar a indução para provar que a conjectura está correta.

  1. O passo básico é estabelecer P(1), que é a equação:

$$P(1) = 2^1 = 2$$

  2. Isso é verdadeiro pois o primeiro elemento da genealogia teve 02 filhos.

  3. Supondo agora que a conjectura está correta para uma geração arbitrária k, $k \geq 1$:

$$P(k) = 2^k$$

- Vamos mostrar que $P(k+1) = 2^{k+1}$
- Nessa família, cada descendente tem 2 filhos, de modo que o número de descendentes na geração k+1 será o dobro da geração k.
  - Ou seja $P(k+1) = 2P(k)$
- Pela hipótese de indução:
  - $P(k) = 2^k$

$$P(k+1) = 2P(k) = 2(2k) = 2^{k+1}$$

De fato, $P(k+1) = 2^{k+1}$

- Ex. 02: Sejam as seguintes definições:

$$2^0 = 1 = 2^1 - 1$$
$$2^0 + 2^1 = 1 + 2 = 3 = 2^2 - 1$$
$$2^0 + 2^1 + 2^2 = 1 + 2 + 4 = 7 = 2^3 - 1$$
$$2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = 15 = 2^4 - 1$$

- No exemplo acima o padrão mais geral parece com:

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

Ex. 03: Demonstre que, para qualquer n, $2^n > n$.

Ex. 04: Prove que $n^2 > 3n$, para $n \geq 4$.

Ex. 05: Prove por indução que a soma dos n primeiros números naturais é dada por $P(n) = n (n+1) / 2$

Aula 07

Dedução natural

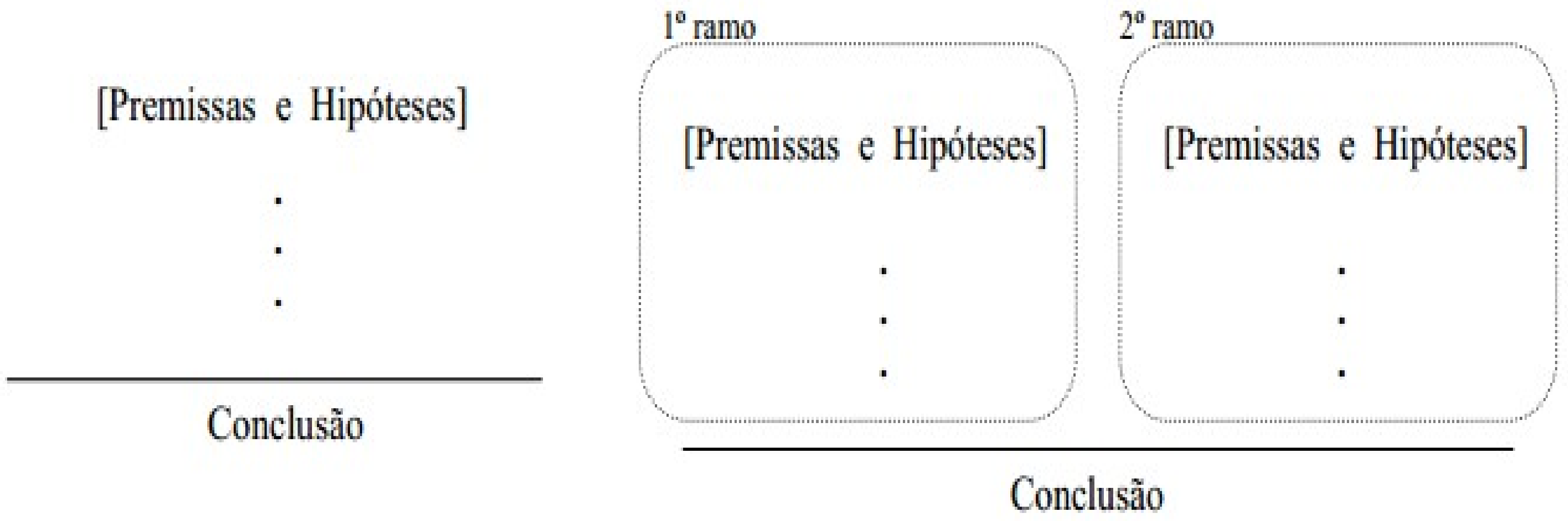
- A dedução natural é um método de demonstração introduzido independentemente por Gerhard Gentzen em 1935 e Stanislaw Jaskowski em 1934.

- Os sistemas de dedução natural caracterizam-se, entre outros aspectos, por não apresentarem um conjunto de axiomas, mas apenas um conjunto de regras de inferências.

- No sistema de dedução natural as regras de inferência são projetadas num padrão de regras de introdução e eliminação de conectivos e quantificadores, que são combinadas para a construção de uma prova.

- Podemos representar as provas por árvores, sobrepondo as instâncias das regras de inferência utilizadas na sua obtenção.

- Portanto, graficamente, uma prova possuirá a seguinte forma:



As regras de inferência

- O Sistema de Dedução Natural para a Lógica Sentencial dispõe de onze regras básicas de inferência, que podem ser divididas em dois grupos: as regras não hipotéticas, e as regras hipotéticas.

As regras não hipotéticas

- Eliminação da implicação(→E)[Modus Ponens]: De um condicional e seu antecedente, podemos inferir seu conseqüente.

$$\frac{\phi \qquad \phi \rightarrow \psi}{\psi} \rightarrow E$$

As regras não hipotéticas

- Exemplo:
  - Prove:

$$p,\quad q \rightarrow r,\ p \rightarrow q \vdash r$$

$$\dfrac{\dfrac{p \qquad p \rightarrow q}{q}\,\rightarrow E \qquad q \rightarrow r}{r}\,\rightarrow E$$

$$\boxed{\begin{array}{l} p, \\ q \rightarrow r \\ p \rightarrow q \end{array}}$$

As regras não hipotéticas

- Eliminação da negação(~E) : De uma sentença ~~φ, podemos inferir φ.

$$\frac{\sim\sim\phi}{\phi}\ \sim\mathbf{E}$$

As regras não hipotéticas

- Exemplo:
  - Prove:

$\sim p \to \sim\sim q , \sim\sim\sim p \vdash q$

$$\dfrac{\dfrac{\dfrac{\sim\sim\sim p}{\sim p}\;{\sim}\mathbf{E} \qquad \sim p \to \sim\sim q}{\sim\sim q}\;{\to}\mathbf{E}}{q}\;{\sim}\mathbf{E}$$

$\sim p \to \sim\sim q$

$\sim\sim\sim p$

As regras não hipotéticas

- Introdução da conjunção (∧I): De quaisquer sentenças φ e Ψ, podemos inferir a conjunção φ ∧ Ψ.

$$\frac{\phi \qquad \psi}{\phi \wedge \psi}\ \wedge I$$

As regras não hipotéticas

- Eliminação da conjunção (∧E): De uma conjunção podemos inferir qualquer um dos seus componentes.

$$\frac{\phi \wedge \psi}{\phi} \wedge E$$

$$\frac{\phi \wedge \psi}{\psi} \wedge E$$

As regras não hipotéticas

- Exemplo:

$$p \wedge q \vdash q \wedge p$$

$$\cfrac{\cfrac{p \wedge q}{q}\,\wedge E \qquad \cfrac{p \wedge q}{p}\,\wedge E}{p \wedge q}\,\wedge I$$

$$\boxed{p \wedge q}$$

As regras não hipotéticas

- Introdução da disjunção ($\vee$I) : Podemos inferir uma disjunção a partir de qualquer um de seus componentes

$$\frac{\phi}{\phi \vee \psi}\ \vee\mathrm{I} \qquad\qquad \frac{\psi}{\phi \vee \psi}\ \vee\mathrm{I}$$

As regras não hipotéticas

- Exemplo:

$$p \vdash (p \vee q) \vee (p \vee r)$$

$$\dfrac{\dfrac{p}{p \vee q}\ \vee I}{(p \vee q) \vee (p \vee r)}\ \vee I$$

p

As regras não hipotéticas

- Introdução do bimplicação (↔ I): A partir de sentenças (φ→ψ) e (ψ→φ) podemos inferir (φ↔ψ).

$$\frac{\phi\rightarrow\psi \qquad\qquad \psi\rightarrow\phi}{\psi\leftrightarrow\phi}\ \mathbf{\leftrightarrow I}$$

As regras não hipotéticas

- Eliminação do bimplicação (↔ E): A partir de uma sentença da forma $(\varphi \leftrightarrow \psi)$ podemos inferir tanto $(\varphi \rightarrow \psi)$ quanto $(\psi \rightarrow \varphi)$.

$$\frac{\psi \leftrightarrow \phi}{\phi \rightarrow \psi} \; \leftrightarrow\mathrm{E}$$

$$\frac{\psi \leftrightarrow \phi}{\psi \rightarrow \phi} \; \leftrightarrow\mathrm{E}$$

As regras não hipotéticas

- Exemplo:

$p \leftrightarrow (q \vee r), q \vdash p$

$$\dfrac{\dfrac{q}{(q \vee r)}\ \vee\mathbf{I} \qquad \dfrac{p \leftrightarrow (q \vee r)}{(q \vee r) \rightarrow p}\ \leftrightarrow\mathbf{E}}{p}\ \rightarrow\mathbf{E}$$

$p \leftrightarrow (q \vee r)$
q

As regras não hipotéticas

- Introdução do ⊥(⊥I): Introduzimos o símbolo ⊥ para identificar a derivação de uma contradição.

$$\frac{\psi \qquad \sim\psi}{\perp}\ \perp I$$

Exercícios

- Considere o conectivo de bi-implicação definido por abreviatura, (

$$\alpha \leftrightarrow \beta \stackrel{\text{def}}{=} (\alpha \to \beta) \wedge (\beta \to \alpha)$$

  Usando o sistema de dedução natural (com regras primitivas para a conjunção, a disjunção, a implicação, a negação e o absurdo) mostre que a bi-implicação define uma relação de equivalência entre as formulas da Lógica Clássica, desde o ponto de vista da relação de consequência formal associada, isto e, exiba derivações para as seguintes conjecturas:

(a) $\vdash_{\mathcal{N}_p} \alpha \leftrightarrow \alpha$

(b) $\alpha \leftrightarrow \beta \vdash_{\mathcal{N}_p} \beta \leftrightarrow \alpha$

(c) $\alpha \leftrightarrow \beta, \beta \leftrightarrow \gamma \vdash_{\mathcal{N}_p} \alpha \leftrightarrow \gamma$