MD 13/AGO/2018

HOJE: APRESENTAÇÃO DO CURSO!

PÁGINA DO CURSO (AINDA NÃO EXISTE, MAS VOU CRIÁ-LA EM BREVE):
http://angg.twu.net/2018.2-MD.html

OU: GOOGLE POR "EDUARDO OCHS", VÁ PARA QUALQUER SUBPÁGINA DO angg.twu.net, E CLIQUE EM "MD" NA BARRA DE NAVEGAÇÃO À ESQUERDA.

LIVRO:
SCHEINERMAN
(TEM NA BIBLIOTECA)

DICA: XEROQUEM O CAP. 1!

DEFINIÇÕES (PRIMO, DIVISIBILIDADE ...)
E PROVAS DE TEOREMAS
MILHARES DE DETALHES.

TOU PREPARANDO LISTAS DE EXERCÍCIOS QUE <u>COMPLEMENTAM</u> O LIVRO.

<u>AVISO</u>
(EU NÃO TENHO LAUDO MÉDICO DISSO, MAS)
EU TENHO <u>MUITA</u> DIFICULDADE COM TERMOS COMO LÁ, ELE, ELA, ISSO.

DICAS PRO 4:
NOMES DAS OPERAÇÕES:
"$\land$": "E"
"$\lor$": "OU"
"$\to$": "IMPLICA"
"$\neg$": "NÃO"

x	y	$x \land y$	$x \lor y$	$\neg x$	$x \to y$
F	F	F	F	V	V
F	V	F	V	V	V
V	F	F	V	F	F
V	V	V	V	F	V

6l) $\forall x \in \{1,2,3,4\}.\ x^2 < 10$

$= (x^2<10)[x:=1]$
$\land\ (x^2<10)[x:=2]$
$\land\ (x^2<10)[x:=3]$
$\land\ (x^2<10)[x:=4]$
$= \underbrace{\underbrace{\underbrace{V \land V}_{V} \land V}_{V} \land F}_{F}$

$(x^2<10)[x:=1]$
$= 1^2 < 10$
$= 1 < 10$
$= V$

6m) $\forall x \in \{1,2,3,4\}.\ V$

$= V[x:=1]$
$\land\ V[x:=2]$
$\land\ V[x:=3]$
$\land\ V[x:=4]$
$= V \land V \land V \land V$
$= V$

5c) $\left(\sum_{a=3}^{4} 10a\right) + 1$
$= (10\cdot 3 + 10\cdot 4) + 1$
$= (30 + 40) + 1$
$= 70 + 1$
$= 71$

5a) JEITO 1:
(PRA QUEM LEMBRA Σ):
$\sum_{i=1}^{5} i = 1+2+3+4+5$

JEITO 2:
(USANDO SUBSTITUIÇÃO):
$\sum_{i=1}^{5} i = i[i:=1]$
$+\ i[i:=2]$
$+\ i[i:=3]$
$+\ i[i:=4]$
$+\ i[i:=5]$
$= 1+2+3+4+5$

$\boxed{\text{MD 14/AGO/2018}}$

HOJE: INTRODUÇÃO AO CURSO!

$\boxed{\text{LISTA L1!}}$

PÁGINA DO CURSO (AINDA NÃO! !! ☹)

GOOGLEM POR "EDUARDO OCHS", ENTREM EM QUALQUER SUBPÁGINA DO http://angg.twu.net/ E CLIQUEM EM "MD" NA BARRA DE NAVEGAÇÃO À ESQUERDA...

$$
\begin{aligned}
6m)\ & \forall x \in \{1,2,3,4\}.\, V \\
&= V[x:=1] \\
&\quad \land V[x:=2] \\
&\quad \land V[x:=3] \\
&\quad \land V[x:=4] \\
&= \underbrace{\underbrace{V \land V}_{V} \land \underbrace{V \land V}_{V}}_{V} \\
&= V
\end{aligned}
$$

$4[x:=1] = 4$

$V[x:=1] = V$

MD 15/AGO/2018

HOJE: COISAS PRA AJUDAR VOCÊS A ENTENDEREM AS SEÇÕES 1.1, 1.2 E 1.3 DO LIVRO !!

DICA: FAÇAM OS EXERCÍCIOS DA SEÇÃO 1.5 EM CASA - MUITOS DELES SÃO BEM FÁCEIS E SE VOCÊS TIVEREM PRÁTICA SUFICIENTE COM ÁLGEBRA DE BOOLE PRA FAZER CONTAS DE CABEÇA ISSO VAI AJUDAR MUITO.

SEÇÃO 1: DEFINIÇÕES
O LIVRO FAZ TUDO "EM PORTUGUÊS" - NA VERDADE NUMA MISTURA DE NOTAÇÃO MATEMÁTICA E PORTUGUÊS.

"UM INTEIRO"
X É INTEIRO $\Leftrightarrow$ $x \in \mathbb{Z}$
"É PAR"
X É PAR
$\Leftrightarrow$ X É DIVISÍVEL POR 2

SE $a, b \in \mathbb{Z}$,
a É DIVISÍVEL POR b
$\Leftrightarrow$ SE EXISTE $c \in \mathbb{Z}$ COM $bc = a$
(NOTAÇÃO: $b|a$
PRONÚNCIA "b DIVIDE a")

SE $a, b \in \mathbb{Z}$
DEF: $b|a \Leftrightarrow \exists c \in \mathbb{Z}.\ bc = a$

OBS: O LIVRO AINDA NÃO INTRODUZIU OS SÍMBOLOS "∃" E "∀" - ELE TÁ USANDO PORTUGUÊS - E A GENTE VAI USAR UMA NOTAÇÃO UM POUCO DIFERENTE DA DELE, COM UM "." COMO SEPARADOR.

SE $a, b \in \mathbb{Z}$,
DEF: a É DIVISÍVEL POR b,
OU: b DIVIDE a,
OU: $b|a$,
$\underbrace{\text{SE E SÓ SE}}_{\text{"}\Leftrightarrow\text{"}}$: $\exists c \in \mathbb{Z}.\ bc = a$

ESSA DEFINIÇÃO DE "DIVISÍVEL" DEVERIA SERVIR PRA CALCULAR COISAS TIPO:

$2|4 = V$
$3|4 = F$
$4|2 = F$
$-2|4 = ?$

$(-2|4) = (\exists c \in \mathbb{Z}.\ (-2)\cdot c = 4)$
$(\underbrace{-2}_{b}|\underbrace{4}_{a}) = (\exists c \in \{\ldots, -2, -1, 0, 1, 2, \ldots\}.\ (-2)\cdot c = 4)$
$= \ldots$
$\lor ((-2)\cdot c = 4)[c := -2]$
$\lor ((-2)\cdot c = 4)[c := -1]$
$\lor ((-2)\cdot c = 4)[c := 0]$
$\lor \ldots$
$= \ldots$
$\lor V$
$\lor F$
$\lor F$
$\lor \ldots$
$= \ldots \lor V \lor F \lor F \lor \ldots$
$= V$

... NESSE PONTO EU ACHO QUE O LIVRO COMPLICA AS COISAS UM POUCO - SERIA MELHOR COMEÇAR COM EXEMPLOS EM QUE TUDO É FINITO...

IMPORTANTE
"$b|a$", "b DIVIDE a", TEM:
- UM SIGNIFICADO "INTUITIVO"
- UMA DEFINIÇÃO FORMAL QUE DEVE (!?!?) CORRESPONDER AO SIGNIFICADO INTUITIVO...

(A DEFINIÇÃO FORMAL ESCLARECE O SIGNIFICADO INTUITIVO EM CASOS DE DÚVIDA...)

OBS:
$10 | 201 = ?$
(DÁ PRA VER QUE $10\cdot 20 = 200 < 201$, $10 \cdot 21 = 210 > 201$...)

LINK PRO GRUPO DO TELEGRAM:
https://bit.ly/2MSTSGU

MAIS DEFINIÇÕES:
DEF: a É ÍMPAR SE E SÓ SE $\exists x \in \mathbb{Z}.\ a = 2x+1$
DEF: p É PRIMO SE E SÓ SE:
$p \in \mathbb{Z}$,
$p > 1$,
"OS ÚNICOS DIVISORES POSITIVOS DE p SÃO 1 E p".

OU: p É PRIMO SE E SÓ SE:
$p \in \mathbb{Z}$, $p > 1$,
$(\forall b \in \mathbb{Z}.\ (b|p \land b > 1 \to b = p))$

$N \neq \mathbb{N}$!!!

$\mathbb{N}$

M.D. 15/ago/2018

Hoje: coisas pra ajudar vocês a entenderem as seções 1.1 e 1.2 do livro!

O livro faz tudo numa mistura de português com notação matemática... Às vezes as coisas ficam mais claras se a gente usa uma notação matemática mais "pura".

1. Definição

"Um inteiro" $\Rightarrow$

"x é um inteiro" $\Rightarrow$

$x \in \mathbb{Z}$

Obs: $\mathbb{N} = \{0,1,2,\ldots\}$ ("naturais")

$\mathbb{Z} = \{\ldots,-2,-1,0,1,2,\ldots\}$ ("inteiros")

$\mathbb{Q}$ ("racionais")

$\mathbb{R}$ ("reais")

Vamos usar estes bem pouco em MD.

Monitor: Matheus Lobo
Grupo: https://bit.ly/2MSTSGU
"Matemática Discreta 2018"

1.1 "Par"

$x \in \mathbb{Z}$ é par se x é divisível por 2;
Se $x \in \mathbb{Z}$, x é par se e só se x é divisível por 2

1.2 "Divisível"

Se $a, b \in \mathbb{Z}$,
Def: a é divisível por b,
ou: b divide a,
ou: $b | a$
(pronúncia: "b divide a")

Quando: $\exists c \in \mathbb{Z}.\ bc = a$

$\Leftrightarrow$

Repare que a gente tinha uma noção intuitiva do que era "ser divisível"... agora a gente tem uma definição formal, que deve coincidir com a noção intuitiva (tomara!), e que nos ajuda a decidir casos em que a gente poderia ter dúvidas...

$2|4 = V$
$3|4 = F$
$4|2 = F$
$-2|4 =$

...Vamos calcular

$\underbrace{-2}_{b} | \underbrace{4}_{a}$!

$$(-2|4) = (\exists c \in \mathbb{Z}. (-2)c = 4)$$
$$= (\exists c \in \{\ldots,-2,-1,0,1,2,\ldots\}. (-2)c = 4)$$
$$= \ldots$$
$$\vee ((-2)c = 4)[c:=-2]$$
$$\vee ((-2)c = 4)[c:=-1]$$
$$\vee ((-2)c = 4)[c:=0]$$
$$\vee ((-2)c = 4)[c:=1]$$
$$\vee ((-2)c = 4)[c:=2]$$
$$\ldots$$
$$= \ldots$$
$$\vee V$$
$$\vee F$$
$$\vee F$$
$$\vee F$$
$$\vee F$$
$$\ldots$$
$$= V$$

~~1.4 "Ímpar"~~

Se $a \in \mathbb{Z}$,
Def: a é ímpar
se e só se: $\exists x \in \mathbb{Z}.\ 2x+1 = a$.

$\Leftrightarrow$

?!?!

Obs: A definição de par que a gente viu é equivalente a esta aqui:

Se $a \in \mathbb{Z}$,
Def: a é par
se e só se $\exists x \in \mathbb{Z}.\ 2x = a$.

1.5 "Primo"

Se $p \in \mathbb{Z}$,
Def: p é primo
Quando: $\forall d \in \mathbb{Z}. ((d|p \wedge d > 0) \to (d = 1 \vee d = p))$

MD 20/AGO/2018

HOJE:

- MARCAR HORÁRIO DE ATENDIMENTO
- SEÇÕES DO LIVRO: "TEOREMA", "PROVA"

SOBRE A SEÇÃO 2 ("TEOREMA")

DEF: $b|a$ ("b divide a") se e só se $\exists c \in \mathbb{Z}.\ bc=a$

OUTRA NOTAÇÃO:

$$b|a \ := \ \exists c \in \mathbb{Z}.\ bc=a$$
$$\mathrm{par}(x) \ := \ \exists a \in \mathbb{Z}.\ 2a=x$$
$$\mathrm{impar}(x) \ := \ \exists a \in \mathbb{Z}.\ 2a+1=x$$
$$\mathrm{primo}(x) \ := \ x \in \mathbb{Z} \ \wedge\ 1<x \ \wedge\ \forall d \in \mathbb{Z}.\ (d|x \to d=1 \vee d=x)$$

(VER P.4)

OS TEOREMAS DO LIVRO TODOS COMEÇAM COM ALGO COMO:

SE X É UM INTEIRO PAR...

LEMBRE QUE "SE... ENTÃO" É TRADUZIDO PRA "$\to$"

SE X É UM INTEIRO PAR ENTÃO X+1 É ÍMPAR.

$$\Rightarrow (x \in \mathbb{Z} \wedge \mathrm{par}(x)) \to \mathrm{impar}(x+1)$$

... LEMBREM QUE A L2 TEM UMA DISCUSSÃO SOBRE VARIÁVEIS...

PODEMOS ENTENDER ESSE TEOREMA COMO:

$$\forall x \in \mathbb{Z}.\ (\mathrm{par}(x) \to \mathrm{impar}(x+1))$$

... E ISSO VIRA ALGO QUE A GENTE SABE CALCULAR (EXCETO PELO PROBLEMA DE QUE EXISTEM INFINITOS $x \in \mathbb{Z}$...)

E SE (☆) É UM TEOREMA QUANDO NÓS CALCULARMOS O (☆) O RESULTADO DEVE SER V...

NA VERDADE A GRAÇA DE UM TEOREMA É QUE ELE NOS DIZ QUE ALGO QUE DARIA UM TRABALHÃO PRA CALCULAR É V!...

NESSE CASO O (☆) DIZ QUE:

$$\vdots$$
$$\mathrm{par}(-3) \to \mathrm{impar}(-3+1),$$
$$\mathrm{par}(-2) \to \mathrm{impar}(-2+1),$$
$$\mathrm{par}(-1) \to \mathrm{impar}(-1+1),\ \ldots$$
$$\vdots$$

UMA DAS UTILIDADES DO "$\to$" É INDICAR "QUE CASOS INTERESSAM"...

$$(☆)\quad \underbrace{\underbrace{\mathrm{par}(-3)}_{F} \to \mathrm{impar}(-3+1)}_{V}$$

O CASO $x=-3$ "NÃO INTERESSA".

P.13: $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.\ (x|y \wedge y|x \to x=-y \vee x=y)$

CASOS: $x=-5,\ y=5,$
$x=4,\ y=4,$
$x=0,\ y=0$

PROVA (SEC. 3)

O LIVRO MOSTRA UM MODO DE DIVIDIR UMA PROVA EM VÁRIOS PASSOS (NUMERADOS)...

A GENTE JÁ VIU ALGO BEM PARECIDO COM ESSE JEITO DE FAZER PROVAS (MAS BEM MAIS SIMPLES)...

PRA RESOLVER SISTEMAS A GENTE COMEÇA COM ALGUMAS HIPÓTESES E A GENTE VAI OBTENDO MAIS "VERDADES" A PARTIR DELAS - ELAS SÃO CONSEQUÊNCIAS DAS LINHAS ANTERIORES...

... E A GENTE ÀS VEZES ESCREVE À DIREITA DE CADA LINHA O QUE A GENTE USOU PRA CONCLUIR ELA.

EM SISTEMAS A GENTE TEM BEM POUCOS MODOS DE OBTER VERDADES NOVAS...

1. SUPONHA $x,y \in \mathbb{R}$.
2. SUPONHA $3x+4y=11$.
3. SUPONHA $5x+6y=17$.
4. ENTÃO $4y=11-3x$. (POR 2)
5. ENTÃO $y=\frac{11}{4}-\frac{3}{4}x$. (POR 5)
6. ENTÃO $5x+6(\frac{11}{4}-\frac{3}{4}x)=17$. (POR 3 E 5)
7. ENTÃO $5x+\frac{2}{3}(11-3x)=17$. (POR 6)
8. ENTÃO $15x+22-6x=51$. (POR 7)
9. ENTÃO $9x=29$

$0=1$

MD 20/AGO/2018

HOJE:
- MARCAR HORÁRIO DE ATENDIMENTO (POR ENQUANTO: TERÇAS 18-20)

VOU REESCREVER A PROVA DA PROPOSIÇÃO 3.2 (P. 18) USANDO UMA LINGUAGEM DIFERENTE E USANDO UMA NUMERAÇÃO DIFERENTE PRAS LINHAS.

(1) VAMOS MOSTRAR QUE $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.\ \mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$.

(2) SUPONHA $x \in \mathbb{Z}$, $y \in \mathbb{Z}$.

(3) SUPONHA $\mathrm{par}(x) \land \mathrm{par}(y)$.

(4) ENTÃO $2|x$. (POR (3) E PELA DEF.)

(5) ENTÃO $2|y$. (POR (3) E PELA DEF.)

(6) ENTÃO $\exists a \in \mathbb{Z}.\ 2a = x$ (POR (4) E PELA DEF.)

(7) ENTÃO $\exists b \in \mathbb{Z}.\ 2b = y$ (POR (5) E PELA DEF.)

(8) SUPONHA $a \in \mathbb{Z}$ COM $2a = x$. (POR (6))

(9) SUPONHA $b \in \mathbb{Z}$ COM $2b = y$. (POR (7))

(10) ENTÃO $2a + 2b = x + y$ (POR (8) E (9))

(11) ENTÃO $2(a+b) = x+y$. (POR (10))

(12) ENTÃO $\exists c \in \mathbb{Z}.\ 2c = x+y$ (POR (11) COM $c = a+b$, E POR (8) E (9))

(13) ENTÃO $2|x+y$ (POR (12) E DEF)

(14) ENTÃO $\mathrm{par}(x+y)$ (POR (13) E DEF)

(15) ENTÃO $\mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$

(16) ENTÃO $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.\ \mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$.

OBS: ISTO AQUI É VERDADE?
$(\exists a \in \mathbb{Z}.\ 2a = 6) \land (\exists a \in \mathbb{Z}.\ 2a = 8)$
E ISTO?
$(\exists a \in \mathbb{Z}.\ 2a = 6 \land 2a = 8)$

$$
\begin{aligned}
&(\exists a \in \mathbb{Z}.\ 2a = 6) \\
&= \ldots \lor (2a = 6)[a := 2] \\
&\quad \lor (2a = 6)[a := 3] \\
&\quad \lor (2a = 6)[a := 4] \\
&\quad \lor \ldots \\
&= \ldots \lor F \lor V \lor F \lor \ldots \\
&= V
\end{aligned}
$$

$$
\begin{aligned}
&(\exists a \in \mathbb{Z}.\ 2a = 8) \\
&= \ldots \lor (2a = 8)[a := 2] \\
&\quad \lor (2a = 8)[a := 3] \\
&\quad \lor (2a = 8)[a := 4] \\
&\quad \lor \ldots \\
&= \ldots \lor F \lor F \lor V \lor \ldots \\
&= V
\end{aligned}
$$

A GRANDE NOVIDADE DESSE MÉTODO DE FAZER PROVAS É QUE HIPÓTESES ("SUPONHA"S) PODEM SER TEMPORÁRIAS!

(3) SUPONHA $\mathrm{PAR}(x) \land \mathrm{PAR}(y)$

⋮

(14) ENTÃO $\mathrm{PAR}(x+y)$

(15) ENTÃO $\mathrm{PAR}(x) \land \mathrm{PAR}(y) \to \mathrm{PAR}(x+y)$

... A PARTIR DA LINHA (15) A HIPÓTESE (3) NÃO EXISTE MAIS! ELA NÃO É MAIS UMA HIPÓTESE - ELA FOI "INCLUÍDA NA CONCLUSÃO"...

NA LINHA 16 IDEM.

A GENTE PODE INDICAR EM CADA LINHA QUAIS SÃO AS HIPÓTESES QUE ELA "FECHA"...

(15) ENTÃO $\mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$ (FECHA HIPS (9), (8), (3))

EXERCÍCIOS PRA AGORA:

(1) ESCREVA A PROVA DA PROP. 3.3 NO FORMATO QUE EU MOSTREI (COM "SUPONHA"S E "ENTÃO"S).

(2) IDEM PRA PROVA DA PROP. 3.4.

(3) IDEM PRA 3.5.

(4) FAÇA OS EXERCÍCIOS DA P. 24.

(1) SUPONHA $x \in \mathbb{Z}$, $x > 2$, $\mathrm{par}(2)$.

(2) ENTÃO $\exists p, q.\ \mathrm{primo}(p) \land \mathrm{primo}(q) \land p+q = x$.

NÃO!!! CASO "ENTÃO" DEVE SER ÓBVIO...

HOJE: COISAS PRA AJUDAR VOCÊS A ENTENDEREM AS SEÇÕES 2 ("TEOREMA") E 3 ("PROVA") DO LIVRO.

AVISO: MARQUEI UM HORÁRIO DE ATENDIMENTO - 3as 18-20 (POR ENQUANTO!)... NÃO TEM LOCAL DEFINIDO, MANDEM MENSAGEM PELO TELEGRAM!

O LIVRO SEMPRE USA UMA LINGUAGEM QUE ESTÁ BEM MAIS PRA "PORTUGUÊS" DO QUE PRA "NOTAÇÃO MATEMÁTICA"...

LEMBREM QUE A LISTA 2 TINHA COISAS (CONVENÇÕES) SOBRE VARIÁVEIS...

ALGUMAS DEFINIÇÕES (NUMA LINGUAGEM MAIS MATEMÁTICA QUE A DO LIVRO):

DEF: x É INTEIRO QUANDO $x \in \mathbb{Z}$
$\Leftrightarrow$,
iff,
SE E SÓ SE

DEF: SE $a, b \in \mathbb{Z}$ (p.3)
ENTÃO $b|a$ (PRONÚNCIA: "b DIVIDE a")
QUANDO $\exists c \in \mathbb{Z}.\ bc = a$.
(OBS: $(2.3 \mid 4.6) =$ ERRO)

DEF: a É PAR
OU: $\mathrm{par}(a)$
QUANDO $\exists x \in \mathbb{Z}.\ 2x = a$

DEF: a É ÍMPAR
OU: $\mathrm{impar}(a)$
QUANDO $\exists x \in \mathbb{Z}.\ 2x+1 = a$

DEF: p É PRIMO
OU: $\mathrm{primo}(p)$
QUANDO: $p \in \mathbb{Z}$
$\land\ p > 1$
$\land\ \forall d \in \mathbb{Z}.\ (d|p \to d \leq 1 \lor d = p)$

$\underbrace{2|4}_{V} \to \underbrace{\underbrace{2 \leq 1}_{F} \lor \underbrace{2=4}_{F}}_{F}$

OBS:
ATÉ AGORA NÓS VIMOS COMO CALCULAR EXPRESSÕES COM "$\forall$" E "$\exists$" USANDO CÓPIAS E SUBSTITUIÇÕES... ÀS VEZES A GENTE TEM INFINITAS CÓPIAS.

$\forall d \in \mathbb{Z}.\ (d|4 \to d \leq 1 \lor d = 4)$

VIRA INFINITAS CÓPIAS, E SÓ ESTA

$(d|4 \to d \leq 1 \lor d = 4)[d := 2]$

DÁ F.

NA PARTE SOBRE PROVAS A GENTE VAI VER OUTROS MODOS DE CALCULAR ("PROVAR") EXPRESSÕES COM $\forall$ E $\exists$.

DICA IMPORTANTE: FAÇAM OS EXERCÍCIOS DA SEÇÃO 2!

OBS: O "$\to$" TEM VÁRIAS PRONÚNCIAS, INCLUINDO "SE-ENTÃO" E UMA DAS UTILIDADES DELE É RESTRINGIR O FOCO AOS CASOS EM QUE O LADO ESQUERDO É VERDADE...

$\underbrace{\underset{F}{A} \to \underset{?}{B}}_{V}$

"$A \to B$" TAMBÉM PODE SER ENTENDIDO COMO "TODA VEZ QUE A É VERDADE O B VAI SER VERDADE TAMBÉM".

OUTRA COISA IMPORTANTE DA SEÇÃO 2 (p.13):

$\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.$
$(x|y \land y|x \to x = y \lor x = -y)$ (☆)

CASOS INTERESSANTES:
$x = 2,\ y = 4$
$x = 3,\ y = 3$
$x = 5,\ y = -5$

$\underbrace{(\underbrace{\underbrace{5|-5}_{V} \land \underbrace{-5|5}_{V}}_{V} \to \underbrace{\underbrace{5=-5}_{F} \lor \underbrace{5=-(-5)}_{V}}_{V})}_{V}$

$(5|-5)$
$= (b|a)[b:=5,\ a:=-5]$
$= (\exists c \in \mathbb{Z}.\ bc = a)[b:=5,\ a:=-5]$
$= (\exists c \in \mathbb{Z}.\ 5c = -5)$
$= \ldots \lor (5c=-5)[c:=-2]$
$\lor (5c=-5)[c:=-1]$
$\lor (5c=-5)[c:=0]$
$\lor \ldots$

$= \ldots F \lor V \lor F \lor \ldots = V$

~~AFIRMAÇÃO 2.2 (p.13)~~

DEF: x É QUADRADO,
OU: $\mathrm{quad}(x)$
QUANDO $\exists a \in \mathbb{Z}.\ x = a^2$.

AFIRMAÇÃO 2.2:
$\forall x \in \mathbb{Z}.\ (\mathrm{quad}(x) \land \mathrm{primo}(x) \to x < 0)$.

(PENSEM NISSO EM CASA!)

PROVAS (OU: DEMONSTRAÇÕES)

VAMOS TENTAR ENTENDER A PROVA DA PROP. 3.2 NA P.18... (EM 10 PASSOS)

VOCÊS JÁ VIRAM UM MODO DE FAZER PROVAS PARECIDO COM ESTE, MAS QUE É BEM MAIS SIMPLES... "SISTEMAS".

EM "SISTEMAS" VOCÊS APRENDERAM A COMEÇAR COM CERTAS HIPÓTESES (EQUAÇÕES) E OBTER CERTAS CONSEQUÊNCIAS DELAS - E EM POUCOS PASSOS A GENTE CONSEGUE OS VALORES DAS VARIÁVEIS.

EXEMPLO:
1. SUPONHA $x \in \mathbb{R},\ y \in \mathbb{Z}$.
2. SUPONHA $3x + 4y = 11$.
3. SUPONHA $5x + 6y = 17$.
4. ENTÃO $15x + 20y = 55$. (POR 2)
5. ENTÃO $15x + 18y = 51$. (POR 3)
6. ENTÃO $2y = 4$. (POR (4) E 5).
7. ENTÃO $y = 2$. (POR 6)
8. ENTÃO $3x + 4 \cdot 2 = 11$ (POR 2 E 7).
9. ENTÃO $3x = 11 - 8 = 3$ (POR 8)
10. ENTÃO $x = 1$ (POR 9)

MD 21/AGO/2018

TRADUÇÃO DA PROVA DA P. 18 PRA UMA LINGUAGEM MAIS "REGULAR"/"HOMOGÊNEA" E QUE DÊ PRA RECONHECER MAIS PADRÕES...

(OBS: A NUMERAÇÃO DOS PASSOS VAI MUDAR!)

1. VAMOS MOSTRAR QUE $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.$ $\mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$.
2. SUPONHA $x \in \mathbb{Z}$, $y \in \mathbb{Z}$.
3. SUPONHA $\mathrm{par}(x)$, $\mathrm{par}(y)$.
4. ENTÃO $2 | x$. (POR 3 E PELA DEF. DE PAR)
5. ENTÃO $2 | y$. (POR 3 E PELA DEF)
6. ENTÃO $\exists a \in \mathbb{Z}.\ 2a = x$. (POR 4 E PELA DEF.)
7. ENTÃO $\exists b \in \mathbb{Z}.\ 2b = y$. (POR 5 E PELA DEF.)
8. SUPONHA $a \in \mathbb{Z}$, $2a = x$. (POR 6)
9. SUPONHA $b \in \mathbb{Z}$, $2b = y$ (POR 7)
10. ENTÃO $2a + 2b = x + y$ (POR 8 E 9)
11. ENTÃO $2(a+b) = x + y$ (POR 10)
12. ENTÃO $a + b \in \mathbb{Z}$ (POR 8 E 9)
13. ENTÃO $\exists c \in \mathbb{Z}.\ 2c = x + y$ (POR 11 E 12 COM $c = a+b$)
14. ENTÃO $2 | x + y$ (POR 13 E PELA DEF)
15. ENTÃO $\mathrm{par}(x+y)$ (POR 14 E PELA DEF)
16. ENTÃO $\mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$ (POR 15; FECHA 9, 8, 3)
17. ENTÃO $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.$ $\mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$ (POR 16, FECHA 2).

EXERCÍCIOS (PRA AGORA):

CALCULEM:

a) $(\exists a \in \mathbb{Z}.\ 2a = 6) \wedge (\exists a \in \mathbb{Z}.\ 2a = 8)$

b) $\exists a \in \mathbb{Z}.\ (2a = 6 \wedge 2a = 8)$.

GRANDE TRUQUE

AS LINHAS 2, 3, 8, 9 SÃO "SUPONHA"S; ELAS "INTRODUZEM HIPÓTESES".

A LINHA 16 ELA "FECHA" AS HIPÓTESES DA LINHA 3...

NA VERDADE UMA DAS REGRAS DO SISTEMA DEDUTIVO QUE A GENTE ESTÁ USANDO É QUE AS HIPÓTESES TEM QUE SER FECHADAS <u>EM ORDEM</u>.

OBS:

1. SUPONHA $x \in \mathbb{Z}$, $\mathrm{par}(x)$, $x > 2$.
2. ENTÃO $\exists a, b \in \mathbb{Z}.\ \mathrm{primo}(a) \wedge \mathrm{primo}(b) \wedge a + b = x$

MD 26/ago/2018

Na aula passada nós vimos uma demonstração que tinha um monte de passos "suponha"...

Suponha $x\in\mathbb{Z}$, $y\in\mathbb{Z}$
Suponha $\mathrm{par}(x)$, $\mathrm{par}(y)$
Suponha $a\in\mathbb{Z}$, $2a=x$
Suponha $b\in\mathbb{Z}$, $2b=y$...

Acho que o melhor modo da gente entender o <u>contexto</u> em que a gente está depois desses "suponha"s é vendo uma coisa que estava um pouco adiante no programa: <u>conjuntos</u>.

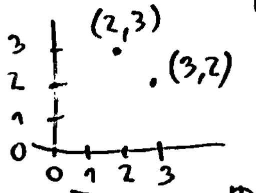
Idéia: <u>quais</u> (não "quantos") são os modos de escolher $x\in\{1,2,3,4\}$ e $y\in\{2,3,4,5\}$ com $x\le y$?

Vamos ter "geradores" que geram todos os valores de x em $\{1,2,3,4\}$ e y em $\{2,3,4,5\}$ e um "filtro" que só aceita casos com $x\le y$.

Notações:

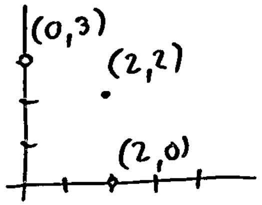
$$\{\underbrace{x\in\{1,2,3,4\}}_{\text{gerador}},\ \underbrace{y\in\{2,3,4,5\}}_{\text{gerador}},\ \underbrace{x\le y}_{\text{filtro}};\ \underbrace{(x,y)}_{\text{resultado ("expressão")}}\}$$

Obs: $(2,3)$ e $(3,2)$



são pontos distintos de $\mathbb{R}^2$ — a ordem das componentes <u>importa</u>.

Em conjuntos a ordem não importa:



$= \{(0,3),(2,2),(2,0)\}$
$= \{(2,0),(2,2),(0,3)\}$

Avisos:

1. Tem uma folha 8 com mais exercícios
2. Tem um gabarito que eu posso mostrar mas não vou distribuir por enquanto
3. Na aula que vem nós vamos usar este conjunto pra entender os "suponha"s da aula passada:

$$\{x\in\mathbb{Z},\ y\in\mathbb{Z},\ \mathrm{par}(x),\ \mathrm{par}(y),\ a\in\mathbb{Z},\ b\in\mathbb{Z},\ 2a=x,\ 2b=y;\ (x,y,a,b)\}$$

Importante:

A folha 5 explica a notação com ";" —

$\{\_,\_,\_;\_\}$

e <u>duas</u> notações diferentes com "|":

$\{\_|\_,\_,\_\}$ e $\{\_|\_\}$

A folha 8 vai ter exercícios sobre as notações com "|" — que são as que vocês vão encontrar nos livros — e sobre <u>produto cartesiano</u>.

Por exemplo:

$$\mathbb{R}^2 = \underbrace{\mathbb{R}}_{\text{cjto}}\times\underbrace{\mathbb{R}}_{\text{cjto}} = \{x\in\mathbb{R},\ y\in\mathbb{R};\ (x,y)\}$$

MD /AGO/2018

NA AULA PASSADA NÓS VIMOS UMA DEMONSTRAÇÃO COM VÁRIOS "SUPONHAS" NO MEIO DELA...

SUPONHA:

$x \in \mathbb{Z}$, $y \in \mathbb{Z}$,
$\mathrm{par}(x)$, $\mathrm{par}(y)$
$a \in \mathbb{Z}$, $2a = x$
$b \in \mathbb{Z}$, $2b = y$ ...

O MELHOR MODO DA GENTE ENTENDER O QUE ELES "QUEREM DIZER" – DE UM JEITO QUE NOS AJUDE A DEBUGAR AS NOSSAS DEMONSTRAÇÕES – USA CONJUNTOS.

IDÉIA: COMO É QUE A GENTE DESCOBRE QUAIS SÃO AS POSSIBILIDADES – "QUAIS", NÃO "QUANTAS" – DE TERMOS $x \in \{1,2,3,4\}$, $y \in \{2,3,4,5\}$, E $x \leq y$?

TEMOS QUE GERAR OS VALORES POSSÍVEIS PRA x, OS VALORES POSSÍVEIS PRA y, E FILTRAR AS COMBINAÇÕES E DEIXAR PASSAR SÓ AS QUE OBEDECEM $x \leq y$...

EM NOTAÇÃO DE CONJUNTOS ISSO VIRA:

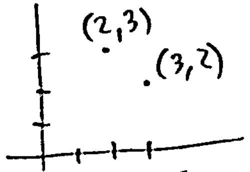
$$\{\underbrace{x \in \{1,2,3,4\}}_{\text{GERADOR}},\ \underbrace{y \in \{2,3,4,5\}}_{\text{GERADOR}},\ \underbrace{x \leq y}_{\text{FILTRO}};\ \underbrace{(x,y)}_{\substack{\text{RESULTADO} \\ \text{("EXPRESSÃO")}}}\}$$

PRA ENTENDER OS "SUPONHA"S DA AULA PASSADA NÓS VAMOS USAR – NA AULA QUE VEM – ESSE CONJUNTO AQUI:

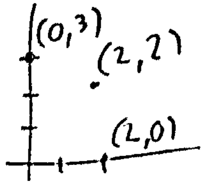
$$\{x \in \mathbb{Z},\ y \in \mathbb{Z},\ \mathrm{par}(x),\ \mathrm{par}(y),\ a \in \mathbb{Z},\ b \in \mathbb{Z},\ 2a = x,\ 2b = y;\ (x,y,a,b)\}$$

OBS: EM LISTAS A ORDEM IMPORTA:

$(2,3) \neq (3,2)$ ...



EM CONJUNTOS A ORDEM NÃO IMPORTA, E NEM REPETIÇÕES:



$= \{(0,3),(2,2),(2,0)\}$
$= \{(2,0),(2,2),(0,3)\}$
$= \{(2,0),(2,2),(0,3),(0,3)\}$

MD 27/AGO/2018

HOJE: EXERCÍCIOS DE DEMONSTRAÇÕES, PRA ENTREGAR! NÃO VALE NOTA, É SÓ PRA EU DESCOBRIR AS DÚVIDAS DE VOCÊS!

FAÇAM NO LADO EM BRANCO DAS FOLHAS DE RASCUNHO A4 QUE EU TROUXE.

TENTEM USAR O FORMATO COM "VAMOS VER QUE"/"SUPONHA"/"ENTÃO" QUE EU MOSTREI NO QUADRO NAS ÚLTIMAS AULAS...

VOU REESCREVER O EXEMPLO AQUI, E EXPLICAR MELHOR O TRUQUE DOS CONTEXTOS.

1. VAMOS MOSTRAR QUE $\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. \mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$.
2. SUPONHA $x \in \mathbb{Z}$, $y \in \mathbb{Z}$.
3. SUPONHA $\mathrm{par}(x), \mathrm{par}(y)$
4. ENTÃO $2|x$. (POR 3, DEF.)
5. ENTÃO $2|y$ (POR 3, DEF.)
6. ENTÃO $\exists a \in \mathbb{Z}.\ 2a = x$. (POR 4, DEF.)
7. ENTÃO $\exists b \in \mathbb{Z}.\ 2b = y$. (POR 5, DEF.)
8. SUPONHA $a \in \mathbb{Z}$, $2a = x$. (POR 6)
9. SUPONHA $b \in \mathbb{Z}$, $2b = y$. (POR 7)
10. ENTÃO $2a + 2b = x+y$. (POR 8, 9)
11. ENTÃO $2(a+b) = x+y$. (POR 10)
12. ENTÃO $a+b \in \mathbb{Z}$. (POR 8, 9)
13. ENTÃO $\exists c \in \mathbb{Z}.\ 2c = x+y$. (POR 11, 12 COM $c = a+b$) [FECHA 9, 8]
14. ENTÃO $2|x+y$. (POR 13, DEF)
15. ENTÃO $\mathrm{par}(x+y)$. (POR 14, DEF)
16. ENTÃO $\mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$. (POR 15) [FECHA 3]
17. ENTÃO $\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. \mathrm{par}(x) \wedge \mathrm{par}(y) \to \mathrm{par}(x+y)$. (POR 16) [FECHA 2]

CONTEXTOS

O CONTEXTO NA LINHA 12 (POR EXEMPLO) É FORMADO POR TODOS OS SUPONHAS ABERTOS NAQUELE PONTO. ELE PODE SER ESCRITO COMO UM GRANDE "SUPONHA",

SUPONHA $x \in \mathbb{Z}, y \in \mathbb{Z}, \mathrm{par}(x), \mathrm{par}(y), a \in \mathbb{Z}, 2a = x, b \in \mathbb{Z}, 2b = y$

OU COMO CONJUNTO:

$C_{12} = \{x \in \mathbb{Z}, y \in \mathbb{Z}, \mathrm{par}(x), \mathrm{par}(y), a \in \mathbb{Z}, 2a = x, b \in \mathbb{Z}, 2b = y; (x,y,a,b)\}$

SUGESTÕES DE EXERCÍCIOS:

(ALGUNS DELES APARECEM NO LIVRO COMO EXERCÍCIOS "MESMO", EM OUTROS O EXERCÍCIO É SÓ TRADUZI-LOS PRO NOSSO FORMATO)...

a) PROP. 3.3, P. 20

b) $\forall x \in \mathbb{Z}. \mathrm{par}(x) \to \mathrm{impar}(x+1)$

c) $\forall x \in \mathbb{Z}. \mathrm{impar}(x+1) \to \mathrm{par}(x)$

d) PROP. 3.5, P. 23

e) EXERCÍCIOS DA P. 24:

e1) EXERCÍCIO 1

e2) EXERCÍCIO 2

⋮

e13) EXERCÍCIO 13

UM MODO DE USAR CONTEXTOS

USANDO CONTEXTOS A GENTE PODE ENTENDER CADA LINHA "ENTÃO" DE UMA DEMONSTRAÇÃO COMO UMA PROPOSIÇÃO. POR EXEMPLO:

$P_{12})\ \forall (x,y,a,b) \in C_{12}.\ a+b \in \mathbb{Z}$.

SE VOCÊ CONSEGUIR MOSTRAR QUE UMA PROPOSIÇÃO DESSAS É FALSA (POR CONTRA-EXEMPLO, TALVEZ? :)) ENTÃO A SUA DEMONSTRAÇÃO TODA ESTÁ ERRADA.

UM EXEMPLO DE PROPOSIÇÃO ERRADA:

$\forall (x,y,a,b) \in C_{12}.\ \mathrm{par}(a)$.

UM CONTRA-EXEMPLO É:

$(6,10,3,5) \in C_{12}$, MAS $\mathrm{par}(3)$ É FALSO.

ALGUNS ERROS COMUNS...

A PROP. 3.3 DA P. 20 COMEÇA COM:

1. VAMOS MOSTRAR QUE $\forall a,b,c \in \mathbb{Z}.\ a|b \wedge b|c \to a|c$
2. SUPONHA $a,b,c \in \mathbb{Z}$.
3. SUPONHA $a|b \wedge b|c$.
4. ENTÃO $\exists x \in \mathbb{Z}.\ ax = b$.
5. ENTÃO $\exists y \in \mathbb{Z}.\ by = c$.

UM ERRO COMUM:

6. ENTÃO $\exists z \in \mathbb{Z}.\ az = c$.

(AQUI A GENTE PULOU OS PASSOS CORRESPONDENTES AOS 8–12 NO EXEMPLO À ESQUERDA).

OUTRO ERRO COMUM:

6. SUPONHA $a|c$.

SE A GENTE FIZER ISTO O CONTEXTO ASSOCIADO À LINHA 6 É...

$C_6 = \{a \in \mathbb{Z}, b \in \mathbb{Z}, c \in \mathbb{Z}, a|b, b|c, a|c; (a,b,c)\}$

... E A CONCLUSÃO À QUE QUERÍAMOS CHEGAR JÁ É UMA DAS NOSSAS HIPÓTESES!...

$\mathrm{impar}(x) \wedge \mathrm{impar}(y)$

$\exists a \in \mathbb{Z}.\ 2a+1 = x$

$\exists b \in \mathbb{Z}.\ 2b+1 = y$

$\underbrace{2}_{a} | \underbrace{6}_{b}$

SE $a|b$ ENTÃO $\exists x \in \mathbb{Z}.\ \underbrace{a}_{2} = \underbrace{b}_{6} x$

ENTÃO $\exists z \in \mathbb{Z}.\ c = az$ (..., COM $z = xy$)

$x = 3,\ y = 5,\ z = 2$?

MD 28/AGOSTO/2018

HOJE: EXERCÍCIOS PRA TIRAR DÚVIDAS SOBRE PROVAS/DEMONSTRAÇÕES!

NÃO VALE NOTA — É PRA GENTE TIRAR AS DÚVIDAS SOBRE COMO ESCREVER DEMONSTRAÇÕES MEIO EM SALA E MEIO FORA — ME ENTREGUEM AS DEMONSTRAÇÕES QUE VOCÊS QUISEREM PRA EU CORRIGIR EM CASA!

SUGESTÕES DE EXERCÍCIOS:
(OBS: ALGUNS APARECEM COMO EXERCÍCIOS "MESMO" NO SCHEINERMAN, OUTROS APARECEM COMO PROPOSIÇÕES LÁ E O EXERCÍCIO É VOCÊS DEMONSTRAREM ESSAS PROPOSIÇÕES USANDO O NOSSO FORMATO, COM "VAMOS VER QUE", "SUPONHA", "ENTÃO"...

a) PROP. 3.3, P. 20
b) $\forall x \in \mathbb{Z}.\ \mathrm{par}(x) \to \mathrm{impar}(x+1)$
c) $\forall x \in \mathbb{Z}.\ \mathrm{impar}(x+1) \to \mathrm{par}(x)$
d) PROP 3.3, P. 23
e) EXERCÍCIOS DA P. 24.
   e1) EXERCÍCIO 1
   e2) EXERCÍCIO 2
   ... e13) EXERCÍCIO 13

UMA DEMONSTRAÇÃO NO NOSSO FORMATO:

1. VAMOS VER QUE $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.$ $\mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$.
2. SUPONHA $x \in \mathbb{Z}$, $y \in \mathbb{Z}$.
3. SUPONHA $\mathrm{par}(x) \land \mathrm{par}(y)$.
4. ENTÃO $2 | x$. (POR 3, DEF.)
5. ENTÃO $2 | y$. (POR 3, DEF.)
6. ENTÃO $\exists a \in \mathbb{Z}.\ 2a = x$. (POR 4, DEF.)
7. ENTÃO $\exists b \in \mathbb{Z}.\ 2b = y$. (POR 5, DEF.)
8. SUPONHA $a \in \mathbb{Z}$, $2a = x$.
9. SUPONHA $b \in \mathbb{Z}$, $2b = y$.
10. ENTÃO $2a + 2b = x + y$. (POR 8, 9)
11. ENTÃO $2(a+b) = x + y$. (POR 10)
12. ENTÃO $a + b \in \mathbb{Z}$. (POR 8, 9)
13. ENTÃO $\exists c \in \mathbb{Z}.\ 2c = x + y$. (POR 12, 11 COM $c := a+b$) (FECHA 9, 8)
14. ENTÃO $2 | x + y$. (POR 13, DEF)
15. ENTÃO $\mathrm{par}(x+y)$. (POR 14, DEF)
16. ENTÃO $\mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$. (POR 15) (FECHA 3)
17. ENTÃO $\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.$ $\mathrm{par}(x) \land \mathrm{par}(y) \to \mathrm{par}(x+y)$. (POR 16) (FECHA 2)

CONTEXTOS

O CONTEXTO DA LINHA 12 (POR EXEMPLO) É FORMADO POR TODOS OS SUPONHAS ABERTOS ATÉ A LINHA 12 — OS DAS LINHAS 2, 3, 8, 9.

UM CONTEXTO É ALGO QUE PODE SER ESCRITO DO LADO ESQUERDO DE UM ";" NUM $\{\_\_;\_\_\}$. O CONTEXTO DA LINHA 12 É:

$x \in \mathbb{Z}, y \in \mathbb{Z}, \mathrm{par}(x) \land \mathrm{par}(y),$
$a \in \mathbb{Z}, 2a = x, b \in \mathbb{Z}, 2b = y.$

NOTE QUE ELE É FEITO DE GERADORES E FILTROS!

ÀS VEZES VAMOS INTERPRETAR UM CONTEXTO COMO UM CONJUNTO:

$$C_{12} = \{x \in \mathbb{Z}, y \in \mathbb{Z}, \mathrm{par}(x) \land \mathrm{par}(y), a \in \mathbb{Z}, 2a = x, b \in \mathbb{Z}, 2b = y; (x, y, a, b)\}.$$

CADA LINHA COM "ENTÃO" PODE SER INTERPRETADA COMO UMA PROPOSIÇÃO.

POR EXEMPLO: ← ABREVIAÇÃO!

P_{12}) $\overbrace{\text{NO CONTEXTO } C_{12} \text{ SEMPRE VALE } a+b \in \mathbb{Z}}$.

UM DOS TRUQUES PRA TESTAR DEMONSTRAÇÕES É: SE ALGUMA DESSAS PROPOSIÇÕES FOR FALSA (TALVEZ POR CONTRA-EXEMPLO !!) ENTÃO A DEMONSTRAÇÃO ESTÁ ERRADA.

FECHANDO "SUPONHA"S

OS "SUPONHA"S TÊM QUE SER FECHADOS EM ORDEM. EXISTEM BEM POUCAS REGRAS QUE FECHAM "SUPONHA"S. ESSAS SÃO AS REGRAS MAIS DIFÍCEIS DE TODAS, E AS QUE A GENTE VAI DISCUTIR COM MAIS DETALHES.

$\boxed{\text{NOTE O "COM } c := a+b\text{" DA 13 !!!}}$

$b | a \ :=\ \exists c \in \mathbb{Z}.\ bc = a$
$\mathrm{par}(x) \ :=\ \exists a \in \mathbb{Z}.\ 2a = x$
$\mathrm{impar}(x) \ :=\ \exists a \in \mathbb{Z}.\ 2a+1 = x$

C_2) $x \in \mathbb{Z}$
C_3) $x \in \mathbb{Z}, \mathrm{par}(x)$
C_6) $\underbrace{x \in \mathbb{Z}}_{\text{ger}}, \underbrace{\mathrm{par}(x)}_{\text{filt}}, \underbrace{x+1 = y}_{?\ !!}$

b)
1. VAMOS VER QUE $\forall x \in \mathbb{Z}.\ \mathrm{par}(x) \to \mathrm{impar}(x+1)$
2. SUPONHA $x \in \mathbb{Z}$.
3. SUPONHA $\mathrm{par}(x)$.
4. ENTÃO $\exists a \in \mathbb{Z}.\ 2a = x$.
5. SUPONHA $a \in \mathbb{Z}$, $2a = x$.
6. ENTÃO $2a + 1 = x + 1$.
7. ENTÃO $\exists b \in \mathbb{Z}.\ 2b + 1 = x + 1$ (POR 5, 6 COM $b := a$)
8. ENTÃO $\mathrm{impar}(x+1)$.

MD 29/AGO/2018

HOJE: MAIS ALGUMAS IDÉIAS SOBRE AS REGRAS DE DEDUÇÃO QUE A GENTE JÁ VIU;
INTRODUÇÃO A ALGUMAS REGRAS QUE ESTÃO BEM MAIS ADIANTE NO LIVRO (PROVAS POR CONTRADIÇÃO);
MAIS SOBRE QUANTIFICADORES.

CONTEXTOS E PROPOSIÇÕES

O CONTEXTO ATÉ A LINHA 12 (POR EXEMPLO) É FORMADO POR TODOS OS SUPONHAS ABERTOS ATÉ A LINHA 12.
UM CONTEXTO É ALGO QUE PODE SER ESCRITO DO LADO ESQUERDO DO ";" NUM $\{\_;\_\}$. O CONTEXTO DA LINHA 12 É:

$x \in \mathbb{Z}, y \in \mathbb{Z}, par(x), par(y), a \in \mathbb{Z}, b \in \mathbb{Z}, 2a=x, 2b=x$.

NOTE QUE ELE É FEITO DE GERADORES E FILTROS!!!

A DEMONSTRAÇÃO QUE USAMOS COMO EXEMPLO NAS ÚLTIMAS AULAS É:

1. VAMOS VER QUE $\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. par(x) \land par(y) \to par(x+y)$.
2. SUPONHA $x \in \mathbb{Z}, y \in \mathbb{Z}$.
3. SUPONHA $par(x), par(y)$.
4. ENTÃO $2|x$. (POR 3, DEF.)
5. ENTÃO $2|y$. (POR 3, DEF.)
6. ENTÃO $\exists a \in \mathbb{Z}. 2a=x$. (POR 4, DEF.)
7. ENTÃO $\exists b \in \mathbb{Z}. 2b=y$. (POR 5, DEF.)
8. SUPONHA $a \in \mathbb{Z}, 2a=x$.
9. SUPONHA $b \in \mathbb{Z}, 2b=x$.
10. ENTÃO $2a+2b=x+y$. (POR 8, 9)
11. ENTÃO $2(a+b)=x+y$. (POR 10)
12. ENTÃO $a+b \in \mathbb{Z}$. (POR 8, 9)
13. ENTÃO $\exists c \in \mathbb{Z}. 2c=x+y$. (POR 12, 11 COM $c:=a+b$) $\boxed{\text{FECHA 9, 8}}$
14. ENTÃO $2|x+y$.
15. ENTÃO $par(x+y)$.
16. ENTÃO $par(x) \land par(y) \to par(x+y)$. $\boxed{\text{FECHA 3}}$
17. ENTÃO $\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. par(x) \land par(y) \to par(x+y)$. $\boxed{\text{FECHA 2}}$

LINHAS COM "ENTÃO" SÃO PROPOSIÇÕES!

POR EXEMPLO, NA LINHA 12 A PROPOSIÇÃO É ESSA:

$$P_{12} := x \in \mathbb{Z}, y \in \mathbb{Z}, par(x), par(y), a \in \mathbb{Z}, b \in \mathbb{Z}, 2a=x, 2b=y \vdash a+b \in \mathbb{Z}.$$

ABREVIAÇÃO:

$$P_{12} := C_{12} \vdash a+b \in \mathbb{Z}$$

PRONÚNCIA:
A PROPOSIÇÃO ASSOCIADA À LINHA 12 É: NO CONTEXTO C_{12} SEMPRE VALE $a+b \in \mathbb{Z}$.

PROPOSIÇÕES SÃO VERDADEIRAS OU FALSAS - A NOTAÇÃO ACIMA PODE SER TRADUZIDA PARA:

$$\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. (par(x) \land par(y) \to (\forall a \in \mathbb{Z}. \forall b \in \mathbb{Z}. (2a=x \land 2b=y \to a+b \in \mathbb{Z}))$$

)

CONTRA-EXEMPLO

(SEÇÃO 4 DO LIVRO)

EXEMPLO (4.1, P.24):

$a \in \mathbb{Z}, b \in \mathbb{Z}, a|b \land b|a \vdash a=b$

(TRADUZIDO PRA NOTAÇÃO COM "$\vdash$"!)

NESSE CONTEXTO SEMPRE VALE $a=b$?

(O "CONTEXTO" É $a \in \mathbb{Z}, b \in \mathbb{Z}, a|b \land b|a$!)

COMO CONJUNTO:

$$C_{4.1} = \{a \in \mathbb{Z}, b \in \mathbb{Z}, a|b \land b|a; (a,b)\}$$

ENCONTRAR UM CONTRA-EXEMPLO PRA PROPOSIÇÃO 4.1 É ENCONTRAR UM VALOR PRO CONTEXTO $C_{4.1}$ NO QUAL SEJA FALSO...

SOLUÇÃO:
$a=5, b=-5$
$\Rightarrow (5,-5) \in C_{4.1}$,
E QUANDO $(a,b)=(5,-5)$
TEMOS $(a=b)=F$!

EXERCÍCIOS:
P.26, EXERCÍCIOS 1,2,3,4

QUE "REGRAS DE DEDUÇÃO" ESTÃO SENDO USADAS ATÉ AGORA?

AS REGRAS MAIS DIFÍCEIS SÃO AS QUE FECHAM "SUPONHA"S!

O MELHOR MODO DE ENTENDER AS REGRAS - NO CASO GERAL - É USANDO PROPOSIÇÕES MAIS ABSTRATAS. LEMBRE QUE NO EXEMPLO DOS ORCS NÓS TÍNHAMOS SÍMBOLOS COMO N, D_i, P_i, M_i, QUE ERAM DEFINIDOS POR TABELAS QUE PODIAM SER ALTERADAS "MUDANDO O UNIVERSO"...

VAMOS VER (VÁRIAS) VERSÕES MAIS GERAIS DAS REGRAS SENDO USADAS NAS LINHAS 13, 16, 17.

20. SUPONHA $x \in \mathbb{Z}, y \in \mathbb{Z}$
21. ENTÃO $f(x,y) \in \mathbb{Z}$.
22. ENTÃO $Q(x,y,f(x,y))$.
23. ENTÃO $\exists c \in \mathbb{Z}. Q(x,y,c)$ (POR 21, 22, COM $c:=f(x,y)$)

$f(0,0)=9$,
$f(0,1)=10$,
$f(2,0)=30$,
$f(x,y)=4$ NOS OUTROS CASOS.

30. SUPONHA P, Q
31. ENTÃO R.
32. ENTÃO $Q \to R$ (POR 31) $\boxed{\text{FECHA 30}}$

40. SUPONHA $x \in \mathbb{Z}$.
41. SUPONHA $y \in \mathbb{Z}$.
42. ENTÃO $P(x,y)$.
43. ENTÃO $\forall y \in \mathbb{Z}. P(x,y)$ (POR 42) $\boxed{\text{FECHA 41}}$

TRADUÇÃO PRA LINGUAGEM COM "$\vdash$":

P_{21}) $x \in \mathbb{Z}, y \in \mathbb{Z} \vdash f(x,y) \in \mathbb{Z}$
P_{22}) $x \in \mathbb{Z}, y \in \mathbb{Z} \vdash Q(x,y,f(x,y))$
P_{23}) $x \in \mathbb{Z}, y \in \mathbb{Z} \vdash \exists c \in \mathbb{Z}. Q(x,y,c)$ $\Leftarrow$

P_{31}) $P, Q \vdash R$
P_{32}) $P \vdash Q \to R$

P_{42}) $x \in \mathbb{Z}, y \in \mathbb{Z} \vdash P(x,y)$
P_{43}) $x \in \mathbb{Z} \vdash \forall y \in \mathbb{Z}. P(x,y)$

MD 29/AGO/2018

MAIS SOBRE QUANTIFICADORES

MAS ANTES...

LEIS DE DE MORGAN

ESTAS EXPRESSÕES SÃO LOGICAMENTE EQUIVALENTES?

a) $\neg P \land \neg Q$ E $\neg(P \lor Q)$

b) $\neg P \lor \neg Q$ E $\neg(P \land Q)$

c) $\neg(P_1 \land P_2 \land P_3)$ E $(\neg P_1 \lor \neg P_2 \lor \neg P_3)$

a) SIM
b) SIM
c) SIM

a)

P	Q	$\neg P \land \neg Q$	$\neg(P \lor Q)$
F	F	V	V
F	V	F	F
V	F	F	F
V	V	F	F

LEMBRE QUE

$(\forall i \in \{2,4,5\}.\ P_i)$

$= P_2 \land P_4 \land P_5$

$$\boxed{\begin{aligned}&(\forall i \in \{2,4,5\}.\ \neg Q_i\\ &= \neg Q_2 \land \neg Q_4 \land \neg Q_5\\ &= \neg(Q_2 \lor Q_4 \lor Q_5)\\ &= \neg \exists i \in \{2,4,5\}.\ Q_i\end{aligned}}$$

DE MORGAN PRA QUANTIFICADORES!!!

$$\underbrace{\underbrace{\neg \underbrace{P}_{F}}_{V} \land \underbrace{\neg \underbrace{Q}_{F}}_{V}}_{V} \qquad \underbrace{\neg \underbrace{(\underbrace{P}_{F} \lor \underbrace{Q}_{F})}_{F}}_{V}$$

$$\underbrace{\underbrace{\neg \underbrace{P}_{F}}_{V} \land \underbrace{\neg \underbrace{Q}_{V}}_{F}}_{F}$$

$(\forall i \in \{2,4,5\}.\ P_i) \land (\forall i \in \{8,9,10\}.\ P_i)$

$= (P_2 \land P_4 \land P_5) \land (P_8 \land P_9 \land P_{10})$

$= P_2 \land P_4 \land P_5 \land P_8 \land P_9 \land P_{10}$

$= \forall i \in \{2,4,5,8,9,10\}.\ P_i$

$= (\forall i \in \{2,4\}.\ P_i) \land (\forall i \in \{5,8,9,10\}.\ P_i)$

$= (\forall i \in \{2\}.\ P_i) \land (\forall i \in \{4,5,8,9,10\}.\ P_i)$

$= (\forall i \in \{\}.\ P_i) \land (\forall i \in \{2,4,5,8,9,10\}.\ P_i)$

(OBS: EU TROUXE IMPRESSÃO DO QUADRO DA OUTRA TURMA PRA NÃO PRECISAR ESCREVER A DEMONSTRAÇÃO TODA DE NOVO NO QUADRO...)

NOVIDADES

1) CONTEXTOS SEMPRE PODEM SER POSTOS NO FORMATO DO QUE APARECE À ESQUERDA DO ";" NUM $\{\_;\_\}$

2) ABREVIAÇÕES NOVAS.
A PROPOSIÇÃO ASSOCIADA À LINHA 12 É:

$$P_{12} := \begin{array}{l} x\in\mathbb{Z}, y\in\mathbb{Z}, \mathrm{par}(x), \mathrm{par}(y), \\ a\in\mathbb{Z}, b\in\mathbb{Z}, 2a=x, 2b=y \\ \vdash a+b\in\mathbb{Z} \end{array}$$

"No contexto C_{12} $\underbrace{\text{sempre vale}}_{\text{"}\vdash\text{"}}$ $a+b\in\mathbb{Z}$".
"CATRACA"

$$P_{12} = \forall x\in\mathbb{Z}.\forall y\in\mathbb{Z}.\ \mathrm{par}(x)\land\mathrm{par}(y)\to(\forall a\in\mathbb{Z}.\forall b\in\mathbb{Z}.\ 2a=x\land 2b=y \to a+b\in\mathbb{Z}).$$

LEMBRE QUE UMA PROPOSIÇÃO PODE SER VERDADEIRA OU FALSA.

SE NUMA DEMONSTRAÇÃO SUA A PROPOSIÇÃO ASSOCIADA À LINHA N É FALSA ENTÃO A SUA DEMONSTRAÇÃO ESTÁ ERRADA.

CONTRA-EXEMPLOS
(SEÇÃO 4 DO LIVRO)

DÁ PRA GENTE PADRONIZAR A LINGUAGEM DELE TRADUZINDO-A PRA UMA NOTAÇÃO MAIS MATEMÁTICA...

EXEMPLO (4.1, p.24):

$a\in\mathbb{Z}, b\in\mathbb{Z}, a|b, b|a$
$\vdash a=b$

(TRADUZIMOS PRA NOTAÇÃO COM "$\vdash$"!)

COMO PADRONIZAR O MODO DE MOSTRAR QUE UMA PROPOSIÇÃO DESSAS É FALSA?

IDÉIA 1: OS "VALORES POSSÍVEIS PRO CONTEXTO" PODEM SER ESCRITOS COMO CONJUNTO...

$$C_{12} = \{\underbrace{a\in\mathbb{Z}}_{\text{GER}}, \underbrace{b\in\mathbb{Z}}_{\text{GER}}, \underbrace{a|b}_{\text{FILT}}, \underbrace{b|a}_{\text{FILT}} ; (a,b)\}$$

O CONTRA-EXEMPLO QUE O LIVRO DÁ É:
$(a,b)=(5,-5)$ (obs: $(a,b)\in C_{12}$),
$a=5,\ b=-5,$

SE $a=5, b=-5$ ENTÃO $a|b, b|a$
MAS $a=b$ É FALSO.
$(a=b)=F$

EXERCÍCIOS PRA AGORA:
p.26, EXERCÍCIOS 1,2,3,4.

...E REVISEM EQUIVALÊNCIA LÓGICA, PRINCIPALMENTE LEIS DE DE MORGAN!!!

DEFS:

$\mathrm{par}(x) := \exists a\in\mathbb{Z}.\ 2a=x$
$\mathrm{impar}(x) := \exists a\in\mathbb{Z}.\ 2a+1=x$
$b|a := \exists c\in\mathbb{Z}.\ bc=a$

$10|4 := \exists c\in\mathbb{Z}.\ 10c=4$

$4|10$
$10|4$

¢

$\mathbb{N} = \{0,1,2,3,\dots\}$
$\mathbb{N}^+ = \{1,2,3,\dots\}$

$\vdash \forall x\in\mathbb{Z}.\forall y\in\mathbb{Z}.\ x|y\to x\le y$

Se $x=1$ e $y=-1$, $\underbrace{x}_{1}|\underbrace{y}_{-1}\to x\le y$

$\vdash \forall x\in\mathbb{Z}.\forall y\in\mathbb{Z}.\ x|y\to(x\le y \lor x=-y)$

Se $x=4$ e $y=0$, $\underbrace{\underbrace{\overset{4}{x}|\overset{0}{y}}_{V} \to \underbrace{\underbrace{(\overset{4}{x}\le\overset{0}{y}}_{F} \lor \underbrace{\overset{4}{x}=-\overset{0}{y})}_{F}}_{F}}_{F}$

MD 3/set/2018

Hoje: mais sobre quantificadores e variáveis; o erro mais comum nas demonstrações que vocês me entregaram

Obs: sec. 9: quantificadores (leiam e façam os exercícios em casa!)

Seja: $A=\{0,1,2\}$.

A sec. 9 tem vários problemas - proposições pra você determinar se são verdadeiras ou falsas - como estes aqui:

a) $\forall x\in\mathbb{Z}.\ \exists y\in\mathbb{Z}.\ x+y=0 \quad = V$

b) $\exists x\in\mathbb{Z}.\ \forall y\in\mathbb{Z}.\ x+y=0 \quad = F$

A gente sabe calcular estes:

c) $\forall x\in A.\ \exists y\in A.\ \mathrm{par}(x+y) \quad = V$

d) $\exists x\in A.\ \forall y\in A.\ \mathrm{par}(x+y) \quad = F$

Repare que

$(\forall y\in A.\ \mathrm{par}(x+y))[x:=2]$

$=(\forall y\in A.\ \mathrm{par}(2+y))$

$=F$

Vocês sabem "calcular" proposições como

$\underbrace{x\in\mathbb{Z}}_{\text{contexto}} \vdash \underbrace{\exists y\in\mathbb{Z}.\ x+y=0}_{\text{parte depois do "então"}}$

e vocês sabem encontrar contra-exemplos pras que são falsas.

Mais sobre quantificadores

O nome da variável "não importa" - ele pode ser mudado...

a) $(\forall x\in\mathbb{Z}.\ \exists y\in\mathbb{Z}.\ x+y=0)$

$=(\forall x\in\mathbb{Z}.\ \exists b\in\mathbb{Z}.\ x+b=0)$

$=(\forall a\in\mathbb{Z}.\ \exists b\in\mathbb{Z}.\ a+b=0)$

$=(\forall y\in\mathbb{Z}.\ \exists x\in\mathbb{Z}.\ y+x=0)$

x+y são "variáveis locais"

Novidade:

$\forall x\in\mathbb{Z}.\ \exists x\in\mathbb{Z}.\ \mathrm{par}(x+x)$

os "x"zes são ligados ao quantificador mais próximo!

$\forall x\in\mathbb{Z}.(\exists y\in\mathbb{Z}.\ \mathrm{par}(y+y))$

O erro nas demonstrações

$a\in\mathbb{Z},\ b\in\mathbb{Z},\ \mathrm{par}(b),(\exists c\in\mathbb{Z}.\ c=ab)\vdash\mathrm{par}(c)$ ‖

‖

$(\exists d\in\mathbb{Z}.\ d=ab)$

$a\in\mathbb{Z},\ b\in\mathbb{Z},\ \mathrm{par}(b),(\exists d\in\mathbb{Z}.\ d=ab)\vdash\mathrm{par}(c)$

Quando a gente tentar calcular par(c) - pra qualquer escolha de a e b - o resultado vai ser sempre o mesmo: erro, porque a variável d está indefinida!!!

Exercício

Há duas aulas atrás eu pedi que vocês escolhessem pelo menos uma das proposições abaixo, fizessem a demonstração dela e me entregassem pra eu descobrir os erros mais comuns...

a) Prop 3.3, p.20

b) $\forall x\in\mathbb{Z}.\ \mathrm{par}(x)\to\mathrm{impar}(x+1)$

c) $\forall x\in\mathbb{Z}.\ \mathrm{impar}(x+1)\to\mathrm{par}(x)$

d) Prop 3.5, p.24

e) Exercícios 1 a 13 da p.24.

$(\forall i\in\{2,3,5\}.\ P_i)\land(\forall i\in\{6,8,10\}.\ P_i)=$

$=P_2\land P_3\land P_5\land P_6\land P_8\land P_{10}$

$=(\forall i\in\{2,3\}.\ P_i)\land(\forall i\in\{5,6,8,10\}.\ P_i)$

$=(\forall i\in\{\}.\ P_i)\land(\forall i\in\{2,3,5,6,8,10\}.\ P_i)$

$=\underbrace{(\forall i\in\{\}.\ P_i)}_{\text{isto tem que ser V!}}\land P_2\land P_3\land P_5\land P_6\land P_8\land P_{10}$

Se for F,

$=F\land P_2\land P_3\land P_5\land P_6\land P_8\land P_1$

$=F$

Se $\underbrace{\underbrace{P_2}_{V}\land\underbrace{P_3}_{V}\land\underbrace{P_5}_{V}\land\underbrace{P_6}_{V}\land\underbrace{P_8}_{V}\land\underbrace{P_{10}}_{V}}_{V}$

$\underbrace{a\in\mathbb{Z}}_{\text{ger}},\underbrace{b\in\mathbb{Z}}_{\text{ger}},\underbrace{a|b}_{\text{filt}},\underbrace{b|c}_{\text{filt}},\underbrace{z:=xy}_{\text{def}}$

$\{\underbrace{a\in\{0,1,2\}}_{\text{ger}},\underbrace{b\in\{0,1,2\}}_{\text{ger}},\underbrace{a<b}_{\text{filt}};\underbrace{(a,b)}_{\text{expr}}\}$

$\underbrace{a|b\land b|c}_{\text{filtro}}\vdash a|c$

Lembre que

$3^1=3$

$3^2=3\cdot3$

$3^3=3\cdot3\cdot3$

$3^0=1$ ← por conveniência!

$3^0\cdot3^4=3^1\cdot3^3=3^2\cdot3^2=\ldots$

e que $1!=1$ e $0!=1$, também por conveniência...

e 0 é par,

1 não é primo,

-3 não é primo,

...

...da mesma forma,

$(\exists i\in\{\}.\ P_i)=F$.

Hoje:
- MAIS SOBRE QUANTIFICADORES E VARIÁVEIS
- O ERRO MAIS COMUM DE TODOS NAS DEMONSTRAÇÕES QUE EU LI

A SEÇÃO 9 DO SCHEINERMAN É SOBRE QUANTIFICADORES. LEIAM E FAÇAM OS EXERCÍCIOS DELA EM CASA!
OS ITENS c E d ABAIXO SÃO "MINIATURAS" DE EXERCÍCIOS DA SEÇÃO 9.
SEJA $A=\{0,1,2\}$.
DETERMINE SE AS PROPOSIÇÕES ABAIXO SÃO VERDADEIRAS OU FALSAS.

a) $\forall x \in A.\ \exists y \in A.\ \mathrm{par}(x+y)$
b) $\exists x \in A.\ \forall y \in A.\ \mathrm{par}(x+y)$
c) $\forall x \in \mathbb{Z}.\ \exists y \in \mathbb{Z}.\ x+y=0$
d) $\exists x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.\ x+y=0$

LEMBRE QUE CALCULAR O VALOR DE UMA EXPRESSÃO É DIFERENTE DE DEMONSTRÁ-LA!

Obs: $(\exists y \in A.\ \mathrm{par}(x+y))[x:=2]$
$= (\exists y \in A.\ \mathrm{par}(2+y))$
$= \mathrm{par}(2+0) \vee \mathrm{par}(2+1) \vee \mathrm{par}(2+2)$

LEMBRE QUE VOCÊ SABE "CALCULAR" SE EXPRESSÕES COM "$\vdash$" SÃO VERDADEIRAS OU FALSAS, E QUE VOCÊ SABE TRADUZIR CADA LINHA COM "ENTÃO" DE UMA DEMONSTRAÇÃO PARA UMA EXPRESSÃO COM "$\vdash$"...

$$\underbrace{\underbrace{a \in \mathbb{Z}}_{\text{GER}},\ \underbrace{\mathrm{par}(a)}_{\text{FILT}},\ \underbrace{b \in \mathbb{Z}}_{\text{GER}}}_{\text{"CONTEXTO" - COISAS NOS "SUPONHA"S ABERTOS}} \vdash \underbrace{\mathrm{par}(a+b)}_{\text{PARTE DEPOIS DO "ENTÃO"}}$$

$\Rightarrow \forall a \in \mathbb{Z}.$
$(\mathrm{par}(a) \to (\forall b \in \mathbb{Z}.\ \mathrm{par}(a+b)))$

... E VOCÊS SABEM ENCONTRAR CONTRA-EXEMPLOS!

OS CONTEXTOS SÃO COISAS QUE PODEM SER ESCRITAS À ESQUERDA DO ";" NO $\{\_\_ ; \_\_\}$...
CONTEXTOS SÃO FEITOS DE GERADORES E FILTROS...

A SEGUNDA LISTA DE EXERCÍCIOS DISCUTIA VÁRIAS COISAS SOBRE VARIÁVEIS - INCLUINDO SITUAÇÕES COM VARIÁVEIS INDEFINIDAS, QUE DAVAM ERRO.

EM LIVROS QUE FALAM MAIS SOBRE QUANTIFICADORES A GENTE APRENDE QUE EXPRESSÕES COMO ESTA SÃO VÁLIDAS:

$$\forall x \in \mathbb{Z}.\ \exists x \in \mathbb{Z}.\ \mathrm{par}(x+x)$$

CADA VARIÁVEL ESTÁ "LIGADA" AO QUANTIFICADOR MAIS PRÓXIMO DELA - MAIS "INTERNO", MENOS "EXTERNO".

$$(\exists x \in A.\ 2x=2) \wedge (\exists x \in A.\ 2x=4)$$

... A GENTE PODE MUDAR NOMES DE VARIÁVEIS SEM MUDAR O VALOR DA EXPRESSÃO, OBTENDO UMA EXPRESSÃO EQUIVALENTE À ANTERIOR...

a) $(\forall x \in A.\ \exists y \in A.\ \mathrm{par}(x+y))$
$= (\forall x \in A.\ \exists a \in A.\ \mathrm{par}(x+a))$
$= (\forall b \in A.\ \exists a \in A.\ \mathrm{par}(b+a))$
$= (\forall y \in A.\ \exists x \in A.\ \mathrm{par}(y+x))$

O ERRO MAIS COMUM

$a \in \mathbb{Z},\ b \in \mathbb{Z},\ \mathrm{par}(b),\ (\exists c \in \mathbb{Z}.\ c=ab) \vdash \mathrm{par}(bc)$ — INDEFINIDO!!!
$\quad\quad (\exists d \in \mathbb{Z}.\ d=ab)$

CALCULAR $\mathrm{par}(bc)$ SEMPRE DÁ ERRO, PRA QUAISQUER VALORES DE a E b, PORQUE c ESTÁ INDEFINIDO - c SÓ ESTAVA DEFINIDO DENTRO DO $(\exists c \in \mathbb{Z}. \_\_)$.

$$\{a \in A,\ \mathrm{par}(a),\ b \in \mathbb{Z} ;\ \mathrm{par}(a+b)\}$$

$a \in A$	$\mathrm{par}(a)$	$b \in \mathbb{Z}$	$\mathrm{par}(a+b)$
0	V	0	V
		1	F
		2	V
1	F		
2	V	0	V
		1	F
		2	V

Exercício
HÁ DUAS (?) AULAS ATRÁS VOCÊS FIZERAM ALGUMAS DEMONSTRAÇÕES DESTA LISTA:
a) PROP. 3.3, P.20
b) $\forall x \in \mathbb{Z}.\ \mathrm{par}(x) \to \mathrm{impar}(x+1)$
c) $\forall x \in \mathbb{Z}.\ \mathrm{impar}(x+1) \to \mathrm{par}(x)$
d) PROP 3.?, P.24
e) EXERCÍCIOS 1 A 13 DA P.24.

... ESCOLHAM ALGUM EXERCÍCIO QUE VOCÊS JÁ TENHAM FEITO, REFAÇAM ELE AGORA - NO FORMATO COM "VAMOS VER QUE", "SUPONHA", "ENTÃO" - E AÍ TENTEM TRADUZIR AS LINHAS COM "ENTÃO" PRO FORMATO COM "$\vdash$" E DESCOBRIR ONDE ESTÁ O ERRO.

$P_?$) $a \in \mathbb{Z},\ b \in \mathbb{Z},\ c \in \mathbb{Z},\ a|b,\ b|c \vdash c = axy$

MD 5/SET/2018

AVISO: A PÁGINA DO CURSO JÁ EXISTE, MAS ESTÁ INCOMPLETA — FALTA PÔR AS LISTAS DE EXERCÍCIOS, O PROGRAMA DO CURSO, ETC — E TEM UM BUG: O PDF COM AS FOTOS DOS QUADROS ESTÁ COM AS PÁGINAS FORA DE ORDEM...

HOJE:
- UM TRUQUE PRA SIMPLIFICAR ALGUMAS DEMONSTRAÇÕES QUE VOCÊS FIZERAM
- PROVAS POR CONTRADIÇÃO (?)
- INTRODUÇÃO À SEGUNDA PARTE DO CURSO: "OBJETOS MATEMÁTICOS" (SÃO 5 PARTES NO TOTAL E A MATÉRIA DA P1 SÃO AS PARTES 1 E 2)

GRAFOS,
RELAÇÕES,
FUNÇÕES,
ETC
($\to$ ALGORITMOS!)
O FACEBOOK USA GRAFOS PRA DESCOBRIR O QUE INTERESSA MAIS PRA QUEM.

(1) VAMOS MOSTRAR QUE SE $x,y\in\mathbb{Z}$ E x E y SÃO ÍMPARES ENTÃO xy É ÍMPAR.
(2) SUPONHA $x\in\mathbb{Z}$, $y\in\mathbb{Z}$
(3) SUPONHA $\mathrm{IMPAR}(x)$
(4) SUPONHA $\mathrm{IMPAR}(y)$
(5) ENTÃO $\exists a\in\mathbb{Z}.\ 2a+1=x$
(6) ENTÃO $\exists b\in\mathbb{Z}.\ 2b+1=y$
(7) SUPONHA $a\in\mathbb{Z}$, $2a+1=x$
(8) SUPONHA $b\in\mathbb{Z}$, $2b+1=y$
(9) ENTÃO $xy=(2a+1)(2b+1)$
$=4ab+2a+2b+1$
$=2(\underbrace{2ab+a+b}_{c})+1$

AQUI A GENTE TEM DUAS POSSIBILIDADES...

(10) ENTÃO $\exists c\in\mathbb{Z}.\ 2c+1=xy$ (COM $c:=2ab+a+b$)

(10') ENTÃO $\exists d\in\mathbb{Z}.\ d=2ab+a+b$
(11') SUPONHA $d\in\mathbb{Z}$, $d=2ab+a+b$
(12') ENTÃO $\exists e\in\mathbb{Z}.\ 2e+1=xy$ (COM $e:=d$)

$\Rightarrow$ $P_{12'}$) $x\in\mathbb{Z}, y\in\mathbb{Z}$, $\mathrm{IMPAR}(x), \mathrm{IMPAR}(y)$, $a\in\mathbb{Z}$, $2a+1=x$, $b\in\mathbb{Z}$, $2b+1=y$, $d\in\mathbb{Z}$, $d=2ab+a+b$ $\vdash \exists e\in\mathbb{Z}.\ 2e+1=xy$

OBS: AS LINHAS COM "ENTÃO" VIRAM PROPOSIÇÕES COM CATRACA... POR EXEMPLO:

P_5) $x\in\mathbb{Z}, y\in\mathbb{Z}, \mathrm{IMPAR}(x), \mathrm{IMPAR}(y)$
$\vdash \exists a\in\mathbb{Z}.\ 2a+1=x$

NOVIDADE: DÁ PRA INTERPRETAR LINHAS COM "SUPONHA" SÓ COMO CONTEXTOS...

C_4) $x\in\mathbb{Z}, y\in\mathbb{Z}, \mathrm{IMPAR}(x), \mathrm{IMPAR}(y)$
$\vdash \ldots$ — É COMO SE ESSA PARTE NÃO EXISTISSE.

"O ERRO" DA AULA PASSADA PODE APARECER EM LINHAS "SUPONHA".
(DETALHES DEPOIS!)

REPARE QUE A PARTE "$c\in\mathbb{Z}$, $c=2ab+a+b$" DO CONTEXTO É TRIVIAL — NO SENTIDO DE QUE SE A GENTE [illegible] OS VALORES POSSÍVEIS PRO CONTEXTO USANDO TABELAS SEMPRE EXISTE EXATAMENTE UM JEITO DE ESCOLHER ESSE c... ESSA PARTE "$c\in\mathbb{Z}$, $c=2ab+a+b$" "NÃO COMPLICASSE A TABELA QUE CALCULA CONTEXTOS".

COMO SIMPLIFICAR A DEMONSTRAÇÃO COM OS PASSOS (10'), (11'), (12')? TRUQUE: USE UM "COM" MAIS COMPLICADO!

P_{10}) $x\in\mathbb{Z}, y\in\mathbb{Z}$, $\mathrm{IMPAR}(x), \mathrm{IMPAR}(y)$, $a\in\mathbb{Z}$, $2a+1=x$, $b\in\mathbb{Z}$, $2b+1=y$ $\vdash \exists c\in\mathbb{Z}.\ 2c+1=xy$

LEMBRE QUE A GENTE PODE INTRODUZIR LINHAS "SUPONHA" NUMA DEMONSTRAÇÃO À VONTADE... MAS ELAS AUMENTAM O CONTEXTO — ELAS "INTRODUZEM HIPÓTESES" E A GENTE VAI TER QUE SE LIVRAR DESSAS HIPÓTESES DEPOIS!

A GENTE QUER CHEGAR A UMA LINHA COMO ISTO:

$\vdash \forall x\in\mathbb{Z}.\forall y\in\mathbb{Z}.(\mathrm{IMPAR}(x)\land \mathrm{IMPAR}(y)\to \mathrm{IMPAR}(x+y))$

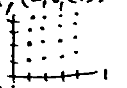
CONTEXTO VAZIO

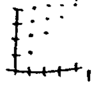
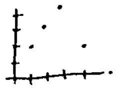
INTRODUZIR HIPÓTESES É RUIM PORQUE A GENTE VAI TER QUE FECHAR ELAS DEPOIS !!

ALGUNS OBJETOS MATEMÁTICOS IMPORTANTES

- LISTAS (CAP. 6)
- CONJUNTOS
- PRODUTO CARTESIANO
- SUBCONJUNTOS
- RELAÇÕES
- FUNÇÕES

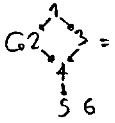
SEJA $A=\{1,2,3,4\}$.
$B=\{a\in A, b\in A, c\in A, a<b, b<c;\ (a,b,c)\}$

(1) QUEM É O CONJUNTO B?
(2) QUANTOS ELEMENTOS ELE TEM?
(3) É POSSÍVEL LISTAR OS ELEMENTOS DELE EM ORDEM?
(4) COMO DEFINIR UMA ORDEM NELE? ALIÁS, COMO DEFINIR UMA ORDEM NO CONJUNTO $C=\{a\in A, b\in A, c\in A;\ (a,b,c)\}$?
(5) SEJAM $D=A\times A=$ 

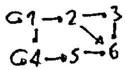
$E=$  , $F=$ 

(6) SEJA $B':=\{a\in A, b\in B, c\in C, a\leq b, b\leq c;\ (a,b,c)\}$.
QUEM É O CONJUNTO B'? QUANTOS ELEMENTOS ELE TEM? LISTE SEUS ELEMENTOS EM ORDEM.

(7) ISTO É UM GRAFO:

G  $=(\{1,2,3,4,5,6\}, \{(1,2),(1,3),(2,2),(2,4),(3,4),(4,5)\})$.

(a) ESCREVA O GRAFO ABAIXO NA FORMA (PONTOS, SETAS):

G 

(b) REPRESENTE GRAFICAMENTE O GRAFO ABAIXO:
$(\{1,2,3\}, \{(1,3),(3,1),(2,2)\})$

MD 5/set/2018

(1) Dá pra calcular o B por uma tabela, mas fica grande...

$a\in A$	$b\in A$	$c\in A$	$a<b$	$b<c$	(a,b,c)
1	1	1	F		
		2	F		
		3	F		
		4	F		
	2	1	V	F	
		2	V	F	
		3	V	V	$(1,2,3)$
		4	V	V	$(1,2,4)$
		...			$(1,3,4)$
					$(2,3,4)$

$B=\{(1,2,3),(1,2,4),(1,3,4),(2,3,4)\}$

Repare que isto é um conjunto de listas de 3 elementos cada — "triplas" — até agora só tínhamos visto conjuntos de pares.

Podemos ter listas de: qualquer comprimento, os elementos delas não precisam ser números!

Exemplos: (V,V,F), $(1,2,F)$, $((1,2),(3,4,5))$, $(\{1,2\},\{3,4,5\},(3,4,5))$.

(2) O B tem 4 elementos.

(3) Todo mundo deve ter chegado a esta ordem pros elementos de B:
$((1,2,3),$
$(1,2,4),$
$(1,3,4),$
$(2,3,4))$

(4) Quantos elementos tem C?
(Obs: isto é a "versão MD" de análise combinatória!)
Resp: $4\cdot4\cdot4=64$.
Repare que
$B\subset C$,
$B\subseteq C$,
$B\subsetneq C$ —
tudo isto é verdade.

Digamos que B "$\subset$" C.
Como é que a gente lista os elementos dele "em ordem"?
Idéia: dá pra gente interpretar cada elemento de C como um número de três dígitos: $(1,3,4) \rightsquigarrow 134$
A gente sabe pôr números de três dígitos em ordem e...

(5) $E\subset D=A\times A$.

$E=\{(1,1),(1,2),(1,3),(1,4),$
$(2,2),(2,3),(2,4),$
$(3,3),(3,4),$
$(4,4)\}$
$=\{a\in A,\ b\in A,\ a\le b;\ (a,b)\}$

O conjunto E diz "quando $a\le b$ é verdade"...

Idéia ("relações"!):
O E "representa" o "$\le$"...
$a\le b$ é algo que responde V ou F, e a gente vai usar uma notação parecida pra outras relações...

$F=\{(1,2),(2,3),(3,4),(4,2)\}$

Expressões como $1F2$, $1F3$, etc vão ser outra notação para: $\underbrace{(1,2)\in F}_{V}$, $\underbrace{(1,3)\in F}_{F}$, ...

Às vezes a gente vai reusar notações conhecidas, atribuindo novos significados pra elas...

$\le_C=\{((a,b,c),(d,e,f))\in C\times C \mid a\le d,\ b\le e,\ c\le f\}$

Diga se cada uma das expressões abaixo é V ou F:

a) $(1,2,3)\le_C(1,2,4)$

b) $(1,2,3)\le_C(4,3,2)$

MD 5/set/2018

Aviso: A página do curso já está no ar - http://angg.twu.net/2018.2-MD.html e ela tem links pras fotos dos quadros e pra uma parte do material extra.
(Eu mandei esse link pro grupo do Telegram agora há pouco).

O programa do curso - que ainda não está na página - explica que o curso é dividido em 5 partes, e a matéria da P1 são as partes 1 ("Lógica Básica") e 2 ("Objetos Matemáticos"). Falta eu mostrar algumas últimas coisas de demonstrações, mas hoje vamos fazer uma introdução à parte 2.

Hoje:
- Listas
- Conjuntos
- Produto cartesiano
- Subconjuntos
- Relações
- Grafos

Lembrem que em listas a ordem importa, e o comprimento também...
$\{2,3,3,4\}=\{4,3,2\}$
Até agora nós quase só vimos listas de comprimento 2 ("pares")...

Seja $A=\{1,2,3,4\}$.

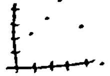
1. Seja $B=\{a\in A, b\in A, c\in A, a<b, b<c; (a,b,c)\}$.
2. Calcule B. Quantos elementos B tem? (Obs: isto é a "versão MD" de análise combinatória).
3. É possível listar os elementos de B em ordem? (Que ordem?)
4. Seja $C=\{a\in A, b\in A, c\in A; (a,b,c)\}$. Quantos elementos C tem? O que é uma ordem em C? Como definir uma ordem em C?

Dica: cada elemento de B ou de C pode ser interpretado como um número de três dígitos...
$(1,3,4) \rightsquigarrow 134$
Isso nos dá um modo de listar os elementos de C em ordem!

Obs: $C=A\times A\times A$ - um produto cartesiano de três conjuntos!

Obs: $B=\{(1,2,3),(1,2,4),(1,3,4),(2,3,4)\}$, e
$B\subset C$,
$B\subseteq C$,
$B\subsetneq C$ são verdade.
B é um subconjunto de C.

Sejam: $D=A\times A=$ 

$E=$  , $F=$ 

$E\subset D$, $F\subset D$.

$E=\{(1,1),(1,2),(1,3),(1,4),(2,2),(2,3),(2,4),(3,3),(3,4),(4,4)\}$
$=\{a\in A, b\in A, a\le b; (a,b)\}$
$=\{(a,b)\in A\times A \mid a\le b\}$

O conjunto E é a "versão conjunto" do $\le$ (em A)...

Vamos interpretar o E como uma "relação" em A - como algo parecido com "$\le$".

Se $a,b\in A$, $a\le b \leftrightarrow (a,b)\in E$

Notação:
$aEb \leftrightarrow (a,b)\in E$
$aFb \leftrightarrow (a,b)\in F$

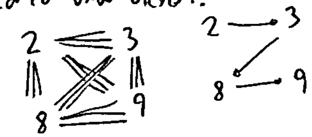
Diga se as expressões abaixo são verdadeiras ou falsas:
a) $1E4$ = V
b) $3E3$ = V
c) $4E2$ = F
d) $1F2$ = V
e) $1F3$ = F

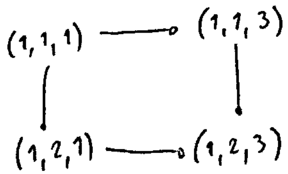
Nós podemos tentar usar essa idéia - essa notação - pra definir uma ordem no conjunto C (problema 4)...

$\underbrace{\le_C}_{\text{nome de um conjunto!}} = R = \{((a,b,c),(d,e,f))\in C\times C \mid a\le d, b\le e, c\le f\}$.

f) $(1,2,3)\,R\,(2,3,4)$ $\quad ((\underbrace{1}_{a},\underbrace{2}_{b},\underbrace{3}_{c}),(\underbrace{2}_{d},\underbrace{3}_{e},\underbrace{4}_{f}))\in R = V$
g) $(1,2,3)\,R\,(4,3,2)$

Problema
Será que esse "$\le_C$" realmente se comporta como uma ordem?





Os elementos $(1,2,1)$ e $(1,1,3)$ são "incomparáveis"...
$(1,2,1)\le_C(1,1,3)$ é falso, e
$(1,1,3)\le_C(1,2,1)$ é falso...

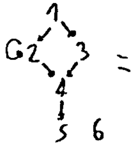
Moral: o conjunto $\le_C$ "não é uma ordem" em C... mas o que isso quer dizer??? !!

$((1,2,1)\le_C(1,1,3)) = ((\underbrace{1}_{a},\underbrace{2}_{b},\underbrace{1}_{c}),(\underbrace{1}_{d},\underbrace{1}_{e},\underbrace{3}_{f}))\in R$
$= \underbrace{\underbrace{1\le 1}_{V} \land \underbrace{2\le 1}_{F} \land \underbrace{1\le 3}_{V}}_{F}$

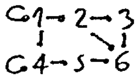
$((1,1,3)\le_C(1,2,1)) = F$

Grafos

Um grafo G é um par (P,S) onde P é um conjunto (de "pontos") e $S\subseteq P\times P$ é um "conjunto de setas".

G  $= (\{1,2,3,4,5,6\}, \{(1,2),(1,3),(2,2),(2,4),(3,4),(4,5)\})$

a) Escreva o grafo abaixo na forma (pontos, setas):



b) Represente graficamente o grafo abaixo:
$(\{1,2,3\}, \{(1,3),(3,1),(2,2)\})$

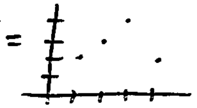
MD 5/set/2018

Funções

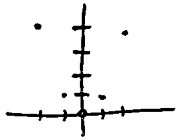
Algumas relações são funções.

Cada função gera uma relação...

Uma função $f: A \to B$ tem um "gráfico" (não é "grafo"!) que é um subconjunto de $A \times B$...

$F =$ 

$= \{(1,2),(2,3),(3,1),(4,2)\}$

$G =$ 

$= \{(-2,4),(-1,1),(0,0),(1,1),(2,4)\}$

$= \{x \in \{-2,-1,0,1,2\} : (x,x^2)\}$

$= \{x \in \{-2,-1,0,1,2\},\ y \in \{0,1,2,3,4\},\ y = x^2 : (x,y)\} =$

x	x^2
-2	4
-1	1
0	0
1	1
2	4

Que subconjuntos de $A \times B$ são gráficos de funções $f: A \to B$?

Idéia: seja $H \subseteq A \times B$. Pra cada $a \in A$ deve existir exatamente um $b \in B$ tal que "$f(a) = b$", ou, $(a,b) \in H$...

Formalmente:

$$\forall a \in A.\ \underbrace{\exists!}_{\text{"existe um único"}} b \in B.\ (a,b) \in H$$

Como traduzir $\exists! c \in C.\ P(c)$ pra termos mais elementares?

Assim: $(\exists c \in C.\ P(c)) \land (\forall c', c'' \in C.\ P(c') \land P(c'') \to c' = c'')$

$$\begin{aligned}(\exists! b \in B.\ (a,b) \in H) &= (\exists b \in B.\ (a,b) \in H) \\ &\land (\forall b', b'' \in B.\ (a,b') \land (a,b'') \to b' = b'')\end{aligned}$$

MD 10/SET/2018

Hoje: introdução a objetos matemáticos, continuação.

Sejam:

$A = \{a,b,c \in \{0,1\};\ 2^a 3^b 5^c\}$

$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$

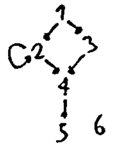
$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$

$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$

Exercícios:

1. Calcule A.
2. Calcule B.
3. Represente graficamente (A,B) como grafo direcionado — A são os seus pontos, B são as suas setas. Dica: cubo.
4. Represente graficamente (A,C).

Exemplo: $(\{1,2,3,4,5,6\},$ $\{(1,2),(1,3),$ $(2,2),$ $(3,4),(2,4),$ $(4,5)\}) =$



Nós vamos ver listas, conjuntos, relações, grafos [direcionados], ordens parciais, partições, funções, etc, numa ordem diferente da do livro e em duas etapas — aplicações primeiro, detalhes depois.

Relações: seção 11.
Grafos: seção 43.
(Produto cartesiano: def 10.3)

Algumas definições importantes:

Uma relação de A em B (ou "de A para B") é um subconjunto $R \subseteq A \times B$.

Uma relação sobre A (ou "em A") é um subconjunto $R \subseteq A \times A$.

Um grafo direcionado é um par (P,S) onde P é um conjunto ("pontos") e $S \subseteq P \times P$ ("setas").

Obs: o livro usa (V,E) ("vertices, edges")

A vantagem de falar de grafos direcionados ao invés de relações é um grafo é um par (éééé!) — mas grafos direcionados são praticamente equivalentes a relações.

Grafos direcionados/relações são reflexivos/simétricos/transitivos quando...

Defs:

$\mathrm{Refl}(P,S) := \forall p \in P.\ pSp$

$\mathrm{Sim}(P,S) := \forall p,q \in P.\ pSq \to qSp$

$\mathrm{Trans}(P,S) := \forall p,q,r \in P.\ (pSq \land qSr \to pSr)$

Dica: no 1 o A tem 8 elementos.

$A = \{\underbrace{a,b,c \in \{0,1\}}_{\text{geradores}};\ \underbrace{2^a, 3^b, 5^c}_{???}\}$ ← ERRO

Resposta:

$A = \{a,b,c \in \{0,1\};\ 2^a \cdot 3^b \cdot 5^c\}$

$A = \{a \in \{0,1\}, b \in \{0,1\}, c \in \{0,1\};\ 2^a 3^b 5^c\}$

$\frac{6}{4} = 1.5$

$6 | 4 = F$

Calcule (os resultados são V ou F):

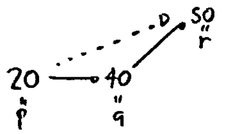
5. Refl(A,B), Refl(A,C), Refl(A,D)
6. Sim(A,B), Sim(A,C), Sim(A,D)
7. Trans(A,B), Trans(A,C), Trans(A,D).

Algumas dicas pros problemas 5, 6, 7...

A gente adora pôr proposições na prova e pedir pra vocês dizerem se elas são verdadeiras ou falsas e justificarem.

A seção 4 — "contra-exemplo" do livro dá técnicas úteis pra mostrar que alguns itens do 5, 6, 7 são falsos, e o jeito mais fácil de demonstrar que algum item do 7 é verdadeiro é usando uma demonstração (com "vamos ver que", "suponha", "então", etc.)

Lembrem que o horário de atendimento é às terças das 18:00 às 19:15 no LEALC, o laboratório que fica no prédio do IHS à direita da rampa no térreo, depois da porta de vidro.



⋮

(20) então $\forall x \in \mathbb{Z}.\ \mathrm{par}(x) \to \mathrm{impar}(x+1)$

⋮

(40) então $\forall x \in \mathbb{Z}.\ \mathrm{impar}(x+1) \to \mathrm{par}(x)$

(41) então $\forall x \in \mathbb{Z}.\ \mathrm{par}(x) \leftrightarrow \mathrm{impar}(x+1)$

MD 11/set/2018

Hoje: mais introdução a objetos matemáticos! (Lembre que vamos ver relações, grafos, ordem, partições, etc, numa ordem diferente da do livro!)

Sejam:

$A = \{a,b,c \in \{0,1\};\ 2^a 3^b 5^c\}$,

$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$

$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$

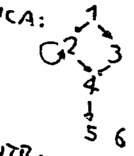
$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$

(1) Calcule A.

(2) Calcule B.

(3) Represente o grafo direcionado (A,B) graficamente.

Dica:



$= (\{1,2,3,4,5,6\}, \{(1,2),(1,3),(2,2),(2,4),(3,4),(4,5)\})$.

Outra dica: cubo.

(4) Qual é o erro de sintaxe aqui? $A' = \{a,b,c \in \{0,1\};\ 2^a, 3^b, 5^c\}$?

Dica: $\frac{6}{20} = 0.3$, $6|20 = F$

(5) Represente o grafo direcionado (A,C) graficamente.

Sobre relações e grafos direcionados

O livro trata relações bem no início (sec. 11) e grafos bem mais pro final (sec. 43) apesar de que são coisas praticamente equivalentes... Nós vamos usar a terminologia de grafos direcionados: "(P,S) é um grafo direcionado" quer dizer que P é um conjunto (de "pontos") e $S \subseteq P \times P$ é o "conjunto das setas"...

Na terminologia de relações isso vira "S é uma relação sobre P".

...Os exercícios de hoje são só uma desculpa pra gente lembrar — ou aprender — o que são relações reflexivas, simétricas e transitivas, e pra gente aprender a trabalhar com as definições formais destes conceitos:

$\mathrm{Refl}(P,S) := \forall p \in P.\ pSp$

$\mathrm{Sim}(P,S) := \forall p,q \in P.\ pSq \to qSp$

$\mathrm{Trans}(P,S) := \forall p,q,r \in P.\ (pSq \land qSr \to pSr)$.

Nas provas — P1, P2, VR, VS — a gente costuma pôr algumas questões de "verdadeiro/falso/justifique". Para cada um dos itens abaixo determine se ele é verdadeiro ou falso:

(6) Refl(A,B), Refl(A,C), Refl(A,D)

(7) Sim(A,B), Sim(A,C), Sim(A,D)

(8) Trans(A,B), Trans(A,C), Trans(A,D)

Nós vamos discutir a parte dos "justifique"s na próxima aula.

(9) Dê um exemplo de um grafo direcionado (P,S) com Refl(P,S) = F.

(10) Idem, mas com Sim(P,S) = F.

(11) Idem, mas com Trans(P,S) = F.

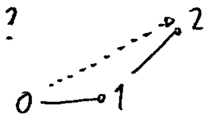
Dicas: (Re)leiam em casa as seções 4 ("contra-exemplo"), e 9 (ou 11?) ("quantificadores"). Usem $P = \{0,1,2\}$.

Se $P = \{0,1,2\}$, $S = \{(0,1),(1,2)\}$

Refl(P,S) = ?

Sim(P,S) = ?

Trans(P,S) = ?



MD 12/set/2018

Hoje: mais introdução a objetos matemáticos! Novidades principais: ordens e funções!

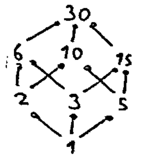
Na aula passada definimos:

$A = \{a,b,c \in \{0,1\} ; 2^a 3^b 5^c\}$,

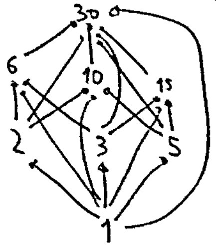
$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$

$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$

$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$

$(A,B) =$ 

(A,C) é um desenho parecido com o acima mas com um "loop" em cada ponto - p.ex.: ↺2, e (A,D) é isto aqui com loops:



Eu pedi pra vocês descobrirem se cada uma destas afirmações é verdadeira ou falsa:

Refl(A,B), Refl(A,C), Refl(A,D),
Sim(A,B), Sim(A,C), Sim(A,D),
Trans(A,B), Trans(A,C), Trans(A,D)

(respostas: F, V, V,
F, F, F,
F, F, V.)

Como "justificar" (demonstrar) cada uma delas?

Exemplos:

Vamos ver que Refl(A,B)=F.
Isto é equivalente a:
$(\forall p \in A.\ pBp) = F$,
que é equivalente a:
$\neg \forall p \in A.\ pBp$, e a:
$\exists p \in A.\ \neg(pBp)$, e a:
$\exists p \in A.\ \neg((p,p) \in B)$, e a:
$\exists p \in A.\ (p,p) \notin B$.

Por exemplo, seja $p=6$.
Então $p \in A$ mas $(6,6) \notin B$.
($(6,6) \notin B$ porque se $x=6$ e $y=6$, $\frac{y}{x} \notin \{2,3,5\}$)

$\text{Refl}(P,S) :=$
$\forall p \in P.\ pSp$

$\text{Sim}(P,S) :=$
$\forall p,q \in P.\ (pSq \to qPp)$

$\text{Trans}(P,S) :=$
$\forall p,q,r \in P.$
$(pSq \land qSr \to pSr)$

Repare que dá pra calcular (explicitamente!)

Refl(A,B) ...

$\text{Refl}(A,B) = \forall p \in A.\ pBp$
$= (1p1 \land 2p2 \land \ldots \land 30p30)$
$= F \land F \land \ldots \land F) \ldots$

Mas é bem difícil calcular explicitamente Trans(A,D)!

$\text{Trans}(A,D) = \underbrace{\forall p,q,r \in A.}_{\text{esses três geradores geram } 8\cdot 8\cdot 8 = 512 \text{ casos!}} (pDq \land qDr \to pDr)$!! ⌢

Vamos mostrar que
$\text{Trans}(A,D) = V$,
ou seja, que
$\forall p,q,r \in A.\ (pDq \land qDr \to pDr)$,
ou seja, que
$\forall p,q,r \in A.\ (\frac{q}{p} \in \mathbb{Z} \land \frac{r}{q} \in \mathbb{Z} \to \frac{r}{p} \in \mathbb{Z})$.

Dica: se você estiver com dificuldades prove primeiro isto:

$\forall p,q,r \in \mathbb{N}^+.\ (\frac{q}{p} \in \mathbb{Z} \land \frac{r}{q} \in \mathbb{Z} \to \frac{r}{p} \in \mathbb{Z})$.

$\mathbb{N}^+ = \{1,2,3,\ldots\}$

Ordens parciais

(Sec. 5.0 do livro)

Uma ordem parcial num conjunto A é uma relação $R \subseteq A \times A$ que obedece algumas propriedades parecidas com o "≤"... Quais?

- $a \le a$ (reflexividade),
- $a \le b \land b \le c \to a \le c$ (transitividade),
- $a \le b \land b \le a \to a = b$ (anti-simetria) ← novidade!

(P,S) é uma ordem parcial se e só se:
- Refl(P,S),
- Trans(P,S),
- Antisim(P,S).

$\text{Antisim}(P,S) :=$
$\forall p,q \in P.$
$(pSq \land qSp \to p=q)$

Determine se estas afirmações são V ou F:

① Antisim(A,B), (=V)
② Antisim(A,C), (=V)
③ Antisim(A,D). (=V)

Encontre grafos direcionados (P,S) que obedeçam:
(Dica: $P=\{2,3\}$)

④ Refl(P,S) ∧ Antisim(P,S)
⑤ Refl(P,S) ∧ ¬Antisim(P,S)
⑥ ¬Refl(P,S) ∧ Antisim(P,S)
⑦ ¬Refl(P,S) ∧ ¬Antisim(P,S)
⑧ Sim(P,S) ∧ Antisim(P,S)
⑨ Sim(P,S) ∧ ¬Antisim(P,S)
⑩ ¬Sim(P,S) ∧ Antisim(P,S)
⑪ ¬Sim(P,S) ∧ ¬Antisim(P,S)

Dica: releiam a parte sobre equivalências lógicas!

$\neg \text{Antisim}(P,S)$
$= \neg \forall p,q \in P.\ (pSq \land qSp \to p=q)$
$= \exists p,q \in P.\ \neg(pSq \land qSp \to p=q)$
$= \exists p,q \in P.\ (pSq \land qSp) \land \neg p=q$
$= \exists p,q \in P.\ (pSq \land qSp) \land p \ne q$

$\neg \text{Sim}(P,S)$
$= \neg \forall p,q \in P.\ pSq \to qSp$
$= \exists p,q \in P.\ \neg(pSq \to qSp)$
$= \exists p,q \in P.\ pSq \land \neg qSp$

$\neg \text{Refl}(P,S)$

$10 \rightleftarrows 42$

Se $p=10$ e $q=42$,
$\underbrace{\underbrace{\underbrace{pSq}_{V} \land \underbrace{qSp}_{V}}_{V} \to \underbrace{p=q}_{F}}_{F}$

Se $(P,S) = \boxed{2 \to 3 \circlearrowleft}$
então Refl(P,S) = ?
Antisim(P,S) = ?

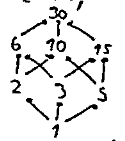
MD 12/SET/2018

HOJE: MAIS INTRODUÇÃO A OBJETOS MATEMÁTICOS NUMA ORDEM BEM DIFERENTE DA DO LIVRO... ORDENS, E TALVEZ FUNÇÕES.

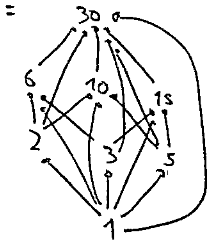
NA AULA PASSADA DEFINIMOS:

$A = \{2^a 3^b 5^c \mid a,b,c \in \{0,1\}\}$,
$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$,
$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$,
$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$;

GRAFICAMENTE,

$(A,B) =$ 

(A,C) É O DESENHO ACIMA COM "LOOPS" ($1\circlearrowleft$, $2\circlearrowleft$, ETC),

$(A,D) =$ 

EU PEDI PRA VOCÊS DESCOBRIREM SE CADA UMA DAS AFIRMAÇÕES ABAIXO É VERDADEIRA OU FALSA:

REFL(A,B), REFL(A,C), REFL(A,D),
SIM(A,B), SIM(A,C), SIM(A,D),
TRANS(A,B), TRANS(A,C), TRANS(A,D)

(RESP: F, V, V,
F, F, F,
F, F, V)

E A GENTE FICOU DE VER HOJE A PARTE DO "JUSTIFIQUE" ("DEMONSTRE")... MAS VAMOS DEIXAR ISTO PRA DAQUI A POUCO.

AS DEFINIÇÕES ERAM:

$\mathrm{Refl}(P,S) :=$
$\quad \forall p \in P.\ pSp$
$\mathrm{Sim}(P,S) :=$
$\quad \forall p,q \in P.\ pSq \to qSp$
$\mathrm{Trans}(P,S) :=$
$\quad \forall p,q,r \in P.$
$\quad (pSq \land qSr \to pSr)$
$\mathrm{Antisim}(P,S) :=$
$\quad \forall p,q \in P.$
$\quad (pSq \land qSp \to p=q)$

AS TRÊS PRIMEIRAS — REFLEXIVIDADE, SIMETRIA, TRANSITIVIDADE, NÓS VIMOS NA AULA PASSADA, E A ÚLTIMA — ANTI-SIMETRIA, É NOVIDADE.

VAMOS COMEÇAR POR EXERCÍCIOS — E PELAS DICAS PRA ELES. ANTI-SIMETRIA É ALGO MEIO MISTERIOSO À PRIMEIRA VISTA...

EXERCÍCIOS:
DÊ, PRA CADA UM DOS PROBLEMAS ABAIXO, UM GRAFO DIRECIONADO (P,S) QUE OBEDECE AS CONDIÇÕES DELE.

1. $\mathrm{Refl}(P,S) \land \mathrm{Antisim}(P,S)$
2. $\mathrm{Refl}(P,S) \land \neg\mathrm{Antisim}(P,S)$
3. $\neg\mathrm{Refl}(P,S) \land \mathrm{Antisim}(P,S)$
4. $\neg\mathrm{Refl}(P,S) \land \neg\mathrm{Antisim}(P,S)$
5. $\mathrm{Sim}(P,S) \land \mathrm{Antisim}(P,S)$
6. $\mathrm{Sim}(P,S) \land \neg\mathrm{Antisim}(P,S)$
7. $\neg\mathrm{Sim}(P,S) \land \mathrm{Antisim}(P,S)$
8. $\neg\mathrm{Sim}(P,S) \land \neg\mathrm{Antisim}(P,S)$

DICAS: CHUTAR E TESTAR!!! DÁ PRA FAZER TODOS OS ITENS COM $P=\{2,3\}$.

LEMBRE QUE NA SEÇÃO SOBRE EQUIVALÊNCIAS LÓGICAS DO LIVRO VOCÊS VIRAM AS "LEIS DE DE MORGAN", QUE NOS DIZEM COMO "PASSAR O '¬' PRA DENTRO DO '∧' E DO '∨'"...

$$\neg(P \land Q) = \neg P \lor \neg Q$$
$$\neg(P \lor Q) = \neg P \land \neg Q$$

...E NA SEÇÃO SOBRE QUANTIFICADORES VOCÊS VIRAM ALGO PARECIDO PARA "∀" E "∃":

$$\neg \forall a \in A.\ P(a) = \exists a \in A.\ \neg P(a)$$
$$\neg \exists a \in A.\ P(a) = \forall a \in A.\ \neg P(a)$$

APLICAÇÃO:

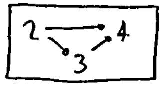
$\neg \mathrm{Antisim}(P,S)$
$= \neg \forall p,q \in P.\ (pSq \land qSp \to p=q)$
$= \exists p,q \in P.\ \neg(pSq \land qSp \to p=q)$
$= \exists p,q \in P.\ (pSq \land qSp) \land \neg(p=q)$
$= \exists p,q \in P.\ (pSq \land qSp) \land p \neq q$

EXERCÍCIO:
FAÇA ALGO PARECIDO PARA:

9. $\neg \mathrm{Refl}(P,S)$
10. $\neg \mathrm{Sim}(P,S)$
11. $\neg \mathrm{Trans}(P,S)$

12. CALCULE $\mathrm{Refl}(P,S)$, $\mathrm{Sim}(P,S)$, $\mathrm{Trans}(P,S)$ E $\mathrm{Antisim}(P,S)$ EM CADA UM DOS CASOS ABAIXO:

a) $(P,S) = \boxed{2 \to 3\circlearrowleft}$

b) $(P,S) =$ 

c) $(P,S) = \boxed{\circlearrowright 4 \rightleftarrows 5 \circlearrowleft}$

..."JUSTIFIQUE"

EM CASOS COMO REFL(A,B) NÓS PODEMOS CHEGAR NA SOLUÇÃO FAZENDO UM CÁLCULO:

$\mathrm{Refl}(A,B)$
$= \forall p \in A.\ pBp$
$= 1B1 \land 2B2 \land 3B3 \land \ldots \land 30B30$
$= F \land F \land F \land \ldots \land F$
$= F$

$\mathrm{Trans}(A,B)$
$= \underbrace{\forall p,q,r \in A}_{\substack{\text{3 geradores} \\ 8 \cdot 8 \cdot 8 = 512 \\ \text{casos !!}}}.\ (pBq \land qBr \to pBr)$

VAMOS VER QUE $\mathrm{Trans}(A,B) = F$, OU SEJA, QUE $\neg\mathrm{Trans}(A,B)$, OU, EQUIVALENTEMENTE:

$\neg \forall p,q,r \in A.\ (pBq \land qBr \to pBr)$,
$\exists p,q,r \in A.\ \neg(pBq \land qBr \to pBr)$,
$\exists p,q,r \in A.\ pBq \land qBr \land \neg pBr$.

SE $p=1$, $q=2$, $r=6$,

$$\underbrace{\underbrace{pBq}_{V} \land \underbrace{qBr}_{V} \land \underbrace{\neg \underbrace{pBr}_{F}}_{V}}_{V}$$

(↑ POR CONTRA-EXEMPLO — OU POR "PROVA DE AFIRMAÇÃO EXISTENCIAL").

VAMOS VER QUE $\mathrm{Trans}(A,D) = V$, OU SEJA, QUE:

$\forall p,q,r \in A.\ pDq \land qDr \to pDr$,
$\forall p,q,r \in A.\ \frac{q}{p} \in \mathbb{Z} \land \frac{r}{q} \in \mathbb{Z} \to \frac{r}{p} \in \mathbb{Z}$

... QUE É PARECIDO COM $a|b \land b|c \to a|c$!

MD 17/SET/2018

Hoje: $\cup, \cap, \exists!$, funsões.

União e intersesão:
Vocês já têm uma nosão de como elas funcionam, então vou só relembrar com exemplos:

$\{1,2,3,4\} \cup \{3,4,5,6\}$
$= \{1,2,3,4,5,6\}$

$\{1,2,3,4\} \cap \{3,4,5,6\}$
$= \{3,4\}$

$\{1,2,3,4\} \setminus \{3,4,5,6\}$
$= \{1,2\}$

Pronúncia: "$\setminus$" é "exceto"; $A \setminus B$ retorna o conjunto dos elementos de A que não estão em B...

$A \setminus B = \{a \in A \mid a \notin B\}$.

"$\exists!$" é "existe um único":

Formalmente,

$(\exists! a \in A.\ P(a)) =$
$(\exists a \in A.\ P(a)) \wedge$
$(\forall a', a'' \in A.\ P(a') \wedge P(a'') \to a' = a'')$.

A segunda parte significa:
Se dois elementos a' e a'' de A obedecem P – isto é, $P(a') \wedge P(a'')$ – então eles são iguais. Obs: isto lembra um pouco anti-simetria...

Funsões

Em MD nós vamos ver funsões como conjuntos.

Se $f : A \to B$ então o conjunto associado a f é $\{a \in A ; (a, f(a))\}$ – o "gráfico" (não "grafo"!) da funsão f.

Def (complicada, importante):
"$f : A \to B$" às vezes vai ser interpretada como uma proposisão que vai ser verdadeira ou falsa. Neste caso,

$(f : A \to B) =$
$(f \subseteq A \times B \ \wedge$
$\forall a \in A.\ \exists! b \in B.\ (a,b) \in f)$.

Exercícios:

1. Seja $f : \{-2,-1,0,1,2\} \to \mathbb{Z}$, $x \mapsto x^2$.
   Calcule o gráfico de f e represente-o graficamente.

2. Chame o gráfico de f de f !!.
   Calcule $f : \{-2,-1,0,1,2\} \to \mathbb{Z}$.

$\Leftarrow$ $f = \{(-2,4), (-1,1), (0,0), (1,1), (2,4)\}$

3. Calcule $f : \{0,1,2\} \to \mathbb{Z}$.

4. Calcule $f : \{0,1,2,3\} \to \mathbb{Z}$.

5. "Passe a negasão pra dentro", como fizemos na última aula:
   a) $\neg \exists! a \in \{0,1,2\}.\ P(a) = ?$
   b) $\neg (f : \{0,1,2\} \to \{3,4,5\}) = ?$

6. Expanda, usando a def (☆):
   a) $\{(0,1),(2,3)\} : \{0,2\} \to \{1,3\}$
   b) $g : \{0,2\} \to \mathbb{Z}$.

(☆)

$$\boxed{\begin{array}{r} f : \{-2,-1,0,1,2\} \to \mathbb{Z} \\ x \mapsto x^2 \end{array}}$$

$f(x) = x^2$

$f = \{\ \ldots\ \}$

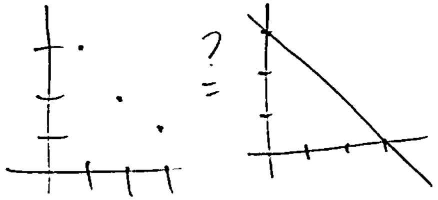
(☆) $\begin{bmatrix} f := \{(0,1),(2,3)\} \\ A := \{5,6,7\} \\ B := \{8,9,10\} \end{bmatrix} =$

$((\{(0,1),(2,3)\} : \{5,6,7\} \to \{8,9,10\}) =$
$(\{(0,1),(2,3)\} \subseteq \{5,6,7\} \times \{8,9,10\} \ \wedge$
$\forall a \in \{5,6,7\}.\ \exists! b \in \{8,9,10\}.\ (a,b) \in \{(0,1),(2,3)\})$

6. a) Se $f = \{(0,1),(2,3)\}$,
$A = \{0,2\}$,
$B = \{1,3\}$
então:

$(f : A \to B) =$
$(f \subseteq A \times B \ \wedge$
$\forall a \in A.\ \exists! b \in B.\ (a,b) \in f) =$
$(f \subseteq \{0,2\} \times \{1,3\} \ \wedge$
$\forall a \in \{0,2\}.\ \exists! b \in \{1,3\}.\ (a,b) \in f) =$
$(V \wedge$
$\ldots)$

$2 \cdot 3 = 6$
$(2,3)$ é um par
$\{0,1\} \times \{2,3\} = \{(0,2),(0,3),(1,2),(1,3)\}$



$(\exists! a \in \{1,2,3\}.\ a < 3) = ?$
$(\exists! a \in \{1,2,3\}.\ F) = ?$
$(\exists! a \in \{1,2,3\}.\ V) = ?$
$\neg(P \wedge Q) = \neg P \vee \neg Q$

MD 18/SET/2018

Hoje: $\cup, \cap, \backslash, \exists!$, Funções...

Antes da gente continuar com relações que são ordens vamos ver relações que são funções.

O início da sec. 2.0 do livro ("Funções") pode ser formalizado com só três definições:

$$\exists! a\in A.\ P(a) := (\exists a\in A.\ P(a) \land \forall a',a''\in A.\ P(a')\land P(a'')\to a'=a'') \qquad (☆)$$

(Obs: vimos algo parecido em anti-simetria!) e...

Funções

Se $f:A\to B$ então $f=\{a\in A;\ (a,f(a))\}$

Ou seja: funções em MD são conjuntos, e a gente chama isto de "o gráfico" (não "grafo"!) de f.

$f:A\to B$ às vezes vai ser uma expressão que retorna V ou F; nestes casos,

$$(f:A\to B) := (f\subseteq A\times B \land \forall a\in A.\ \exists! b\in B.\ (a,b)\in f). \qquad (☆☆)$$

Lembre que funções às vezes (p.ex. em C1) são definidas com uma notação em duas linhas:

nome, domínio, contradomínio

$$f:\{0,1,2\}\to\mathbb{Z}$$
$$x\mapsto x^2$$

variável, expressão

A segunda linha diz "como a função age" — neste caso, $f(x)=x^2$ — e a primeira linha diz que os inputs de f estão sempre em $\{0,1,2\}$ e os outputs em $\mathbb{Z}$...

$f(3)$ dá erro porque $3\notin\{0,1,2\}$.

Outro detalhe: as setas são diferentes!

$\longrightarrow$

$\longmapsto$

"$\exists! a\in A.\ P(a)$" é "existe um único $a\in A$ que obedece $P(a)$"

Exemplos:

Se $A=\{0,1,2\}$,

$(\exists! a\in A.\ a=1)=V$

$(\exists! a\in A.\ a<2)=F$

$(\exists! a\in A.\ V)=F$

$(\exists! a\in A.\ F)=F$

A expansão de "$\exists! a\in A.\ P(a)$" é complicada... A segunda parte, depois do "$\land$", diz que se $a'\in A$ e $a''\in A$ obedecem $P(a')$ e $P(a'')$ então $a'=a''$.

Exercícios:

1. Calculem $f:\{-2,-1,0,1,2\}\to\mathbb{Z}$, $x\mapsto x^2$

O resultado é algo como $f=\{\ldots\}$, que mostra f como conjunto de pares.

2. Expanda:

a) $\exists! b\in\{3,4,5\}.\ Q(b)$

b) $\{(0,1),(2,3)\}:\{0,2\}\to\{1,3\}$

c) $g: B\times C\to D\times E$

Dica:

A gente pode usar "se"s pra entender e usar as definições (☆) e (☆☆)...

P.ex.:

Se $f=\{(5,6)\}$, $A=\{1,2\}$ e $B=\mathbb{Z}$ então

$(f:A\to B) =$

$(f\subseteq A\times B \land \forall a\in A.\ \exists! b\in B.\ (a,b)\in f) =$

$(\{(5,6)\}\subseteq\{1,2\}\times\mathbb{Z} \land \forall a\in\{1,2\}.\ \exists! b\in\mathbb{Z}.\ (a,b)\in\{(5,6)\})$

Se $f(x)=x^2$ e $A=\{-2,-1,0,1,2\}$ então

$f = \{a\in A;\ (a,f(a))\}$

$= \{a\in\{-2,-1,0,1,2\};\ (a,a^2)\}$

$=$

Na aula passada nós usamos várias "fórmulas de De Morgan" pra passar o "$\neg$" pra dentro do $\exists, \forall, \land, \neg, \to$...

Agora faça o mesmo para o "$\exists!$". O truque é expandir a expressão com "$\exists!$" antes de "passar o '$\neg$' pra dentro".

Exercícios:

"Passe o '$\neg$' pra dentro":

3. a) $\neg\exists! b\in\{3,4,5\}.\ Q(b)$

b) $\neg\exists! a\in A.\ P(a)$

c) $\neg(f:A\to B)$

d) $\neg(g:B\times C\to D\times E)$

e) $\neg(\{(0,1),(2,3)\}:\{0,2\}\to\{1,3\})$

Na aula passada vimos vários exercícios de "calcular" (no olhômetro) que relações, ou grafos direcionados, eram reflexivos, simétricos, transitivos, anti-simétricos...

Agora vamos fazer algo parecido, mas calculando se $(f:A\to B)$ dá V ou F...

Seja $g:\{0,1,2\}\to\mathbb{Z}$, $x\mapsto x^2$.

Repare que g é um conjunto: $g=\{(0,0),(1,1),(2,4)\}$.

Exercício: Calculem:

4. a) $g:\{0,1,2\}\to\{0,1,2,3,4\}$

b) $g:\{0,1,2\}\to\{0,1,2\}$

c) $g:\{0,1,2,3\}\to\{0,1,2,3,4\}$

d) $g:\{0,1\}\to\{0,1,2,3,4\}$

e) $\{(0,1),(0,2)\}:\{0,1\}\to\{1,2\}$.

F !!

f

F: $A\in\{0,1,2,3\}$!!

$(\{8\}) = \{8\} \neq 8 = (8)$

$\{8\} = \{(8)\}$

Obs: na seção sobre listas do livro o autor não discute notação para listas de um elemento! Será que (8) é 8? Ou é uma lista de comprimento 1?

MD 19/set/2018

Hoje:
Funções injetivas, sobrejetivas e bijetivas; inversas de relações e funções.

Defs:
Se $f: A \to B$ então a imagem de f, $\mathrm{Im}(f)$, é definida por: $\mathrm{Im}(f) := \{a \in A; f(a)\}$.
(Note que $\mathrm{Im}(f) \subseteq B$).

Uma função $f: A \to B$ é injetiva se ela leva elementos diferentes em elementos diferentes.
Defs:
$f: A \to B$ é injetiva
$:= \forall a', a'' \in A.\ f(a') = f(a'') \to a' = a''$.
Uma função $f: A \to B$ é sobrejetiva se $\forall b \in B.\ \exists a \in A.\ f(a) = b$.

Ser injetiva ou sobrejetiva são condições extras sobre uma função...
Ex: $f: A \to B$ é sobrejetiva
$\leftrightarrow (f \subseteq A \times B \land \forall a \in A.\ \exists! b \in B.\ (a,b) \in f)$
$\land (\forall b \in B.\ \exists a \in A.\ f(a) = b)$.

Exercícios

1) "Passe o '¬' pra dentro" como na aula passada, e consiga uma caracterização com "∃" para
a) Funções não-injetivas
b) Funções não-sobrejetivas.

2) Exiba uma função $f: A \to B$ que
a) seja injetiva,
b) não seja injetiva,
c) seja sobrejetiva,
d) não seja sobrejetiva.

3) Exiba duas funções diferentes $f, g: A \to B$ que sejam ao mesmo tempo injetivas e sobrejetivas. Use $A = \{0,1,2\}$ e $B = \{3,4,5\}$.

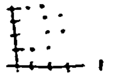
4) Tente fazer a mesma coisa que no exercício anterior mas com $A = \{0,1,2\}$ e $B = \{3,4\}$.

5) Idem, mas agora com $A = \{0,1,2\}$ e $B = \{3,4,5,6\}$.

Agora vamos voltar pra relações...
Lembre que algumas relações $R \subseteq A \times B$ são funções, mas não todas.

Algumas definições sobre relações reusam termos que definimos para funções.

Se $R \subseteq A \times B$, então
$\mathrm{Dom}(R) := \{(a,b) \in R; a\}$,
$\mathrm{Im}(R) := \{(a,b) \in R; b\}$,
$R^{-1} := \{(a,b) \in R; (b,a)\}$.

6) Se $A = \{1,2,3\}$, $B = \{1,2,3,4\}$, e $R =$ 

Então:
a) $\mathrm{Dom}(R) = ?$
b) $\mathrm{Im}(R) = ?$
c) $R^{-1} = ?$
d) $(R: A \to B) = ?$

7) Ainda com $A = \{1,2,3\}$ e $B = \{1,2,3,4\}$, exiba relações $R \subseteq A \times B$ tais que:
a) $\mathrm{Dom}(R) = \{2,3\}$
b) $\mathrm{Im}(R) = \{3,4\}$
c) $R: A \to B$
d) $R^{-1}: B \to A$

8) $\forall a \in A.\ \exists b \in B.\ aRb$
9) $\forall a \in A.\ \neg\exists b \in B.\ aRb$
10) $\exists a \in A.\ \forall b \in B.\ aRb$

11) Exiba uma função $f: A \to B$ com $A = \{1,2\}$, $B = \{(3,4),(5,6)\}$.

Obs (só para programadores): dá pra gente definir o "lambda" de algumas linguagens de programação usando a notação de conjuntos.
Exemplo:
$(\lambda x \in \{0,1,2\}.\ x+3)$
$= \{x \in \{0,1,2\}; (x, x+3)\}$
$= \{(0,3),(1,4),(2,5)\}$

Definição geral:
$(\lambda \underbrace{a}_{\text{var}} \in \underbrace{A}_{\text{conj}}.\ \underbrace{f(a)}_{\text{expr}}) = \{\underbrace{a \in A}_{\text{ger}}; \underbrace{(a, f(a))}_{\text{expr}}\}$

$(f: A \to B) = (f \subseteq A \times B$
$\land \forall a \in A.\ \exists! b \in B.\ (a,b) \in f)$

$\{\ \}: \{\ \} \to \{\ \}$

$f: \{(\ ,\ ),(\ ,\ )\} \to \ldots$
$f = \{(\ ,\ ),(\ ,\ )\}$

$A = \{1,2\}$, $B = \{(3,4),(5,6)\}$
$f = \{(1,3),(3,4)\}$,
$f: A \to B$
$A \times B = \{a \in A, b \in B; (a,b)\}$

a	b	(a,b)
1	(3,4)	(1,(3,4))
1	(5,6)	(1,(5,6))
2	(3,4)	(2,(3,4))
2	(5,6)	(2,(5,6))

$A =$

AGO
13 15
20 22
27 29 } 6
SET
03 05
10 12
17 19
24 26 } 8
1 | 3

P1: qualquer dia de 3/out em diante.

((1,2), 3)

MD 19/out/2018

Hoje: Funções injetivas e sobrejetivas; mais sobre relações

Lembre que

$(f: A \to B) :=$

$(f \subseteq A \times B \;\land$

$\forall a \in A.\ \exists! b \in B.\ (a,b) \in f)$...

Injetividade e sobrejetividade são condições extras sobre funções.

Uma função $f: A \to B$ é injetiva se $(\forall a', a'' \in A.$

$f(a') = f(a'') \to a' = a'')$ —

e se além disto vale $(f: A \to B)$.

Uma função $f: A \to B$ é sobrejetiva se $\forall b \in B.\ \exists a \in A.\ f(a) = b$

(e além disto $f: A \to B$).

Mais curto:

$f: A \to B$ é injetiva quando $\forall a', a'' \in A.\ f(a') = f(a'') \to a' = a''$,

$f: A \to B$ é sobrejetiva quando $\forall b \in B.\ \exists a \in A.\ f(a) = b$.

Exercícios:

1. Exiba uma função $f: A \to B$ tal que:
   a) f é injetiva,
   b) f não é injetiva,
   c) f é sobrejetora,
   d) f não é sobrejetora.

2. Use o truque de "passar o '¬' pra dentro" pra obter caracterizações com "∃" nos casos abaixo; suponham que $f: A \to B$ (← esta parte não vai ser negada).
   a) f não é injetiva,
   b) f não é sobrejetiva

3. Exiba duas funções diferentes, $f, g: A \to B$, que sejam ao mesmo tempo injetivas e sobrejetivas: use $A = \{0,1,2\}$, $B = \{3,4,5\}$.

4. Tente fazer o mesmo que acima mas com $B = \{3,4\}$. O que acontece?

5. Tente fazer o mesmo que acima mas com $B = \{3,4,5,6\}$. O que acontece?

Agora vamos voltar para relações.

Lembre que algumas relações $R \subseteq A \times B$ são funções $R: A \to B$, mas nem todas.

Algumas definições sobre relações reusam termos que nós definimos sobre funções.

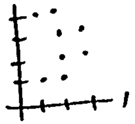
Defs:

$\mathrm{Dom}(R) := \{(a,b) \in R;\ a\}$

$\mathrm{Im}(R) := \{(a,b) \in R;\ b\}$

$R^{-1} := \{(a,b) \in R;\ (b,a)\}$

6. Se $A = \{1,2,3\}$, $B = \{1,2,3,4\}$,

$R =$ 

Então
   a) $\mathrm{Dom}(R) = ?$
   b) $\mathrm{Im}(R) = ?$
   c) $R^{-1} = ?$
   d) $(R: A \to B) = ?$

7. Ainda com $A = \{1,2,3\}$ e $B = \{1,2,3,4\}$, exiba relações $R \subseteq A \times B$ tais que:
   a) $\mathrm{Dom}(R) = \{1,2\}$,
   b) $\mathrm{Im}(R) = \{3,4\}$,
   c) $R: A \to B$
   d) $R^{-1}: B \to A$
   e) $\forall a \in A.\ \exists b \in B.\ aRb$
   f) $\forall a \in A.\ \exists b \in B.\ \neg aRb$
   g) $\forall a \in A.\ \neg \exists b \in B.\ aRb$
   h) $\forall a \in A.\ \neg \exists b \in B.\ \neg aRb$
   i) $\exists a \in A.\ \forall b \in B.\ aRb$

8. Exiba uma função $f: A \to B$ com $A = \{1,2\}$, $B = \{(3,4),(5,6)\}$.

$\forall a', a'' \in \{0,1,2\}.\ a' + a'' < 4$

$\forall a' \in \{0,1,2\}.\ \forall a'' \in \{0,1,2\}.\ a' + a'' < 4$

$(\forall a'' \in \{0,1,2\}.\ a' + a'' < 4)[a' := 0]$

$\land\ (\qquad)[a' := 1]$

$\land\ (\qquad)[a' := 2]$

$(\forall a'' \in \{0,1,2\}.\ a' + a'' < 4)[a' := 0]$

$= (\quad 0 + \quad)$

$=$

$=$

MD 27/set/2018

Hoje:
Bijeções,
caminhos em
grafos direcionados...

Lembre que:
$\exists! a \in A.\ P(a) :=$
$(\exists a \in A. P(a)\ \wedge$
$\forall a', a'' \in A.\ P(a') \wedge P(a'') \to a' = a'')$

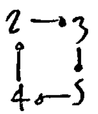
$(f : A \to B) :=$
$(f \subseteq A \times B\ \wedge$
$\forall a \in A. \exists! b \in B. (a,b) \in f)$

Se $f : A \to B$, então:
$\mathrm{Inj}(A,B,f) :=$
$(\forall a', a'' \in A.\ f(a') = f(a'') \to a' = a'')$
$\mathrm{Sobrej}(A,B,f) :=$
$(\forall b \in B. \exists a \in A. f(a) = b)$

Novidade: uma função $f : A \to B$ é bijetiva quando
$(\forall a \in A. \exists! b \in B. (a,b) \in f\ \wedge$
$\forall b \in B. \exists! a \in A. (a,b) \in f)$

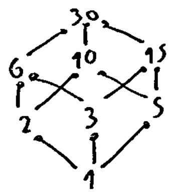
Depois vamos ver várias outras definições de bijetividade equivalentes a esta.

Exemplo:



Há muitas aulas atrás usamos isto aqui para exemplos:
$A = \{a,b,c \in \{0,1\};\ 2^a 3^b 5^c\}$
$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$
$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$
$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$

Def (novidade!):
Um caminho num grafo (P,S) ("em n passos") é uma função
$f : \{1, \dots, n+1\} \to P$
tal que $\forall i \in \{1, \dots, n\}.\ f(i) S f(i+1)$.

$(A,B) =$ 

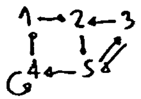
Exemplo: $\{(1,2),(2,6),(3,30)\} : \{1,2,3\} \to P$
$n+1;$
$n=2$
é um caminho em dois passos em (P,S)...
$(\forall i \in \{1,2\}.\ f(i) S f(i+1))$
$= (f(1) S f(2)\ \wedge$
$f(2) S f(3))$
$= (2S6 \wedge 6S30)$

Exercícios:
1. Exiba dois caminhos em três passos, diferentes, em (A,B).
2. Exiba um caminho em ciclo passos em (A,C).

Dizemos que um caminho $f : \{1, \dots, n+1\} \to P$ vai de a para b quando $f(1) = a$ e $f(n+1) = b$.

3. Exiba um caminho de 3 para 30 em (A,B).
4. Exiba um caminho de 1 para 30 em 5 passos em (A,C).

Seja (E,F) este grafo direcionado:



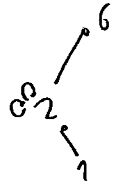
Dizemos que um caminho $f : \{1, \dots, n+1\} \to P$ em (P,S) é um ciclo quando $f(n+1) S f(1)$.

5. Exiba um caminho $f : \{1, \dots, n+1\} \to P$ em (E,F) que seja um ciclo para:
   a) $n=3$
   b) $n=2$
   c) $n=1$
   d) $n=0$
   e) $n=4$
   f) $n=5$

...Depois que vocês terminarem estes exercícios leiam o início da seção sobre "Grafos" no Scheinerman (seção 43 na 1ª edição) até a definição 43.3 ("adjacência").

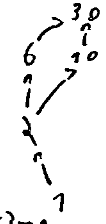
Aí
6. Faça o exercício 1 da seção 43.
7. Represente o grafo (c) do exercício na forma (V,E).
8. Seja "$\sim$" a relação de adjacência deste grafo; $\sim \subseteq V \times V$. Represente $\sim$ como conjunto.
9. Represente $(V, \sim)$ como grafo direcionado.

Para casa:
Leia o início da seção ("Árvores") - seção 46 na 1ª edição.
Entenda as definições de floresta e árvore.
O Scheinerman usa nessa seção uma definição de "ciclo" diferente da nossa - e você vai ter que ler as seções anteriores pra entender alguns conceitos que ele usa.



$f(1) = 2$
$f(2) = 5$
$f(3) = 4$
$f(n+1) S f(1)$?

$n=0,$
$\{(1,4)\} : E \to F$
f
$f(n+1) S f(1)$
$f(0+1)$
$f(1)$



$f : \{1, \dots, 6\} \to A$
$f(1) = 1$
$f(2) = 2$
$f(3) = 6$
$f(4) = 10$
$f(5) = 30$
$f(6) = 30$

$\underbrace{f(3) S f(4)}_{F}$
6 10

[ITU - /SET/2018]

HOJE: GRAFOS (SEÇÃO 43 DO SCHEINERMAN), E TALVEZ DÊ PRA GENTE VER UMAS COISAS SOBRE FUNÇÕES BIJETIVAS, INJETIVAS E SOBREJETIVAS...

VAMOS USAR UM EXEMPLO DE MUITAS AULAS ATRÁS:

$A = \{a,b,c \in \{0,1\}; 2^a 3^b 5^c\}$

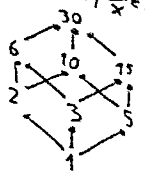
$A' = \{a,b,c \in \{0,1\}; 10 \cdot 2^a 3^b 5^c\}$

$B = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{2,3,5\}\}$

$C = \{(x,y) \in A \times A \mid \frac{y}{x} \in \{1,2,3,5\}\}$

$D = \{(x,y) \in A \times A \mid \frac{y}{x} \in \mathbb{Z}\}$

$(A,B) =$



LEMBRE QUE:

$\exists! a \in A.\ P(a) :=$
$(\exists a \in A.\ P(a)) \wedge (\forall a', a'' \in A.\ P(a') \wedge P(a'') \to a' = a'')$

$(f: A \to B) :=$
$(f \subseteq A \times B \ \wedge\ \forall a \in A.\ \exists! b \in B.\ (a,b) \in f)$

DEF (NOVIDADE):
UM CAMINHO (EM n PASSOS) NUM GRAFO DIRECIONADO (P,S) É UMA FUNÇÃO
$f: \{1,2,\ldots,n+1\} \to P$
QUE OBEDECE
$\forall i \in \{1,\ldots,n\}.\ f(i)\,S\,f(i+1)$.

EXEMPLO:
$f = \{(1,5),(2,15),(3,30)\}$
É UM CAMINHO EM 2 PASSOS EM (A,B) — REPARE QUE $n=2$, E
$(\forall i \in \{1,2\}.\ f(i)\,B\,f(i+1))$
$= (f(1)\,B\,f(2) \wedge f(2)\,B\,f(3))$
$= (5,15) \in B \wedge (15,30) \in B$.

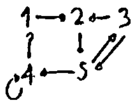
EXERCÍCIOS:
1. EXIBA DOIS CAMINHOS EM TRÊS PASSOS, DIFERENTES, EM (A,B).
2. EXIBA UM CAMINHO EM CINCO PASSOS EM (A,C).

DIZEMOS QUE UM CAMINHO $f: \{1,\ldots,n+1\} \to P$ VAI DE a PARA b QUANDO $f(1) = a$ E $f(n+1) = b$.

3. EXIBA UM CAMINHO DE 3 PARA 30 EM (A,B).
4. EXIBA UM CAMINHO DE 3 PARA 30 EM 5 PASSOS EM (A,C).

SEJA

$(E,F) =$



DIZEMOS QUE UM CAMINHO $f: \{1,\ldots,n+1\} \to P$ EM (P,S) É UM CICLO QUANDO $f(n+1)\,S\,f(1)$

5. EXIBA UM CAMINHO $f: \{1,\ldots,n+1\} \to P$ EM (E,F) QUE SEJA UM CICLO, PARA:
   a) $n=3$
   b) $n=2$
   c) $n=1$
   d) $n=0$
   e) $n=4$
   f) $n=5$

DEPOIS QUE VOCÊS TERMINAREM TUDO ISTO LEIAM O INÍCIO DA SEÇÃO SOBRE GRAFOS DO SCHEINERMAN (SEÇÃO 43 NA 1ª EDIÇÃO) ATÉ A DEFINIÇÃO 43.3 ("ADJACÊNCIA").

AÍ:
6. FAÇA O EXERCÍCIO 1 DA SEÇÃO 43.
7. REPRESENTE O GRAFO (c) DO EXERCÍCIO ANTERIOR NA FORMA (V,E)
8. SEJA "$\sim$" A RELAÇÃO DE EQUIVALÊNCIA DESTE GRAFO; $\sim \subseteq V \times V$. REPRESENTE $\sim$ COMO CONJUNTO.
9. REPRESENTE $(V,\sim)$ COMO GRAFO DIRECIONADO.

PRA CASA: LEIA O INÍCIO DA SEÇÃO "ÁRVORES" - SEC. 46 NA 1ª EDIÇÃO. ENTENDA AS DEFINIÇÕES DE FLORESTA E ÁRVORE. O SCHEINERMAN USA UMA DEFINIÇÃO DE "CICLO" DIFERENTE DA NOSSA - E VOCÊ VAI TER QUE LER AS SEÇÕES ANTERIORES PRA ENTENDER ALGUNS CONCEITOS QUE ELE USA.

I) $f = \{(1,1),(2,2),(3,5),(4,4)\}$

II) $f = \{(1,1),(2,2),(3,5),(4,4),(5,1)\}$

A f DO I É UM CICLO?
$n=4$; $f(\underbrace{\underbrace{4+1}_{5}}_{1})\,F\,\underbrace{f(1)}_{1}$

1. TRÊS PASSOS:
$n = 3$,
$f: \{1,2,3,4\} \to P$,
$P = A$.

AGORA: CHUTAR E TESTAR!

$f = \{(1,6),(2,6),(3,6),(4,6)\}$
ISTO É UM CAMINHO EM 3 PASSOS EM (A,B)?
SE FOR, ELE DEVE OBEDECER
$(\forall i \in \{1,2,3\}.\ f(i)\,B\,f(i+1))$
$= (f(1)\,B\,f(1+1)) \wedge (f(2)\,B\,f(2+1)) \wedge (f(3)\,B\,f(3+1))$
$= (6B6 \wedge 6B6 \wedge 6B6)$
$= F \wedge F \wedge F$
$= F$!!

OUTRO CHUTE:
$f = \{(1,1),(2,2),(3,6),(4,30)\}$
ISTO É UM CAMINHO EM 3 PASSOS EM (A,B)?
SE FOR, ELE DEVE OBEDECER
$(\forall i \in \{1,2,3\}.\ f(i)\,B\,f(i+1))$
$= f(1)\,B\,f(2) \wedge f(2)\,B\,f(3) \wedge f(3)\,B\,f(4)$
$= 1B2 \wedge 2B6 \wedge 6B30$
$= V \wedge V \wedge V$
$= V$!!

OBSERVAÇÕES (PRÓXIMA AULA!):
I) O SCHEINERMAN DEFINE "CAMINHOS" E "PASSEIOS" — E A IDÉIA DE FUNÇÃO INJETIVA VAI SER ÚTIL PRA FORMALIZAR TUDO...
II) EM (V,E) O E É UM CONJUNTO DE CONJUNTOS DE DOIS ELEMENTOS CADA... QUAL A DEFINIÇÃO FORMAL DE "$\{42,99,200,42\}$ TEM 3 ELEMENTOS"?

MD 26/set/2018

Se organizem em grupos pra todo mundo poder consultar o Scheinerman! Vamos começar revendo uns exercícios...

① Represente o grafo do exercício (c) na forma (V,E) ← Seção 43 ("Grafos") Exercícios: p. 391

② Represente a relação de adjacência $\sim \subseteq V \times V$ como conjunto

③ Represente $(V,\sim)$ como grafo direcionado.

④ Entenda as definições de passeio, caminho e ciclo do Scheinerman.
OBS: ele usa definições diferentes das nossas!
Dê exemplos de passeios, caminhos e ciclos no grafo (c).

⑤ Releia as definições de função injetiva e função sobrejetiva no Scheinerman. Ele usa definições diferentes das nossas, mas equivalentes às nossas.

⑥ Sejam $A=\{1,2,3\}$ e $B=\{1,2,3,4\}$.
Existem funções
ⓐ injetivas de A em B?
ⓑ injetivas de B em A?
ⓒ sobrejetivas de A em B?
ⓓ sobrejetivas de B em A?

Aviso: o livro intercala, no meio das seções sobre objetos matemáticos, técnicas de prova.
Por exemplo, como escrever uma demonstração de que uma função é injetiva (como séries de passos)

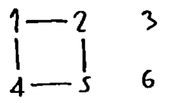
Hip: $\sim = \{1, 2, (3,4)\}$!! ⌢

Hip: $\sim = \{\{1,2\},\{1,4\},\{2,5\},\{4,5\}\}$

$1 \sim 2 \leftrightarrow (1,2) \in \sim$

Que condições o conjunto $\sim$ deve obedecer?
$\sim \subseteq V \times V$,
$(1,2) \in \sim$,
$(2,3) \notin \sim$,

$\{\{(1,2),(2,1)\},\{(1,4),(4,1)\}\}$



$1 \sim 2 = V$
$2 \sim 3 = F$
$\{\underbrace{1 \sim 2}_{V}\} = \{V\} \neq V$!! ⌢

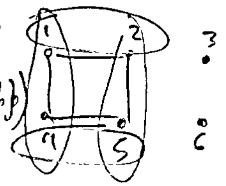
$uRv \leftrightarrow (u,v) \in R$
$u \sim v \leftrightarrow (u,v) \in \sim$

$1 \sim 2 \quad (1,2) \in \sim$

$(A,B) = (\{1,2\},\{\{3,4\},\{5,6\}\})$
$\sim = \{1,2\},\{3,4\},\{5,6\}$!! ⌢

$(1,2) = (2,1)$
$\{1,2\} = \{2,1\}$

$G = (\{1,2,3,4,5,6\},\{\{1,2\},\{2,5\},\{1,4\},\{4,5\}\})$



V, E

V: {1,2,3,4,5,6}

MD 26/set/2018

Vamos voltar pros exercícios da última aula...

(Re)leia a seção sobre grafos no livro (sec. 4.3 na 1ª edição).

① Represente o grafo do item (c) do exercício 1 dessa seção na forma (V,E).

② A relação de adjacência $\sim\ \subseteq V \times V$ é um conjunto. Que conjunto é esse?

③ Represente graficamente o grafo direcionado $(V,\sim)$.

Aviso: a gente vai passar a usar o livro cada vez mais — e vamos traduzir várias das coisas que ele faz meio em português e meio em linguagem matemática pra uma linguagem mais formal...

④ Leia as definições do livro de <u>passeio</u>, <u>caminho</u> e <u>ciclo</u>. Elas são um pouco diferentes das nossas, e algumas <u>não são equivalentes</u> às que eu pus no quadro. Exiba alguns passeios, caminhos e ciclos — no sentido do Scheinerman — como listas e conjuntos.

⑤ Leia as definições do livro de função injetiva e sobrejetiva. Elas são um pouco diferentes das nossas, mas são equivalentes às nossas definições formais. Sejam $A=\{1,2,3\}$ e $B=\{1,2,3,4\}$.

Descubra se existem funções

ⓐ injetivas de A em B,

ⓑ injetivas de B em A,

ⓒ sobrejetivas de A em B,

ⓓ sobrejetivas de B em A.

Dica: testar idéias concretas — exemplos concretos — é fácil, mas testar idéias mais abstratas é difícil... Truque: <u>escreva</u> sua idéia <u>como hipótese</u> e <u>teste-a</u>. Exemplo:

Hip: $\sim\ = \{1, 2, \{3, 4\}\}$

⋮

!!

Hip:

$\boxed{\text{Que condições o} \sim \text{deve obedecer?}}$

⑥ "Traduza" os passeios, caminhos e ciclos do seu ④ para funções $f:\{1,\dots,n+1\} \to P$. Quais dessas funções são injetivas?

Nestas últimas aulas nós só entendemos informalmente o que certas definições querem dizer e calculamos — geralmente "no olhômetro" — se certas sentenças são verdadeiras ou falsas. A partir da aula que vem nós vamos voltar para demonstrações — usando, por exemplo, os "esquemas de prova" do capítulo sobre funções.

(O livro intercala a exposição sobre objetos matemáticos novos com técnicas de demonstração sobre eles.)

Dica: o ② é <u>muito</u> importante

Dica: lembrem da notação para relações!

$aRb \leftrightarrow (a,b) \in R$

$a \sim b \leftrightarrow (a,b) \in \sim$

(c)

$$\begin{tikzcd}[arrows=dash] 1 \arrow[r] \arrow[d] & 2 \arrow[d] & 3 \\ 4 \arrow[r] & 5 & 6 \end{tikzcd}$$

$1 \sim 2 \leftrightarrow (1,2) \in \sim$

$1 \sim 2 = V$
$2 \sim 3 = F$
$6 \sim 6 = F$

Exercícios pra quem desistiu dos anteriores !!:

⑦ Liste todas as funções de $\{1,2,3\}$ em $\{4,5\}$.

⑧ Quais delas são injetivas?

⑨ Quais são sobrejetivas?

⑩ Liste todas as funções de $\{1,2\}$ em $\{3,4,5\}$.

⑪ Quais são injetivas?

⑫ Quais são sobrejetivas?

Algumas respostas...

① $G = (V,E)$
$= (\{1,2,3,4,5,6\},$
$\{\{1,2\},\{1,4\},\{2,5\},\{4,5\}\})$

② $V \times V = \{(1,1),(1,2),\dots,(1,6),$
$(2,1),(2,2),\dots,(2,6),$
$\vdots$
$(6,1),(6,2),\dots,(6,6)\}$ (6×6 = 36 elementos)

$\sim\ \subseteq V \times V$

$1 \sim 1 = F \quad 1 \sim 2 = V \quad 1 \sim 3 = F \quad \dots \quad 1 \sim 6 = F$
$2 \sim 1 = V \quad 2 \sim 2 = F \quad \dots$
$\vdots$
$6 \sim 6 = F$

$(1,1) \notin \sim \quad (1,2) \in \sim \quad (1,3) \notin \sim \quad \dots$
$(6,6) \notin \sim$

$\sim\ = \{(1,2),(1,4),(2,1),(2,5),$
$(4,1),(4,5),(5,2),(5,4)\}$

③ $(V,\sim)$ é um grafo direcionado

$$\begin{tikzcd} 1 \arrow[r, shift left] \arrow[d, shift left] & 2 \arrow[l, shift left] \arrow[d, shift left] & 3 \\ 4 \arrow[u, shift left] \arrow[r, shift left] & 5 \arrow[u, shift left] \arrow[l, shift left] & 6 \end{tikzcd}$$

MD 2/OUT/2018

OBS: ONTEM EU NÃO DEI AULA PRA TURMA GRANDE PORQUE EU ESTAVA DOENTE.
HOJE VAI SER SÓ UMA AULA DE REVISÃO E DÚVIDAS.

PRIORIDADES:

- MATERIAL SOBRE CONJUNTOS (FOLHAS 5 A 9 DE UM MATERIAL QUE EU FIZ PRA GEOMETRIA ANALÍTICA)
- <u>CONTEXTOS</u> EM <u>DEMONSTRAÇÕES</u> (AULAS DE 26/AGO ATÉ 5/SET)
  - NOTAÇÃO COM "$\vdash$",
  - CONTRA-EXEMPLOS,
  - O ERRO MAIS COMUM (VER LISTA MANUSCRITA 2 - AS COISAS SOBRE VARIÁVEIS NA TERCEIRA COLUNA DELA)

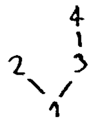
MD 8/out/2018

Hoje:

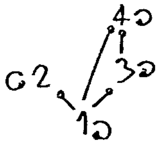
- Conjuntos parcialmente ordenados (cap. 10, sec. 50)
- Operações sobre conjuntos (seção 10)

O livro usa uma notação chamada "diagramas de Hasse" para representar conjuntos P.O.s...

Exemplo:



Em notação de grafos direcionados isto vira:



Mais precisamente... Se $R \subseteq A \times A$ então o fecho reflexivo de R é uma relação $S \subseteq A \times A$ que "acrescenta à R as setas necessárias para que ela fique reflexiva"... (os loops)

E o fecho transitivo de $R \subseteq A \times A$ é uma relação $T \subseteq A \times A$ que "acrescenta à R as setas necessárias para que ela fique transitiva"... (as compostas).

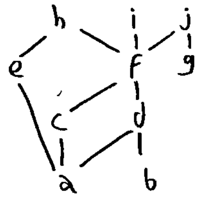
Notação: se $R \subseteq A \times A$ então denotamos o fecho reflexivo e transitivo de R por R^*.

(Mas vamos voltar a isto depois).

Idéia: aR^*b, ou $a \le b$, se e só se dá pra ir de a pra b seguindo as setas sem andar na contramão... ou, ao invés de setas, seguindo as linhas do diagrama de Hasse andando sempre pra cima...

$\boxed{\text{P1: 29/out}}$

Exercício 1, p. 459 na 1ª edição...



$a \le d$ = V
$a \le f$ = V
$c \le j$ = V
$a \le b$ = F
$f \le b$ = F
$b \le a$ = F
$g \le g$ = V

Dica: Leiam a seção 10!!!

Exercício 20:

"Os símbolos $\wedge$ e $\vee$ são versões (em conjuntos) dos símbolos $\cap$ e $\cup$"

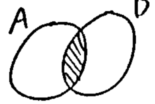
$$\underbrace{\begin{array}{l} x \in A \cap B \\ x \in A \cup B \end{array}}_{\text{"conjuntos"}} \begin{array}{c} \leftrightarrow \\ \leftrightarrow \end{array} \underbrace{\begin{array}{l} x \in A \wedge x \in B \\ x \in A \vee x \in B \end{array}}_{\text{"lógica"}}$$

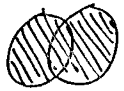
Outra forma: (lembrem que a gente agora entende proposições "abstratas"...)

$$\{a \in A \mid P(a)\} \cap \{a \in A \mid Q(a)\} = \{a \in A \mid P(a) \wedge Q(a)\}$$
$$\{a \in A \mid P(a)\} \cup \{a \in A \mid Q(a)\} = \{a \in A \mid P(a) \vee Q(a)\}$$

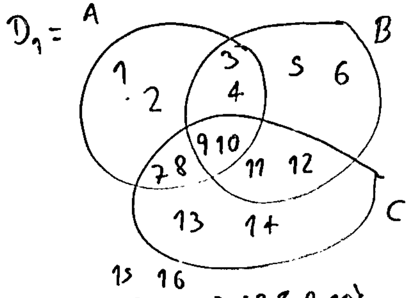
Vamos usar isso pra visualizar propriedades (como conjuntos).

O livro usa diagramas como estes:

$A \cap B =$ 

$A \cup B =$ 

Exercícios de tradução:

$D_1 =$ 

$A = \{1, 2, 3, 4, 7, 8, 9, 10\}$
$B =$
$C =$
$A \cap B =$
$B \cup C =$

$B \setminus C =$
$(A \cup B) \cap C =$
$A \cup (B \cap C) =$

... e representem graficamente, numa notação como esta, cada um dos conjuntos acima.

O teorema 10.3 tem uma idéia muito importante - e ele aponta pra vários outros teoremas e exercícios relacionados.

A demonstração dele usa uma técnica de tradução que nós vamos usar bastante - e introduz uma novidade (pra nós):

$$\{x : x \in A \vee x \in (B \cup C)\}$$
$$\text{"="} \ \{x \in \mathcal{U} \mid x \in A \vee x \in (B \cup C)\}$$

O livro às vezes usa geradores sem "$\in$". O exercício 17 discute a idéia por trás disto - a de que existe um "conjunto global" ou "universo", $\mathcal{U}$, de todos os objetos matemáticos...

MD 8/out/2018

A demonstração do 10.3 – aliás, de uma das afirmações do teorema 10.3 – usa traduções...

$A\cap(B\cap C)$
$= \{x : x\in A\cap(B\cap C)\}$
$= \{x : x\in A \wedge x\in B\cap C\}$
$= \{x : x\in A \wedge (x\in B \wedge x\in C)\}$
$= \{x : (x\in A \wedge x\in B) \wedge x\in C\}$
$= \{x : x\in A\cap B \wedge x\in C\}$
$= \{x : x\in (A\cap B)\cap C\}$
$= (A\cap B)\cap C$

Exercício importante, pra agora:
mostre que
$A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$.
Dica: use a tradução acima e as "equivalências lógicas" da seção 5.

O "conjunto das partes"

Na notação do livro,
$$2^B = \{A : A\subseteq B\}$$
A notação padrão é "$\mathcal{P}(B)$" ao invés de "2^B".

Exemplo: $\mathcal{P}(\{3,4\}) = \{\emptyset, \{3\}, \{4\}, \{3,4\}\}$.

Exercício: calcule $\mathcal{P}(\{2,3,(4,5)\})$.

O conjunto das funções de A em B

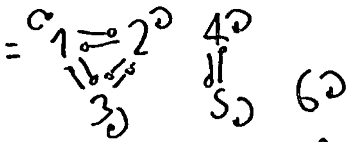
... é escrito como B^A.
Toda função $f: A\to B$ é um elemento de B^A.
Exercício: sejam $A=\{2,3,(4,5)\}$ e $B=\{0,1\}$.
Calcule B^A.

Uma das últimas idéias muito importantes que a gente vai ter que ver – superficialmente – pra P1 é a idéia de partições.

Def 13.1 do livro:
Seja A um conjunto.
Uma partição de A é um conjunto $\mathcal{A}$ de subconjuntos não-vazios de A, disjuntos dois a dois, cuja união é A.

$\Rightarrow$ Se $B\in\mathcal{A}$ então $B\subseteq A$, $B\neq\emptyset$;
Se $B,C\in\mathcal{A}$, $B\neq C\to B\cap C=\emptyset$;
$\bigcup\mathcal{A} = A$ (???)

Def: $\bigcup\mathcal{A} = \{x : \exists A\in\mathcal{A}. x\in A\}$.

Isto está relacionado com relações de equivalência, que são relações reflexivas, simétricas e transitivas.
P. ex.: $P=\{1,2,3,4,5,6\}$,
$S=$ 

A partição associada a (P,S) é
$\{\{1,2,3\},\{4,5\},\{6\}\}\subseteq\mathcal{P}(P)$
$\in\mathcal{P}(\mathcal{P}(P))$

Exercícios:
Seja $\mathcal{C} = \{\{2,3\},\{3,4,5\}\}$.
Tente mostrar, usando as traduções que vimos hoje, que $2\in\bigcup\mathcal{C}$ e que $6\notin\bigcup\mathcal{C}$.

MD – 23/out./2018

HOJE: LISTA DE EXERCÍCIOS SOBRE ORDEM PARCIAL EM PROPOSIÇÕES!

A LISTA TEM ALGUNS ERROS DE DIGITAÇÃO...

AS DEFINIÇÕES DAS PROPOSIÇÕES P, Q, R SAÍRAM SEM ALGUNS PARÊNTESES NA LISTA.

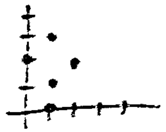
O CERTO É:

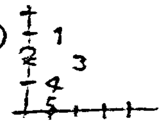
$P = \{((x,y),z) \mid (x,y) \in A,\ z = (x \leq 1 \wedge y \geq 1)\}$

$Q = \{((x,y),z) \mid (x,y) \in A,\ z = (1 \leq x \leq 2 \wedge y \geq 1)\}$

$R = \{((x,y),z) \mid (x,y) \in A,\ z = (0 \leq x \leq 2 \wedge y \leq 1)\}$

GABARITO DE ALGUNS EXERCÍCIOS:

1) 

2) 

$(x,y) \in A$	z
(0,0)	F
(1,0)	
(2,0)	
(3,0)	
(0,1)	

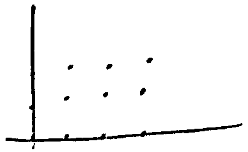
P = V V F F / V V F F / F F F F

Q = F V V F / F V V F / F F F F

x	y	$P(x,y) \wedge Q(x,y)$
1	2	V

$\underbrace{\underbrace{x \leq 1}_{\underbrace{0}_{V}} \wedge \underbrace{y \geq 1}_{\underbrace{0}_{F}}}_{F}$

$P(x,y) \to Q(x,y) =$ F V V V / F V V V / V V V V



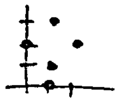
P	Q	$P \wedge Q$	$P \vee Q$	$P \to Q$
F	F	F	F	V
F	V	F	V	V
V	F	F	V	F
V	V	V	V	V

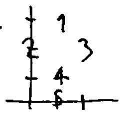
$\underbrace{\underbrace{P(x,y)}_{} \vee \underbrace{(\underbrace{Q(x,y)}_{} \wedge \underbrace{R(x,y)}_{})}_{}}_{}$

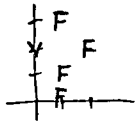
MD 24/OUT/2018

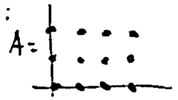
HOJE:
- DÚVIDAS DA LISTA DE EXERCÍCIOS
- ÚLTIMOS AVISOS ANTES DA PROVA

DICAS:

1: 

2: 

3: 

4: 

$P = \begin{array}{cccc} V & V & F & F \\ V & V & F & F \\ \cancel{F} & \cancel{F} & \cancel{F} & \cancel{F} \end{array}$

FICA MAIS FÁCIL DESENHAR E PENSAR SE A GENTE NÃO DESENHA OS EIXOS E DESENHA A FRONTEIRA ENTRE OS Vs E Fs...

$P = \begin{array}{cccc} V & V & F & F \\ V & V & F & F \\ F & F & F & F \end{array}$

ERROS DE DIGITAÇÃO NA LISTA:
- NAS DEFINIÇÕES DE P, Q, R ERA $(x,y) \in A$, NÃO $x, y \in A$.
- 11) $P(x,y) \vee (Q(x,y) \wedge R(x,y))$

UMA DAS COISAS MAIS IMPORTANTES DA PROVA É VOCÊS SABEREM LIDAR BEM COM DEFINIÇÕES.

VÁRIAS PESSOAS TIVERAM DIFICULDADE COM ISTO AQUI:

$$P \leq Q := \forall (x,y) \in A.\ P(x,y) \to Q(x,y)$$

DICA: A SEÇÃO 50 ("FUNDAMENTOS DOS CONJUNTOS PARCIALMENTE ORDENADOS") TEM UM TRECHO QUE TEM O TÍTULO "NOTAÇÃO E LINGUAGEM".

ELEMENTOS DE S:

$\top = \begin{array}{cccc} V & V & V & V \\ V & V & V & V \\ V & V & V & V \end{array}$

$\bot = \begin{array}{cccc} F & F & F & F \\ F & F & F & F \\ F & F & F & F \end{array}$

$P(x,y) = \begin{array}{cccc} V & V & F & F \\ V & V & F & F \\ F & F & F & F \end{array}$

$Q(x,y) = \begin{array}{cccc} F & V & V & F \\ F & V & V & F \\ F & F & F & F \end{array}$

$P(x,y) \wedge Q(x,y) = \begin{array}{cccc} F & V & F & F \\ F & V & F & F \\ F & F & F & F \end{array}$

$P(x,y) \vee Q(x,y) = \begin{array}{cccc} V & V & V & F \\ V & V & V & F \\ F & F & F & F \end{array}$

$R(x,y) = \begin{array}{cccc} F & F & F & F \\ V & V & V & F \\ V & V & V & F \end{array}$

$P(x,y) \to Q(x,y) = \begin{array}{cccc} F & V & V & V \\ F & V & V & V \\ V & V & V & V \end{array}$

OBS: $\top = V$
$\bot = F$

$$a \not\leq b \;:=\; \neg (a \leq b)$$

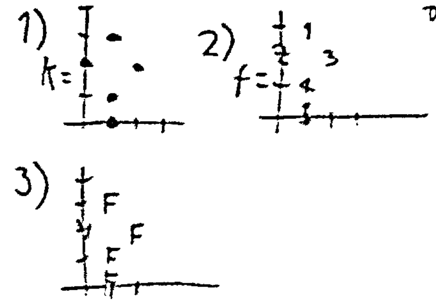
$(x \leq y) \leq Q =$
$\forall (x,y) \in A.\ (x \leq y) \to Q(x,y)$

$P(x,y) \wedge Q(x,y) \leq P(x,y) =$
$\forall (x,y) \in A.\ \underbrace{P(x,y) \wedge Q(x,y)}_{\begin{array}{cccc} F & V & F & F \\ F & V & F & F \\ F & F & F & F \end{array}} \to \underset{\begin{array}{cccc} V & V & F & F \\ V & V & F & F \\ F & F & F & F \end{array}}{P(x,y)}$

MD 24/out/2018

HOJE: ÚLTIMA AULA COM MATÉRIA DA P1! VAMOS TRABALHAR EM CIMA DA LISTA DE EXERCÍCIOS QUE EU MANDEI NA SEGUNDA — ELA É UM DESCULPA PRA GENTE APRENDER NA PRÁTICA AS IDÉIAS MAIS IMPORTANTES DE ORDENS PARCIAIS, E A ORDEM PARCIAL SOBRE AS PROPOSIÇÕES VAI SER MUITO ÚTIL PRA GENTE APRENDER LÓGICA "A SÉRIO" NA SEGUNDA PARTE DO CURSO.

DICAS:



DICA: NÃO DESENHE OS EIXOS E DESENHE A FRONTEIRA ENTRE OS Vs E Fs...

$$P = \begin{matrix} \boxed{\begin{matrix} V & V \\ V & V \end{matrix}} & \begin{matrix} F & F \\ F & F \end{matrix} \\ \begin{matrix} F & F \end{matrix} & \begin{matrix} F & F \end{matrix} \end{matrix}$$

DICA PRA PROVA: A PROVA VAI TER DEFINIÇÕES QUE VOCÊS NUNCA VIRAM ANTES... ENTÃO REVEJAM COM CUIDADO COMO NÓS FIZEMOS CADA DEFINIÇÃO DO CURSO ATÉ AGORA PRA SE FAMILIARIZAR COM A LINGUAGEM.

OBS: MUITA GENTE DA OUTRA TURMA SE ENROLOU COM A DEFINIÇÃO

$$\boxed{\begin{array}{l} P \le Q \;:= \\ \forall (x,y) \in A.\ P(x,y) \to Q(x,y). \end{array}} \quad ☆$$

$$☆ \left[P(x,y) := x \le y \right] =$$

$$\begin{array}{l} (x \le y) \le Q \;:= \\ \forall (x,y) \in A.\ (x \le y) \to Q(x,y) \end{array}$$

x	y	$x \le 1 \land y \ge 1$
0	0	F

$((0,0),F)$
x y z

x	y	P(x,y)	Q(x,y)	P(x,y) → Q(x,y)
0	0			
0	1			
0	2			
1	0			
1	1			
1	2			
2	0			
2	1			
2	2			
3	0			
3	1			
3	2			

MD 30/OUT/2018

QUESTÃO 1 DA PROVA DA TURMA O1[illegible]DE:

(*) TODO INTEIRO ÍMPAR É SOMA DE UM PAR E UM ÍMPAR.

1) REESCREVA ISSO DANDO NOMES PRAS VARIÁVEIS.

TODO INTEIRO ÍMPAR a...

2) ESCREVA A SUA DEMONSTRAÇÃO EM PORTUGUÊS.

3) TESTE A IDÉIA DA SUA DEMONSTRAÇÃO EM CASOS PARTICULARES - P.EX. a=43.

4) MOSTRE VÁRIOS MODOS DE EXPRESSAR a=42 COMO SOMA DE UM PAR E UM ÍMPAR.

5) ESCOLHA UM NÚMERO PAR E UM NÚMERO ÍMPAR. CALCULE A SOMA DOS DOIS. O RESULTADO DEU UM NÚMERO ÍMPAR?

$\{a \in \{2,3,4\}; (a,b)\}$

a	k	p
11	10	1
11	8	3
11	6	5
11	4	7
11	2	9
11	0	11
11	-2	13
11	-4	15
43	0	43
21	0	21
1	0	1
5	0	5
-5	0	-5
-99	0	-99

a (ÍMPAR)	k (PAR)	p (ÍMPAR)	k+p=a
43	20	23	V
21	20	1	V
1	0	1	V
5	2	3	V
-5	0	-5	V
-99	-98	-1	V

a	k	p
43	0	43
21	0	21
1	0	1
5	0	5
-5	0	-5
-99	0	-99

IDÉIAS:
$k=0$
$p=a$
$k+p=43$

UM ÍMPAR a=3
É SOMA DE
UM PAR k=2
E UM ÍMPAR a=3

$$\underbrace{a = k + a}_{} \quad \underbrace{3 = \underbrace{2+3}_{5}}_{F}$$

UM ÍMPAR a=43
É SOMA DE
UM PAR k=0
E UM ÍMPAR p=a=43

TODO ÍMPAR a
É SOMA DE
UM PAR k=0
E UM ÍMPAR p=a

k=a...

$a=3$

$a+k+a=$

$3+2+3=6$

$3+2+3=8$

$a+k+a$

DEF PAR: $N=2k$

" ÍMPAR: $P=2k+1$

1. V.

V.

5. $43=22+21$

$43=20+23$

$43=1+42$

$\{(k \in \mathbb{Z}; \ldots); k+p=a; \ldots\}$

[illegible]

[illegible]

1) [illegible]

[illegible]

2) [illegible]

3) [illegible]

4) [illegible]

5) [illegible]

[illegible]

[illegible]

[illegible]

[illegible]

MD 31/out/2018

HOJE: VAMOS COMEÇAR A VER DOIS SISTEMAS DEDUTIVOS "SÉRIOS", MAIS PRECISOS QUE OS QUE USAMOS ATÉ AGORA.

LEMBRE QUE NA LISTA DE EXERCÍCIOS DE ALGUMAS AULAS ATRÁS USAMOS:

$A =$,

$P = \begin{array}{cccc} \boxed{V\,V} & F & F \\ V\,V & F & F \\ F\,F & F & F \end{array}$,

$Q = \begin{array}{cccc} F & \boxed{V\,V} & F \\ F & V\,V & F \\ F & F\,F & F \end{array}$,

$R = \begin{array}{cccc} F & F & F & F \\ \boxed{V} & V & V & F \\ V & V & V & F \end{array}$.

SEJAM B, C, D OS SEGUINTES SUBCONJUNTOS DE A: $B =$, $C =$, $D =$

NOTE QUE $(x,y) \in B \leftrightarrow P(x,y)$,
$(x,y) \in C \leftrightarrow Q(x,y)$,
$(x,y) \in D \leftrightarrow R(x,y)$.

PRA ENTENDER SISTEMAS DEDUTIVOS "SERIOS" A GENTE PRECISA SABER LIDAR BEM COM PROPOSIÇÕES "ARBITRÁRIAS" (ABSTRATAS).

EXERCÍCIO:
DIGA ALGUNS VALORES DE $(x,y) \in A$ QUE OBEDECEM:

1

			(x,y)
P	Q	R	$(1,1)$
P	Q	$\neg R$	
P	$\neg Q$	R	
P	$\neg Q$	$\neg R$	
$\neg P$	Q	R	
$\neg P$	Q	$\neg R$	
$\neg P$	$\neg Q$	R	
$\neg P$	$\neg Q$	$\neg R$	

2

		x
$par(x)$	$primo(x)$	
$par(x)$	$\neg primo(x)$	
$\neg par(x)$	$primo(x)$	
$\neg par(x)$	$\neg primo(x)$	

OBS: NOS SISTEMAS QUE VAMOS VER A ORDEM "DIDÁTICA" CERTA É:
$\land, \to, \lor, \neg,$
$\forall, \exists$

O LIVRO USA A NOTAÇÃO "$\overline{B}$" PARA O "COMPLEMENTO" DO CONJUNTO B (COM RELAÇÃO A UM DETERMINADO UNIVERSO).

NA LISTA DE EXERCÍCIOS O "UNIVERSO" ERA O CONJUNTO A, E $\overline{B} = A \setminus B$.

3 REPRESENTE GRAFICAMENTE ALGUNS CONJUNTOS ASSOCIADOS ÀS PROPOSIÇÕES DA TABELA 1. POR EXEMPLO:

$\{(x,y) \in A \mid P(x,y) \land \neg Q(x,y) \land \neg R(x,y)\} =$
$B \cap \overline{C} \cap \overline{D} =$
$\cap$ $\cap$ $=$
$= \{(0,2)\}$.

... AGORA A GENTE VAI APRENDER A VISUALIZAR PROPOSIÇÕES COMO

$P, Q \vdash R$,

VISUALIZANDO QUANDO (OU: ONDE) ELAS SÃO VERDADEIRAS.

LEMBREM DAS TRADUÇÕES:

$P, Q \vdash R$

É ABREVIAÇÃO PARA

$P(x,y), Q(x,y) \vdash R(x,y)$

MAS VAMOS OMITIR OS "(x,y)"S E MANTER O UNIVERSO FIXO ($=A$).

$P, Q \vdash R$

PODE SER TRADUZIDO PARA $P \land Q \to R$, E

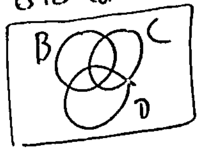
OS PONTOS DE A QUE OBEDECEM $P \land Q \to R$ SÃO OS EM QUE $P \land Q \to R$ É VERDADE, OU SEJA, OS EM QUE $\neg(P \land Q) \lor R$ É VERDADE, I.E.,

$(\neg P \lor \neg Q) \lor R =$

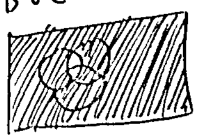
$\lor$ $\lor$ $=$

.

LEMBRE QUE TAMBÉM PODEMOS USAR UMA OUTRA NOTAÇÃO - MAIS GERAL E MAIS PADRÃO - PARA REPRESENTAR GRAFICAMENTE ESTES CONJUNTOS:



$\overline{B} \cup \overline{C} \cup D =$



LEMBRE QUE PODEMOS TRADUZIR CADA LINHA DE UMA PROVA COM "SUPONHA"S E "ENTÃO"S PARA UMA PROPOSIÇÃO COM "$\vdash$", E A PARTE DO "(POR ...)" À DIREITA INDICA QUE A LINHA NOVA É CONSEQUÊNCIA DE ALGUMAS LINHAS ANTERIORES...

MAIS NOTAÇÃO:

$$\frac{P \vdash Q \land R}{P \vdash R \land Q}$$

(com barra dupla)

A BARRA DUPLA É COMO UMA SANFONA FECHADA - QUE PODE SER EXPANDIDA (PRA UMA ÁRVORE TODA FEITA DE REGRAS VÁLIDAS).

NOTAÇÃO NOVA:

10) $P \vdash Q$
11) $P \vdash R$
12) $P \vdash Q \land R$

$$\Rightarrow \quad \frac{P \vdash Q \quad P \vdash R}{P \vdash Q \land R} \land I$$

A BARRA HORIZONTAL DIZ QUE SE AS PROPOSIÇÕES ACIMA DELA SÃO VERDADE A PROPOSIÇÃO ABAIXO VAI SER VERDADE TAMBÉM - PELA REGRA "$\land I$" ("INTRODUÇÃO DO $\land$").

OUTRA COMPLICAÇÃO:
QUANDO A GENTE DIZ QUE ISSO AQUI É UMA REGRA DE DEDUÇÃO,

$$\frac{P \vdash Q \quad P \vdash R}{P \vdash Q \land R} \land I \qquad (\star)$$

ESTAMOS DIZENDO QUE ESSA REGRA VALE PRA QUALQUER "INSTÂNCIA DE SUBSTITUIÇÃO" DISTO...

POR EXEMPLO,

$$(\star) \begin{bmatrix} P := a \in \mathbb{Z} \\ Q := primo(a) \\ R := impar(a) \end{bmatrix} =$$

$$\frac{a \in \mathbb{Z} \vdash primo(a) \quad a \in \mathbb{Z} \vdash impar(a)}{a \in \mathbb{Z} \vdash primo(a) \land impar(a)} \land I$$

VISUALMENTE:

$$\frac{P \to Q \quad P \to R}{P \to Q \land R} \land I$$

$(P \to Q) \land (P \to R) \to (P \to Q \land R)$

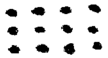
EXERCÍCIO: VISUALIZEM OS SUBCONJUNTOS DE A EM QUE

$$\underbrace{\underbrace{\underbrace{(P \to Q)}_{E} \land \underbrace{(P \to R)}_{F}}_{G} \to \underbrace{(P \to Q \land R)}_{H}}_{I}$$

MD 31/out/2018

Hoje: vamos começar a ver dois sistemas dedutivos "sérios", mais precisos que os que usamos até agora.

Lembre que na lista de exercícios de algumas aulas atrás usamos:

A = ,

$P = \begin{array}{cccc} \boxed{V\,V} & F & F \\ \boxed{V\,V} & F & F \\ F\,F & F & F \end{array}$,

$Q = \begin{array}{cccc} F & \boxed{V\,V} & F \\ F & \boxed{V\,V} & F \\ F & F\,F & F \end{array}$,

$R = \begin{array}{cccc} F & F & F & F \\ \boxed{V & V & V} & F \\ \boxed{V & V & V} & F \end{array}$.

Sejam B, C, D os seguintes subconjuntos de A:

B = ,

C = ,

D = .

Note que $(x,y) \in B \leftrightarrow P(x,y)$,
$(x,y) \in C \leftrightarrow Q(x,y)$,
$(x,y) \in D \leftrightarrow R(x,y)$.

O exercício de "visualize" ajuda a gente a entender onde as proposições são verdade...

Onde $P \to Q$
e $P \to R$
forem ambas verdade,
$P \to Q \land R$
vai ser verdade também.

(É mais fácil entender isto com "quando").

DEF: uma regra é admissível quando a sua tradução para uma expressão só com $\land, \lor, \to, \neg$, etc, é uma "tautologia" - isto é, é sempre verdadeira.

Exercício: mostre que

$$\dfrac{P \vdash Q \lor R}{P \vdash Q}$$

não é admissível, e

• mostrem que

$$\dfrac{P \vdash Q}{P \vdash Q \lor R}$$

é admissível.

Eu vou tentar apresentar as regras "básicas" deste sistema de árvores a partir de exemplos de árvores de dedução que usam elas - p.ex.:

$$\dfrac{\overline{P,Q,R \vdash R} \qquad \dfrac{\overline{P,Q,R \vdash Q} \qquad \overline{P,Q,R \vdash P}}{P,Q,R \vdash Q \land P}\land I}{P,Q,R \vdash R \land (Q \land P)}\land I$$

Uma solução:

$$\dfrac{P \vdash Q \lor R}{P \vdash Q}$$

vira

$(P \to Q \lor R) \to (P \to Q)$,

e podemos testar isto para cada valor de $P, Q, R \in \{F, V\}$...

P	Q	R	$(P \to Q \lor R) \to (P \to Q)$
F	F	F	V
F	F	V	V
F	V	F	V
F	V	V	V
V	F	F	V
V	F	V	F
V	V	F	V
V	V	V	V

MD 31/OUT/2018

Hoje: introdução a sistemas dedutivos "sérios"... Vamos primeiro ver uma versão do sistema "LK" de Gentzen (de "cálculo de sequentes") e depois vamos passar para Fitch.

Lembre que nas folhas de exercícios sobre proposições de algumas aulas atrás usamos:

$A = \{(x,y) \mid x \in \{0,1,2,3\}, y \in \{0,1,2\}\}$

e P, Q, R eram proposições sobre A:

$P = \begin{matrix} V&V&F&F \\ V&V&F&F \\ F&F&F&F \end{matrix}$, $Q = \begin{matrix} F&V&V&F \\ F&V&V&F \\ F&F&F&F \end{matrix}$, $R = \begin{matrix} F&F&F&F \\ V&V&V&F \\ V&V&V&F \end{matrix}$

$P(0,2) = V$
$P(1,0) = F$

No exercício 1 (do quadro da outra turma, que eu imprimi e distribuí), estamos abreviando $P(x,y)$ por P, $Q(x,y)$ por Q, $R(x,y)$ por R.

Quando e onde

Se sabemos que $x \in \mathbb{Z}$, $\neg par(x)$ e $primo(x)$, então x pode ser $1, 9, 15, \ldots$, ou $-1, -3, \ldots$.

Vamos ver uns truques pra visualizar onde cada proposição é verdadeira.

Dá pra representar subconjuntos de A com uma notação parecida com esta)...

Sejam $B = \{(0,2),(1,2),(0,1),(1,1)\}$,
C,
D;

Note que para todo $(x,y) \in A$ temos:

$P(x,y) \leftrightarrow (x,y) \in B$
$Q(x,y) \leftrightarrow (x,y) \in C$
$R(x,y) \leftrightarrow (x,y) \in D$

O livro usa a notação "$\overline{B}$" para o "complemento" de B; como nosso universo é A, $\overline{B} = A \setminus B$.

(3) O conjunto de soluções de cada linha da tabela do exercício (1) pode ser expresso em termos de $B, \overline{B}, C, \overline{C}, D, \overline{D}$.

Por exemplo, (x,y) obedece P, Q e $\neg R$ se e só se $(x,y) \in B \cap C \cap \overline{D}$.

"Traduza" as proposições abaixo para notação de conjuntos:

a) $P \land \neg Q$
b) $\neg P \land Q$
c) $P \to Q$
d) $P \to (Q \to R)$
e) F
f) V

Nós estávamos fazendo demonstrações usando um sistema com linhas numeradas que começavam com "vamos ver que", "suponha" e "então". Se traduzirmos cada linha dessas para a notação com "$\vdash$" deixando o contexto dela explícito, podemos ter algo assim:

10) $P \vdash Q$
11) $P \vdash R$
12) $P \vdash Q \land R$ (por 11, 12, por $\land I$)

(Compare com os passos 4, 5, 6 do gabarito da questão 1 da prova)

No sistema LK nós vamos escrever as demonstrações como árvores. O trecho acima vira:

$$\dfrac{P \vdash Q \quad P \vdash R}{P \vdash Q \land R} \land I \qquad (\star)$$

Vamos aos poucos ver quais são as regras "básicas" do LK.

Mais notação:

$$\dfrac{P \vdash Q \land R}{P \vdash R \land Q}$$

Que regras são admissíveis?

Dá pra traduzir $(\star)$ para:

$(P \to Q) \land (P \to R) \to (P \to Q \land R)$

As regras admissíveis são aquelas cujas traduções dão expressões sempre verdadeiras ("tautologias").

Verifiquem — usando tabela verdade — que estas regras são admissíveis:

a) $\dfrac{P \vdash Q \land R}{P \vdash Q}$

b) $\dfrac{P \vdash R}{P, Q \vdash R}$

c) $\dfrac{P \vdash R \quad Q \vdash R}{P \lor Q \vdash R}$

d) $\dfrac{}{\vdash P \lor \neg P}$

E que estas não são admissíveis:

e) $\dfrac{P \vdash Q \lor R}{P \vdash Q}$

f) $\dfrac{P \land Q \vdash R}{P \vdash R}$

MD 5/nov/2018

Hoje: (mais) introdução a dois sistemas dedutivos "sérios":

- Sequent calculus (material: Wikipedia)
- Fitch (material: livro do Barwise e Etchemendy)

Ainda não pus os PDFs na página do curso, mas trouxe algumas cópias.

Na aula passada vimos o que eram regras "admissíveis" e "inadmissíveis".

O sistema LK (de cálculo de sequentes) tem uma série de "regras de dedução", que são algumas das regras admissíveis.

$$\overline{P,Q,R\vdash P}\ (1)$$

$$\overline{P,Q,R\vdash Q}\ (2)$$

$$\overline{P,Q,R\vdash R}\ (3)$$

Na Wikipedia tem uma regra assim:

$$\overline{\Gamma,P,\Delta\vdash P}$$

O "Γ" e o "Δ" são listas de hipóteses...

$$\left(\overline{\Gamma,P,\Delta\vdash P}\right)\begin{bmatrix}\Gamma := P,Q\\ P := R\\ \Delta :=\end{bmatrix} = \left(\overline{P,Q,R\vdash R}\right)$$

"Exercício": Deem uma olhada na dedução grande da p.10 e entendam ela...

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{B\vdash B}\,(I)\qquad \overline{C\vdash C}\,(I)}{B\lor C\vdash B,C}\,(\lor L)}{B\lor C\vdash C,B}\,(PR)}{B\lor C,\neg C\vdash B}\,(\neg L)\qquad \overline{\neg A\vdash\neg A}\,(I)}{B\lor C,\neg C,B\to\neg A\vdash\neg A}\,(\to L)}{B\lor C,\neg C,(B\to\neg A)\land\neg C\vdash\neg A}\,(\land L)$$

$\vdots$

OBS: $P,Q\vdash R$ corresponde a: $P\land Q\to R$; e $P,Q\vdash R,S$ corresponde a: $P\land Q\vdash R\lor S$

Exercícios: Encontre deduções no sistema LK para:

(a) $\overline{P\land Q\vdash Q\land P}$

(b) $\overline{(P\land Q)\land R\vdash(R\land Q)\land P}$

(c) $\overline{\vdash P\land Q\to Q\land P}$

(d) $\overline{P\lor Q\vdash Q\lor P}$

Exercícios: Qual é a substituição certa aqui?

$$\left(\dfrac{\Gamma\vdash A,\Delta\quad \Sigma\vdash B,\Pi}{\Gamma,\Sigma\vdash A\land B,\Delta,\Pi}(\land R)\right)\begin{bmatrix}?:=?\\ ?:=?\\ \vdots\end{bmatrix} = \left(\dfrac{P\vdash Q\quad P\vdash R}{P,P\vdash Q\land R}(\land R)\right)$$

Dica pro (a):

$$\dfrac{\dfrac{\dfrac{\overline{Q\vdash Q}}{P\land Q\vdash Q}\qquad\dfrac{\overline{P\vdash P}}{P\land Q\vdash P}}{P\land Q,P\land Q\vdash Q\land P}}{P\land Q\vdash Q\land P}$$

Algumas regras (Wikipedia):

$$\dfrac{\Gamma,A\land B\vdash\Delta}{\Gamma,A,B\vdash\Delta}(L\land)\qquad \dfrac{\Gamma\vdash\Delta,A\land B}{\Gamma\vdash\Delta,A}(R\land)$$

$$\dfrac{\Gamma,A\lor B\vdash\Delta}{\Gamma,A\vdash\Delta}(L\lor)\qquad \dfrac{\Gamma\vdash\Delta,A\land B}{\Gamma\vdash\Delta,B}(R\land)$$

$$\dfrac{\Gamma,A\lor B\vdash\Delta}{\Gamma,B\vdash\Delta}(L\lor)\qquad \dfrac{\Gamma\vdash\Delta,A\lor B}{\Gamma\vdash\Delta,A,B}(R\lor)$$

pág 5

$$\dfrac{\Gamma,A\to B\vdash\Delta}{\Gamma\vdash\Delta,A}(L\to)$$

$$\dfrac{\Gamma,A\to B\vdash\Delta}{\Gamma,B\vdash\Delta}(L\to)$$

$$\dfrac{\Gamma\vdash\Delta,A\to B}{\Gamma,A\vdash\Delta,B}(R\to)$$

pág 6

$\overline{P,R\vdash Q,R}$ (axiom) pág. 6

pág. 8: $\overline{P\vdash P}$ (I)

(não use o "cut"!)

$$\dfrac{\Gamma,A\vdash\Delta}{\Gamma,A\land B\vdash\Delta}(\land L_1)$$

$$\dfrac{\Gamma,B\vdash\Delta}{\Gamma,A\land B\vdash\Delta}(\land L_2)$$

$$\dfrac{\Gamma\vdash A,\Delta\quad \Sigma\vdash B,\Pi}{\Gamma,\Sigma\vdash A\land B,\Delta,\Pi}(\land R)$$

$$\dfrac{\Gamma\vdash\Delta}{\Gamma,A\vdash\Delta}(WL)\qquad \dfrac{\Gamma\vdash\Delta}{\Gamma\vdash A,\Delta}(WR)$$

$$\dfrac{\Gamma,A,A\vdash\Delta}{\Gamma,A\vdash\Delta}(CL)\qquad \dfrac{\Gamma\vdash A,A,\Delta}{\Gamma\vdash A,\Delta}(CR)$$

IMD 6/nov/2018

Hoje: nosso primeiro sistema dedutivo "sério": o sistema LK de cálculo de sequentes.

Vamos usar o artigo da Wikipedia em inglês sobre "sequent calculus" – aliás, as figuras dele. A página do curso tem um link pra ele.

(Objetivos: preparar a gente pro "Fitch" e pra regras sobre "ou", "não" e indução)

Um "sequente" é algo desta forma:

$P_1, P_2, \ldots, P_n \vdash Q_1, \ldots, Q_m$

onde $P_1, \ldots, P_n, Q_1, \ldots, Q_m$ são proposições.

A interpretação de algo como

$A, B \vdash C, D$

é

$(A \wedge B) \to (C \vee D)$

(as vírgulas à direita são interpretadas como "∨".

Na aula vimos regras admissíveis e inadmissíveis; vamos ver também as regras básicas de um sistema (pro sistema LK) – com exercícios de demonstrar coisas usando só regras "básicas".

Regras do LK:

Regras estruturais: weakening, permutation, contraction.

$$\frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta}\,(\mathrm{WL}) \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A}\,(\mathrm{WR})$$

$$\frac{\Gamma, A, B, \Delta \vdash \Sigma}{\Gamma, B, A, \Delta \vdash \Sigma}\,(\mathrm{PL}) \qquad \frac{\Gamma \vdash \Delta, A, B, \Sigma}{\Gamma \vdash \Delta, B, A, \Sigma}\,(\mathrm{PR})$$

$$\frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,(\mathrm{CL}) \qquad \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}\,(\mathrm{CR})$$

Onde A, B são proposições quaisquer e Γ, Δ, Σ são listas – talvez vazias – de proposições.

Obs:

$$\left(\frac{\Gamma, A, B, \Delta \vdash \Sigma}{\Gamma, B, A, \Delta \vdash \Sigma}\,(\mathrm{PL})\right) \begin{bmatrix} \Gamma := P, Q \\ A := R(1) \\ B := S \\ \Delta := \\ \Sigma := \mathrm{primo}(1) \end{bmatrix}$$

$$= \left(\frac{P, Q, R(1), S \vdash \mathrm{primo}(1)}{P, Q, S, R(1) \vdash \mathrm{primo}(1)}\,(\mathrm{PL})\right)$$

Regras lógicas

Pro "∧":

$$\frac{\Gamma \vdash A, \Delta \qquad \Sigma \vdash B, \Pi}{\Gamma, \Sigma \vdash A \wedge B, \Delta, \Pi}\,(\wedge R)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\,(\wedge L_1)$$

$$\frac{\Gamma, B \vdash \Delta}{\Gamma, A \wedge B \vdash \Delta}\,(\wedge L_2)$$

Exercícios:

a) $(\wedge R) \begin{bmatrix} \Gamma := P \\ \Sigma := P \\ \Delta := \\ \Pi := \\ A := Q \\ B := R \end{bmatrix} = ?$

b) Demonstre

$$\frac{A, B, C \vdash D}{B, A, C \vdash D}$$

c) $$\frac{A, A, B \vdash C}{A, B \vdash C}$$

Diga a substituição certa para:

d) $\dfrac{A, B, C, D \vdash E}{A, B, D, C \vdash E}\,(\mathrm{PL}) = (\mathrm{PL}) \begin{bmatrix} \Gamma := ? \\ A := ? \\ B := ? \\ \Delta := ? \\ \Sigma := ? \end{bmatrix}$

e) $\dfrac{A \vdash B, C, D, E}{A \vdash C, B, D, E}\,(\mathrm{PR}) = (\mathrm{PR})\,[?]$

Exemplos (Wikipedia):

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \vdash A}\,(\mathrm{I})}{\vdash \neg A, A}\,(\neg R)}{\vdash A \vee \neg A, A}\,(\vee R_2)}{\vdash A, A \vee \neg A}\,(\mathrm{PR})}{\vdash A \vee \neg A, A \vee \neg A}\,(\vee R_1)}{\vdash A \vee \neg A}\,(\mathrm{CR}) \quad = \quad \frac{}{\vdash A \vee \neg A}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{B \vdash B}\,(\mathrm{I}) \quad \cfrac{}{C \vdash C}\,(\mathrm{I})}{B \vee C \vdash B, C}\,(\vee L)}{B \vee C \vdash C, B}\,(\mathrm{PR})}{B \vee C, \neg C \vdash B}\,(\neg L) \quad \cfrac{}{\neg A \vdash \neg A}\,(\mathrm{I})}{B \vee C, \neg C, B \to \neg A \vdash \neg A}\,(\to L)}{B \vee C, (B \to \neg A) \wedge \neg C, \neg C \vdash \neg A}\,(\mathrm{PL})}{B \vee C, (B \to \neg A) \wedge \neg C, (B \to \neg A) \wedge \neg C, \neg C \vdash \neg A}\,(\wedge L_2)}{B \vee C, (B \to \neg A) \wedge \neg C, \neg C \vdash \neg A}\,(\mathrm{CL}) \; ???$$

$$\cfrac{\cfrac{\cfrac{\cfrac{A, A, B \vdash C}{A, B, A \vdash C}\,(\mathrm{PL})}{B, A, A \vdash C}\,(\mathrm{PL})}{B, A \vdash C}\,(\mathrm{CL})}{A, B \vdash C}\,(\mathrm{PL}) \quad = \quad \frac{A, A, B \vdash C}{A, B \vdash C}$$

MD 7/Nov/2018

Hoje: exercícios de cálculo de sequentes!

Demonstre:

(a) $\dfrac{A, B, C \vdash D, E}{C, B, A \vdash E, D}$

(b) $\overline{\overline{P \wedge Q \vdash Q \wedge P}}$

(c) $\overline{\overline{P \wedge (Q \wedge R) \vdash R \wedge (Q \wedge P)}}$

(d) $\overline{\overline{P \vdash \neg\neg P}}$

(e) $\overline{\overline{\neg\neg P \vdash P}}$

(f) $\overline{\overline{A, A \to B \vdash B}}$

(g) $\dfrac{A \vdash B \quad A \vdash B \to C}{A \vdash C}$

$\overline{P \vdash P} \qquad \overline{Q \vdash Q}$

$\vdots$

$\overline{P \wedge Q \vdash Q \wedge P}\,(R\wedge)$

$a \in \mathbb{N}$

$par(a) = V$

$\neg par(a) = F$

$\neg(\neg par(a)) = V$

$P \vee Q \vdash P$ é sempre verdade?

P	Q	$P \vee Q \to P$
F	F	V
F	V	F ‼
V	F	V
V	V	V

$P \wedge Q \vdash P$ é sempre verdade? sim!

$(a + b = b + a)\begin{bmatrix} a := 2 \\ b := 3 \\ b := 4 \\ a := 5 \end{bmatrix}$

$= (2 + 3 = 4 + 5)$

$\left(\overline{A \vdash A}\,(I)\right)[A := P \wedge Q]$

$= \left(\overline{P \wedge Q \vdash P \wedge Q}\,(I)\right)$

$\left(\dfrac{\Gamma, A, A, \Delta \vdash \Sigma}{\Gamma, A, \Delta \vdash \Sigma}\,(CL)\right)\begin{bmatrix} \Delta := \\ \Sigma := \Delta \end{bmatrix} =$

$= \left(\dfrac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta}\,(CL)\right)$

$\left(\dfrac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Pi}{\Gamma, \Sigma \vdash A \wedge B, \Delta, \Pi}\,(R\wedge)\right)\begin{bmatrix} \Gamma := \\ A := \\ \Delta := \\ \Sigma := \\ B := \\ \Pi := \end{bmatrix} =$

$\left(\dfrac{P \vdash Q \quad P \vdash R}{P, P \vdash Q \wedge R}\,(R\wedge)\right)$

$P \wedge Q \wedge R$

$(P \wedge Q) \wedge R$

$\left(\dfrac{\Delta, \Gamma \vdash \Sigma}{\Delta, A, \Gamma \vdash \Sigma}\,(WL)\right)\begin{bmatrix} \Delta := P, Q \\ A := R \\ \Gamma := \\ \Sigma := S \end{bmatrix}$

$= \left(\dfrac{P, Q \vdash S}{P, Q, R \vdash S}\,(WL)\right)$

$(A \wedge B) \vee \Delta$

$= \Delta \vee (A \wedge B)$

$P \vee Q = Q \vee P$

$\dfrac{\dfrac{\overline{A \vdash A}\,(I)}{\vdash A \to A}}{B \vdash A \to A}$

MD /Nov/2018

Hoje: introdução ao Fitch e regras com quantificadores!

Mas antes...
Dizemos que $\Gamma\vdash\Delta$ e $\Sigma\vdash\Pi$ são equivalentes, ou interderiváveis, quando é possível provar tanto

$$\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}$$

quanto

$$\dfrac{\Sigma\vdash\Pi}{\Gamma\vdash\Delta}$$

usando só as regras de LK.

Notação:

$$\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}(\updownarrow) \quad \text{é} \quad \dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi} \;\text{e}\; \dfrac{\Sigma\vdash\Pi}{\Gamma\vdash\Delta}.$$

OBS: No Fitch

P	quer dizer
Q	$P\vdash Q$
R	$P\vdash R$
S	$P,S\vdash T$
T	$P\vdash S\to T$
$S\to T$	

Exercícios.
Prove:

① $\dfrac{A,B\vdash C}{A\land B\vdash C}(\updownarrow)$

② $\dfrac{A\vdash B,C}{A\vdash B\lor C}(\updownarrow)$

③ $\dfrac{A,B\vdash C}{A\vdash B\to C}(\updownarrow)$

④ $\dfrac{A\vdash (B\to D)\land(C\to D)}{A\vdash B\lor C\to D}(\updownarrow)$

⑤ $\dfrac{A\vdash (B\to C)\land(B\to D)}{A\vdash B\to C\land D}(\updownarrow)$

$\dfrac{A,B\vdash C}{A\land B\vdash C}(?)$ Como fazer isso???
Dica: usem $\dfrac{}{A\land B\vdash A\land B}(I)$, o (CUT), e $\dfrac{}{A\land B\vdash A}$ e $\dfrac{}{A\land B\vdash B}$

① $\dfrac{A,B\vdash C}{A\land B\vdash C} = \dfrac{\dfrac{}{A\land B\vdash B} \quad \dfrac{\dfrac{\dfrac{}{A\land B\vdash A} \quad A,B\vdash C}{A\land B,B\vdash C}(CUT)}{B,A\land B\vdash C}(PL)}{\dfrac{A\land B,A\land B\vdash C}{A\land B\vdash C}(CL)}(CUT)$

$\dfrac{A\land B\vdash C}{A,B\vdash C} = \dfrac{A\land B\vdash C}{A,B\vdash C}(L\land)$

Na aula que vem nós vamos ver como visualizar as regras pro $\forall$ e $\exists$...

$$P = \begin{matrix}FVVV\\FFVV\\FFFV\end{matrix}$$

$$Q = FFFV$$

$$\left(\dfrac{\Gamma\vdash\Delta,A \quad A,\Sigma\vdash\Pi}{\Gamma,\Sigma\vdash\Delta,\Pi}(CUT)\right)\begin{bmatrix}\Gamma:=\\ \Delta:=\\ A:=\\ \Sigma:=\\ \Pi:=\end{bmatrix} =$$

$$\left(\dfrac{A,B\vdash B\to C,B}{A\vdash B\to C}(CUT)\right)$$

$$\dfrac{\dfrac{}{A\vdash A}(I) \quad \dfrac{}{B\vdash B}(I)}{A,B\vdash A\land B}$$

$$\dfrac{}{A\land B\vdash A\land B}(I)$$

$$\dfrac{}{B,C\vdash B\lor C}$$

Introdução às regras com quantificadores

Vamos começar com um caso bem concreto...
Sejam: $A=\{0,1,2,3\}$,
$B=\{0,1,2\}$,
$P: A\times B\to\{F,V\}$,
$Q: A\to\{F,V\}$,
$R: A\times B\to\{F,V\}$

Pra casa: fazer e entregar as questões ① até ⑤ acima. Vale até 0.3 pontos na P2.

No LK as regras com quantificadores são estas: pro $\forall$,

$$\dfrac{\Gamma, A[t/x]\vdash\Delta}{\Gamma,\forall x.A\vdash\Delta}(\forall L)$$

$$\dfrac{\Gamma\vdash A[y/x],\Delta}{\Gamma\vdash\forall x.A,\Delta}(\forall R)$$

Exemplo:

$$\dfrac{P(x,y),Q(x,y)\vdash R(x,y)}{P(x,y),\forall y\in B.Q(x,y)\vdash R(x,y)}$$

$$\dfrac{P(x)\vdash Q(x,y)}{P(x)\vdash\forall y\in B.Q(x,y)}$$

Ou:

$$\dfrac{a\in A, b\in B, P(a,b), Q(a,b)\vdash R(a,b)}{a\in A, b\in B, P(a,b), \forall y\in B.Q(a,y)\vdash R(a,b)}$$

$$\dfrac{a\in A, b\in B, P(a)\vdash Q(a,b)}{a\in A, P(a)\vdash\forall y\in B.Q(a,b)}$$

INTRODUÇÃO

HOJE: MAIS EXERCÍCIOS DE SEQUENTES (SISTEMA LK), E TALVEZ INTRODUÇÃO ÀS REGRAS DO LK PARA QUANTIFICADORES ($\forall, \exists$).

O QUE A GENTE VAI FAZER HOJE É PREPARAÇÃO PARA:

- FITCH
- REGRAS DO $\vee$ E DA INDUÇÃO
- ENTENDER MELHOR LEMAS E OUTRAS IDEIAS DO CAP. 1

... APESAR DE QUE O QUE A GENTE VAI FAZER HOJE PARECE TOTALMENTE ABSTRATO.

DEF: "$\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}(\updownarrow)$" QUER DIZER DIZER "$\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}$ E $\dfrac{\Sigma\vdash\Pi}{\Gamma\vdash\Delta}$", E

"PROVE $\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}(\updownarrow)$" QUER DIZER "PROVE $\dfrac{\Gamma\vdash\Delta}{\Sigma\vdash\Pi}$ E $\dfrac{\Sigma\vdash\Pi}{\Gamma\vdash\Delta}$".

EXERCÍCIOS

(OBS: QUANDO VOCÊS TIVEREM AS RESPOSTAS PASSEM A LIMPO E ME ENTREGUEM - ELES VALEM PONTOS EXTRAS NA P2):

① PROVE $\dfrac{A,B\vdash C}{A\wedge B\vdash C}(\updownarrow)$.

② PROVE $\dfrac{A\vdash B,C}{A\vdash B\vee C}(\updownarrow)$.

③ PROVE $\dfrac{A\vdash B\to C}{A,B\vdash C}(\updownarrow)$.

⓪ PROVE:

ⓐ $\dfrac{}{A\wedge B\vdash A}$ E $\dfrac{}{A\wedge B\vdash B}$

ⓑ $\dfrac{}{A\vdash A\vee B}$ E $\dfrac{}{B\vdash A\vee B}$

ⓒ $\dfrac{}{A, A\to B\vdash B}$

① $\dfrac{A,B\vdash C}{A\wedge B\vdash C} = \dfrac{\dfrac{\dfrac{}{A\wedge B\vdash A\wedge B}(\mathrm{I})}{A\wedge B\vdash B}(\mathrm{R}\wedge_2) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{A\wedge B\vdash A\wedge B}(\mathrm{I})}{A\wedge B\vdash A}(\mathrm{R}\wedge_1) \quad A,B\vdash C}{A\wedge B, B\vdash C}(\mathrm{Cut})}{B, A\wedge B\vdash C}(\mathrm{PL})}{\dfrac{A\wedge B, A\wedge B\vdash C}{A\wedge B\vdash C}(\mathrm{CL})}(\mathrm{Cut})$

$\dfrac{A\wedge B\vdash C}{A,B\vdash C} = \dfrac{A\wedge B\vdash C}{A,B\vdash C}(\mathrm{L}\wedge)$

② $\dfrac{A\vdash B,C}{A\vdash B\vee C} = \dfrac{\dfrac{? \quad ?}{A\vdash B\vee C, B\vee C}(\mathrm{Cut})}{A\vdash B\vee C}(\mathrm{CR})$

$\dfrac{A\vdash B\vee C}{A\vdash B,C} = \dfrac{A\vdash B\vee C}{A\vdash B,C}(\mathrm{R}\vee)$

ⓑ $\dfrac{}{A\vdash A\vee B} = \dfrac{\dfrac{}{A\vee B\vdash A\vee B}(\mathrm{I})}{A\vdash A\vee B}(\mathrm{L}\vee_1)$

$\dfrac{}{A, A\to B\vdash B} = \dfrac{\dfrac{}{A\vdash A}(\mathrm{I}) \quad \dfrac{}{B\vdash B}(\mathrm{I})}{A, A\to B\vdash B}(\to\mathrm{L})$

$\left(\dfrac{}{A\vdash A}(\mathrm{I})\right)[A:=A\wedge B] =$

$\left(\dfrac{\Gamma\vdash\Delta, A \quad A,\Sigma\vdash\Pi}{\Gamma,\Sigma\vdash\Delta,\Pi}(\mathrm{Cut})\right)\begin{bmatrix}\Gamma:= \\ \Delta:= \\ A:= \\ \Sigma:= \\ \Pi:=\end{bmatrix} =$

MD 14/nov/2018

Hoje:

- Lemas (em LK)
- Regras derivadas
- Uma técnica pra fazer demonstrações
- Quantificadores em LK
- A ordem parcial das proposições

Exercícios (a maioria você já deve ter feito)

Obs: cada exercício vai ter um nome e vai virar uma "regra derivada".

$$\dfrac{}{\overline{A\land B\vdash A}}(M1)$$

$$\dfrac{}{\overline{A\land B\vdash B}}(M2)$$

$$\dfrac{}{\overline{A\vdash A\lor B}}(M3)$$

$$\dfrac{}{\overline{B\vdash A\lor B}}(M4)$$

$$\dfrac{}{\overline{A, A\to B\vdash B}}(M5)$$

$$\dfrac{A,B\vdash C}{\overline{A\land B\vdash C}}(M6)$$

$$\dfrac{A\land B\vdash C}{\overline{A,B\vdash C}}(M7)$$

$$\dfrac{A\vdash B\lor C}{\overline{A\vdash B, C}}(M8)$$

$$\dfrac{A\vdash B, C}{\overline{A\vdash B\lor C}}(M9)$$

$$\dfrac{A\vdash B\to C}{\overline{A,B\vdash C}}(M10)$$

$$\dfrac{A,B\vdash C}{\overline{A\vdash B\to C}}(M11)$$

Sobre a folha com as soluções do (M6), (M7), (M8), (M9)...

Se a gente cria uma tabela de coisas que a gente já viu como demonstrar a gente vai escrever árvores em LK de um jeito mais curto... E isso é parecido com demonstrações em português.

$$\dfrac{A,B\vdash C}{\overline{A\land B\vdash C}}(M6) = \dfrac{\dfrac{}{\overline{A\land B\vdash B}} \quad \dfrac{\dfrac{\overline{A\land B\vdash A} \quad A,B\vdash C}{A\land B, B\vdash C}}{B, A\land B\vdash C}}{\dfrac{A\land B, A\land B\vdash C}{A\land B\vdash C}}$$

Isso pode ser visto como uma abreviação pra árvore completa... Algumas barras de inferência não tem nome (mas é só colocar) e algumas barras duplas podem ser expandidas...

Obs 1: depois que a gente demonstra, p.ex., (M1),

$$\dfrac{\overline{A\land B\vdash A\land B}^{(I)}}{A\land B\vdash A}(R\land_1)$$

a gente você gente usar "instâncias de substituição" disso...

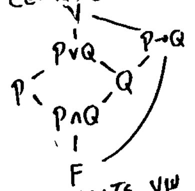
$$\dfrac{}{\overline{(P\land Q)\land R\vdash P\land Q}}(M1)$$

$$\left(\dfrac{}{\overline{A\land B\vdash A}}(M1)\right)\begin{bmatrix}A:=P\land Q\\ B:=R\end{bmatrix} = \dfrac{}{\overline{(P\land Q)\land R\vdash P\land Q}}(M1)$$

$$\left(\dfrac{\overline{A\land B\vdash A\land B}^{(I)}}{A\land B\vdash A}(R\land_1)\right)\begin{bmatrix}A:=P\land Q\\ B:=R\end{bmatrix} = \dfrac{\overline{(P\land Q)\land R\vdash (P\land Q)\land R}^{(M1)}}{(P\land Q)\land R\vdash P\land Q}(R\land_1)$$

Uma técnica pra demonstrações (usando a ordem parcial em proposições)

Lembre que:



... a gente viu um diagrama de Hasse de proposições.

Se a gente tem prática suficiente com isso - e a gente sabe que proposições são "mais falsas" ou "mais verdadeiras" que outras isso

nos dá uma técnica pra fazer esboços de demonstrações...

Dizer que $A\vdash B$ é demonstrável é dizer que "B é tão verdadeiro ou mais quanto A"...

E aí podemos fazer:

$$\dfrac{\Gamma, A, \Delta\vdash\Sigma}{\overline{\Gamma, B, \Delta\vdash\Sigma}}$$

trocamos uma hipótese por outra mais forte,

$$\dfrac{\Gamma\vdash\Delta, B, \Sigma}{\Gamma\vdash\Delta, A, \Sigma}$$

e aqui trocamos uma conclusão por outra mais fraca.

Como?

Exercício!

Dica: use o cut para demonstrar que

$$\dfrac{A, B\vdash D \quad B\vdash C}{A, C\vdash D}(M12)$$

e

$$\dfrac{A\vdash B, D \quad C\vdash D}{A\vdash B, C}(M13).$$

... isso vai nos ajudar a entender as regras sobre quantificadores.

Vamos começar com um caso bem concreto.

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

$B=\{0,1,2\}$,

e vamos considerar algumas proposições sobre $A\times B$ e sobre A e representá-las usando notação bidimensional.

P.ex.: $P: A\times B\to\{F,V\}$

$(x,y)\mapsto x>y$

$$P = \begin{matrix}F&F&F&V\\ F&F&V&V\\ F&V&V&V\end{matrix}$$

Exercício:

Sejam

$Q: A\to\{F,V\}$

$x\mapsto \exists y\in B.\, P(x,y)$,

$R: A\to\{F,V\}$

$x\mapsto \forall y\in B.\, P(x,y)$,

$Q': A\times B\to\{F,V\}$

$(x,y)\mapsto Q(x)$,

$R': A\times B\to\{F,V\}$

$(x,y)\mapsto R(x)$.

Represente graficamente Q, R, Q', R'.

Dica: $Q = FVVV$.

$Q: \{0,1,2,3\}\to\{F,V\}$

$Q(0) = \exists y\in\{0,1,2\}.\, P(0,y)$

$= P(0,0)\lor P(0,1)\lor P(0,2)$

$= F\lor F\lor F$

$= F$

$Q(1) = ?$

$Q(2) = ?$

$Q(3) = ?$

$$\begin{matrix}F&F&F&V\\ F&F&V&V\\ F&V&V&V\end{matrix} \qquad \begin{matrix}F&V&V&V\\ F&V&V&V\\ F&V&V&V\end{matrix}$$

$$\begin{matrix}F&F&F&V\\ F&F&F&V\\ F&F&F&V\end{matrix}$$

MD 14/nov/2018

Hoje:

- Lemas (em LK)
- Regras derivadas
- Uma técnica pra fazer demonstrações
- Quantificadores em LK
- A ordem parcial das proposições

Lembrem que é comum deixar as variáveis implícitas...

Se x é par e y é ímpar então x+y é ímpar

$\mathrm{par}(x), \mathrm{impar}(y) \vdash \mathrm{impar}(x+y)$

$\mathrm{par}(x) \land \mathrm{impar}(y) \to \mathrm{impar}(x+y)$

$\underbrace{\forall x \in \mathbb{Z}.\ \forall y \in \mathbb{Z}.}_{\text{implícito}}\ \mathrm{par}(x) \land \mathrm{impar}(y) \to \mathrm{impar}(x+y)$

As regras pros quantificadores em LK também deixam as variáveis implícitas...

Vimos as seguintes proposições em $A \times B$:

$P(a,b)$

$\forall y \in B. P(a,y)$

$\exists y \in B. P(a,y)$

Pelo menos no caso do exemplo/exercício, temos: (diagrama de Hasse)

$\exists y \in B. P(a,y)$

|

$P(a,b)$

|

$\forall y \in B. P(a,y)$

$\forall y \in B. P(a,y) \vdash P(a,b)$

$P(a,b) \vdash \exists y \in B. P(a,y)$

Variáveis implícitas!!!: $a \in A$, $b \in B$.

Mais complicado:

$\mathrm{par}(x) \vdash \mathrm{par}(x \cdot y)$

(variáveis implícitas: $x \in \mathbb{Z}$, $y \in \mathbb{Z}$)

$\forall a \in A. \forall b \in B. (\forall y \in B. P(a,y)) \to P(a,b)$

$\forall a \in A. \forall b \in B. P(a,b) \to (\exists y \in B. P(a,y))$

... essas são as regras básicas pros quantificadores em <u>algum</u> sistemas...

Exemplos concretos:

Pra qualquer $P: A \times B \to \{F, V\}$

Temos: $P(3,2) \to \exists y \in B. P(3,y)$

$(\forall y \in B. P(3,y)) \to P(3,2)$

$\quad \| $

$P(3,0) \land P(3,1) \land P(3,2)$

MD 14/nov/2018

Hoje:
- Regras derivadas
- ... "são" lemas
- Uma técnica pra fazer demonstrações
- A ordem parcial das proposições
- Quantificadores (em LK e fora)

Idéia:
Se fizermos uma tabela com cada um dos exercícios da aula passada e a sua solução, e nomearmos cada um dos problemas, vamos ter uma lista de coisas que sabemos demonstrar...

$$\overline{\overline{A\land B\vdash A}}\,(m1)$$

$$\overline{\overline{A\land B\vdash B}}\,(m2)$$

$$\overline{\overline{A\vdash A\lor B}}\,(m3)$$

$$\overline{\overline{B\vdash A\lor B}}\,(m4)$$

$$\overline{\overline{A, A\to B\vdash B}}\,(m5)$$

$$\dfrac{A,B\vdash C}{A\land B\vdash C}\,(m6)$$

$$\dfrac{A\land B\vdash C}{A,B\vdash C}\,(m7)$$

$$\dfrac{A\vdash B,C}{A\vdash B\lor C}\,(m8)$$

$$\dfrac{A\vdash B\lor C}{A\vdash B,C}\,(m9)$$

$$\dfrac{A\vdash B\to C}{A,B\vdash C}\,(m10)$$

$$\dfrac{A,B\vdash C}{A\vdash B\to C}\,(m11)$$

(A folha que eu distribuí tem as soluções do (m6), (m7), (m8), (m9)).

Se abreviarmos a solução do m6 na folha teremos algo que pode ser visto como um esboço de uma demonstração completa...

$$\dfrac{A,B\vdash C}{A\land B\vdash C}\,(m6) \;=\; \dfrac{\overline{A\land B\vdash B} \quad \dfrac{\dfrac{\overline{A\land B\vdash A} \quad A,B\vdash C}{A\land B, B\vdash C}}{B, A\land B\vdash C}}{\dfrac{A\land B, A\land B\vdash C}{A\land B\vdash C}}$$

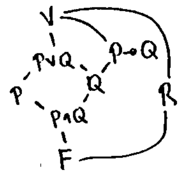
Aqui faltam os nomes de várias regras – mas é fácil completar – e se nomearmos e expandirmos as barras duplas teremos uma demonstração completa em LK.

Algumas técnicas e idéias

$$\left(\overline{\overline{A\land B\vdash A}}\,(m1) = \dfrac{\overline{A\land B\vdash A\land B}\,(I)}{A\land B\vdash A}\,(R\land_1)\right)\begin{bmatrix}A := P\land Q\\ B := R\land S\end{bmatrix}$$

$$= \left(\overline{\overline{(P\land Q)\land(R\land S)\vdash P\land Q}}\,(m1) = \dfrac{\overline{(P\land Q)\land(R\land S)\vdash(P\land Q)\land(R\land S)}\,(I)}{(P\land Q)\land(R\land S)\vdash P\land Q}\,(R\land_1)\right)$$

E lembre que a gente fez uma folha exercícios que sobre a ordem parcial das proposições...



...agora a gente entende o que são proposições "mais verdadeiras" e "mais falsas"...

Isso pode ser aplicado ao LK!

$$\dfrac{\Gamma, B, \Delta\vdash\Sigma \quad A\vdash B}{\Gamma, A, \Delta\vdash\Sigma}$$

Dá pra gente substituir uma hipótese mais fraca à esquerda do "$\vdash$" por outra mais forte...

Tradução (pra português):

$A\vdash B$: B é mais verdadeiro que A
A é menos verdadeiro que A
B é verdade em mais situações que A
A é verdade em menos situações que B

Exercício:
Demonstre:

$$\dfrac{B\vdash C \quad A,C\vdash D,E}{A,B\vdash D,E}\,(m12)$$

$$\dfrac{A,B\vdash C,D \quad D\vdash E}{A,B\vdash C,E}\,(m13)$$

(Dica: cut)

Quantificadores

Vamos começar com um caso bem concreto:

$A=\{0,1,2,3\}$,
$B=\{0,1,2\}$
$P: A\times B\to\{F,V\}$
$(x,y)\mapsto x>y$

Obs: esta notação foi explicada em 18/set – consulte o PDF dos quadros!

$$P = \begin{matrix}FFFV\\FFVV\\FVVV\end{matrix} = \begin{matrix}FFFV\\FFVV\\FVVV\end{matrix}$$

Sejam:

$Q: A\to\{F,V\}$
$a\mapsto \exists y\in B. P(a,y)$,

$R: A\to\{F,V\}$
$a\mapsto \forall y\in B. P(a,y)$,

$Q': A\times B\to\{F,V\}$
$(a,b)\mapsto Q(a)$

$R': A\times B\to\{F,V\}$
$(a,b)\mapsto R(a)$

Exercícios:
Calcule:
$P(1,2)$,
$P(2,1)$,
$Q(0)$,
$Q(1)$,
$R(2)$,
$R(3)$,
$Q'(1,2)$,
$R'(1,2)$,
e represente graficamente Q, R, Q', R'.
Dica: $Q = FVVV$

$$Q(0) = \exists y\in\{0,1,2\}. P(0,y)$$
$$= P(0,0)\lor P(0,1)\lor P(0,2)$$
$$= F \lor F\lor F$$
$$= F$$

Resp: $Q = FVVV$, $R = FFFV$

$Q' = \begin{matrix}FVVV\\FVVV\\FVVV\end{matrix}$, $R' = \begin{matrix}FFFV\\FFFV\\FFFV\end{matrix}$

$\begin{matrix}FVVV\\FVVV\\FVVV\end{matrix} = \exists y\in B. P(a,b)$

$\begin{matrix}FFFV\\FFVV\\FVVV\end{matrix} = P(a,b)$

$\begin{matrix}FFFV\\FFFV\\FFFV\end{matrix} = \forall y\in B. P(a,b)$

MD 14/nov/2018

Hoje:

- Regras derivadas
- ... "são" lemas
- Uma técnica pra fazer demonstrações
- A ordem parcial das proposições
- Quantificadores (em LK e fora)

A gente vai ver isso no sistema LK e em outros...

$P(a,0) \land P(a,1) \land P(a,2)$

$\forall a \in A.\ (\forall y \in B.\ P(a,y)) \to P(a,2)$

$\forall a \in A.\ P(a,2) \to (\exists y \in B.\ P(a,y))$

$\quad = P(a,0) \lor P(a,1) \lor P(a,2)$

Sequentes com variáveis (implícitas)

Isto é comum (em português):

Se a é par e b é ímpar então a+b é ímpar

$\text{par}(a), \text{impar}(b) \vdash \text{impar}(a+b)$

$\text{par}(a) \land \text{impar}(b) \to \text{impar}(a+b)$

$\underbrace{\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}}_{\text{implícito}}.\ \text{par}(a) \land \text{impar}(b) \to \text{impar}(a+b)$

Como é que a gente interpreta estes sequentes?

$P(a,b) \vdash Q(a)$

$\forall y \in B.\ P(a,b) \vdash Q(a)$

$\exists y \in B.\ P(a,b) \vdash Q(a)$

$R(a) \vdash P(a,b)$

$R(a) \vdash \forall y \in B.\ P(a,b)$

$R(a) \vdash \exists y \in B.\ P(a,b)$

Quais implicam quais?

Exemplo:

$$\frac{R(a) \vdash P(a,2)}{R(a) \vdash \exists y \in B.\ P(a,y)}$$

MD 21/nov/2018

Aviso: pus algumas coisas novas na página do curso...

- Um PDF com os 25 "esquemas de prova" do Scheinerman
  (Obs: todos eles exceto a "prova por tabela verdade" podem ser traduzidos pra LK)
- Um PDF com o capítulo 1 do livro da Judith Gersting; eu trouxe cópias das páginas que falam sobre variáveis livres, ligadas e "mudas" ("dummy variables").

Hoje:
Algumas regras pra indução!
Mas antes uma revisão de regras admissíveis e inadmissíveis...

Exercício:

(A) Descubra - usando $A=\{0,1,2,3\}$, $B=\{0,1,2\}$, e $P=\begin{matrix} FFFV \\ FFVV \\ FVVV \end{matrix}$

Quais das regras abaixo são inadmissíveis:

$$\frac{}{\exists y\in B.P(x,y)\vdash P(x,y)}\ (A1)$$

$$\frac{}{\forall y\in B.P(x,y)\vdash P(x,y)}\ (A2)$$

$$\frac{}{P(x,y)\vdash \exists y\in B.P(x,y)}\ (A3)$$

$$\frac{}{P(x,y)\vdash \forall y\in B.P(x,y)}\ (A4)$$

Dica: comecem representando graficamente estas funções:

$f_1: A\times B\to\{V,F\}$
$(x,y)\mapsto P(x,y)$

$f_2: A\times B\to\{V,F\}$
$(a,b)\mapsto \forall y\in B.P(a,y)$

$f_3: A\times B\to\{V,F\}$
$(a,b)\mapsto \exists y\in B.P(a,y)$

A gente ainda não usou o termo "variável livre" no curso - mas a gente já usou a idéia!

Não dá pra calcular o valor de

$$\forall x\in\{0,1,2\}.\ x\leq y$$

por y está "indefinida" - compare isso com a idéia de que y está "livre".

Aviso: vou tentar digitar estes exercícios - e as dicas pra eles, que vou pôr abaixo, e pôr o PDF no site.

Façam em casa -

Se a gente tem uma boa noção do que são regras inadmissíveis tudo sobre regras de dedução fica fácil!

Dicas:

$P: A\times B\to\{F,V\}$,

$P=\begin{matrix} \cancel{F}FFV \\ \cancel{F}FVV \\ \cancel{FVVV} \end{matrix}$

$P(1,2)=F$

$(\exists y\in B.P(x,y))$
$=(\exists b\in B.P(x,b))$,

$\exists y\in B.P(x,y)\vdash P(x,y)$

tem variáveis livres, e "$\forall$"s "implícitos", e é equivalente a:

$\exists b\in B.P(x,b)\vdash P(x,y)$

$x\in A, y\in B, \exists b\in B.P(x,b)\vdash P(x,y)$

$\forall x\in A.\forall y\in B.((\exists b\in B.P(x,b))\to P(x,y))$

$$\frac{A\vdash B \quad C\vdash D}{E\vdash F} \Rightarrow (A\to B)\land(C\to D)\to(E\to F)$$

$$\frac{}{E\vdash F} \Rightarrow V\to(E\to F)$$
ou $(E\to F)$

$\frac{}{P\lor Q\vdash P}$ é inadmissível. Porquê? Contra-exemplo!

"$\underbrace{\underbrace{\underbrace{P}_{F}\lor \underbrace{Q}_{V}}_{V}\to \underbrace{P}_{F}}_{F}$ é sempre verdade" é falso!

MD 21/nov/2018

Aviso: pus algumas coisas novas na página do curso...

- um PDF com os 23 "esquemas de prova" do Scheinerman (obs: todos eles exceto A "prova por tabela verdade" podem ser traduzidos pra LK)
- um PDF com o capítulo 1 do livro da Judith Gersting; eu trouxe cópias das páginas que falam sobre variáveis livres, ligadas e "mudas" ("dummy variables").

Hoje:
Algumas regras pra indução!
Mas antes uma revisão de regras admissíveis e inadmissíveis...

Exercício:

(A) Descubra — usando $A=\{0,1,2,3\}$, $B=\{0,1,2\}$, e $P = \begin{smallmatrix} F&F&F&V \\ F&F&V&V \\ F&V&V&V \end{smallmatrix}$ quais das regras abaixo são inadmissíveis:

$$\dfrac{}{\exists y\in B.P(x,y) \vdash P(x,y)}(A1)$$

$$\dfrac{}{\forall y\in B.P(x,y) \vdash P(x,y)}(A2)$$

$$\dfrac{}{P(x,y) \vdash \exists y\in B.P(x,y)}(A3)$$

$$\dfrac{}{P(x,y) \vdash \forall y\in B.P(x,y)}(A4)$$

Dica: comecem representando graficamente estas funções:

$f_1: A\times B \to \{V,F\}$
$(x,y) \mapsto P(x,y)$

$f_2: A\times B \to \{V,F\}$
$(a,b) \mapsto \forall y\in B.P(a,y)$

$f_3: A\times B \to \{V,F\}$
$(a,b) \mapsto \exists y\in B.P(a,y)$

A gente ainda não usou o termo "variável livre" no curso — mas a gente já usou a idéia!

Não dá pra calcular o valor de $\forall x\in\{0,1,2\}. x\le y$ por y está "indefinida" — compare isso com a idéia de que y está "livre".

Aviso: vou tentar digitar estes exercícios — e as dicas pra eles, que vou pôr abaixo, e pôr o PDF no site.
Façam em casa —

Se a gente tem uma boa noção do que são regras inadmissíveis tudo sobre regras de dedução fica fácil!

Dicas:

$P: A\times B \to \{F,V\}$,

$P = \begin{smallmatrix} F&F&F&V \\ F&F&V&V \\ F&V&V&V \end{smallmatrix}$

$P(1,2)=F$

$(\exists y\in B.P(x,y))$
$=(\exists b\in B.P(x,b))$,

$\exists y\in B.P(x,y) \vdash P(x,y)$
tem variáveis livres, e "$\forall$"s "implícitos", e é equivalente a:

$\exists b\in B.P(x,b) \vdash P(x,y)$

$x\in A, y\in B, \exists b\in B.P(x,b) \vdash P(x,y)$

$\forall x\in A.\forall y\in B.((\exists b\in B.P(x,b)) \to P(x,y))$

Introdução à Indução

Exemplo:

$\underbrace{1+3+5}_{3 \text{ termos}} = 9 = 3^2$

$\underbrace{1+3+5+7}_{4 \text{ termos}} = 16 = 4^2$

$\sum_{i=1}^{4}(2i-1) = 4^2$

$\sum_{i=1}^{n}(2i-1) = n^2$

Afirmação geral

Def: $F(n) = \sum_{i=1}^{n}(2i-1)$

$F(0)=0$
$F(1)=(2\cdot1-1)$
$F(2)=(2\cdot1-1)+(2\cdot2-1)$
$F(3)=\underbrace{(2\cdot1-1)}_{1}+\underbrace{(2\cdot2-1)}_{3}+\underbrace{(2\cdot3-1)}_{5}$

Proposição:
Def: $P(n) = (F(n)=n^2)$
ex: $P(3) = \underbrace{(\underbrace{F(3)}_{9} = \underbrace{3^2}_{9})}_{V}$

Como a gente demonstra:

$P(1000)$?

$\forall n\in\mathbb{N}. P(n)$?

Truque:
é mais ou menos fácil demonstrar que:
$P(k) \to P(k+1)$

Exemplo:
$(P(20) \to P(21))$
$= (F(20)=20^2 \to F(21)=21^2)$

Exercício:

$F(21) - F(20) = 2\cdot21-1$

$21^2 - 20^2 = (20+1)^2 - 20^2$
$= (\cancel{20^2} + 2\cdot20+1) - \cancel{20^2}$
$= 2\cdot20+1$
$= 2\cdot21-1$

$F(21) = F(20) + 2\cdot21-1$
$21^2 = 20^2 + 2\cdot21-1$

Se $F(20)=20^2$
então $F(21)=21^2$

Dá pra demonstrar o caso geral...

Seja $Q(k) = (P(k) \to P(k+1))$

(acabamos de ver que $Q(20)$ é verdade).

Digamos que a gente prove isto:

$\forall k\in\mathbb{N}. Q(k)$

isto é: $\forall k\in\mathbb{N}. P(k) \to P(k+1)$

$= (P(0)\to P(1)) \land$
$(P(1)\to P(2)) \land$
$(P(2)\to P(3)) \land$
$\vdots$

Se sabemos $P(0)$
e $\forall k\in\mathbb{N}. P(k)\to P(k+1)$
então: $P(1000)$,
$\forall n\in\mathbb{N}. P(n)$.

MD [illegible]/2018

TODOS OS PROFESSORES DE MD DO MUNDO ADORAM PÔR PROBLEMAS DE INDUÇÃO NAS PROVAS...

OS MAIS FÁCEIS ENVOLVEM SOMATÓRIOS.

REGRAS PRA INDUÇÃO:

$$\cfrac{\Gamma \vdash P(0) \qquad \Gamma \vdash \forall k \in \mathbb{N}.\ P(k) \to P(k+1)}{\cfrac{\Gamma \vdash \forall n \in \mathbb{N}.\ P(n)}{\Gamma \vdash P(1000)}}$$

ÀS VEZES O $\Gamma \vdash \forall k \in \mathbb{N}.\ P(k) \to P(k+1)$ É EXPRESSA DE OUTROS JEITOS...

$$\Gamma, k \in \mathbb{N}, P(k) \vdash P(k+1)$$

OBS:

$$\cfrac{\cfrac{\Gamma, k \in \mathbb{N}, P(k) \vdash P(k+1)}{\Gamma, k \in \mathbb{N} \vdash P(k) \to P(k+1)}}{\Gamma \vdash \forall k \in \mathbb{N}.\ P(k) \to P(k+1)}$$

MD 21/nov/2018

Hoje:

- Revisão de regras admissíveis e inadmissíveis (porque se a gente entende isso bem tudo de sistemas dedutivos fica bem mais fácil)
- Quais regras com quantificadores são admissíveis/inadmissíveis?
- Variáveis livres e ligadas
- Introdução a indução

Lembre que

$$\frac{A \vdash B \quad C \vdash D}{E \vdash F} \quad (\star)$$

pode ser "traduzida para notação padrão", e vira:

$$(A \to B) \land (C \to D) \to (E \to F) \quad (\star\star)$$

Essa regra é admissível se a sua tradução é sempre verdade, e inadmissível se não — isto é, se a sua tradução é falsa em algum caso.

Um sequente como

$\text{par}(a) \vdash \text{impar}(a+1)$

tem uma variável implícita ($a \in \mathbb{Z}$), e a sua tradução é:

$\forall a \in \mathbb{Z}.\ \text{par}(a) \to \text{impar}(a)$

Exercícios

(Meio pra hoje, meio pra casa pra entregar):

(A) Quais das regras abaixo são inadmissíveis?

Dica: procure o contra-exemplo usando:

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

$B = \{0,1,2\}$

$P : A \times B \to \{F, V\}$

$P = \begin{matrix} F & F & F & V \\ F & F & V & V \\ F & V & V & V \end{matrix}$

$$\frac{}{\exists y \in B.\ P(x,y) \vdash P(x,y)} \ (A1)$$

$$\frac{}{\forall y \in B.\ P(x,y) \vdash P(x,y)} \ (A2)$$

$$\frac{}{P(x,y) \vdash \exists y \in B.\ P(x,y)} \ (A3)$$

$$\frac{}{P(x,y) \vdash \forall y \in B.\ P(x,y)} \ (A4)$$

Dicas:

Leia as pags 13-14 do livro da Judith Gersting e entenda:

(1) Variáveis livres, ligadas, mudas,

(2) $(\forall y \in B.\ P(x,y)) = (\forall b \in B.\ P(x,b))$.

(3) Descubra quais são as variáveis livres em cada sequente do item (A) e faça a tradução dele para notação padrão.

(4) Represente graficamente as funções:

$f_1 : A \times B \to \{F, V\}$

$(a,b) \mapsto P(a,b)$

$f_2 : A \times B \to \{F, V\}$

$(a,b) \mapsto \exists y \in B.\ P(a,y)$

$f_3 : A \times B \to \{F, V\}$

$(a,b) \mapsto \forall y \in B.\ P(a,y)$

Introdução às demonstrações por indução

$0 = 0^2$

$1 = 1^2$

$1 + 3 = 2^2$

$1 + 3 + 5 = 3^2$

$1 + 3 + 5 + 7 = 4^2$

$\underbrace{1 + 3 + 5 + 7 + 9}_{5 \text{ termos}} = 5^2$

$t_1 + t_2 + t_3 + t_4 + t_5$, com $t_1 = 1$, $t_2 = 3$, $t_3 = 5$, $t_4 = 7$, $t_5 = 9$; $t_i = 2i-1$

$\sum_{i=1}^{n} t_i = n^2$

$\sum_{i=1}^{n} (2i-1) = n^2$

Def: $F(n) = \sum_{i=1}^{n} (2i-1)$

$F(4) = \sum_{i=1}^{4} (2i-1)$

$= \underbrace{(2\cdot1-1)}_{1} + \underbrace{(2\cdot2-1)}_{3} + \underbrace{(2\cdot3-1)}_{5} + \underbrace{(2\cdot4-1)}_{7}$

Def: $P(n) = (F(n) = n^2)$

Ex: $P(4) = (F(4) = 4^2)$

$= (16 = 16)$

$= V$

Como é que a gente prova

$P(1000)$?

$\forall n \in \mathbb{N}.\ P(n)$?

Grande truque:

É fácil calcular:

$F(21) - F(20)$, $= \sum_{i=1}^{21} t_i - \sum_{i=1}^{20} t_i = t_{21} = \boxed{2\cdot21-1}$

$21^2 - 20^2$, $= (20+1)^2 - 20^2 = (20^2 + 2\cdot20\cdot1 + 1) - 20^2$

$= 2\cdot20 + 1$

$= 2\cdot21 - 1$

$F(n+1) - F(n)$,

$(n+1)^2 - n^2$,

e é mais ou menos fácil provar que

$P(20) \to P(21)$,

$P(n) \to P(n+1)$,

$\forall n \in \mathbb{N}.\ P(n) \to P(n+1)$

Se $P(20) = V$,

então $F(20) = 20^2$;

$\underbrace{\underbrace{F(20)}_{\shortparallel} + \underbrace{(F(21) - F(20))}_{2\cdot21-1}}_{F(21)} = \underbrace{20^2}_{\shortparallel} + \underbrace{(21^2 - 20^2)}_{2\cdot21-1} = 21^2$

... $P(21)$ é verdade!

$P(20) \to P(21)$.

Dá pra demonstrar isto:

$\forall n \in \mathbb{N}.\ P(n) \to P(n+1)$

$(P(0) \to P(1)) \land$

$(P(1) \to P(2)) \land$

$(P(2) \to P(3)) \land \ldots$

Se sabemos $P(0)$

e $\forall n \in \mathbb{N}.\ P(n) \to P(n+1)$

então $P(1000)$

e $\forall k \in \mathbb{N}.\ P(k)$.

Indução

$$\frac{\dfrac{\Gamma \vdash P(0) \qquad \Gamma \vdash \forall n \in \mathbb{N}.\ P(n) \to P(n+1)}{\Gamma \vdash \forall k \in \mathbb{N}.\ P(k)}}{\Gamma \vdash P(1000)}$$

Todos os professores de MD do mundo adoram pôr questões de indução nas provas!

O Scheinerman tem vários exercícios de indução na seção 19 ("Indução"). Comecem fazendo estes:

a) $1 + 4 + 7 + \ldots + (3n-2) = \frac{n(3n-1)}{2}$

c) $9 + 9\cdot10 + 9\cdot100 + \ldots + 9\cdot10^{n-1} = 10^n - 1$

MD 26/nov/2018

Hoje:

- Uma visão rápida do que faltava ver sobre as regras do "ou" e dos quantificadores em LK e outros sistemas; pretendo entregar isso digitado e uma lista de exercícios na quarta.
- (Tentar) marcar P2, VR, VS.
- Introdução a estruturas algébricas (e aritmética modular, e grupos)
- Acho que consigo entregar as P1s corrigidas na quarta. !!

Demonstração por casos:

Exemplo:

Vamos provar que $\forall a \in \mathbb{Z}.\, \mathrm{par}(a^2+a)$

(Obs: $0^2+0=0$: par
$1^2+1=2$ = par
$2^2+2=6$ = par)

Demonstração (esboço):

$$\left.\begin{array}{l} a\in\mathbb{Z}, \mathrm{par}(a) \vdash \mathrm{par}(a^2+a) \\ a\in\mathbb{Z}, \mathrm{impar}(a) \vdash \mathrm{par}(a^2+a) \end{array}\right\}$$

$a\in\mathbb{Z} \vdash \mathrm{par}(a) \lor \mathrm{impar}(a)$

$$\frac{\Gamma, P \vdash R \qquad \Gamma, Q \vdash R}{\Gamma, P \lor Q \vdash R}$$

$a\in\mathbb{Z}$ par(a) impar(a) par(a^2+a)

Regras pro "∃"

$$\overline{P(2) \vdash \exists b\in B.\, P(b)}$$ ⇐ fácil

$$\frac{\Gamma \vdash \exists b\in B.\, P(b) \qquad \Gamma, b\in B, P(b) \vdash Q}{\Gamma \vdash Q}$$ ⇐ uma espécie de cut

Regras pro "∀"

$$\overline{\forall b\in B.\, P(b) \vdash P(2)}$$

$$\frac{P(a), b\in B \vdash Q(a,b)}{\underbrace{P(a)}_{} \vdash \forall b\in B.\, Q(a,b)}$$

b não pode ser uma variável livre aqui!!!

"mod"

"mod" é o resto da divisão

a	a mod 3
0	0
1	1
2	2
3	0
4	1
5	2
6	0
−1	2
−2	1

Obs: C tem funções diferentes pra "operações módulo" diferentes... Uma dessas funções retorna −1 com inputs −1 e 3; outra dessas funções retorna 2 com inputs −1 e 3 — o C tem várias funções diferentes que arredondam números de ponto flutuante...

round(2.1) = 2
round(2.9) = 3
floor(2.1) = 2
floor(2.9) = 2

Uma definição mais precisa do mod

- a mod b está definido quando: $a\in\mathbb{Z}$, $b\in\mathbb{N}$, $b>0$.

4 mod 0 ⇒ erro
4 mod −3 ⇒ erro
−4 mod 3 =
−4+3 mod 3 =
−1 mod 3 =
−1+3 mod 3 =
2 mod 3 = 2

- a mod b = a+kb mod b para $k\in\mathbb{Z}$.
- Se $a\in\{0,1,\dots,b-1\}$ então a mod b = a.

Exercícios:

(1) Calcule:
10 mod 3 =
100 mod 7 =
100 mod 5 =
100 mod 7 =
−10 mod 7 =
−20 mod 7 =

(2) Em cada um dos casos abaixo encontre o k que faz com que $a+kb\in\{0,1,\dots,b-1\}$:

a	b	k
10	3	
100	7	
100	5	
−10	7	
−20	7	

Aritmética módulo n

Defs:

$\mathbb{Z}_n = \{0,1,\dots,n-1\}$
$a +_n b = (a+b) \bmod n$
$a \cdot_n b = (a\cdot b) \bmod n$

Exercícios:

(3) Complete a tabela:

a	b	$a+_3b$	$a\cdot_3b$
0	0		
0	1		
0	2		
1	0		
1	1		
1	2		
2	0		
2	1		
2	2		

(4) Faça o mesmo que no (3) mas com tabelas em outro formato:

$+_3$	0	1	2
0			
1			
2			

$\cdot_3$	0	1	2
0			
1			
2			

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot_5$	0	1
0		
1		
2		
3		
4		

Defs (mais precisas):

$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(a,b) \mapsto (a+b) \bmod n$

$\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(a,b) \mapsto (a\cdot b) \bmod n$

Obs: $+_n$ e $\cdot_n$ são conjuntos finitos!

Exemplo:

$+_3 = \{((0,0),0), ((0,1),1), ((0,2),2), ((1,0),1), \dots \}$

Exercício:

(5) Represente $\cdot_3$ como conjunto.

MD 26/nov/2018

Usando as tabelas pro $+_5$ e $\cdot_5$ que você montou encontre as soluções (os "b"s) de cada um dos problemas abaixo...

(6) a) $0 +_5 b = 0$
b) $1 +_5 b = 0$
c) $2 +_5 b = 0$
d) $3 +_5 b = 0$
e) $4 +_5 b = 0$
f) $1 \cdot_5 b = 1$
g) $2 \cdot_5 b = 1$
h) $3 \cdot_5 b = 1$
i) $4 \cdot_5 b = 1$
} muito importantes

(7) Agora faça a tabela para o $\cdot_6$ e diga quais são as soluções de cada um dos problemas abaixo:
a) $1 \cdot_6 x = 0$
b) $2 \cdot_6 x = 0$
c) $3 \cdot_6 x = 0$
d) $4 \cdot_6 x = 1$
} idem

Obs: tudo que a gente viu sobre mod até agora está na seção 33 ("Aritmética modular") do livro (com uma notação um pouco diferente).

Próximos passos:
· Definir $-_n$ e inv_n
(exemplos: $2 -_5 4 = 3$, $\mathrm{inv}_5(2) = 3$)

Obs: $a \cdot_n \mathrm{inv}_n(a) = 1$

Estruturas algébricas

Idéia: "provas algébricas" são as que envolvem contas com $+, \cdot, -$, etc...

A gente sabe "fazer álgebra" nesta estrutura:

$\mathbb{Z}$ "=" $(\mathbb{Z}, 0, 1, +, \cdot, -)$

$\mathbb{Z}_5$ "=" $(\mathbb{Z}_5, 0, 1, +_5, \cdot_5, -_5, \mathrm{inv}_5)$

conj

$\mathrm{inv}_5 : \mathbb{Z}_5 \setminus \{0\} \to \mathbb{Z}_5 \setminus \{0\}$

Aula que vem: como interpretar polinômios e equações em $\mathbb{Z}_n$.

Permutações

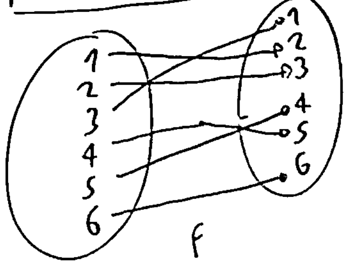
Uma permutação do (ou "no") conjunto A é uma função $f : A \to A$ que seja uma bijeção — ou seja: f é injetiva, f é sobrejetiva, f^{-1} é função.

Def: (temporária): $A_k = \{1, 2, \ldots, k\}$.

Exemplo:
$A_6 = \{1, 2, 3, 4, 5, 6\}$
$f = \{(1,2), (2,3), (3,1), (4,5), (5,4), (6,6)\}$.

Exercício: calculem f^{-1}.

Notações para permutações

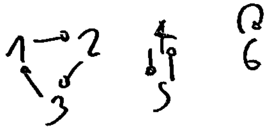


Exercício:
Sejam: $f = (1\ 2\ 3)\ (4\ 5)$
$g = (2\ 4\ 6\ 5)$

Lembrem que $(f \circ g)(x) = f(g(x))$

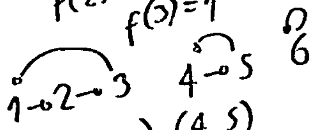
(8) Calculem: $(f \circ g)(1)$
$(f \circ g)(2)$
$\vdots$
$(f \circ g)(6)$
e representem $f \circ g$ na notação de ciclos.

(9) Represente em notação de ciclos:
a) $(g \circ f)$
b) $f \circ f$
c) $f \circ f \circ f$



f

Ciclos: $f(1) = 2$
$f(2) = 3$
$f(3) = 1$



Notação nova (para ciclos): $(1\ 2\ 3)\ (4\ 5)$

MD 2?/NOV/2019

Avisos:

1) A gente tem que ver os últimos detalhes sobre as 3 (ou mais) regras de dedução mais difíceis... mas estou digitando um material sobre isto, então vamos deixar isto pra amanhã...

Hoje: introdução à:
- Aritmética modular (sec. 33 do livro)
- Permutações
- Grupos (sec. 36)
- Estruturas algébricas

"mod"

A operação mod é uma espécie de resto da divisão.

Ex: (comparar com o operador "%" do C):

a	b	$a \bmod b$	$a\%b$
0	3	0	0
1	3	1	1
2	3	2	2
3	3	0	0
4	3	1	1
5	3	2	2
6	3	0	0
7	3	1	1
0	3	0	0
-1	3	2	-1
-2	3	1	-2
-3	3	0	0
-4	3	2	-1
-5	3	1	-2
-6	3	0	0

- $a \bmod b$ só está definido quando:
  $a \in \mathbb{Z}$,
  $b \in \mathbb{N}$, $b > 0$
  (b inteiro positivo)
- $a \bmod b$
  $= (a+b) \bmod b$
  $= (a+2b) \bmod b$
  $= (a+kb) \bmod b$ $(\forall k \in \mathbb{Z})$
- Se $a \in \{0,1,2,\ldots,b-1\}$ então $a \bmod b = a$.
- $(a \bmod b) \in \{0,1,\ldots,b-1\}$.

Exercícios

① Em cada caso abaixo encontre o (único!) $k \in \mathbb{Z}$ que faz com que $0 \leq a+kb < b$.

a	b	k	$a+kb$
10	3		
100	7		
100	5		
-10	7		
-20	7		

② Calcule:
$10 \bmod 3 =$
$100 \bmod 7 =$
$100 \bmod 5 =$
$-10 \bmod 7 =$
$-20 \bmod 7 =$

Aritmética módulo n

Defs (obs: estamos usando uma notação um pouco diferente da do livro).

$a +_n b = (a+b) \bmod n$
$a \cdot_n b = (a \cdot b) \bmod n$
$a -_n b = (a-b) \bmod n$
$-_n b = (-b) \bmod n$

$\mathbb{Z}_n = \{0,1,\ldots,n-1\}$

④ Complete as tabelas abaixo:

a (linhas), b (colunas)

$+_3$	0	1	2
0			
1			
2			

$\cdot_3$	0	1	2
0			
1			
2			

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot_5$	0	1	2	3	4
0					
1					
2					
3					
4					

$\cdot_6$	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

Defs (mais precisas):

$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(a,b) \mapsto (a+b) \bmod n$

$\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$
$(a,b) \mapsto (a \cdot b) \bmod n$

etc.

⑤ Complete:
$+_3 = \{((0,0),0), ((0,1),1), ((0,2),2), ((1,0),1), \ldots$

Obs: as funções $+_n$ e $\cdot_n$ são [illegible]

⑥ Usando as tabelas que você montou encontre todas as soluções (os "b"s) de cada uma das equações abaixo:

a) $0 +_5 b = 0$
b) $1 +_5 b = 0$
c) $2 +_5 b = 0$
d) $3 +_5 b = 0$
e) $4 +_5 b = 0$
f) $1 \cdot_6 b = 0$
g) $2 \cdot_6 b = 0$
h) $3 \cdot_6 b = 0$
i) $4 \cdot_6 b = 0$
j) $5 \cdot_6 b = 0$
k) $4 \cdot_6 b = 1$
l) $5 \cdot_6 b = 1$

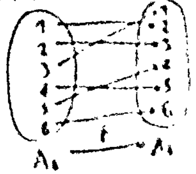
Permutações

Uma permutação do (ou "no") conjunto A é uma função $f: A \to A$ que seja uma bijeção — ou seja: f é injetiva, f é sobrejetiva, f^{-1} é função.

Def (temporária):
$A_k = \{1,2,\ldots,k\}$

Exemplo:
$A_6 = \{1,2,3,4,5,6\}$
$f = \{(1,2),(2,3),(3,1),(4,5),(5,4),(6,6)\}$
f é uma permutação de A_6, e
$f^{-1} = \{(2,1),(3,2),(1,3),(5,4),(4,5),(6,6)\}$

Notações para permutações:



f: $1 \to 2 \to 3 \to 1$, $4 \leftrightarrows 5$, $6 \circlearrowleft$

f: $1 \to 2 \to 3 \to 1$, $4 \to 5 \to 4$, $6 \to 6$

Notação de ciclos:
$f = (1\ 2\ 3)(4\ 5)$
(ciclos de comprimento 1 são omitidos).

Seja $g = (2\ 4\ 6\ 5)$,
ou seja, g = $2 \to 4 \to 6 \to 5 \to 2$, $1 \to 1$, $3 \to 3$.

Lembre que $(f \circ g)(x) = f(g(x))$.

⑦ Calcule: $(f \circ g)(1)$
$(f \circ g)(2)$
$\vdots$
$(f \circ g)(6)$
e represente $f \circ g$ na notação de ciclos.

⑧ Represente em notação de ciclos:
a) $g \circ f$
b) $f \circ f$
c) $f \circ f \circ f$

$\boxed{\text{MD 28/nov/2018}}$

Hoje: "5 regras complicadas" - discussão do PDF; mais sobre aritmética modular, permutações e grupos.

Eu mudei a primeira página do PDF sobre sequentes - agora a parte sobre quantificadores diz:

$$\frac{\Gamma \vdash P, \Delta}{\Gamma \vdash \forall y.P, \Delta}(\forall R)^* \qquad \frac{\Gamma \vdash P[y:=t], \Delta}{\Gamma \vdash \exists y.P, \Delta}(\exists R)$$

$$\frac{\Gamma, P[y:=t] \vdash \Delta}{\Gamma, \forall y.P \vdash \Delta}(\forall L) \qquad \frac{\Gamma, P \vdash \Delta}{\Gamma, \exists y.P \vdash \Delta}(\exists L)^*$$

Nas regras $(\forall R)^*$ e $(\exists L)^*$ o '*' quer dizer que o y não pode aparecer como variável livre em Γ ou Δ.

1.1 Demonstrações por casos

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \lor Q \vdash R}(DC)$$

Dá pra demonstrar ela usando a $(\lor L)$ e também dá pra ver facilmente que ela é admissível:

$$(\Gamma \land P \to R) \land (\Gamma \land Q \to R) \to (\Gamma \land (P \lor Q) \to R) \quad (\#)$$

É fácil provar $(\#)$ usando tabela-verdade...

Γ	P	Q	R	$(\#)$
F	F	F	F	
F	F	F	V	
F	F	V	F	
F	F	V	V	
⋮				
V	V	V	V	

1.2 Regra fácil pro '∀'

Obs: $[x:=t]$

Versão com quantificadores ilimitados - mais curta, mas mais abstrata... $(\forall FI)$

$P := \mathrm{Par}(a) \lor \mathrm{Impar}(a)$

$P[a:=3] = \mathrm{Par}(3) \lor \mathrm{Impar}(3)$

$P[a:=2k+1] = \mathrm{Par}(2k+1) \lor \mathrm{Impar}(2k+1)$

Alguns textos usam letras diferentes pra variáveis e pra termos.

Exemplo:

3 é uma constante
$\Rightarrow$ 3 é um termo
k é uma variável
$\Rightarrow$ k é um termo
$k+3$ é um termo
$3(k+3)$ é um termo

Versão limitada: $(\forall F)$
inclui "$\forall b \in B$"

1.3 Regra difícil pro '∀'

$(\forall R)^*$ tem a condição "y não é variável livre em Γ ou Δ"

No livro da Judith Gersting, nas págs 13-15 (?) ela define "WFF" (well-formed formula)...

A definição de WFF é recursiva, como a definição de termos... e ela define precisamente, recursivamente, o que são as variáveis livres de uma WFF...

Uma WFF (geralmente) tem sub-fórmulas (sub-WFFs)

$$(\forall x \in A.\ \mathrm{par}(x+y)) \land \forall x \in A.\ \exists y \in B.\ \mathrm{par}(xy)$$

$$\frac{a \in \mathbb{Z} \vdash \mathrm{par}(a) \to \mathrm{impar}(a+1)}{\vdash \forall a \in \mathbb{Z}.\ \mathrm{par}(a) \to \mathrm{impar}(a+1)}$$

$$\frac{a \in A \vdash P}{\vdash \forall a \in A.P} \qquad P[a:=3] \neq P$$

Porque isto é importante?

Não dá pra demonstrar isto - esta regra é inadmissível!

$$\frac{P(a) \vdash Q(a)}{P(a) \vdash \forall x \in A.Q(x)} \quad !!!!$$

1.4 A regra fácil pro '∃'

A regra fácil pro '∃' é a que não tem a restrição '*'!

Exemplos:

$\mathrm{impar}(5)$
$5 \in \mathbb{Z}$
$\vdots$
$\exists a \in \mathbb{Z}.\ \mathrm{impar}(a)$

1.5 A regra difícil pro '∃'

...quando a gente ver ela em detalhes a gente vai ver que ela está por trás disto:

10) $\exists a \in \mathbb{Z}.\ ab=c$
11) Suponha $a \in \mathbb{Z}$, $ab=c$

$$\frac{\Gamma \vdash \exists y \in B.P(y) \quad \Gamma, y \in B, P(y) \vdash Q}{\Gamma \vdash Q}$$

A "regra difícil pro ∃" é uma espécie de cut.

MD 28/NOV/2018

HOJE: "5 REGRAS COMPLICADAS" - DISCUSSÃO DO PDF; MAIS SOBRE ARITMÉTICA MODULAR, PERMUTAÇÕES E GRUPOS.

DEFS:

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\} = \{k \in \mathbb{Z} \mid 0 \leq k < n\}$$

$$+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(a, b) \longmapsto (a+b) \bmod n$$

$$\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(a, b) \longmapsto (a \cdot b) \bmod n$$

PORQUE É QUE ESSAS OPERAÇÕES $+_n$ E $\cdot_n$ MERECEM SER CHAMADAS DE "+" E "."?

OBS: O SCHEINERMAN NÃO USA O SUBSCRITO n - ELE CHAMA AS OPERAÇÕES NOVAS DE "+" E "."! ("NO CONTEXTO DE $\mathbb{Z}_5$", "EM $\mathbb{Z}_5$", "MÓDULO 5"...)

LEMBREM QUE O + E O · "CONVENCIONAIS" OBEDECEM VÁRIAS PROPRIEDADES...

$$\left.\begin{array}{l} \left.\begin{array}{l} a+b = b+a \\ a \cdot b = b \cdot a \end{array}\right\} \text{COMUTATIVIDADES} \\ \left.\begin{array}{l} (a+b)+c = a+(b+c) \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \end{array}\right\} \text{ASSOCIATIVIDADES} \\ \left.\begin{array}{l} a+0 = a \\ a \cdot 1 = a \end{array}\right\} \text{ELEMENTO NEUTRO} \\ a \cdot (b+c) = a \cdot b + a \cdot c \; \} \text{ DISTRIBUTIVIDADE} \end{array}\right\} \text{(CAED)}$$

LEMBREM QUE A GENTE TAMBÉM SABE SOMAR E MULTIPLICAR MATRIZES...

$$\underbrace{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{B} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = AB$$
$$\#$$
$$\underbrace{\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}}_{A} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = BA$$

EM MATRIZES ESTA PROPRIEDADE VALE? $AB = BA$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e \\ g \end{pmatrix} = \begin{pmatrix} ae+bg \\ ce+dg \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

COMO É QUE A GENTE DEMONSTRA, POR EXEMPLO, QUE

$$(a +_n b) +_n c = a +_n (b +_n c) \; ?$$

$$\underbrace{(\underbrace{4 +_7 5}_{2}) +_7 6}_{1} \stackrel{?}{=} \underbrace{4 +_7 (\underbrace{5 +_7 6}_{4})}_{1}$$

$$\underbrace{\underbrace{(4 +_7 5)}_{(4+5) \bmod 7} +_7 6}_{(((4+5) \bmod 7) + 6) \bmod 7}$$

EXERCÍCIO: DEMONSTRE QUE $\forall n \in \mathbb{Z}$ COM $n \geq 1$ E $\forall a, b, c \in \mathbb{Z}$ TEMOS:

$$(((a+b) \bmod n) + c) \bmod n = (a + ((b+c) \bmod n)) \bmod n$$

DICA: $a \bmod n = b \bmod n \leftrightarrow \exists k \in \mathbb{Z}.\ a + kn = b$

LISTA DE EXERCÍCIOS

(PARA CASA! IMPORTANTE!)

PROVE QUE AS OPERAÇÕES $+_n$ E $\cdot_n$ OBEDECEM AS 7 PROPRIEDADES DE (CAED).

DICA: QUANDO VOCÊS FOREM ESCREVER AS DEMONSTRAÇÕES NUNCA CONFUNDA "$\stackrel{?}{=}$" COM "="

"$\stackrel{?}{=}$": QUEREMOS VER QUE ESTA IGUALDADE VALE

"=": É FÁCIL VER QUE ESTA IGUALDADE VALE.

PERMUTAÇÕES

OBJETIVO: QUEREMOS VER QUE A COMPOSIÇÃO DE PERMUTAÇÕES "MERECE SER CHAMADA DE MULTIPLICAÇÃO".

$$f = 1 \to 2 \to 3 \quad 4 \to 5 \quad 6$$
$$(1\ 2\ 3)\ (4\ 5) \quad \leftarrow \text{NOTAÇÃO DE CICLOS}$$

$$g = (2\ 4\ 6\ 5)$$
$$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$$
$$2 \to 4 \to 6 \to 5 \quad 1 \quad 6$$

$$(f \circ g) = ?$$
$$(f \circ g)(1) = f(\overbrace{g(1)}^{1})^{2}$$
$$(f \circ g)(2) = f(\underbrace{g(2)}_{4}) = f(4) = 5$$

$$(f \circ g) = \{(1,2), (2,5), (3,1), (4,6), (5,3), (6,4)\} = (1\ 2\ 5\ 3)(4\ 6)$$

NA AULA PASSADA EU PASSEI ALGUNS EXERCÍCIOS DE CALCULAR COISAS COMO $f \circ g$, $g \circ f$, $f \circ f \circ f$, ETC...

HOJE: DEMONSTRE QUE PARA QUALQUER CONJUNTO A E QUAISQUER PERMUTAÇÕES f, g, h EM A TEMOS: $f \circ (g \circ h) = (f \circ g) \circ h$

E DESCUBRA QUAL É O ELEMENTO NEUTRO e QUE OBEDECE $f \circ e = f = e \circ f$.

MD 28/NOV/2018

(TURMA B)

- VAMOS USAR OS QUADROS DA OUTRA TURMA
- FAÇAM OS EXERCÍCIOS PRA CASA QUE EU PASSEI PRA ELES

$\boxed{\text{MD 3/dez/2018}}$

Hoje:

- Tô com as notas das P1s
- A vista de prova pode ser feita em qualquer uma das próximas aulas (e hoje)
- Definições recursivas

(Obs: cai na P2! Façam todos os exercícios que eu distribuí! O último é muito importante!)

Definições recursivas

O livro da Judith define "definições recursivas", mas alguns exemplos dela não têm detalhes suficientes... Os exercícios que eu trouxe hoje complementam isso.

Obs: definições recursivas - e strings - ligam vários assuntos que a gente começou a ver...

- indução,
- estruturas algébricas (a concatenação de strings é uma espécie de multiplicação)
- demonstrações - o último exercício mostra como definir precisamente o que são expressões de um determinado tipo, e o livro da Judith define "fórmulas bem formadas" ("WFFs") mais ou menos precisamente... Dá pra definir precisamente proposição, sequente, demonstração, etc.

Dicas pros exercícios

(1) Dá pra calcular $B(34)$ tanto "a partir do 34",

$$B(34) = 10\,B(17) = 10(B(16)+1) = \ldots$$

e tanto numa conta só, como acima, quanto em várias contas:

$$B(34) = 10\,B(17)$$
$$B(17) = B(16)+1$$
$$B(16) = 10\,B(8)$$
$$\vdots$$

e também dá pra organizar as contas de outro jeito - "a partir de baixo":

$$B(0) = 0$$
$$B(1) = B(0)+1 = 1$$
$$B(2) = \ldots$$
$$\vdots$$
$$B(17) = \ldots$$
$$B(34) = \ldots$$

Duas seções que eu não digitei...

2.8. Outros conjuntos de expressões

Aqui vamos usar os símbolos E_D, E_N, E_m, E_s com um significado diferente da seção 2.7, e vamos usar uma convenção sobre nomes de variáveis:

$d, d', d'' \in E_D$,
$n, n', n'' \in E_N$,
$m, m', m'' \in E_m$,
$s, s', s'' \in E_s$.

Os conjuntos E_D, E_N, E_m, E_s obedecem:

(ED) $\text{"0"}, \text{"1"}, \ldots, \text{"9"} \in E_D$

(EN1) $\underbrace{d \in E_D \to}_{\text{mas vamos deixar esta parte implícita, e escrever só:}} d \in E_N$

$d \in E_N$

(EN2) $n..d \in E_N$

(Fica implícito "$\forall n \in E_N.\ \forall d \in E_D$"

(Em1) $n \in E_m$

(Em2) $m..\text{"*"}..n \in E_m$

(Es1) $m \in E_s$

(Es2) $s..\text{"+"}..m \in E_s$

(EP) $\text{"("}..s..\text{")"} \in E_N$

2.9. Valores de expressões

Sabemos que:

$E_D \subset E_N$
$E_N \subset E_m$
$E_m \subset E_s$

e agora vamos definir uma função $V: E_s \to \mathbb{N}$, por:

(VD) $V(\text{"0"}) = 0, \ldots, V(\text{"9"}) = 9$

(VN2) $V(n..d) = 10V(n) + V(d)$

(Vm2) $V(m..\text{"*"}..n) = V(m) \cdot V(n)$

(Vs2) $V(s..\text{"+"}..m) = V(s) + V(m)$

(VP) $V(\text{"("}..s..\text{")"}) = V(s)$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\text{"1"} \in E_D}\,(ED)}{\text{"1"} \in E_N}\,(EN1) \quad \dfrac{}{\text{"2"} \in E_D}\,(ED)}{\text{"12"} \in E_N}\,(EN2) \quad \dfrac{}{\text{"3"} \in E_D}\,(ED)}{\text{"123"} \in E_N}}{\text{"123"} \in E_m}\,(Em1) \quad \dfrac{}{\text{"45"} \in E_N}}{\text{"123*45"} \in E_m}\,(Em2)}{\text{"123*45"} \in E_s}\,(Es1)}{\text{"(123*45)"} \in E_N}\,(EP) \quad \dfrac{}{\text{"6"} \in E_D}\,(ED)}{\text{"(123*45)6"} \in E_N}\,(EN2)$$

$$(mm)\begin{bmatrix} a := 0 \\ b := 5 \end{bmatrix} = \Big(\underbrace{m(\overbrace{0+5}^{5}, 5)}_{0} = \underbrace{m(0,5)}_{0}\Big)$$

$$m(5,5) = 0$$

$$m(a,b)$$

$$(DP)\,[n := 0] = \Big(\underbrace{\text{se } \underbrace{D(0)}_{0} = 0}_{V} \to D(1) = \underbrace{\underbrace{10\,\underbrace{D(0)}_{0}}_{0} + 9}_{9}\Big)$$

$$(DC)\,[n := 1] = \Big(\underbrace{\text{se } D(1) \neq 1}_{V} \to \underbrace{D(2)}_{9} = \underbrace{D(1)}_{9}\Big)$$

7/dez/2010

Hoje:

Definições recursivas!

MATERIAL:

- Livro da Judith Scheinerman, seção 2.3 até a "Prática 10"
- Quadro da aula de ontem da turma A
- Exercícios que eu digitei ("Definições recursivas")

OBS: as idéias de hoje têm a ver com:

- Demonstrações por indução
- Estruturas algébricas (a concatenação é uma espécie de multiplicação)
- Demonstrações em geral!!! A gente hoje vai entender o que são "expressões bem formadas"

Dicas pros exercícios

(1) Dá pra organizar as contas do $B(34)$ de vários jeitos. Experimente!

P. ex.:

(a)
$$\begin{aligned} B(34) &= 10\,B(17) \\ &= 10(B(16)+1) \\ &= 10(10\,B(8)+1) \\ &\vdots \end{aligned}$$

(b)
$$\begin{aligned} B(34) &= 10\,B(17) \\ B(17) &= B(16)+1 \\ B(16) &= 10\,B(8) \\ &\vdots \end{aligned} \qquad \begin{aligned} &\vdots \\ B(2) &= 10 \\ B(1) &= 1 \\ B(0) &= 0 \end{aligned}$$

(c)
$$\begin{aligned} B(0) &= 0 \\ B(1) &= 1 \\ B(2) &= 10 \\ B(3) &= 11 \\ &\vdots \\ B(34) &= \ldots \end{aligned}$$

(2) Todos os matemáticos e cientistas da computação "adultos" fazem substituições de cabeça muito bem.

Se você ainda não tiver prática suficiente, faça assim:

$(BP) = (B(2n) = 10\,B(n))$

$(BI) = (B(2n+1) = B(2n)+1)$

$(MB) = (0 \le a < b \to M(a,b) = a)$

$(MM) = (M(a+b,b) = M(a,b))$

E faça estas substituições pra treinar:

$(BP)[n:=0] =$

$(BI)[n:=0] =$

$(BP)[n:=1] =$

$(BP)[n:=2] =$

$(MB)\begin{bmatrix} a:=4 \\ b:=5 \end{bmatrix} =$

$(MB)\begin{bmatrix} a:=6 \\ b:=5 \end{bmatrix} =$

$(MM)\begin{bmatrix} a:=1 \\ b:=5 \end{bmatrix} =$

2.8) Outro subconjunto de expressões

- E_D, E_N, E_B, E_M, E_S são conjuntos de strings
- Convenção (em nomes de variáveis): $d, d', d'' \in E_D$, $n, n', n'' \in E_N$, $b, b', b'' \in E_B$, $m, m', m'' \in E_M$, $s, s', s'' \in E_S$
- Regras (com "$\forall$"s implícitos):

(ED) "0", "1", ..., "9"

(EN1) $d \in E_N$ (ou $\forall d \in E_D$)

(EN2) $n..d \in E_N$

(EB1) $n \in E_B$

(EM1) $b \in E_M$

(EM2) $m..\text{"*"}..b \in E_M$

(ES1) $m \in E_S$

(ES2) $s..\text{"+"}..m \in E_S$

(EBP) $\text{"("}..s..\text{")"} \in E_B$

Exercícios:

1) Prove que "123+4*56+78" $\in E_S$
2) Prove que "(123+4)*56" $\in E_M$

Pra entregar na próxima aula, valendo pontos extras na P2: os exercícios 1 e 2 acima. Obs: você não precisa organizar as suas demonstrações em árvore. Entregue também todos os exercícios das folhas de hoje!

Truque (que nenhum livro usa!)

Dá pra fazer em árvore!

$$\dfrac{\dfrac{\dfrac{}{\text{"1"} \in E_D}\,(ED)}{\text{"1"} \in E_N}\,(EN1) \qquad \dfrac{}{\text{"2"} \in E_D}\,(ED)}{\text{"12"} \in E_N}\,(EN2)$$

1) "1" $\in E_D$
2) "1" $\in E_N$ (por (EN1) com d = "1")
3) "2" $\in E_D$
4) "12" (por ...)

$\vdots$

"4" $\in E_M$

"56" $\in E_B$

"4*56" $\in E_M$

MD 5/dez/2018

Hoje: expressões (e talvez algo mais)

Eu aumentei o material sobre definições recursivas e trouxe algumas cópias — e algumas cópias da BNF do C por curiosidade.

Na aula passada nós vimos que dava pra organizar as provas da seção 2.7 ("2.7. Um conjunto de expressões") bidimensionalmente, em árvore...
Hoje vamos ver um outro jeito bidimensional de fazer isto.

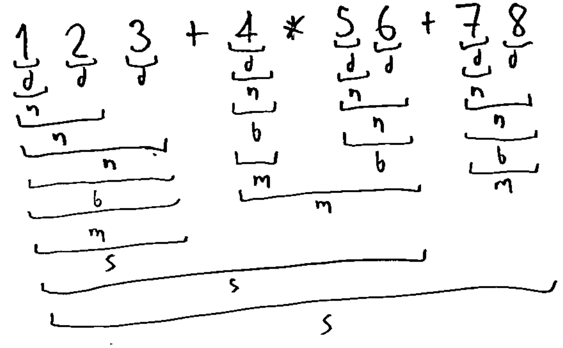
MARCAR AULAS EXTRAS!!!

Substrings
"123" ∈ E_n
"12" ∈ E_n

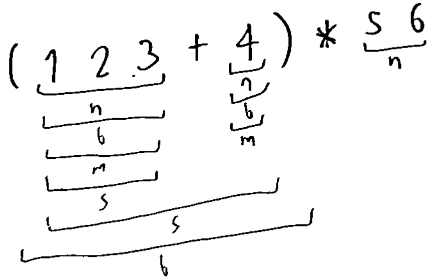
(ES2) $s, t \in E_s \Rightarrow$
$s, s' \in E_s \Rightarrow$

2.8)

1)



2)



A seção 2.9 mostra como definir valores de expressões (strings) — números

Exemplos mais complicados:

- Variáveis livres

$\forall b \in \{2,3,4\}.\ a+b<5$

VL: a, b
VL: a, b
VL: a

- Valores de expressões lógicas — sem quantificadores, depois com

Notações pro conjunto vazio: {} ou ∅
Isto aqui é outra coisa: {∅} = {{}}

Dá pra definir formalmente quase toda a sintaxe que estamos usando em MD para expressões — e para contextos, conjuntos, sequentes, árvores (em LK), demonstrações com suponha e então...

Obs: em alguns lugares a gente acrescenta alguns detalhes à sintaxe "óbvia"...

$\forall a, b \in \mathbb{Z}.\ a<b$ — duas variáveis!

$\forall (a,b) \in \mathbb{Z}^2.\ a<2$ — par

∀ ímpar !!

∀ x (ímpar) !!

Sobre a matéria da P2

Hoje vimos definições recursivas sobre strings (expressões)...

Vimos indução no caso mais simples:

$(P(0) \land \forall n \in \mathbb{N}.\ P(n) \to P(n+1)) \to \forall n \in \mathbb{N}.\ P(n)$

Depois disso vem "indução forte" que eu não vou mostrar (ou pelo menos não vou cobrar nas provas)

Quando a gente cresce e vira programador a gente usa muito "indução estrutural", principalmente sobre expressões...

Vai cair indução (simples) na P2.

Vai cair algum exercício de definições recursivas (sobre números)

Vai cair algo sobre partições, permutações, etc

{1,2,3}=V

$\{a \in \{0,1,2\};\ a<1\} = \{V,F,F\}$
$= \{F,V\}$

a	a<1
0	V
1	F
2	F

E pode cair na P2 — certamente cai na VR e na VS — algo sobre aritmética modular...

As demonstrações de comutatividade, associatividade, etc, que eu deixei pra casa.

Treinem em casa! (Dica: ao longo de vários dias)

$\overset{\text{ímpar}}{a} = \overset{\text{par}}{b} + \overset{\text{ímpar}}{c}$

1001 = 200 + 801

$\{a \in \mathbb{Z}, b \in \mathbb{Z};\ a<b\}$ = A proposição é falsa pro caso $a \in \mathbb{Z}, a=5$, $a \in \mathbb{Z}, b=2$

MD 5/dez/2018

Hoje: algumas coisas extras sobre expressões! Vamos usar as folhas que eu preparei sobre definições recursivas.

No fim da aula passada nós vimos um modo bidimensional de provar que certos strings são expressões válidas; hoje vamos ver outra.

Se a gente aplica a convenção do 2.8 ao 2.7 as regras (do 2.7) ficam:

(ED) $"0", \ldots, "9" \in E_D$

(EN1) $d \in E_N$

(EN2) $n..d \in E_N$

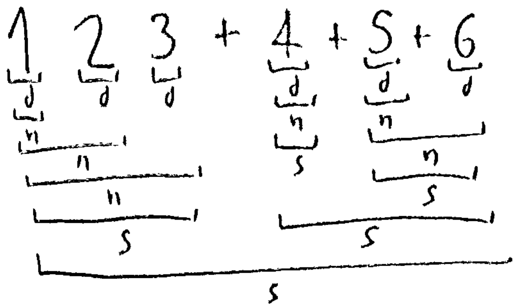
(ES1) $n \in E_S$

(ES2) $s.."+"..s' \in E_S$

(ESP) $"("..s..")" \in E_N$

Como ver que

2) $"123+4+56" \in E_S$?



Esse diagrama pode ser visto como uma abreviação de uma prova formal, completa, de que $"123+4+56" \in E_S$...

$$\underbrace{(1\ 2\ 3 + 4 + 5\ 6) + 7\ 8}_{s}$$

$"ab".."cd" = "abcd"$

$"12" \in E_S$

Seja $s = "12"$

Então $\underbrace{"("..s..")"}_{"(12)"} \in E_N$

MD /DEZ/2018

HOJE: ESTRUTURAS ALGÉBRICAS - ALIÁS, UMA ESTRUTURA ALGÉBRICA: GRUPOS.

MARCAR AULAS EXTRAS E PROVAS!

DICA: IMPRIMAM O PDF DOS QUADROS! EU TENTO SER BEM CUIDADOSO COM A SINTAXE NO QUADRO, PELO MENOS NAS PARTES QUE NÃO SÃO RASCUNHO... ENTÃO VOCÊS PODEM RELER OS QUADROS PRA TIRAR DÚVIDAS SOBRE A SINTAXE, E PRA VER COMO DÁ PRA RESOLVER COISAS EM MD USANDO SÓ A SINTAXE CERTA (OBS: ISTO É QUE NEM FAZER PROGRAMAS EM C NA SINTAXE VÁLIDA).

UM <u>GRUPO</u> É UMA 4-UPLA

$(G, \cdot_G, e_G, \mathrm{inv}_G)$

ONDE:

1) G É UM CONJUNTO.
2) $\cdot_G : G \times G \to G$,
3) $e_G \in G$,
4) $\mathrm{inv}_G : G \to G$
5) $(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$
6) $a \cdot_G e_G = e_G \cdot_G a = a$
7) $\mathrm{inv}_G(a) \cdot_G a = e_G = a \cdot_G \mathrm{inv}_G(a)$

NOTE QUE ESCREVEMOS "e_G", "$\cdot_G$", "inv_G" PARA O ELEMENTO NEUTRO, A OPERAÇÃO ("MULTIPLICAÇÃO") E A INVERSA EM G; OS SUBSCRITOS SÃO PARA DISTINGUIR ESSAS OPERAÇÕES DAS OPERAÇÕES USUAIS.

FATO:

ISTO É UM GRUPO: !!

$$\underbrace{\mathbb{Z}_6}_{\text{ABUSO DE LINGUAGEM}} = (\underbrace{\mathbb{Z}_6}_{\{0,1,2,3,4,5\}}, +_6, 0, \underbrace{-_6}_{\text{O "MENOS" UNÁRIO: } -_6 1 = 5})$$

OUTROS EXEMPLOS (QUE VAMOS VER DEPOIS):

- GRUPOS DE PERMUTAÇÕES
- GRUPOS DE STRINGS (COM UM TRUQUE PRA INVERSAS)...

NOS EXERCÍCIOS SOBRE EXPRESSÕES (INTRODUÇÃO A LINGUAGENS FORMAIS E AUTÔMATOS!) NÓS TÍNHAMOS ALGUMAS CONVENÇÕES SOBRE NOMES DE VARIÁVEIS...

P. EX.:

5) $(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$

IMPLÍCITO: $\forall a,b,c \in G$

OBS: NO CASO DE $\mathbb{Z}_6$, $(a \cdot_G b) \cdot_G c = a \cdot_G (b \cdot_G c)$ ← NOTAÇÃO GERAL

CORRESPONDE A:

$\forall a,b,c \in \mathbb{Z}_6.$
$(a +_6 b) +_6 c = a +_6 (b +_6 c)$

OUTRA OBS:

UM GRUPO NÃO PRECISA OBEDECER ISTO:

8) $a \cdot_G b = b \cdot_G a$

(UM GRUPO QUE OBEDECE ISSO É UM "GRUPO ~~COMUTATIVO~~" ABELIANO)

<u>UM GRUPO DE STRINGS</u>

SEJA $A = \{$"A", "a", "B", "b", "C", "c"$\}$.

SEJA A^* O CONJUNTO DE TODOS OS STRINGS FORMADOS PELOS CARACTERES DE A. EX: "AaBC" $\in A^*$, "Hello" $\notin A^*$, "" $\in A^*$.

DEF: $\mathrm{red}: A^* \to A^*$

A OPERAÇÃO red DELETA TODOS OS SUBSTRINGS DESTAS FORMAS:

"Aa", "aA", "Bb", "bB", "Cc", "cC".

EXEMPLO:

red("a$\underline{B\overline{bB}c}$$\underline{cCC}$A")

= "aBA"

DEF:

$\alpha \# \beta = \mathrm{red}(\alpha \cdot\cdot \beta)$

EXEMPLO:

"ABC" # "cbc" =
red("ABC" .. "cbc") =
red("ABCcbc") =
red("ABbc") =
red("Ac") =
"Ac"

EXERCÍCIOS:

① ENCONTRE UM $e \in A^*$ QUE OBEDEÇA: "ABC" # e = "ABC"

② CALCULE red(e) PARA O e DO ITEM ANTERIOR.

③ ENCONTRE $\beta \in A^*$ TAL QUE "ABC" # β = e; CALCULE β # "ABC".

SEJA:

$S = \{\alpha \in A^* \mid \mathrm{red}(\alpha) = \alpha\}$

P.EX: "ABCcC" $\notin S$

$\mathbf{S} = (S, \#, "", \mathrm{inv})$

ONDE A FUNÇÃO $\mathrm{inv}: S \to S$ INVERTE A ORDEM DO STRING E TROCA MAIÚSCULAS POR MINÚSCULAS E VICE-VERSA.

EX: inv("ABC") = "cba".

EXERCÍCIO:

VERIFIQUE (NÃO PRECISA PROVAR, SÓ SE CONVENCER) QUE $\mathbf{S} = (S, \#, "", \mathrm{inv})$ OBEDECE AS 7 CONDIÇÕES DE GRUPO.

5) $(a \# b) \# c \overset{?}{=} a \# (b \# c)$

ISTO VALE? FAÇAM EXEMPLOS.

OBS:

$(a \# b) \# c$
$= \mathrm{red}(a \cdot\cdot b) \# c$
$= \mathrm{red}(\mathrm{red}(a \cdot\cdot b) \cdot\cdot c)$
$\overset{?}{=} \mathrm{red}((a \cdot\cdot b) \cdot\cdot c)$
$= \mathrm{red}(a \cdot\cdot b \cdot\cdot c)$

... E ISTO É PARECIDO COM UM DEVER DE CASA DIFÍCIL QUE EU PASSEI:

$(a +_6 b) +_6 c = a +_6 (b +_6 c)$

MD 10/dez/2018

Que coisas a gente pode provar em todos os grupos — e que vão valer mesmo pros grupos estranhos?

Vamos usar a notação geral:

$G = (G, \cdot, e, inv)$

① Se $e', e'' \in G$ obedecem:

$\forall a \in G.\ a \cdot e' = a$

$\forall a \in G.\ a \cdot e'' = a$

Então:

(Teorema: $e' = e'' = e$)

$$a \cdot e' = a$$
$$inv(a) \cdot (a \cdot e') = inv(a) \cdot a$$
$$(inv(a) \cdot a) \cdot e' \overset{\shortparallel}{=} e$$
$$\shortparallel$$
$$e \cdot e'$$
$$\shortparallel$$
$$e'$$

② $(\forall a \in G.\ a \cdot e' = a) \to e' = e$

③ $(\forall a \in G.\ e' \cdot a = a) \to e' = e$

E "inversas laterais"?

"ABC" ++ "cba" = ""

"cba" ++ "ABC" = ""

④ Se $a \cdot b = e$

e $a \cdot b' = e$

Então

$$inv(a) \cdot (a \cdot b) = inv(a) \cdot e$$
$$\shortparallel \qquad\qquad \shortparallel$$
$$(inv(a) \cdot a) \cdot b \qquad inv(a)$$
$$\shortparallel$$
$$e \cdot b$$
$$\shortparallel$$
$$b$$

...ou seja, $b = inv(a)$, $b' = inv(a)$, $b = b'$.

⑤ Se $b \cdot a = e$

e $a \cdot b' = e$

então podemos fazer algo parecido e concluir que $b = inv(a)$, $b' = inv(a)$, $b = b'$

Subgrupos

$\mathbb{Z}_6 = (\mathbb{Z}_6, +_6, 0, -_6)$

(Exemplos:

$4 +_6 5 = (4+5) \bmod 6 = 9 \bmod 6 = 3$

$-_6 1 = (-1) \bmod 6 = 5$)

Será que a gente consegue construir um grupo menor a partir desse reduzindo o conjunto $\mathbb{Z}_6$ e restringindo as funções?

Exemplo (que não funciona):

$B \subset \mathbb{Z}_6$

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

$(B, +_6|_B, 0, -_6|_B)$

A "restrição ao conjunto B", "$|_B$", reduz o domínio da função...

$-_6 = \{(0,0), (1,5), (2,4), (3,3), (4,2), (5,1)\}$

$-_6|_B = \{(0,0), (1,5), (2,4), (3,3)\}$

Problema: às vezes o resultado do $-_6|_B$ tá fora do B...

$(-_6|_B)(1) = 5 \notin B$!!

Exemplo (que funciona):

$C \subset \mathbb{Z}_6$, $C = \{0,2,4\}$

$C = (C, +_C, 0, -_C)$, $+_C = +_6|_C$, $-_C = -_6|_C$

$+_C$	0	2	4
0	0	2	4
2	2	4	0
4	4	2	0

$-_C = \{(0,0), (2,4), (4,2)\}$

Subgrupos (definição mais formal)

$G = (G, \cdot_G, e_G, inv_G)$

um subgrupo $H \subset G$

$H = (H, \cdot_H, e_H, inv_H)$

é definido por:

1) $H \subset G$ (subconjunto!),
2) $\cdot_H$ é a restrição da $\cdot_G$ pro H (se isso funcionar)
3) $e_H = e_G$ (obs: pra isso funcionar precisamos de $e_H \in H$)
4) inv_H é a inv_G restrita a H (se isso funcionar)

Exemplo:

Os subgrupos de $\mathbb{Z}_6$ são:

$$\begin{tikzcd}
 & \mathbb{Z}_6 = \{0,1,2,3,4,5\} \arrow[dl, dash] \arrow[dr, dash] & \\
\{0,2,4\} \arrow[dr, dash] & & \{0,3\} \arrow[dl, dash] \\
 & \{0\} &
\end{tikzcd}$$

P2, VR, VS:

2ª	4ª	
10	12	
17	18	19
P2	VR	VS

Se todo mundo concordar... vou perguntar pelo Telegram!

MD /DEZ/2018

HOJE:
- VISTA DE PROVA (TAMBÉM PODE SER FEITA NOS OUTROS DIAS)
- REVISÃO DE DEMONSTRAÇÕES
- DÚVIDAS

DEMONSTRAÇÕES

TODAS AS REGRAS SEM QUANTIFICADORES QUE A GENTE USA SÃO CONSEQUÊNCIA DISSO AQUI (EXEMPLO):

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash \neg B}{\Gamma \vdash \neg A}\ (R1)$$

① ESSA REGRA É ADMISSÍVEL?

LEMBRANDO: UMA REGRA É ADMISSÍVEL QUANDO A TRADUÇÃO DELA PRA NOTAÇÃO SEM "——" E SEM "⊢" É SEMPRE VERDADEIRA (LEMBRE DE EQUIVALÊNCIAS LÓGICAS!)

TRADUÇÃO DA R1:

$$(\Gamma \to (A \to B)) \land (\Gamma \to \neg B) \to (\Gamma \to \neg A)$$

OBS: Γ PODE SER UMA LISTA DE PROPOSIÇÕES. P.EX: $\Gamma = P, Q, R$

MAS O Γ ESTÁ SEMPRE À ESQUERDA DA "⊢" ENTÃO ESSE P, Q, R É PRA SER INTERPRETADO COMO $P \land Q \land R$...

O VALOR DE Γ VAI SER O VALOR DE $P \land Q \land R$.

ABREVIAÇÕES:

$\alpha = (\Gamma \to (A \to B))$

$\beta = (\Gamma \to \neg B)$

$\gamma = (\Gamma \to \neg A)$

QUEREMOS VER SE $\alpha \land \beta \to \gamma$ É SEMPRE VERDADEIRO.

Γ	A	B	α	β	γ	$\alpha\land\beta\to\gamma$
F	F	F	V	V	V	V
F	F	V	V	V	V	V
F	V	F	V	V	V	V
F	V	V	V	V	V	V
V	F	F	V	V	V	V
V	F	V	V	F	V	V
V	V	F	F	V	F	V
V	V	V	V	F	F	V

... ENTÃO A REGRA (R1) É ADMISSÍVEL!

O SISTEMA FITCH TEM UMA REGRA (TÁ NO LIVRÃO SOBRE ELE, QUE NÓS NÃO USAMOS) TEM UMA REGRA QUE GERA MUITAS REGRAS DE UMA VEZ... VAMOS CHAMÁ-LA DE (AD).

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash \neg B}{\Gamma \vdash \neg A}\ (AD)$$

ISSO AQUI É VÁLIDO PORQUE ESSA "——" É ADMISSÍVEL.

LEMBRA DE COMO A GENTE DEFINIU "REGRAS DERIVADAS":

EXEMPLO:

$$\frac{\Gamma \vdash A \to B \quad \Gamma \vdash \neg B}{\Gamma \vdash \neg A}\ (R1) \quad := \quad \frac{\Gamma \vdash A \to B \quad \Gamma \vdash \neg B}{\Gamma \vdash \neg A}\ (AD)$$

... E AGORA EU POSSO USAR O R1 NAS MINHAS DEMONSTRAÇÕES.

O LK TINHA UM MONTÃO DE REGRAS. QUASE TODAS ELAS SÃO CONSEQUÊNCIAS DA AD.

DEIXÔ CONTAR UMA COISA (SEM DEMONSTRAÇÃO): DÁ PRA PROVAR (R1) PROVANDO SÓ QUE

$$(A \to B) \land (\neg B) \to (\neg A)$$

PORQUE O CONTEXTO (Γ) É SEMPRE O MESMO...

REGRAS ESTRANHAS

- REGRAS PROS QUANTIFICADORES (DUAS PRO $\forall$, DUAS PRO $\exists$)
- INDUÇÃO
- DEMONSTRAÇÃO POR CASOS (DÁ PRA PROVAR PELA (AD), MAS O CONTEXTO MUDA)
- UMA DAS REGRAS PRO "→".

SUGESTÃO:

TREINEM DEMONSTRAÇÕES!!!

NA P2 VAI TER UMA QUESTÃO DE INDUÇÃO.

PRA VR E PRA VS VALE A PENA VOCÊS ESTUDAREM BASTANTE DEMONSTRAÇÕES - PRINCIPALMENTE AS QUE USAM $\forall, \exists$.

MAIS SUGESTÕES:

② FAÇA SUAS DEMONSTRAÇÕES EM PORTUGUÊS, DEPOIS TRADUZA CADA PONTO IMPORTANTE DA DEMONSTRAÇÃO PRA "⊢", DEPOIS TENTE ARRUMAR ISSO NUMA DEMONSTRAÇÃO QUE SÓ USE REGRAS CONHECIDAS.

EXEMPLOS DE REGRAS QUE MUDAM O CONTEXTO:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}$$

$$\frac{\Gamma, y \in B \vdash C}{\Gamma \vdash \forall y \in B.\, C}$$

$$\frac{\Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma, A \lor B \vdash C}$$

EXERCÍCIOS

③ $\forall n \in \mathbb{N}.\ \mathrm{impar}(n) \to \mathrm{impar}(n^2)$

OBS:

$\mathrm{impar}(x) := \exists a \in \mathbb{Z}.\ x = 2a+1$

MD / DEC.

Γ	A	B
F	F	F
F	F	V
F	V	F
F	V	V
V	F	F
V	F	V
V	V	F
V	V	V

VM $\forall n \in \mathbb{N} . \text{impar}(n) \to \text{impar}(n^2)$

(2) Suponha $n \in \mathbb{N}$, impar(n)
(3) Então impar(n)

$n \in \mathbb{N}, \text{impar}(n) \vdash \text{impar}(n)$
$n \in \mathbb{N}, \text{impar}(n) \vdash \exists x \in \mathbb{Z} .\ n = 2x+1$

(2) Suponha $n \in \mathbb{N}$. impar(n)
(3) Então $\exists n \in \mathbb{N}$. impar(n)
(4) Então $\exists n \in \mathbb{N} . \exists x \in \mathbb{N} .\ n = 2x+1$
(5) Suponha $x \in \mathbb{N} .\ 2x+1 = n$
(6) Então $n^2 = 4x^2 + 4x + 1$
(7) Suponha $j \in \mathbb{N} .\ j = 2x^2 + 2x$
(8) Então $2j = 4x^2 + 4x$
(9) Então $2j + 1 = 4x^2 + 4x + 1$
(10) Então $2j+1 = n^2$
(11) Então $\exists c \in \mathbb{Z} .\ 2c+1 = n^2$ (com $c := j$)
(12) Então impar(n^2)

$n \in \mathbb{N}, \text{impar}(n), x \in \mathbb{Z}, 2x+1 = n \vdash n^2 = 4x^2 + 4x + 1$
$n \in \mathbb{N}, \text{impar}(n), x \in \mathbb{Z}, 2x+1 = n, j \in \mathbb{N}, j \vdash \ldots$