Regras estruturais:
weakening, permutation, contraction

$$\frac{\Delta \vdash \Gamma}{\Delta, A \vdash \Gamma}\ (WL-) \qquad \frac{\Delta \vdash \Gamma}{\Delta \vdash \Gamma, A}\ (WR-)$$

$$\frac{\Delta, \Gamma \vdash \Sigma}{\Delta, A, \Gamma \vdash \Sigma}\ (WL) \qquad \frac{\Delta \vdash \Gamma, \Sigma}{\Delta \vdash \Gamma, A, \Sigma}\ (WR)$$

$$\frac{\Delta, A, B, \Gamma \vdash \Sigma}{\Delta, B, A, \Gamma \vdash \Sigma}\ (PL) \qquad \frac{\Delta \vdash \Gamma, A, B, \Sigma}{\Delta \vdash \Gamma, B, A, \Sigma}\ (PR)$$

$$\frac{\Delta, A, A \vdash \Gamma}{\Delta, A \vdash \Gamma}\ (CL-) \qquad \frac{\Delta \vdash \Gamma, A, A}{\Delta \vdash \Gamma, A}\ (CR-)$$

$$\frac{\Delta, A, A, \Gamma \vdash \Sigma}{\Delta, A, \Gamma \vdash \Sigma}\ (CL) \qquad \frac{\Delta \vdash \Gamma, A, A, \Sigma}{\Delta \vdash \Gamma, A, \Sigma}\ (CR)$$

Identidade e cut:

$$\frac{}{A \vdash A}\ (I)$$

$$\frac{\Gamma \vdash \Delta, A \quad A, \Sigma \vdash \Pi}{\Gamma, \Sigma \vdash \Delta, \Pi}\ (Cut)$$

Regras lógicas pro $\wedge$:

$$\frac{\Gamma \vdash \Delta, A \wedge B}{\Gamma \vdash \Delta, A}\ (R\wedge_1)$$

$$\frac{\Gamma \vdash \Delta, A \wedge B}{\Gamma \vdash \Delta, B}\ (R\wedge_2)$$

$$\frac{\Gamma, A \wedge B \vdash \Delta}{\Gamma, A, B \vdash \Delta}\ (L\wedge)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Pi}{\Gamma, \Sigma \vdash A \wedge B, \Delta, \Pi}\ (R\wedge)$$

Regras lógicas pro $\vee$:

$$\frac{\Gamma, A \vee B \vdash \Delta}{\Gamma, A \vdash \Delta}\ (L\vee_1)$$

$$\frac{\Gamma, A \vee B \vdash \Delta}{\Gamma, B \vdash \Delta}\ (L\vee_2)$$

$$\frac{\Gamma \vdash A \vee B, \Delta}{\Gamma \vdash A, B, \Delta}\ (R\vee)$$

$$\frac{\Gamma, A \vdash \Delta \quad \Sigma, B \vdash \Pi}{\Gamma, \Sigma, A \vee B \vdash \Delta, \Pi}\ (L\vee)$$

Regras lógicas pro $\rightarrow$:

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma, B \vdash \Pi}{\Gamma, \Sigma, A \rightarrow B \vdash \Delta, \Pi}\ (\rightarrow L)$$

$$\frac{\Gamma \vdash A, \Delta \quad \Sigma \vdash B, \Pi}{\Gamma \vdash A \rightarrow B, \Delta}\ (\rightarrow R)$$

Regras lógicas pro $\neg$:

$$\frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta}\ (\neg L)$$

$$\frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \neg A, \Delta}\ (\neg R)$$

Regras lógicas para o $\forall$:

$$\frac{\Gamma \vdash P, \Delta}{\Gamma \vdash \forall y.P, \Delta}\ (\forall R)^*$$

$$\frac{\Gamma, P[y := t] \vdash \Delta}{\Gamma, \forall y.P \vdash \Delta}\ (\forall L)$$

Regras lógicas para o $\exists$:

$$\frac{\Gamma \vdash P[y := t], \Delta}{\Gamma \vdash \exists y.P, \Delta}\ (\exists R)$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma, \exists y.P \vdash \Delta}\ (\exists L)^*$$

Nas regras $(\forall R)^*$ e $(\exists L)^*$ o '$*$' quer dizer que o y não pode aparecer como variável livre em Γ ou Δ.

$$\frac{A \wedge B \vdash C}{\overline{A, B \vdash C}} = \frac{A \wedge B \vdash C}{A, B \vdash C}\,(L\wedge)$$

$$\frac{A \wedge B \vdash C}{\overline{A, B \vdash C}} = \dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,(I)}{A \wedge B \vdash B}\,(R\wedge_2) \qquad \dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,(I)}{A \wedge B \vdash A}\,(R\wedge_2) \qquad A, B \vdash C}{A \wedge B, B \vdash C}\,(Cut)}{B, A \wedge B \vdash C}\,(PL)}{A \wedge B, A \wedge B \vdash C}\,(Cut)}{A \wedge B \vdash C}\,(CL)$$

$$\frac{A \vdash B \vee C}{\overline{A \vdash B, C}} = \frac{A \vdash B \vee C}{A \vdash B, C}\,(R\vee)$$

$$\frac{A \vdash B, C}{\overline{A \vdash B \vee C}} = \dfrac{\dfrac{A \vdash B, C \qquad \dfrac{\dfrac{}{B \vee C \vdash B \vee C}\,(I)}{C \vdash B \vee C}\,(L\vee_2)}{A \vdash B, B \vee C}\,(Cut)}{A \vdash B \vee C, B}\,(PR) \qquad \dfrac{\dfrac{}{B \vee C \vdash B \vee C}\,(I)}{B \vdash B \vee C}\,(R\wedge_2)}{A \vdash B \vee C, B \vee C}\,(Cut)}{A \vdash B \vee C}\,(CR)$$

1 Cinco regras complicadas

1.1 Demonstrações por casos

A regra básica é esta aqui, que parece com a $(L\vee)$:

$$\frac{\Gamma, P \vdash R \quad \Gamma, Q \vdash R}{\Gamma, P \vee Q \vdash R}\ (DC)$$

Um exemplo de uso:

$$\dfrac{\dfrac{}{a \in \mathbb{Z} \vdash \mathsf{par}(a) \vee \mathsf{impar}(a)} \quad \dfrac{\dfrac{}{a \in \mathbb{Z}, \mathsf{par}(a) \vdash \mathsf{par}(a^2+a)} \quad \dfrac{}{a \in \mathbb{Z}, \mathsf{impar}(a) \vdash \mathsf{par}(a^2+a)}\ (DC)}{a \in \mathbb{Z}, \mathsf{par}(a) \vee \mathsf{impar}(a) \vdash \mathsf{par}(a^2+a)}\ (Cut)}{a \in \mathbb{Z} \vdash \mathsf{par}(a^2+a)}$$

Ainda não consegui encontrar exemplos ou exercícios de demonstração por casos no Scheinerman. A P1 do Fernando Naufel de 2012.2 ("md-122-p1-manha-gab.pdf") para a turma da manhã tem vários exemplos de provas por casos em Fitch.

1.2 A regra fácil para o '∀'

A regra fácil para o '∀' *escolhe um caso particular*: por exemplo, a partir de $\forall a \in \mathbb{Z}.\mathsf{par}(a) \vee \mathsf{impar}(a)$ podemos provar $\mathsf{par}(3) \vee \mathsf{impar}(3)$ ou $\mathsf{par}(2k+1) \vee \mathsf{impar}(2k+1)$. Ela é escrita como:

$$\frac{}{\forall x.P \vdash P[x := t]}\ (\forall FI) \qquad \text{ou} \qquad \frac{}{t \in B, \forall b \in B.P \vdash P[b := t]}\ (\forall F)$$

Lembre que no curso nós quase só usamos quantificadores "limitados", como "$\forall b \in B$", porque os "ilimitados" como "$\forall x$" são abstratos demais, no sentido de que é difícil calcular expressões com eles; aliás só usamos quantificadores ilimitados na aula de 8/outubro.

Em alguns lugares — por exemplo, no artigo da Wikipedia — algumas letras, como x, sempre são usadas para *variáveis*, e outras, como t, sempre são usadas para "termos".

1.3 A regra difícil para o '∀'

A regra difícil para o '∀' diz que se conseguimos provar $Q(x, y)$ num contexto que não impõe nenhuma restrição para o y então podemos provar $\forall y.Q(x, y)$ a partir disto; a versão limitada dela diz que se conseguimos provar $Q(x, y)$ num contexto em que a única restrição para o y seja $y \in B$ então podemos provar $\forall y \in B.Q(x, y)$. Escrevendo estas regras no estilo de LK elas viram:

$$\frac{P(x) \vdash Q(x, y)}{P(x) \vdash \forall y.Q(x, y)}\ (\forall DI) \qquad \text{ou} \qquad \frac{P(x) \vdash Q(x, y)}{P(x), y \in B \vdash \forall y \in B.Q(x, y)}\ (\forall D)$$

Na wikipedia essa regra é exposta de um jeito bem mais abstrato:

$$\frac{\Gamma \vdash P, \Delta}{\Gamma \vdash \forall y.P, \Delta}\ (\forall R)^*$$

onde "a variável y não aparece livre em Γ ou Δ".

Um exemplo de uso dela parecido com as coisas que estávamos provando até a P1 é:

$$\frac{a \in \mathbb{Z} \vdash \mathsf{par}(a) \to \mathsf{impar}(a+1)}{\vdash \forall a \in \mathbb{Z}.\mathsf{par}(a) \to \mathsf{impar}(a+1)}\ (\forall D)$$

1.4 A regra fácil para o '∃'

A regra fácil para o '∃' diz que se conseguimos provar $P(x,t)$ para algum "termo" t, por exemplo $t := 3$, ou $t := x^2$, então a partir disto conseguimos provar que $\exists y.P(x,y)$. Esta é a versão *ilimitada* da regra; a versão limitada é $(t \in B \wedge P(x,t)) \to \exists y \in B.P(x,y)$. No estilo do LK, temos:

$$\frac{}{P[y := t] \vdash \exists y.P}\ (\exists FI) \qquad \text{ou} \qquad \frac{}{t \in B, P[y := t] \vdash \exists y \in B.P}\ (\exists F)$$

Um exemplo de uso:

$$\dfrac{\Gamma \vdash \mathsf{impar}(5) \qquad \dfrac{\dfrac{}{\vdash 5 \in \mathbb{Z}} \quad \dfrac{}{5 \in \mathbb{Z}, \mathsf{impar}(x)[x := 5] \vdash \exists x \in \mathbb{Z}.\mathsf{impar}(x)}\ (\exists F)}{\mathsf{impar}(x)[x := 5] \vdash \exists x \in \mathbb{Z}.\mathsf{impar}(x)}\ (Cut)}{\Gamma \vdash \exists x \in \mathbb{Z}.\mathsf{impar}(x)}$$

1.5 A regra difícil para o '∃'

A regra difícil para o '∃' é uma espécie de "Cut" — mas ela usa uma conclusão da forma $\exists y \in B.P(y)$ para cortar duas hipótese: $y \in B$ e $P(y)$. No sistema que nós vimos primeiro ela era assim:

1) Suponha Γ
2) (...)
3) Então $\exists y \in B.P(y)$
4) Suponha $y \in B, P(y)$
5) (...)
6) Então Q (Fecha 4)

Nós discutimos "suponhas abertos" e regras que "fecham suponhas" na aula de 27/ago/2018. Em LK essa regra fica assim:

$$\frac{\Gamma \vdash \exists y \in B.P(y) \quad \Gamma, y \in B, P(y) \vdash Q}{\Gamma \vdash Q}\ (\exists D)$$

A versão ilimitada dela é:

$$\frac{\Gamma \vdash \exists y.P \quad \Gamma, P \vdash Q}{\Gamma \vdash Q}\ (\exists DI) \qquad := \qquad \dfrac{\Gamma \vdash \exists y.P \quad \dfrac{\Gamma, P \vdash Q}{\Gamma, \exists y.P \vdash Q}\ (\exists L)^*}{\Gamma \vdash Q}\ (Cut)$$

2 Definições recursivas

Os livros de matemática e computação "pra adultos" às vezes fazem umas definições ridiculamente curtas para sequências, funções e conjuntos e aí supõem que o leitor vai entender essas definições. O livro da Judith Gersting explica definições recursivas a partir da p.67; vamos ver alguns exemplos extras mais difíceis e alguns truques para entender estas definições.

2.1 Fake binary

Seja $B : \mathbb{N} \to \mathbb{N}$ a função que obedece estas duas condições:

(BP) $\forall n \in \mathbb{N}. B(2n) = 10 \cdot B(n)$

(BI) $\forall n \in \mathbb{N}. B(2n+1) = B(2n) + 1$

Note que fazendo $n = 0$ em (BP) obtemos que $B(0) = 0$, e com $n = 0$ em (BI) obtemos $B(1) = 1$. Usando $n = 1$, $n - 2$, etc em (BP) e (BI) obtemos $B(2)$, $B(3)$, etc. Exercícios: 1) entenda o padrão da função B; 2) descubra o valor de $B(34)$; mostre os passos necessários para calcular $B(34)$.

2.2 Módulo

Seja $\mathbb{N}^+ = \{\, n \in \mathbb{N} \mid 0 < n \,\}$, e seja $M : \mathbb{Z} \times \mathbb{N}^+ \to \mathbb{N}$ a função que obedece estas duas condições:

(MB) Se $0 \leq a < b$ então $M(a, b) = a$,

(MM) $M(a + b, b) = M(a, b)$.

Repare que agora não estamos usando '$\forall$' e nem dizendo em que conjuntos os valores de a e b moram — estamos copiando o que muitos livros de matemática e computação fazem: estamos deixando tudo implícito! Tanto em (MB) quanto em (MM) fica implícito que $a \in \mathbb{Z}$ e $b \in \mathbb{N}^+$.

Exercícios: 1) Use (MB) para calcular $M(0, 5), M(1, 5), \ldots, M(4, 5)$; 2) Use (MM) para calcular $M(5, 5), M(6, 5), \ldots$; 3) Use (MM) para calcular $M(-1, 5), M(-2, 5), \ldots$.

2.3 Noves

Seja $D : \mathbb{N} \to \mathbb{N}$ a função que obedece estas três condições:

(DZ) $D(0) = 0$

(DP) Se $D(n) = n$ então $D(n + 1) = 10D(n) + 9$

(DC) Se $D(n) \neq n$ então $D(n + 1) = D(n)$

Exercícios: 1) Calcule $D(0), D(1), \ldots, D(11)$. 2) Entenda o padrão e descubra os valores de $D(99), D(100), D(101), \ldots, D(999), D(1000), D(1001)$.

2.4 Concatenação de números

Seja $C : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ a função que obedece:

(CD) $C(a, b) = a \cdot (D(b) + 1) + b$

Exercícios: 1) Calcule $C(12, 345)$; 2) Calcule $C(12, 0)$; 3) Calcule $C(0, 12)$.

2.5 Um conjunto de números

Seja $S \subseteq \mathbb{N}$ o conjuntos que obedece:

(S0) $0 \in S$,

(S2) Se $n \in S$ então $10n + 2 \in S$,

(S3) Se $n \in S$ então $10n + 3 \in S$.

Exercícios: 1) Prove que $23322 \in S$; 2) Explique porque não dá pra provar que $45 \in S$.

2.6 Strings

O "Exemplo 23" na página 70 do livro da Judith define *strings*, que às vezes são chamados de *sequências de caracteres* ou de *cadeias de caracteres* — ou só *cadeias* — em português. Alguns exemplos de strings: "`Hello`", "`1+2`", "", "`)+`". Vamos usar '..' (como em Lua) para a operação de concatenação de strings. Exemplos:

"`Hello`".."`1+2`" = "`Hello1+2`"

"".."`)+`" = "`)+`"

2.7 Um conjunto de expressões

Digamos que os conjuntos de strings $\mathsf{E_D}$, $\mathsf{E_N}$ e $\mathsf{E_S}$ obedecem:

(ED) "`0`", "`1`", ..., "`9`" $\in \mathsf{E_D}$

(EN1) Se $d \in \mathsf{E_D}$ então $d \in \mathsf{E_N}$

(EN2) Se $n \in \mathsf{E_N}$ e $d \in \mathsf{E_D}$ então $n..d \in \mathsf{E_N}$

(ES1) Se $n \in \mathsf{E_N}$ então $n \in \mathsf{E_S}$

(ES2) Se $s, t \in \mathsf{E_S}$ então $s..$"`+`"$..t \in \mathsf{E_S}$

(ESP) Se $s \in \mathsf{E_S}$ então "`(`"$..s..$"`)`" $\in \mathsf{E_N}$

Exercícios: 1) Prove que "`123`" $\in \mathsf{E_N}$; 2) Prove que "`123`" $\in \mathsf{E_S}$ e "`123+4+56`" $\in \mathsf{E_S}$; 3) Prove que "`(123+4+56)`" $\in \mathsf{E_N}$; 4) Prove que "`(123+4+56)`" $\in \mathsf{E_S}$; 5) Prove que "`(123+4+56)+78`" $\in \mathsf{E_S}$.

2.8 Outro conjunto de expressões

Vamos *reusar* os símbolos $\mathsf{E_D}$, $\mathsf{E_N}$ e $\mathsf{E_S}$ do item anterior — com outro significado.

Digamos que os conjuntos de strings $\mathsf{E_D}$, $\mathsf{E_N}$, $\mathsf{E_B}$, $\mathsf{E_M}$ e $\mathsf{E_S}$ obedecem:

(ED) "`0`", "`1`", ..., "`9`" $\in \mathsf{E_D}$

(EN1) $d \in \mathsf{E_N}$

(EN2) $n..d \in \mathsf{E_N}$

(EB1) $n \in \mathsf{E_B}$

(EM1) $b \in \mathsf{E_M}$

(EM2) $m..$"`*`"$..b \in \mathsf{E_M}$

(ES1) $m \in \mathsf{E_S}$

(ES2) $s..$"`+`"$..m \in \mathsf{E_S}$

(EBP) "`(`"$..s..$"`)`" $\in \mathsf{E_B}$

Agora estamos usando uma convenção no nome das variáveis para deixar a especificação mais curta. A convenção é:

$d, d', d'' \in \mathsf{E_D}$

$n, n', n'' \in \mathsf{E_N}$

$b, b', b'' \in \mathsf{E_B}$

$m, m', m'' \in \mathsf{E_M}$

$s, s', s'' \in \mathsf{E_S}$

e os '∀'s ficam implícitos. Por exemplo, (EM2) por extenso é:

$\forall m \in \mathsf{E_M}.\forall b \in \mathsf{E_M}.m..$"`*`"$..b \in \mathsf{E_M}$.

Exercícios: 1) prove que "`123+4*56+78`" $\in \mathsf{E_S}$; 2) prove que "`(123+4)*56`" $\in \mathsf{E_M}$.

2.9 Valores de expressões

É fácil ver que os conjuntos $\mathsf{E_D}$, $\mathsf{E_N}$, $\mathsf{E_B}$, $\mathsf{E_M}$ e $\mathsf{E_S}$ do item anterior obedecem $\mathsf{E_D} \subset \mathsf{E_N} \subset \mathsf{E_B} \subset \mathsf{E_M} \subset \mathsf{E_S}$. Vamos definir uma função $V : \mathsf{E_S} \to \mathbb{N}$ da seguinte forma:

(VD) $V(\text{“}\mathtt{0}\text{”}) = 0, V(\text{“}\mathtt{1}\text{”}) = 1, \ldots, V(\text{“}\mathtt{9}\text{”}) = 9$

(VN2) $V(n..d) = 10V(n) + V(d)$

(VM2) $V(m..\text{“}\mathtt{*}\text{”}..b) = V(m) \cdot V(b)$

(VS2) $V(s..\text{“}\mathtt{+}\text{”}..m) = V(s) \cdot V(m)$

(VP) $V(\text{“}\mathtt{(}\text{”}..s..\text{“}\mathtt{)}\text{”}) = V(s)$