$\mathbf{LMT}^{\rightarrow}$

Um Procedimento Unificado para Prova e Geração de Contra-Exemplos na Lógica Minimal Implicacional

Jefferson de Barros Santos
Bruno Lopes Vieira
Edward Hermann Haeusler

VII Workshop de Verão UnB
Departamento de Informática
Pontifícia Universidade Católica do Rio de Janeiro

Fevereiro, 2015

Visão Geral

Objetivo

Apresentar resultados iniciais de nossa pesquisa sobre provadores de teoremas para a Lógica Proposicional Minimal Implicacional $\mathsf{M}_{\rightarrow}$

Outline

- Justificar a importância de $\mathsf{M}_{\rightarrow}$ para a área de prova de teoremas
- Apresentar nossos resultados na busca de um sistema dedutivo unificado para prova e geração de contra-exemplos em $\mathsf{M}_{\rightarrow}$
- Comparar nossa proposta com trabalhos relacionados

Visão Geral

Objetivo

Apresentar resultados iniciais de nossa pesquisa sobre provadores de teoremas para a Lógica Proposicional Minimal Implicacional $\mathsf{M}_{\rightarrow}$

Outline

- Justificar a importância de $\mathsf{M}_{\rightarrow}$ para a área de prova de teoremas
- Apresentar nossos resultados na busca de um sistema dedutivo unificado para prova e geração de contra-exemplos em $\mathsf{M}_{\rightarrow}$
- Comparar nossa proposta com trabalhos relacionados

Lógicas Proposicionais

Dedução Natural (ND) para Lógica Clássica, Intuicionista and Minimal

- N.D. para Lógica Minimal. O $\bot$ não tem nenhum significado especial. ▸ M
- N.D. para Lógica Intuicionista inclui $\bot$-Int. ▸ I
- N.D. para Lógica Clássica inclui ambos, $\bot$-Cla e $\bot$-Int. ▸ C

Um pouco sobre complexidade

Lógica Clássica

- Saber se uma fórmula é satisfatível ou não é NP-Completo
- Saber se uma fórmula é tautologia (construir provas) é coNP-Completo
- Encontrar contra-exemplos também é coNP-Completo

Lógica Intuicionista e Minimal Completa

- TAUT é PSPACE-Completo.
- COUNTER também.

Um pouco sobre complexidade

Lógica Clássica

- Saber se uma fórmula é satisfatível ou não é NP-Completo
- Saber se uma fórmula é tautologia (construir provas) é coNP-Completo
- Encontrar contra-exemplos também é coNP-Completo

Lógica Intuicionista e Minimal Completa

- TAUT é PSPACE-Completo.
- COUNTER também.

A Lógica Minimal Implicacional $\mathbf{M}_{\rightarrow}$

A Lógica Minimal restrita apenas ao conectivo $\rightarrow$

Por que $\mathbf{M}_{\rightarrow}$ é interessante?

- TAUT($\mathbf{M}_{\rightarrow}$) é PSPACE-Completo
- COUNTER($\mathbf{M}_{\rightarrow}$) é PSPACE-Completo também

- $\mathbf{M}_{\rightarrow}$ codifica polinomialmente qualquer lógica com ND e propriedade da subfórmula
  - $\mathbf{M}_{\rightarrow}$ é tão difícil de implementar quanto outras lógicas proposicionais mais populares
  - A existência de provas "grandes" na Lógica Clássica está relacionados à questão se NP≠CoNP

A Lógica Minimal Implicacional

Por que $\mathbf{M}_{\rightarrow}$ é interessante?

- A existência de provas polinomiais para todas as tautologias em $\mathbf{M}_{\rightarrow}$ implica que PSPACE=NP
- Contra-modelos têm limite superior superpolinomial
- Algumas tautologias têm limite inferior exponencial em ND com provas normais

O Cálculo de Sequente de Gentzen (Adaptado)

$$\frac{}{\Gamma,\alpha \Rightarrow \Delta,\alpha}\,\mathbf{Ax}$$

$$\frac{\Gamma \Rightarrow \Delta,\alpha \qquad \Gamma',\alpha \Rightarrow \Delta'}{\Gamma,\Gamma' \Rightarrow \Delta,\Delta'}\,\mathbf{Corte}$$

$$\frac{\Gamma,\alpha,\beta \Rightarrow \Delta}{\Gamma,\alpha \wedge \beta \Rightarrow \Delta}\,\wedge\mathbf{L} \qquad \frac{\Gamma \Rightarrow \Delta,\alpha \qquad \Gamma \Rightarrow \Delta,\beta}{\Gamma \Rightarrow \Delta,\alpha \wedge \beta}\,\wedge\mathbf{R}$$

$$\frac{\Gamma,\alpha \Rightarrow \Delta \qquad \Gamma,\beta \Rightarrow \Delta}{\Gamma,\alpha \vee \beta \Rightarrow \Delta}\,\vee\mathbf{L} \qquad \frac{\Gamma \Rightarrow \Delta,\alpha,\beta}{\Gamma \Rightarrow \Delta,\alpha \vee \beta}\,\vee\mathbf{R}$$

$$\frac{\Gamma \Rightarrow \alpha,\Delta \qquad \Gamma,\beta \Rightarrow \Delta}{\Gamma,\alpha\rightarrow\beta \Rightarrow \Delta}\,\rightarrow\mathbf{L} \qquad \frac{\Gamma,\alpha \Rightarrow \Delta,\beta}{\Gamma \Rightarrow \Delta,\alpha\rightarrow\beta}\,\rightarrow\mathbf{R}$$

$$\frac{\Gamma \Rightarrow \Delta,\alpha}{\Gamma,\neg\alpha \Rightarrow \Delta}\,\neg\mathbf{L} \qquad \frac{\Gamma,\alpha \Rightarrow \Delta}{\Gamma \Rightarrow \Delta,\neg\alpha}\,\neg\mathbf{R}$$

Provando tautologias na Lógica Clássica

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow \neg B, A}{\Rightarrow \neg A, \neg B, A}\,\neg\text{-dir}}{\Rightarrow \neg A \vee \neg B, A}\,\vee\text{-dir} \qquad \dfrac{\dfrac{\dfrac{B \Rightarrow \neg A, B}{\Rightarrow \neg A, \neg B, B}\,\neg\text{-dir}}{\Rightarrow \neg A \vee \neg B, B}\,\vee\text{-dir}}{\Rightarrow (\neg A \vee \neg B), A \wedge B}\,\wedge\text{-dir}}{\neg(A \wedge B) \Rightarrow (\neg A \vee \neg B)}\,\neg\text{-esq}}{\Rightarrow \neg(A \wedge B) \rightarrow (\neg A \vee \neg B)}\,\rightarrow\text{-dir}$$

Gerando contra-exemplos para não tautologias

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow A}{\Rightarrow \neg A, A}\,\neg\text{-dir} \quad \dfrac{B \Rightarrow A}{\Rightarrow \neg B, A}\,\neg\text{-dir}}{\Rightarrow \neg A \wedge \neg B, A}\,\wedge\text{-dir} \quad \dfrac{\dfrac{A \Rightarrow B}{\Rightarrow \neg A, B}\,\neg\text{-dir} \quad \dfrac{B \Rightarrow B}{\Rightarrow \neg B, B}\,\neg\text{-dir}}{\Rightarrow \neg A \wedge \neg B, B}\,\wedge\text{-dir}}{\Rightarrow (\neg A \wedge \neg B), A \wedge B}\,\wedge\text{-dir}}{\neg(A \wedge B) \Rightarrow (\neg A \wedge \neg B)}\,\neg\text{-esq}}{\Rightarrow \neg(A \wedge B) \rightarrow (\neg A \wedge \neg B)}\,\rightarrow\text{-dir}$$

Saindo da Lógica Clássica

- Regras para a Lógica Intuicionista e Minimal não são todas inversíveis
- Exemplo: precisamos repetir a fórmula principal da conclusão de um $\rightarrow$-esq na premissa da esquerda

$$\frac{\Delta, \alpha_1 \rightarrow \alpha_2 \Rightarrow \alpha_1 \qquad \Delta, \alpha_2 \Rightarrow \beta}{\Delta, \alpha_1 \rightarrow \alpha_2 \Rightarrow \beta} \rightarrow\text{-left}$$

- Precisamos de *loop checkers* para que o procedimento de busca termine

Um Cálculo de Sequentes Focado: $\mathbf{LMT}^{\rightarrow}$

- Usamos foco para controlar a geração de contra-exemplos
- A forma geral de um sequente em $\mathbf{LMT}^{\rightarrow}$ é:

$$\{\Delta'\}, \Delta^{p_1}, \Delta^{p_2}, ..., \Delta^{p_n}, \Delta \Rightarrow \varphi, [p_n, ..., p_2, p_1]$$

- Onde φ é uma fórmula em $\mathcal{L}$
- Δ, Δ' são bags de formulas
- Δ^{p_i} fórmulas rotuladas como associadas à proposição p_i

Axiomas e Regras em $\mathbf{LMT}^{\rightarrow}$

$$\frac{}{\{\Delta'\}, \Delta, \mathbf{p} \Rightarrow \mathbf{p}, [\Gamma]}\ \mathit{axiom} \qquad \frac{}{\{\Delta', \mathbf{p}\}, \Delta \Rightarrow \mathbf{p}, [\Gamma]}\ \mathit{axiom}_{\{\}}$$

$$\frac{\{\Delta', \boldsymbol{\alpha}\}, \alpha, \Delta \Rightarrow \beta, [\Gamma]}{\{\Delta'\}, \boldsymbol{\alpha}, \Delta \Rightarrow \beta, [\Gamma]}\ \text{focus} \qquad \frac{\{\}, \Delta \Rightarrow \boldsymbol{\gamma}, [\Gamma, \beta]}{\{\boldsymbol{\Delta'}\}, \Delta \Rightarrow \beta, [\boldsymbol{\gamma}, \Gamma]}\ \text{restart}$$

$$\frac{\{\Delta'\}, \boldsymbol{\alpha}, \Delta \Rightarrow \boldsymbol{\beta}, [\Gamma]}{\{\Delta'\}, \Delta \Rightarrow \boldsymbol{\alpha} \rightarrow \boldsymbol{\beta}, [\Gamma]}\ \rightarrow\text{-right}$$

$$\frac{\{\alpha_1 \rightarrow \alpha_2, \Delta'\}, \Delta \Rightarrow \boldsymbol{\alpha_1}, [\beta, \Gamma] \qquad \{\alpha_1 \rightarrow \alpha_2, \Delta', \boldsymbol{\alpha_2}\}, \Delta \Rightarrow \beta, [\Gamma]}{\{\boldsymbol{\alpha_1} \rightarrow \boldsymbol{\alpha_2}, \Delta'\}, \Delta \Rightarrow \beta, [\Gamma]}\ \rightarrow\text{-left}$$

Estratégia de Prova

Estratégia de Prova

1. O sequente de conclusão tem a forma $\{\}, \Delta \Rightarrow \varphi, []$
2. Aplique $\rightarrow$-dir sempre que possível
3. Aplique focus e $\rightarrow$-esq quando não for possível aplicar $\rightarrow$-dir
4. Quando todas as fórmulas de um sequente já foram expandidas, aplique o restart
5. A cada nova aplicação de regra a partir desse ponto, um *loop-checker* deve ser executado.

Esquema Geral de Prova

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\{\}, \Delta^{p}, \Delta^{q}, \ldots, \Theta^{a}, \Delta \Rightarrow z, [\ldots, q, p, a]}{\{\Delta'\}, \Delta^{p}, \Delta^{q}, \ldots, \Delta^{z}, \Theta \Rightarrow a, [z, \ldots, q, p]}\ \text{restart}}{\vdots}}{\{\varphi \rightarrow \psi\}, \Delta^{p}, \varphi_{1}, \ldots, \varphi_{n} \Rightarrow q, [p]}\ \text{focus and } \rightarrow\text{-left}}{\vdots}}{\{\varphi \rightarrow \psi\}, \Delta^{p} \Rightarrow \varphi, [p]}\ \rightarrow\text{-right} \qquad \dfrac{\vdots}{\{\varphi \rightarrow \psi, \psi\}, \Delta \Rightarrow p, []}}{\{\varphi \rightarrow \psi\}, \Delta \Rightarrow p, []}\ \rightarrow\text{-left}}{\{\}, \Delta \Rightarrow p, []}\ \text{focus}}{\vdots}}{\{\} \Rightarrow \alpha, []}\ \rightarrow\text{-right}$$

Correção

Definição

Um sequente $\{\Delta'\}, \Delta^{p_1}, \Delta^{p_2}, \ldots, \Delta^{p_n}, \Delta \Rightarrow \varphi, [p_n, \ldots, p_2, p_1]$ *é válido de acordo com a estratégia de prova, se e somente se,* $\Delta', \Delta^{p_1}, \Delta^{p_2}, \ldots, \Delta^{p_n}, \Delta \models \varphi$ *ou* $\exists i \Delta^{p_i} \models p_i$.

Definição

Uma regra é correta de acordo com a estatégia de prova, se e somente se, se as premissas do sequente (gerado pela estratégia) são válidas, então a conclusão também é.

Correção

Definição

Um sequente $\{\Delta'\}, \Delta^{p_1}, \Delta^{p_2}, \ldots, \Delta^{p_n}, \Delta \Rightarrow \varphi, [p_n, \ldots, p_2, p_1]$ *é válido de acordo com a estratégia de prova, se e somente se,* $\Delta', \Delta^{p_1}, \Delta^{p_2}, \ldots, \Delta^{p_n}, \Delta \models \varphi$ *ou* $\exists i \Delta^{p_i} \models p_i$.

Definição

Uma regra é correta de acordo com a estatégia de prova, se e somente se, se as premissas do sequente (gerado pela estratégia) são válidas, então a conclusão também é.

Correção

Proposição

Considerando a validade de um sequente como definida acima, $\mathbf{LMT}^{\rightarrow}$ *é correta.*

Prova

Provamos a correção mostrando que cada regra de $\mathbf{LMT}^{\rightarrow}$ *é correta de acordo com as definições acima.*

Correção

Proposição

Considerando a validade de um sequente como definida acima, $\mathbf{LMT}^{\rightarrow}$ *é correta.*

Prova

Provamos a correção mostrando que cada regra de $\mathbf{LMT}^{\rightarrow}$ *é correta de acordo com as definições acima.*

Completude

- Provamos que todas as regras exceto o restart são inversíveis
- Mostraremos que entre um ponto e outro, após a busca parar pelo uso do *loop-checker*, é possível construir um contra-modelo (usando Semântica de Kripke) que se propaga até a conclusão

Trabalhos Relacionados

- Diversos sistemas focados: LJQ (Dickhoff e Legrand), LJF (Lang e Miller)
  - Sistemas focados que inspiraram nossa estratégia
- Pinto e Dyckhoff
  - Dois "sistemas dedutivos": um para prova, outro para contra-exemplos:
- Ferrari, Fiorentini e Fiorino
  - Semelhante ao trabalho de Pinto e Dyckhoff, mas garantindo a Propriedade da Subfórmula e a geração de contra-modelos de comprimento mínimo

Conclusões e Trabalhos Futuros

Trabalhos Futuros...

- Prova da completude do sistema de acordo com a estratégia
- Implementar a prova automática/geração de contra-modelos (Semântica de Kripke) no provador

Obrigado!!!

Lógica Minimal, Intuicionista e Clássica

Lógica Minimal return

$$\frac{A \wedge B}{A}\ \wedge_1\text{-e} \qquad \frac{A \quad B}{A \wedge B}\ \wedge\text{-i} \qquad \frac{A \wedge B}{B}\ \wedge_2\text{-e}$$

$$\frac{A \vee B \quad \begin{array}{c}[A]\\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]\\ \vdots \\ C\end{array}}{C}\ \vee\text{-e} \qquad \frac{A}{A \vee B}\ \vee_1\text{-i} \qquad \frac{B}{A \vee B}\ \vee_2\text{-i}$$

$$\frac{A \quad \neg A}{\bot}\ \neg\text{-e} \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ \bot\end{array}}{\neg A}\ \neg\text{-i}$$

$$\frac{A \quad A \to B}{B}\ \to\text{-e} \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}\ \to\text{-i}$$

Lógica Minimal, Intuicionista e Clássica

Lógica Intuicionista return

$$\text{Lógica Minimal} \quad + \quad \boxed{\frac{\bot}{A}\ \bot\text{-Int}}$$

Lógica Minimal, Intuicionista e Clássica

Lógica Intuicionista return

$$\text{Lógica Minimal} \quad + \quad \boxed{\dfrac{\bot}{A}\ \bot\text{-Int}}$$

Lógica Clássica return

$$\text{Lógica Minimal} \quad + \quad \boxed{\begin{array}{c}[\neg A]\\ \vdots\\ \dfrac{\bot}{A}\end{array}\ \bot\text{-Cla}}$$

ou ....

$$\text{Lógica Intuicionista} \quad + \quad \boxed{\begin{array}{c}[\neg A]\\ \vdots\\ \dfrac{\bot}{A}\end{array}\ \bot\text{-Cla}}$$