1
Introdução

Existem diversas interconexões entre Teoria da prova e Ciência da Computação que merecem citação destacada tais como: procedimentos de tipagem para linguagens de programações, geração de programas por meio de extração de conteúdo computacional de provas lógicas, complexidade computacional, estimativa de tamanho de provas normais em certos sistemas lógicos e outros. Por outro lado, são bem conhecidas as hierarquias de análise computacional geradas por meio de problemas de decisão lógica. Para cada classe hierárquica pode se fornecer um problema completo representado em lógica formal. Alguns destes problemas envolvem validade de uma fórmula em uma certa lógica, o que implica existência de prova. É amplamente conhecido que o tamanho de uma prova é um tema relevante tanto na teoria quanto na prática.

Especificamente as provas curtas podem ser uma contra-parte de uma prova teórica de computações viáveis, onde por definição o comprimento de uma prova curta é polinomial em relação ao comprimento de sua conclusão. O comprimento de uma fórmula ou de uma prova é dado pelo número de símbolos usado para escrevê-la. O fato de que toda tautologia clássica possui uma prova curta implica que $CoNP = NP$, e a existência de tautologias que não possuem esta propriedade em qualquer sistema de prova implica que $CoNP \neq NP$, e assim $NP \neq P$, de acordo com o teorema de Cook (CR79). Para lógica intuicionista a existência de provas curtas para cada tautologia implica $NP = PSPACE$. Além disso, Seldin mostrou que em sistemas de Dedução Natural (doravante DN), qualquer tautologia clássica pode ser provada com no máximo uma aplicação da regra do absurdo clássico. A prova deste fato é realizada fornecendo uma transformação de uma prova em DN de α em uma prova de α em dedução natural tendo no máximo uma aplicação da regra do absurdo e, caso a prova precise da regra, esta seria a última regra aplicada. Posteriormente é verificado se a prova anterior é polinomial em relação ao tamanho de α então a posterior também será. Desta forma, $\vdash_{Cla}^{Poly(|\alpha|)} \alpha$ se, e somente se, $\vdash_{Int}^{Poly(|\alpha|)} \neg\alpha \rightarrow \bot$. Portanto, a existência de provas polinomiais para cada tautologia intuicionista implica na existência de provas polinomiais para cada tautologia clássica, assim neste caso $CoNP = PSPACE = NP$. Em outras palavras, a existência de provas polinomiais para toda tautologia intuicionista

é equivalente a $NP = CoNP = PSPACE$ enquanto para o caso clássico $NP = CoNP$. Estas provas devem ser consideradas em sistemas de provas que polinomialmente simulam sistemas de deduções conhecidos, tais como Dedução Natural ou Cálculo de Seqüentes.

A decisão se as igualdades $CoNP = PSPACE$, $NP = PSPACE$ e $NP = CoNP$ são válidas ou não é uma tarefa difícil e provoca debates instigantes. Por outro lado, enquanto não são encontradas as respostas para estas questões, há exemplos bem conhecidos de limites inferiores grandes para provas de tipos específicos tratadas em certos sistemas de prova. Um caso que vale mencionar é o limite inferior super polinomial para a prova do Princípio das Casas de Pombos (doravante PHP) quando tratado em sistema de provas em Resolução. Este limite inferior é o mesmo para Cálculo de Seqüentes livres de corte. Este exemplo tem sido muito útil para argumentar em favor da regra do corte para fornecer provas em Lógica Proposicional, uma vez que tais limites inferiores grandes não são conhecidos para qualquer tautologia proposicional em cálculo de seqüentes com regra do corte.

Assim, dada uma prova Π em DN, sua correspondente prova normal Π' tem limite inferior hiper-polinomial conhecido com relação ao tamanho de Π bem como alguns exemplos com limite inferior hiper-polinomial com relação a Π. Um destes exemplos pode ser encontrado em Troelstra (vide (TS00, pp. 215)) e usa a representação tipada de numerais de Church para construir um prova de tamanho polinomial de uma tautologia que tem uma correspondente prova normal que não pode ser limite de qualquer função elementar. Para lógica de primeira ordem, Orekov apresenta exemplos de fórmulas com provas de tamanho linear para o qual qualquer prova normal tem um limite inferior hiper-polinomial.

Toda esta discussão acima aponta para a necessidade de mecanismos para comprimir provas. Pode se argumentar sobre o uso de já conhecidos algoritmos de compactação para tal fato. Contudo, o seu uso é baseado no fato de que a prova já seja conhecida. A regra do corte é comumente colocada de lado em qualquer implementação de provadores de teoremas, e claramente este é o problema com provas demasiadamente grandes. O mesmo pode ser dito sobre provadores de teoremas em Dedução Natural que são feitos para construir provas normais. Para inclusão da regra do corte na implementação (ou permitir que a implementação construa provas não normais), o implementador deve considerar uma grande quantidade de alternativas em cada passo da prova. Isto tornará a implementação pouco eficiente. Por outro lado, se algumas estratégias pontuais que permitem que a regra do corte (uma fórmula máxima em terminologia de DN) sejam previamente conhecidas acarreta implementação melhor do que a anterior, sendo capaz de produzir provas curtas para casos em que implementações livres do corte não podem.

Propomos dois métodos para a redução do tamanho de provas proposicionais.

O primeiro, denominado método horizontal, atinge a eficiência desejada quando adiciona regras de atenuação conjuntamente com uma unificação via substituição de variáveis (proposicionais). Também apresentamos um método que gera tal unificação durante o processo de construção da prova.

O segundo, denominado método vertical, alcança a eficiência desejada por meio do uso de axiomas de extensão. Apresentamos um procedimento que gera tais axiomas de extensão.

Capítulo 2 apresenta a terminologia básica usada no artigo, alguns resultados também básicos de hierarquia computacional, uma introdução de sistemas de provas com ênfase em sistemas de Frege, o princípio das casas de pombos e alguns resultadas conhecidos de aplicação em sistemas de Frege em Resolução. Também mostramos no final do capítulo 2 uma tradução da lógica clássica para a lógica intuicionista. No capítulo 3 apresentamos o método Horizontal com exemplos em dedução Natural e formalização em um cálculo de seqüentes simplificado, SEQ_0. No capítulo 4 é apresentado o método Vertical para redução de provas. Por fim, no capítulo 5 são apresentadas as conclusões e trabalhos futuros.