

Proof Structuring and Compression by Atomic Cut-Introduction by Resolution **CIRes**

Bruno Woltzenlogel Paleo

Theoretische Informatik und Logik
Institut für Computersprachen
Technische Universität Wien

2009, November 25th

- Proof-Theoretical Motivation for Cut-Introduction
- Mathematical and Computational Motivations for Cut-Introduction
- Broader Motivation for Cut-Introduction
- Naive Reductive Cut-Introduction
- Essential Improvements of Cut-Elimination by Resolution
- Atomic-Cut-Introduction by Resolution
- Exponential Compression of Proofs

- In theory:
 - Elimination of cuts can cause non-elementary blow-up in size
 - Introduction of cuts could lead to non-elementary compression in size
- In practice:
 - Proof-carrying code (verification)
 - Automated deduction techniques (theorem provers, SMTSolvers, . . .)
produce large analytic proofs
 - Cut-introduction could compress these proofs

- Cuts correspond to lemmas
- Lemmas are useful for structuring proofs
- Conditional Lemmas are closely related to the definition of new concepts in mathematics:
 - $((\forall x, y, z \in M)(x.y).z = x.(y.z)) \wedge ((\exists e \in M)(\forall x \in M)(e.x = x.e = x)) \rightarrow$
 $HasUsefulProperty(M)$
 - $Monoid(M) \rightarrow HasNiceProperty(M)$
- Cut-Introduction could, in principle, structure (collections of) mathematical proofs and automatically discover new mathematical concepts

- Curry-Howard Isomorphism:
 - Proofs \Leftrightarrow Lambda Expressions (Programs)
 - Cut-Elimination \Leftrightarrow Beta-reduction (Execution of Programs)
 - Cut-Introduction \Leftrightarrow (Structuring of Programs)
- Structuring of Programs:
 - Modularity
 - Composition of smaller programs
 - Code-reuse
 - OOP

- Knowledge = proof (e.g. a book of Mathematics)
- Proofs in a broader sense (i.e. experimental procedures are proofs too)
- Organization of knowledge = proof structuring
- Proof structuring = Cut-Introduction
- “Science is built up with facts, as a house is with stones. But a collection of facts is not more a science than a heap of stones is a home.” - Henri Poincaré
- Organization of knowledge is one of the most fundamental tasks of Science.
- **Cut-introduction: one of the most fundamental tasks of science, from a foundational and formal point of view.**
- “entities must not be multiplied beyond necessity” (“the simplest ‘theory’[collection of proofs] is the best”) - William of Ockham
- **Cut-introduction: a possible precise and automatic way for achieving “simpler” ‘theories’**

- Reductive cut-elimination pushes cuts upwards, decomposing and instantiating them and eliminating atomic cuts when they reach the axioms
- Naive idea for cut-introduction:
 - ① Add atomic cuts on the axioms of the cut-free proof
 - ② Apply the reductive rules in the opposite direction, pushing cuts downwards, composing, quantifying and **contracting** them when possible/desirable.
- Problem: non-determinism, non-confluence...
 - Many possible ways to push cuts downwards, but only a few may allow **contractions** and result in the desired compression.

Naive Reductive Cut-Introduction

The Importance of Contractions

$$\frac{\frac{\varphi_l}{\Gamma \vdash \Delta, A, A} \text{ } c_r \quad \frac{\varphi_r}{A, \Pi \vdash \Lambda} \text{ } cut}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{ } cut$$

⇓

$$\frac{\frac{\varphi_l}{\Gamma \vdash \Delta, A, A} \quad \frac{\varphi_r}{A, \Pi \vdash \Lambda} \text{ } cut}{\Gamma, \Pi \vdash \Delta, \Lambda, A} \text{ } cut \quad \frac{\varphi'_r}{A, \Pi \vdash \Lambda} \text{ } cut}{\frac{\Gamma, \Pi, \Pi \vdash \Delta, \Lambda, \Lambda, \quad c_l^*, c_r^*}{\Gamma, \Pi \vdash \Delta, \Lambda} \text{ } cut} \text{ } cut$$

Cut-Elimination by Resolution

An Example

$$\frac{\frac{\frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)}{\rightarrow_l}}{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)}{\rightarrow_r}}{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))}{\exists_r}}{\frac{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall_l}}{\frac{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))}{\forall_r}} \quad \frac{\frac{\frac{\frac{P(a) \vdash P(a) \quad Q(v) \vdash Q(v)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)}{\rightarrow_l}}{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)}{\rightarrow_r}}{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists_r}}{\frac{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists_l}}{\frac{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall_l}} \quad \text{cut}$$
$$\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))$$

Cut-Elimination by Resolution

An Example

$$\frac{
 \frac{
 \frac{
 \frac{P(u) \vdash P(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)}{\rightarrow_l}
 \quad
 \frac{Q(u) \vdash Q(u)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)}{\rightarrow_l}
 }{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)}{\rightarrow_r}
 \quad
 \frac{Q(v) \vdash Q(v)}{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)}{\rightarrow_r}
 }{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))}{\exists_r}
 \quad
 \frac{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists_r}
 }{
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall_l}
 \quad
 \frac{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists_l}
 }{
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))}{\forall_r}
 \quad
 \frac{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall_l}
 }{
 \forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y)) \text{ cut}
 }$$

$$S_\varphi \equiv (\neg P(u) \otimes Q(u)) \oplus (P(a) \oplus \neg Q(v))$$

$$C_\varphi^W \equiv \{P(u) \vdash Q(u) ; \vdash P(a) ; Q(v) \vdash\}$$

$$\frac{
 \frac{\vdash P(a) \quad P(u) \vdash Q(u)}{\vdash Q(a)} \quad R
 \quad
 Q(v) \vdash R
 }{\vdash}$$

Cut-Elimination by Resolution

An Example

$$\begin{array}{c}
 \frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_l \\
 \frac{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)}{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \rightarrow_r \\
 \frac{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))} \exists_r \\
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_l \\
 \frac{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))}{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_r \\
 \frac{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cut}
 \end{array}$$

$$\frac{\frac{\vdash P(a) \quad P(u) \vdash Q(u)}{\vdash Q(a)} R \quad Q(v) \vdash R}{\vdash R} R$$

$\llbracket \varphi \rrbracket_{\vdash P(a)}^O :$

$$\frac{\frac{\frac{P(a) \vdash P(a)}{P(a) \vdash P(a), Q(v)} w_r}{\vdash P(a), P(a) \rightarrow Q(v)} \rightarrow_r}{\vdash P(a), \exists y(P(a) \rightarrow Q(y))} \exists_r$$

Cut-Elimination by Resolution

An Example

$$\frac{
 \frac{
 \frac{
 \frac{P(u) \vdash P(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_r
 \quad
 \frac{Q(u) \vdash Q(u)}{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)} \rightarrow_r
 }{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \exists_r
 \quad
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow_r
 \quad
 \frac{Q(v) \vdash Q(v)}{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)} \rightarrow_r
 }{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r
 \quad
 \frac{
 \frac{
 \frac{
 \frac{P(x) \rightarrow Q(x) \vdash \exists y(P(x) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(x) \rightarrow Q(y))} \forall_i
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_r
 }{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_i
 }{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cut}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))}$$

$$\frac{
 \frac{
 \frac{\vdash P(a)}{\vdash Q(a)} R
 \quad
 \frac{P(u) \vdash Q(u)}{Q(v) \vdash} R
 }{\vdash}$$

$\llbracket \varphi \rrbracket_{Q(v) \vdash}^{\circ}$:

$$\frac{
 \frac{
 \frac{Q(v) \vdash Q(v)}{Q(v), P(a) \vdash Q(v)} w_i
 \quad
 \frac{Q(v) \vdash P(a) \rightarrow Q(v)}{Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\vdash}$$

Cut-Elimination by Resolution

An Example

$$\begin{array}{c}
 \frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_i \quad \frac{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)}{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \rightarrow_r \quad \exists_r \\
 \frac{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))} \forall_i \\
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_r \\
 \hline
 \forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))
 \end{array}
 \qquad
 \begin{array}{c}
 \frac{P(a) \vdash P(a) \quad Q(v) \vdash Q(v)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow_i \quad \frac{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)}{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \rightarrow_r \quad \exists_r \\
 \frac{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_i \\
 \frac{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_i \\
 \hline
 \forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y)) \quad \text{cut}
 \end{array}$$

$$\frac{\frac{\vdash P(a) \quad P(u) \vdash Q(u)}{\vdash Q(a)} R \quad Q(v) \vdash R}{\vdash R} R$$

$\llbracket \varphi \rrbracket_{P(u) \vdash Q(u)}^{\circ}$:

$$\frac{\frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_i}{P(u), \forall x(P(x) \rightarrow Q(x)) \vdash Q(u)} \forall_i$$

Cut-Elimination by Resolution

An Example

$$\begin{array}{c}
 \frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_I \\
 \frac{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)}{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \rightarrow_r \\
 \frac{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))} \exists_r \\
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_I \\
 \frac{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_r \\
 \frac{P(a) \vdash P(a) \quad Q(v) \vdash Q(v)}{P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow_I \\
 \frac{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)}{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \rightarrow_r \\
 \frac{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))}{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r \\
 \frac{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_I \\
 \frac{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))}{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cut}
 \end{array}$$

$$\begin{array}{c}
 \frac{P(a) \vdash P(a)}{P(a) \vdash P(a), Q(v)} w_r \\
 \frac{P(a) \vdash P(a), Q(v)}{\vdash P(a), P(a) \rightarrow Q(v)} \rightarrow_r \\
 \frac{\vdash P(a), P(a) \rightarrow Q(v)}{\vdash P(a), \exists y(P(a) \rightarrow Q(y))} \exists_r \\
 \frac{\vdash P(a), \exists y(P(a) \rightarrow Q(y))}{\vdash Q(a)} \exists_r \\
 \frac{P(u) \vdash P(u) \quad Q(u) \vdash Q(u)}{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_I \\
 \frac{P(u), P(u) \rightarrow Q(u) \vdash Q(u)}{P(u), \forall x(P(x) \rightarrow Q(x)) \vdash Q(u)} \forall_I \\
 \frac{P(u), \forall x(P(x) \rightarrow Q(x)) \vdash Q(u)}{\vdash Q(a)} R \\
 \frac{Q(v) \vdash Q(v)}{Q(v), P(a) \vdash Q(v)} w_l \\
 \frac{Q(v), P(a) \vdash Q(v)}{Q(v) \vdash P(a) \rightarrow Q(v)} \rightarrow_r \\
 \frac{Q(v) \vdash P(a) \rightarrow Q(v)}{Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r \\
 \frac{Q(v) \vdash \exists y(P(a) \rightarrow Q(y))}{\vdash} R
 \end{array}$$

Cut-Elimination by Resolution

An Example

$$\frac{
 \frac{
 \frac{
 \frac{P(u) \vdash P(u)}{} \rightarrow_l \quad \frac{Q(u) \vdash Q(u)}{} \rightarrow_l
 }{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_r
 }{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)} \rightarrow_r
 }{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \exists_r
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))} \forall_l
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_r
 }{
 \frac{
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{} \rightarrow_l \quad \frac{Q(v) \vdash Q(v)}{} \rightarrow_l
 }{P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow_r
 }{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)} \rightarrow_r
 }{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_l
 }{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_l
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cut}
 }$$

$$\frac{
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{} \text{wr}
 }{P(a) \vdash P(a), Q(v)} \rightarrow_r
 }{\vdash P(a), P(a) \rightarrow Q(v)} \rightarrow_r
 }{\vdash P(a), \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\forall x(P(x) \rightarrow Q(x)) \vdash Q(a), \exists y(P(a) \rightarrow Q(y))}
 }{
 \frac{
 \frac{
 \frac{
 \frac{P(u) \vdash P(u)}{} \rightarrow_l \quad \frac{Q(u) \vdash Q(u)}{} \rightarrow_l
 }{P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_r
 }{P(u), \forall x(P(x) \rightarrow Q(x)) \vdash Q(u)} \forall_l
 }{P(u), \forall x(P(x) \rightarrow Q(x)) \vdash Q(a), \exists y(P(a) \rightarrow Q(y))} R
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y)), \exists y(P(a) \rightarrow Q(y))}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cr}
 }$$

Cut-Elimination by Resolution

An Example

$$\frac{
 \frac{
 \frac{
 \frac{P(u) \vdash P(u)}{\vdash P(u), P(u) \rightarrow Q(u) \vdash Q(u)} \rightarrow_r
 }{P(u) \rightarrow Q(u) \vdash P(u) \rightarrow Q(u)} \rightarrow_l
 }{P(u) \rightarrow Q(u) \vdash \exists y(P(u) \rightarrow Q(y))} \exists_r
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(u) \rightarrow Q(y))} \forall_l
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \forall x \exists y(P(x) \rightarrow Q(y))} \forall_r
 }{
 \frac{
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{\vdash P(a), P(a) \rightarrow Q(v) \vdash Q(v)} \rightarrow_r
 }{P(a) \rightarrow Q(v) \vdash P(a) \rightarrow Q(v)} \rightarrow_l
 }{P(a) \rightarrow Q(v) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\exists y(P(a) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_l
 }{\forall x \exists y(P(x) \rightarrow Q(y)) \vdash \exists y(P(a) \rightarrow Q(y))} \forall_l
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} \text{cut}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))}$$

$$\frac{
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{\vdash P(a) \vdash P(a), Q(a)} w_r
 }{\vdash P(a), P(a) \rightarrow Q(a)} \rightarrow_r
 }{\vdash P(a), \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\forall x(P(x) \rightarrow Q(x)) \vdash Q(a), \exists y(P(a) \rightarrow Q(y))}
 }{
 \frac{
 \frac{
 \frac{
 \frac{P(a) \vdash P(a)}{\vdash P(a), P(a) \rightarrow Q(a) \vdash Q(a)} \rightarrow_l
 }{P(a), \forall x(P(x) \rightarrow Q(x)) \vdash Q(a)} \forall_l
 }{\vdash P(a), \exists y(P(a) \rightarrow Q(y))} \text{cut}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash Q(a), \exists y(P(a) \rightarrow Q(y))}
 }{
 \frac{
 \frac{
 \frac{
 \frac{Q(a) \vdash Q(a)}{\vdash Q(a), P(a) \vdash Q(a)} w_l
 }{Q(a) \vdash P(a) \rightarrow Q(a)} \rightarrow_r
 }{Q(a) \vdash \exists y(P(a) \rightarrow Q(y))} \exists_r
 }{\exists y(P(a) \rightarrow Q(y))} \text{cut}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y)), \exists y(P(a) \rightarrow Q(y))}
 }{\forall x(P(x) \rightarrow Q(x)) \vdash \exists y(P(a) \rightarrow Q(y))} c_r
 }$$

Cut-Elimination by Resolution

A Problem

- An interesting fact about CERes: ACNFs produced by CERes have atomic cuts in the bottom of the proof (closer to the root).
- A related problem:
 - If CERes is applied to a proof already in ACNF, but with cuts in the top, CERes produces a new ACNF with cuts in the bottom
 - CERes unnecessarily pushes down the atomic cuts! (unnecessarily from the point of view of cut-elimination)
- Problem solved in my thesis... But is it really a problem?

Cut-Introduction by Resolution

Two Problems = One Solution

- Problem 1: how to push down the cuts in a good way when doing naive reductive cut-introduction?
- Problem 2: how to prevent CERes from pushing down the atomic cuts?
- Solution (CIRes) for problem 1: use CERes' bug (i.e. problem 2) as a feature!
 - ① Add atomic cuts to the top of the proof
 - ② Use CERes to push them down!
- Question: will it compress proofs?
- Intuitive Answer: Probably yes, because...
 - refutations contain factorings/contractions (exactly what we need for compression)
 - O-projections are very non-redundant

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

A short proof ψ with cut (length 5, atomic size 26, symbolic size 32):

$$\frac{\frac{\frac{A \vdash A}{A \vee A \vdash A, A} \vee_l \quad \frac{A \vdash A}{A, A \vdash A \wedge A} \wedge_r}{A \vee A \vdash A} c_r \quad \frac{\frac{A \vdash A}{A, A \vdash A \wedge A} c_l \quad \frac{A \vdash A}{A \vdash A \wedge A} \wedge_r}{A \vee A \vdash A \wedge A} cut$$

One of the shortest proofs without cut, φ (length 6, atomic size 32, symbolic size 41):

$$\frac{\frac{\frac{A \vdash A}{A, A \vdash A \wedge A} \wedge_r \quad \frac{A \vdash A}{A \vdash A \wedge A} c_l}{A \vee A \vdash A \wedge A, A \wedge A} \vee_l \quad \frac{\frac{A \vdash A}{A, A \vdash A \wedge A} c_l \quad \frac{A \vdash A}{A \vdash A \wedge A} \wedge_r}{A \vee A \vdash A \wedge A} c_r$$

Can CIRes output ψ when given φ as input?

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

φ' (with atomic cuts added to the top):

$$\frac{\frac{\frac{A \vdash A \quad A \vdash A}{A \vdash A} \text{ cut} \quad \frac{A \vdash A \quad A \vdash A}{A \vdash A} \wedge_r \text{ cut}}{\frac{A, A \vdash A \wedge A}{A \vdash A \wedge A} c_l} \quad \frac{\frac{\frac{A \vdash A \quad A \vdash A}{A \vdash A} \text{ cut} \quad \frac{A \vdash A \quad A \vdash A}{A \vdash A} \wedge_r \text{ cut}}{\frac{A, A \vdash A \wedge A}{A \vdash A \wedge A} c_l} \vee_l}{\frac{A \vee A \vdash A \wedge A, A \wedge A}{A \vee A \vdash A \wedge A} c_r} c_r$$

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

$$\frac{
 \frac{
 \frac{
 \frac{A \vdash A}{-} \quad \frac{A \vdash A}{-} \quad \text{cut}
 }{A \vdash A}
 \quad \frac{
 \frac{
 \frac{A \vdash A}{-} \quad \frac{A \vdash A}{-} \quad \text{cut}
 }{A \vdash A}
 \quad \frac{A \vdash A}{-} \quad \wedge_r
 }{A, A \vdash A \wedge A} \quad c_l
 }{A \vdash A \wedge A} \quad c_l
 }{A \vee A \vdash A \wedge A, A \wedge A}
 \quad \frac{
 \frac{
 \frac{
 \frac{A \vdash A}{-} \quad \frac{A \vdash A}{-} \quad \text{cut}
 }{A \vdash A}
 \quad \frac{
 \frac{
 \frac{A \vdash A}{-} \quad \frac{A \vdash A}{-} \quad \text{cut}
 }{A \vdash A}
 \quad \frac{A \vdash A}{-} \quad \wedge_r
 }{A, A \vdash A \wedge A} \quad c_l
 }{A \vdash A \wedge A} \quad v_l
 }{A \vee A \vdash A \wedge A} \quad c_r
 }{A \vee A \vdash A \wedge A} \quad c_r$$

$$\mathcal{S}_{\varphi'} \equiv ((A \oplus \neg A) \otimes^{**} (A \oplus \neg A)) \otimes^{***} ((A \oplus \neg A) \otimes^{**} (A \oplus \neg A))$$

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

$$\frac{\frac{\frac{A \vdash A}{A \vdash A} \text{ cut} \quad \frac{A \vdash A}{A \vdash A} \text{ cut}}{\frac{A, A \vdash A \wedge A}{A \vdash A \wedge A} c_l} \wedge_r \quad \frac{\frac{\frac{A \vdash A}{A \vdash A} \text{ cut} \quad \frac{A \vdash A}{A \vdash A} \text{ cut}}{\frac{A, A \vdash A \wedge A}{A \vdash A \wedge A} c_l} \wedge_r}{\frac{A \vee A \vdash A \wedge A, A \wedge A}{A \vee A \vdash A \wedge A} c_r}$$

$$\begin{aligned}
 S_{\varphi'} &\equiv ((A \oplus \neg A) \otimes^{**} (A \oplus \neg A)) \otimes^{***} ((A \oplus \neg A) \otimes^{**} (A \oplus \neg A)) \\
 &\rightsquigarrow_{\otimes \otimes W} (A \oplus A \oplus (\neg A \otimes^{**} \neg A)) \otimes^{***} ((A \oplus \neg A) \otimes^{**} (A \oplus \neg A)) \\
 &\rightsquigarrow_{\otimes \otimes W} (A \oplus A \oplus (\neg A \otimes^{**} \neg A)) \otimes^{***} (A \oplus A \oplus (\neg A \otimes^{**} \neg A)) \\
 &\rightsquigarrow_{\otimes \otimes W} (A \otimes^{***} A) \oplus (A \otimes^{***} A) \oplus (A \otimes^{***} A) \oplus (A \otimes^{***} A) \oplus (\neg A \otimes^{**} \neg A) \oplus (\neg A \otimes^{**} \neg A)
 \end{aligned}$$

$$C_{\varphi'}^W \equiv \{ \vdash A, A ; \vdash A, A ; \vdash A, A ; \vdash A, A ; A, A \vdash ; A, A \vdash \}$$

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

$$\frac{
 \frac{
 \frac{
 \frac{A \vdash A}{A \vdash A} \text{ cut} \quad \frac{A \vdash A}{A \vdash A} \text{ cut}
 }{A, A \vdash A \wedge A} c_l
 \quad
 \frac{
 \frac{A \vdash A}{A \vdash A} \wedge_r
 }{A \vee A \vdash A \wedge A} c_r
 }{A \vee A \vdash A \wedge A} \vee_l
 }{A \vee A \vdash A \wedge A} c_r$$

$$C_{\varphi'}^W \equiv \{ \vdash A, A ; \vdash A, A ; \vdash A, A ; \vdash A, A ; A, A \vdash ; A, A \vdash \}$$

δ :

$$\frac{
 \frac{\vdash A, A}{\vdash A} f_r \quad \frac{A, A \vdash}{A \vdash} f_l
 }{\vdash} R$$

Testing the Method (can it really compress proofs?)

A Simple Example: $A \vee A \vdash A \wedge A$

φ^* :

$$\frac{\frac{\frac{A \vdash A}{A \vee A \vdash A, A} \vee_l \quad \frac{A \vdash A}{A, A \vdash A \wedge A} \wedge_r}{A \vee A \vdash A \wedge A} \text{cut}}{A \vee A \vdash A \wedge A} \text{cut}$$

- Can CIRes output ψ when given φ as input?
 - Yes, φ^* equal to ψ !

- Consider the sequence of unsatisfiable sets of clauses:

$$C_m = \{\pm P^1 \vee \pm P_{\pm}^2 \vee \pm P_{\pm\pm}^3 \vee \dots \vee \pm P_{\pm\dots\pm}^m | \dots\}$$

- For example:

$$C_2 = \{P^1 \vee P_+^2, \neg P^1 \vee P_-^2, P^1 \vee \neg P_+^2, \neg P^1 \vee \neg P_-^2\}$$

- It is known (from [Cook-Reckhow, 1971]) that:
 - $size(C_m) \in O((2m)2^m)$.
 - $length(\delta_m) \in O(2^{km})$, if δ_m is an optimal resolution refutation of C_m .
 - $length(\psi_m) \in \Omega(2^{2^{cm}})$, if ψ_m is an optimal tableaux refutation of C_m .

Testing the Method

A More Interesting Example

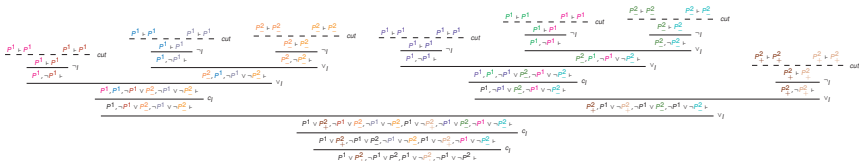
φ (length 17, atomic size 97, symbolic size 169):

$$\begin{array}{c}
 \frac{\frac{P^1 \vdash P^1}{P^1, \neg P^1 \vdash} \neg_I}{P^1, P^1, \neg P^1 \vee P^2, \neg P^1 \vee \neg P^2 \vdash} \neg_I \quad \frac{\frac{\frac{P^1 \vdash P^1}{P^1, \neg P^1 \vdash} \neg_I \quad \frac{P^2 \vdash P^2}{P^2, \neg P^2 \vdash} \neg_I}{P^2, P^1, \neg P^1 \vee \neg P^2 \vdash} \vee_I}{P^1, \neg P^1 \vee P^2, \neg P^1 \vee \neg P^2 \vdash} \vee_I \quad \frac{\frac{P^1 \vdash P^1}{P^1, \neg P^1 \vdash} \neg_I \quad \frac{\frac{P^2 \vdash P^2}{P^2, \neg P^2 \vdash} \neg_I}{P^2, P^1, \neg P^1 \vee \neg P^2 \vdash} \vee_I}{P^1, P^1, \neg P^1 \vee P^2, \neg P^1 \vee \neg P^2 \vdash} \vee_I \quad \frac{P^2 \vdash P^2}{P^2, \neg P^2 \vdash} \neg_I \\
 \frac{\frac{\frac{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I \quad \frac{\frac{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I \\
 \frac{\frac{\frac{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I}{P^1 \vee P^2_+, \neg P^1 \vee P^2_-, \neg P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_-} \vee_I
 \end{array}$$

Testing the Method

A More Interesting Example

φ' :



$$S_{\varphi'} \equiv ((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm}))$$

$$\begin{aligned}
 S_{\varphi'} &\equiv ((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm})) \\
 &\rightsquigarrow_{\otimes \otimes W} ((P^1 \oplus \neg P^1) \otimes^{**} (P^1 \oplus P^2_{\pm} \oplus \neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} (((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm})) \\
 &\rightsquigarrow_{\otimes \otimes W} (P^1 \oplus P^1 \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} (((P^1 \oplus \neg P^1) \otimes^{**} ((P^1 \oplus \neg P^1) \otimes^{**} (P^2_{\pm} \oplus \neg P^2_{\pm}))) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm})) \\
 &\rightsquigarrow_{\otimes \otimes W} (P^1 \oplus P^1 \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} (((P^1 \oplus \neg P^1) \otimes^{**} (P^1 \oplus P^2_{\pm} \oplus \neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm})) \\
 &\rightsquigarrow_{\otimes \otimes W} (P^1 \oplus P^1 \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} ((P^1 \oplus P^1 \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} (P^2_{\pm} \oplus \neg P^2_{\pm})) \\
 &\rightsquigarrow_{\otimes \otimes W} (P^1 \oplus P^1 \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \otimes^{***} ((P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm}) \oplus P^2_{\pm}) \\
 &\rightsquigarrow_{\otimes \otimes W} ((P^1 \otimes^{***} P^2_{\pm}) \oplus (P^1 \otimes^{***} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})) \oplus ((P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm}) \oplus P^2_{\pm}) \\
 &\equiv (P^1 \otimes^{***} P^2_{\pm}) \oplus (P^1 \otimes^{***} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm}) \oplus (P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (P^1 \otimes^{***} \neg P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} P^2_{\pm}) \oplus (\neg P^1 \otimes^{**} \neg P^2_{\pm})
 \end{aligned}$$

$$C_{\varphi'}^W \equiv \{ \vdash P^1, P^2_{\pm} ; \vdash P^1, P^2_{\pm} ; P^1 \vdash P^2_{\pm} ; P^1, P^2_{\pm} \vdash ; P^2_{\pm} \vdash P^1 ; P^2_{\pm} \vdash P^1 ; P^1 \vdash P^2_{\pm} ; P^1, P^2_{\pm} \vdash \}$$

δ :

$$\frac{\frac{\vdash P^1, P^2_{\pm} \quad P^2_{\pm} \vdash P^1}{\vdash P^1, P^1} R \quad \frac{P^1 \vdash P^2_{\pm} \quad P^1, P^2_{\pm} \vdash}{P^1 \vdash P^1} R}{\vdash} R$$

Testing the Method

A More Interesting Example

φ^* (length 13, atomic size 70, symbolic size 105):

$$\begin{array}{c}
 \frac{\frac{p^1 \vdash p^1}{p^1 \vee p^2_+ \vdash p^1, p^2_+} \vee_I \quad \frac{\frac{p^2_+ \vdash p^2_+}{p^2_+, \neg p^2_+ \vdash} \neg_I}{p^2_+, p^1 \vee \neg p^2_+ \vdash p^1} \vee_I}{\frac{p^1 \vee p^2_+, p^1 \vee \neg p^2_+ \vdash p^1, p^1}{p^1 \vee p^2_+, p^1 \vee \neg p^2_+ \vdash p^1} \text{cut}} \text{cut} \\
 \frac{\frac{p^1 \vdash p^1}{p^1, \neg p^1 \vdash} \neg_I \quad \frac{p^2_- \vdash p^2_-}{p^2_-, p^1, \neg p^1 \vee \neg p^2_- \vdash} \vee_I}{\frac{p^1, p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash}{p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash} \text{cut}} \text{cut} \\
 \frac{\frac{p^1 \vee p^2_+, p^1 \vee \neg p^2_+ \vdash p^1, p^1}{p^1 \vee p^2_+, p^1 \vee \neg p^2_+ \vdash p^1} \text{cr} \quad \frac{\frac{p^1 \vee p^2_+, p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash}{p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash} \text{cr}}{p^1 \vee p^2_+, p^1 \vee \neg p^2_+, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash} \text{cut}
 \end{array}$$

φ (length 17, atomic size 97, symbolic size 169):

$$\begin{array}{c}
 \frac{\frac{p^1 \vdash p^1}{p^1, \neg p^1 \vdash} \neg_I \quad \frac{\frac{p^1 \vdash p^1}{p^1, \neg p^1 \vdash} \neg_I \quad \frac{p^2_- \vdash p^2_-}{p^2_-, \neg p^2_- \vdash} \neg_I}{p^2_-, p^1, \neg p^1 \vee \neg p^2_- \vdash} \vee_I}{\frac{p^1, p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash}{p^1, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash} \text{C}_1} \text{C}_1 \\
 \frac{\frac{p^1 \vdash p^1}{p^1, \neg p^1 \vdash} \neg_I \quad \frac{\frac{p^2_- \vdash p^2_-}{p^2_-, \neg p^2_- \vdash} \neg_I \quad \frac{p^1 \vdash p^1}{p^1, \neg p^1 \vdash} \neg_I}{\frac{p^2_-, p^1, \neg p^1 \vee \neg p^2_- \vdash}{p^2_+, p^1 \vee \neg p^2_+, \neg p^1 \vee \neg p^2_- \vdash} \vee_I} \vee_I \\
 \frac{\frac{p^1 \vee p^2_+, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash}{p^1 \vee p^2_+, \neg p^1 \vee \neg p^2_- \vdash} \text{C}_1 \quad \frac{\frac{p^1 \vee p^2_+, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash}{p^1 \vee p^2_+, \neg p^1 \vee \neg p^2_- \vdash} \text{C}_1}}{p^1 \vee p^2_+, \neg p^1 \vee p^2_-, \neg p^1 \vee \neg p^2_- \vdash} \text{C}_1
 \end{array}$$

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2_{\pm} \vee \pm P^3_{\pm\pm} \vee \dots \vee \pm P^m_{\pm\dots\pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_{+}, \neg P^1 \vee P^2_{-}, P^1 \vee \neg P^2_{+}, \neg P^1 \vee \neg P^2_{-} \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}([\varphi_m]_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2 \vee \pm P^3 \vee \dots \vee \pm P^m_{\pm \dots \pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_+, \neg P^1 \vee P^2_-, P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_- \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
 - Mentioned, though neither proved nor cited, in Cook-Reckhow's "On the Lengths of Proofs in the Propositional Calculus".
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}([\varphi_m]_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2 \vee \pm P^3 \vee \dots \vee \pm P^m_{\pm \dots \pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_+, \neg P^1 \vee P^2_-, P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_- \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
 - Follows from the fact that cut-free sequent calculus and analytic tableaux p-simulate each other.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}([\varphi_m]_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2_{\pm} \vee \pm P^3_{\pm\pm} \vee \dots \vee \pm P^m_{\pm\dots\pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_+, \neg P^1 \vee P^2_-, P^1 \vee \neg P^2_+, \neg P^1 \vee \neg P^2_- \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
 - Mentioned, though neither proved nor cited, in Cook-Reckhow's "On the Lengths of Proofs in the Propositional Calculus". Nevertheless, easy to prove.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}(\lfloor \varphi_m \rfloor_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P_{\pm}^2 \vee \pm P_{\pm\pm}^3 \vee \dots \vee \pm P_{\pm\dots\pm}^m | \dots\}$
(e.g. $T_2 = P^1 \vee P_{+}^2, \neg P^1 \vee P_{-}^2, P^1 \vee \neg P_{+}^2, \neg P^1 \vee \neg P_{-}^2 \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
 - Follows from the correspondence between profile/swapped normalization and inference swapping (lemma proved in my thesis), together with the fact that most branching inferences in φ_m are independent from each other.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}(\lfloor \varphi_m \rfloor_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2_{\pm} \vee \pm P^3_{\pm\pm} \vee \dots \vee \pm P^m_{\pm\dots\pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_{+}, \neg P^1 \vee P^2_{-}, P^1 \vee \neg P^2_{+}, \neg P^1 \vee \neg P^2_{-} \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
 - Follows immediately from Lemma 4.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}(\lfloor \varphi_m \rfloor_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2 \vee \pm P^3_{\pm\pm} \vee \dots \vee \pm P^m_{\pm\dots\pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_{+}, \neg P^1 \vee P^2_{-}, P^1 \vee \neg P^2_{+}, \neg P^1 \vee \neg P^2_{-} \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}(\lfloor \varphi_m \rfloor_c^O) \in O(m)$.
 - $\lfloor \varphi_m \rfloor_c^O$ will have exactly $m - 1$ \vee_I inferences and at most m \neg_I inferences.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.

Theorem (Exponential Proof Compression via CIRes)

There exists a sequence of sequents T_m such that:

- if φ_m is a sequence of shortest cut-free proofs of T_m , then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$ (for some positive rational c).
- $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$ (for some k).

Proof Sketch

- 1 Let T_m be the sequent corresponding to: $C_m = \{\pm P^1 \vee \pm P^2_{\pm} \vee \pm P^3_{\pm\pm} \vee \dots \vee \pm P^m_{\pm\pm\pm} | \dots\}$
(e.g. $T_2 = P^1 \vee P^2_{+}, \neg P^1 \vee P^2_{-}, P^1 \vee \neg P^2_{+}, \neg P^1 \vee \neg P^2_{-} \vdash$)
- 2 Lemma 1: Let ψ_m be a shortest analytic tableaux refutation of C_m . Then $\text{length}(\psi_m) \in \Omega(2^{2^{cm}})$.
- 3 Lemma 2: Let φ_m be the cut-free sequent calculus proof of T_m corresponding to ψ_m . Then $\text{length}(\varphi_m) \in \Omega(2^{2^{cm}})$.
- 4 Lemma 3: Let δ_m be the shortest resolution refutation of C_m . Then $\text{length}(\delta_m) \in O(2^{km})$.
- 5 Lemma 4: $C_m \subseteq C_{\varphi_m}^W$.
- 6 Lemma 5: δ_m is a refutation of $C_{\varphi_m}^W$.
- 7 Lemma 6: Let $c \in C_{\varphi_m}^W$. Then $\text{length}(\lfloor \varphi_m \rfloor_c^O) \in O(m)$.
- 8 Finally: $\text{length}(\text{CIRes}(\varphi_m)) \in O(m \cdot 2^{km})$.
 - Follows immediately from Lemmas 3, 5, 6, because $\text{CIRes}(\varphi_m)$ is a composition of δ_m and exponentially many projections of linear size.

- Enrich the clause set with more information from the cut-free proof, and use the additional information to constrain the search for refutations of the clause set.
- Try to extend the method so that *complex* propositional cuts could also be introduced. (This might be possible with a mixed structural clause form transformation of the cut-pertinent struct).
- Modify the concept of projection and modify how they are combined with the refutation, so that atomic cuts do not necessarily appear in the bottom of the proof.

- Thanks!
- Questions? Comments? Suggestions?