Diplomarbeitspräsentationen der Fakultät für Informatik

Integrating Theories into Inference Systems

Masterstudium
Computational Intelligence

Martin Riener

Technische Universität Wien
Institut für Computersprachen
Arbeitsbereich: Theoretische Informatik und Logik
Betreuer: Univ.Prof. Dr.phil. Alexander Leitsch

Problem Description

The sequent calculus proofs transformed by the CERES (Cut-Elimination by Resolution) method tend to be huge. The characteristic clause set and its resolution refutation extracted during the process gives insight into the way the lemmas were used. Its size is considerably smaller but still contains lots of inferences over a fixed background theory. The goal of the thesis was the formulation of CERES for deduction modulo, in which the sequent calculus allows reasoning modulo an equational theory. In particular we were interested in the theory modulo associativity and commutativity with a unit element.

Cut-Elimination by Resolution

What is cut-elimination?

Gentzen's Hauptsatz showed that the cut rule in sequent calculus is admissible. From this the completeness of sequent calculus (and thus of first order predicate logic) follows. Also Craig's interpolation theorem and Herbrand's theorem are closely related to it.

What is its relation to analysis of mathematical proofs?

The cut formulas of a proof correspond to the lemmas being used during the mathematical argument. Of all the rules in sequent calculus it is the only one which is not analytical - this means that the cut formula does not appear in the conclusion of the rule. Also the inferences contributing to the cut are separated in the subproof above the cut. In a cut-free proof the interaction of these parts with the rest of the proof is made explicit which helps in the analysis of the proof.

Why CERES?

The CERES method does not work locally like reductive cut-elimination and thus has a lower computational complexity. Additionally, the characteristic clause set extracted is a shorter characterization of the derivations of the cut formulas.

How does it work?

- Skolemize the proof
  We remove the strong quantifiers going into the end-sequent since they are exactly those quantifiers introduced by rules with an eigenvariable condition. Since we later add formulas to the sequents of the proof, we need no special treatment of eigenvariables.
- Calculate the characteristic clause set
  We trace the ancestors of the cut formulas to their respective axiom introduction rules and inductively build the characteristic clause set from them. Unary rules do not change the characteristic clause set. If a binary rule applies to ancestors of a cut formula, the two clause sets are combined via set union(⊕); if it works on non-ancestors of a cut formula, the two clause sets are merged(⊗).
- Find a (ground) resolution refutation of the characteristic clause set
- Project the proof to the clauses in the characteristic clause set
  We prove the end-sequent with an additional clause from the characteristic clause set by starting from the axioms introducing the clause and repeating those parts of the proof relevant to this clause only.
- Repeat the resolution refutation with the projections
  Now we can replay the resolution proof with the projections by simulating a resolution step with a cut over an atomic formula. In the end every clause will be removed with a proof of the end-sequent with only atomic cuts remaining. This usually suffices for most applications; also atomic cuts are easier eliminated than cuts over arbitrary formulas.

Deduction Modulo

Deduction modulo provides a resolution, a natural deduction and a sequent calculus modulo a background theory which consists of a set of equations and rewriting rules on terms and also ones from propositional to arbitrary formulas.

Extended Narrowing and Resolution

Resolution

$$\frac{\{P_1,\ldots,P_n,Q_1,\ldots,Q_m\}[\mathscr{C}_1] \qquad \{\neg R_1,\ldots,\neg R_p,S_1,\ldots,S_q\}[\mathscr{C}_2]}{\{Q_1,\ldots,Q_m,S_1,\ldots,S_q\}[\mathscr{C}_1 \cup \mathscr{C}_2 \cup \{P_1 \equiv_{\mathcal{E}} \ldots \equiv_{\mathcal{E}} P_n \equiv_{\mathcal{E}} S_1 \equiv_{\mathcal{E}} \ldots \equiv_{\mathcal{E}} S_q\}]}$$

Extended Narrowing

$$\frac{U[\mathscr{C}]}{U'[\mathscr{C} \cup \{U|_\omega \equiv_{\mathcal{E}} l\}]} \text{ if } l \longrightarrow r \in \mathcal{R},\ U|_\omega \text{ atomic proposition and } U' \in cl(\{U[r$$

Since we only look at equalities on terms, the extended narrowing rule will never be applied. The extended resolution rule still needs an efficient way to unify sets of clauses for which we chose a semantic unification procedure. The equational theory may be of finitary or even infinitary unification type, which means there is more than one possible substitution allowing an inference. This is usually handled by backtracking and lazy unification approaches.

Associative Commutative Unification

The main observation of ACU unification is that only the number of terms matter, not their position or nesting within parentheses. So for each unification problem $\{s_1 \overset{?}{=} t_1\ ,\ \ldots\ ,\ s_n \overset{?}{=} t_n\}$ we can find a set of linear diophantine equations whose basis finitely describes the unifiers in the elementary case. In the general case, terms are generalized by variables to reduce to elementary unification, but during the reinsertion of the terms some solutions may not describe a unifier anymore.

Sequent Calculus modulo

$$\frac{\Gamma_1, P \vdash_{\mathcal{RE}} \Delta_1 \qquad \Gamma_2 \vdash_{\mathcal{RE}} Q, \Delta_2}{\Gamma_1, \Gamma_2 \vdash_{\mathcal{RE}} \Delta_1, \Delta_2}\,\text{cut}$$

cut $(P \equiv_{\mathcal{RE}} Q)$

$$\frac{}{P \vdash_{\mathcal{RE}} Q} \qquad\qquad \frac{}{R \vdash_{\mathcal{RE}}}\,\bot,l$$

axiom introduction $(P \equiv_{\mathcal{RE}} Q)$ bottom introduction $(R \equiv_{\mathcal{RE}} \bot)$

$$c,l\,\frac{\Gamma, Q_1, Q_2 \vdash_{\mathcal{RE}} \Delta}{\Gamma, P \vdash_{\mathcal{RE}} \Delta} \qquad\qquad \frac{\Gamma \vdash_{\mathcal{RE}} Q_1, Q_2 \Delta}{\Gamma \vdash_{\mathcal{RE}} P, \Delta}\,c,r$$

contraction $(P \equiv_{\mathcal{RE}} Q_1 \equiv_{\mathcal{RE}} Q_2)$

$$w,l\,\frac{\Gamma \vdash_{\mathcal{RE}} \Delta}{\Gamma, P \vdash_{\mathcal{RE}} \Delta} \qquad\qquad \frac{\Gamma \vdash_{\mathcal{RE}} \Delta}{\Gamma \vdash_{\mathcal{RE}} P, \Delta}\,w,r$$

weakening

$$\wedge,l\,\frac{\Gamma, P, Q \vdash_{\mathcal{RE}} \Delta}{\Gamma, R \vdash_{\mathcal{RE}} \Delta} \qquad\qquad \frac{\Gamma_1 \vdash_{\mathcal{RE}} P, \Delta_1 \qquad \Gamma_2 \vdash_{\mathcal{RE}} Q, \Delta_2}{\Gamma_1, \Gamma_2 \vdash_{\mathcal{RE}} R, \Delta_1, \Delta_2}\,\wedge,r$$

conjunction $(R \equiv_{\mathcal{RE}} P \wedge Q)$

$$\vee,l\,\frac{\Gamma_1, P \vdash_{\mathcal{RE}} \Delta_1 \qquad \Gamma_2, Q \vdash_{\mathcal{RE}} \Delta_2}{\Gamma_1, \Gamma_2, R \vdash_{\mathcal{RE}} \Delta_1, \Delta_2} \qquad\qquad \frac{\Gamma \vdash_{\mathcal{RE}} P, Q, \Delta}{\Gamma \vdash_{\mathcal{RE}} R, \Delta}\,\vee,r$$

disjunction $(R \equiv_{\mathcal{RE}} P \vee Q)$

$$\Rightarrow,l\,\frac{\Gamma_1 \vdash_{\mathcal{RE}} P, \Delta_1 \qquad \Gamma_2, Q \vdash_{\mathcal{RE}} \Delta_2}{\Gamma_1, \Gamma_2, R \vdash_{\mathcal{RE}} \Delta_1, \Delta_2} \qquad\qquad \frac{\Gamma, P \vdash_{\mathcal{RE}} Q, \Delta}{\Gamma \vdash_{\mathcal{RE}} R, \Delta}\,\Rightarrow,r$$

implication $(R \equiv_{\mathcal{RE}} P \Rightarrow Q)$

$$\frac{\Gamma \vdash_{\mathcal{RE}} P, \Delta}{\Gamma, R \vdash_{\mathcal{RE}} \Delta}\,\neg,r \qquad\qquad \frac{\Gamma, P \vdash_{\mathcal{RE}} \Delta}{\Gamma \vdash_{\mathcal{RE}} R, \Delta}\,\neg,r$$

negation $(R \equiv_{\mathcal{RE}} \neg P)$

$$\forall,l\,\frac{\Gamma, \{t/x\}Q \vdash_{\mathcal{RE}} \Delta}{\Gamma, P \vdash_{\mathcal{RE}} \Delta} \qquad\qquad \forall,r\,\frac{\Gamma \vdash_{\mathcal{RE}} \{v/x\}Q, \Delta}{\Gamma \vdash_{\mathcal{RE}} P, \Delta}$$

universal quantification $(P \equiv_{\mathcal{RE}} \forall x\ Q$ and v is a fresh free variable)

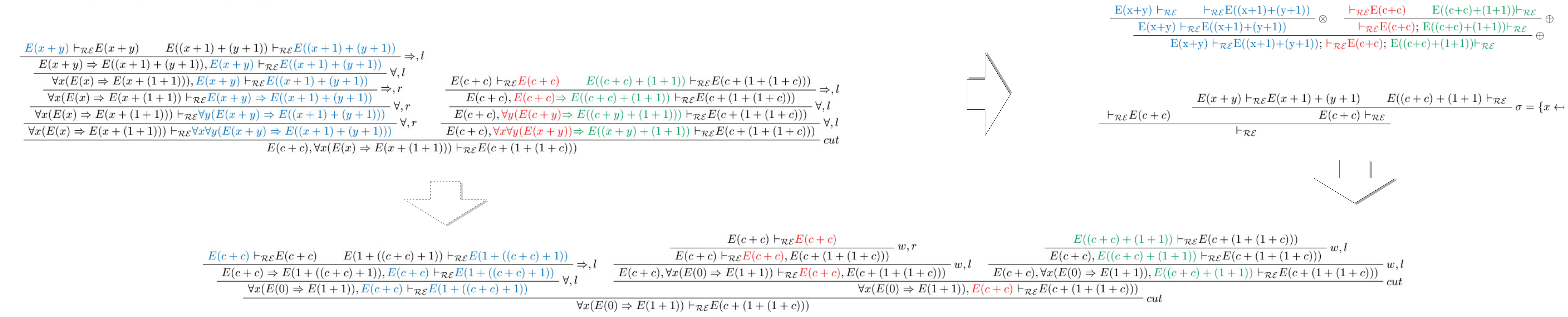
$$\exists,l\,\frac{\Gamma, \{v/x\}Q \vdash_{\mathcal{RE}} \Delta}{\Gamma, P \vdash_{\mathcal{RE}} \Delta} \qquad\qquad \exists,r\,\frac{\Gamma \vdash_{\mathcal{RE}} \{t/x\}Q, \Delta}{\Gamma \vdash_{\mathcal{RE}} P, \Delta}$$

existential quantification $(P \equiv_{\mathcal{RE}} \exists x\ Q$ and v is a fresh free variable)

CERES modulo equational theories

CERES was successfully proven to be applicable to a sequent calculus with integrated equational theories. We give here a small example in the theory of associative-commutative monoids of how it works:

cut formula: $\forall x \forall y(E(x+y) \Rightarrow E((x+1)+(y+1)))$



$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{E(x+y) \vdash_{\mathcal{RE}} E(x+y) \qquad E((x+1)+(y+1)) \vdash_{\mathcal{RE}} E((x+1)+(y+1))}{E(x+y) \Rightarrow E((x+1)+(y+1)), E(x+y) \vdash_{\mathcal{RE}} E((x+1)+(y+1))}\Rightarrow,l}{\forall x(E(x) \Rightarrow E(x+(1+1))), E(x+y) \vdash_{\mathcal{RE}} E((x+1)+(y+1))}\forall,l}{\forall x(E(x) \Rightarrow E(x+(1+1)) \vdash_{\mathcal{RE}} E(x+y) \Rightarrow E((x+1)+(y+1))}\Rightarrow,r}{\forall x(E(x) \Rightarrow E(x+(1+1))) \vdash_{\mathcal{RE}} \forall y(E(x+y) \Rightarrow E((x+1)+(y+1)))}\forall,r}{\forall x(E(x) \Rightarrow E(x+(1+1))) \vdash_{\mathcal{RE}} \forall x \forall y(E(x+y) \Rightarrow E((x+1)+(y+1)))}\forall,r \qquad \dfrac{\dfrac{\dfrac{E(c+c) \vdash_{\mathcal{RE}} E(c+c) \qquad E((c+c)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}{E(c+c), E(c+c) \Rightarrow E((c+c)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\Rightarrow,l}{E(c+c), \forall y(E(c+y) \Rightarrow E((c+y)+(1+1))) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\forall,l}{E(c+c), \forall x \forall y(E(x+y)) \Rightarrow E((x+y)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\forall,l}{E(c+c), \forall x(E(x) \Rightarrow E(x+(1+1))) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\,cut$$

$$\dfrac{\dfrac{\mathrm{E(x+y)} \vdash_{\mathcal{RE}} \qquad \vdash_{\mathcal{RE}} \mathrm{E((x+1)+(y+1))}}{\mathrm{E(x+y)} \vdash_{\mathcal{RE}} \mathrm{E((x+1)+(y+1))}}\otimes \qquad \dfrac{\vdash_{\mathcal{RE}} \mathrm{E(c+c)} \qquad \mathrm{E((c+c)+(1+1))} \vdash_{\mathcal{RE}}}{\vdash_{\mathcal{RE}} \mathrm{E(c+c)};\ \mathrm{E((c+c)+(1+1))} \vdash_{\mathcal{RE}}}\oplus}{\mathrm{E(x+y)} \vdash_{\mathcal{RE}} \mathrm{E((x+1)+(y+1))};\ \vdash_{\mathcal{RE}} \mathrm{E(c+c)};\ \mathrm{E((c+c)+(1+1))} \vdash_{\mathcal{RE}}}\oplus$$

$$\dfrac{\vdash_{\mathcal{RE}} E(c+c) \qquad \dfrac{E(x+y) \vdash_{\mathcal{RE}} E(x+1)+(y+1) \qquad E((c+c)+(1+1) \vdash_{\mathcal{RE}}}{E(c+c) \vdash_{\mathcal{RE}}}\,\sigma = \{x \mapsfrom 0; y \mapsfrom c+c\}}{\vdash_{\mathcal{RE}}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{E(c+c) \vdash_{\mathcal{RE}} E(c+c) \qquad E(1+((c+c)+1)) \vdash_{\mathcal{RE}} E(1+((c+c)+1))}{E(c+c) \Rightarrow E(1+((c+c)+1)), E(c+c) \vdash_{\mathcal{RE}} E(1+((c+c)+1))}\Rightarrow,l}{\forall x(E(0) \Rightarrow E(1+1)), E(c+c) \vdash_{\mathcal{RE}} E(1+((c+c)+1))}\forall,l \qquad \dfrac{\dfrac{\dfrac{E(c+c) \vdash_{\mathcal{RE}} E(c+c)}{E(c+c) \vdash_{\mathcal{RE}} E(c+c), E(c+(1+(1+c)))}w,r}{E(c+c), \forall x(E(0) \Rightarrow E(1+1)) \vdash_{\mathcal{RE}} E(c+c), E(c+(1+(1+c)))}w,l \qquad \dfrac{\dfrac{E((c+c)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}{E(c+c), E((c+c)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}w,l}{E(c+c), \forall x(E(0) \Rightarrow E(1+1)), E((c+c)+(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}w,l}{\forall x(E(0) \Rightarrow E(1+1)), E(c+c) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\,cut}{\forall x(E(0) \Rightarrow E(1+1)) \vdash_{\mathcal{RE}} E(c+(1+(1+c)))}\,cut$$

The original proof that $2c+2$ is an even number (top left) uses the lemma that for all x, y if $x+y$ is even, then also $x+y+2$ is even. We now calculate the characteristic clause set, its resolution refutation (both top right) and the proof projections. To make the corresponding parts better visible, subformulas of the same clause of the characteristic clause set have the same color (blue, red and green). From the ground refutation and the projections we construct a cut-free proof in atomic-cut normal form (bottom).

Contact: riener@logic.at