Proof search in cut-elimination

Daniel Weller

February 28, 2011

Motivation

- Apply cut-elimination to concrete (mathematical) proofs.
- Remove unwanted Lemmas.
- Find analytic kernels of synthetic proofs.

Cut-elimination

- Syntactic methods.
- Semantic methods.

Syntactic cut-elimination

Theorem

Let π be a proof of S. Then there exists a cut-free proof of S.

Proof.

By giving a set of rewrite rules that rewrites proofs with cuts, and giving a terminating strategy. □

Semantic cut-elimination

Theorem

Let S be a valid sequent. Then there exists a cut-free proof of S.

Proof.

By an indirect argument: if cut-free proof search fails, we can construct a counter-model for S. □

Syntactic vs. semantic

Syntactic	**Semantic**
$+$ Direct (sometimes non-deterministic) construction.	- Uses search.
- Space of reachable proofs limited.	$+$ All possible proofs reachable.
- Unsuitable for user-guidance.	$+$ User can guide proof search.

User interaction

- During proof search, a user can
  - *introduce* Lemmas.
  - be an oracle for non-deterministic choices.

Proof search in cut-elimination

- In this talk, we consider how to improve the semantic approach in this context.
- In particular, we want to see how information from a proof with cuts can be used to simplify proof search.

Outline

Outline

Cut-elimination by resolution

- First implementation of this idea: CERES (Baaz, Leitsch 2000).
- Cut-elimination method for classical first-order logic.
- Rough overview:
  1. Assign to a proof π of S a set of clauses $\mathrm{CL}(\pi)$.
  2. From a resolution refutation of $\mathrm{CL}(\pi)$, construct a cut-free proof of S.

Cut-elimination by resolution

- Two main data structures:
  1. *Characteristic clause set* $\mathrm{CL}(\pi)$: a set of clauses.
  2. *Proof projections* $\mathrm{Proj}(\pi)$: a set of cut-free proofs.

Proposition

$\mathrm{CL}(\pi)$ *is unsatisfiable.*

CERES vs. Gentzen

Theorem (Speed-up (Baaz, Leitsch 2000))

There exists a sequence of **LK***-proofs* $(\psi_n)_{n\in\mathbb{N}}$ *with the following properties:*

1. *The Gentzen method produces proof trees with* $> \frac{s(n)}{2}$ *nodes on (input)* ψ_n*, where* s *is defined as* $s(0) = 1$ *and* $s(n+1) = 2^{s(n)}$ *for* $n \in \mathbb{N}$*.*
2. *CERES constructs a cut-free proof out of* ψ_n *in* $\leqslant c2^{dn}$ *steps, where* c *and* d *are constants independent of* n*.*

CERES vs. Gentzen

Theorem (Simulation (Baaz, Leitsch 2006))

Let φ be an **LK***-derivation and ψ be an ACNF of φ under a cut reduction relation $>_{\mathcal{R}}$ based on $\mathcal{R}$. Then there exists an ACNF χ of φ under CERES s.t.*

$$l(\chi) \leqslant l(\varphi) * l(\psi) * 2^{2*l(\psi)} + 2$$

Fast cut-elimination

- Non-elementary blow-up only due to size of refutations γ of $\mathrm{CL}(\pi)$.
- Hence: fast proof search for $\mathrm{CL}(\pi) \rightsquigarrow$ fast cut-elimination for π.

Fast cut-elimination

- For cut-free proofs: There exist constant-size γ.
- For proofs with only propositional cuts: There exist propositonal γ.
- Further classes are studied in (Baaz, Leitsch 2010)

Refinements of CERES

- The CERES method for first-order logic has been refined:
- By improving the construction of $\mathrm{CL}(\pi)$.
- By defining formal resolution refinements.

The proof profile

- The *proof profile* $\mathrm{P}^{\Omega}(\pi)$ (Hetzl 2007).

Proposition (Hetzl 2007)

Let φ *be an* **LK**-*proof. Then* $\mathrm{P}^{\Omega}(\varphi)$ *propositionally subsumes* $\mathrm{CL}(\varphi)$.

The proof profile

- Together with a refined notion of proof projection a CERES method can be obtained.
- A non-elementary speed-up over regular CERES is possible.

Resolution refinements

- A common technique in resolution theorem proving:
- Find *resolution refinements* that prune the search space while retaining completeness.
- In (Woltzenlogel Paleo 2009) such refinements are developed.
- Informal idea: Prune parts of the search space that are not reachable by the Gentzen method.

Example (Cut-linkage (Woltzenlogel Paleo 2009))

$$\dfrac{\dfrac{P\alpha \vdash P\alpha}{(\forall x)Px \vdash (\forall x)(\neg Px \supset Px)} \qquad \dfrac{\dfrac{Ps \vdash Ps \quad Ps \vdash Ps}{(\forall x)(\neg Px \supset Px) \vdash Ps} \quad \dfrac{Ps \vdash Ps}{Ps \vdash (\exists y)Py}}{(\forall x)(\neg Px \supset Px) \vdash (\exists y)Py}\, cut}{(\forall x)Px \vdash (\exists y)Py}\, cut$$

Resolution refinements

- Refinements $\mathbf{R_{acl}} \subset \mathbf{R_{scl}} \subset \mathbf{R_{cls}} \subset \mathbf{R_{cl}}$ are given.
- All these refinements lead to a complete CERES method:

Theorem (Completeness, (Woltzenlogel Paleo 2009))

For any proof φ, there exists a $\mathbf{R_{acl}}$-refutation of the swapped clause set $\mathcal{C}^W_{\varphi|S^*}$ of φ with respect to a $\rightsquigarrow_{\oplus\otimes_W}$-normal-form S^* of $\mathbf{S}_\varphi$.

Resolution refinements

- By the informal idea, the most restrictive refinement should "restrict CERES to the Gentzen method".

Conjecture ((Woltzenlogel Paleo 2009))

$\triangleright^{\downarrow}_{\tilde{a}}$ CR-simulates CERes^{O}_{W} with $\mathbf{R}_{\mathbf{acl}}$.

CERES in other logics

- CERES methods have been defined for
  - Many-valued logics (Baaz, Leitsch 2005),
  - first-order Gödel logic (Baaz, Ciabattoni, Fermüller 2008),
  - higher-order classical logic (Weller 2010).

CERES — summary

- Cut-elimination problem for $\pi \rightsquigarrow$ proof search problem for $\mathrm{CL}(\pi)$.
- $\mathrm{CL}(\pi)$ contains information about the cuts in π.
- Definition of $\mathrm{CL}(\pi)$ can be refined by incorporating more information.
- CERES method can be refined by restricting proof search using information from π.
- Usually: Simulates Gentzen's method, has speed-up over it.

CERES — summary

- The CERES method generates nice normal forms:
- The ACNF is obtained by attaching projections (i.e. cut-free "subproofs" of π) to the leaves of a refutation of $\mathrm{CL}(\pi)$.

Extending CERES

- But transformations are used that may not be available:
  - Skolemization,
  - Clause normal form.
- Is it possible to come up with a CERES-like method that does not depend on these normal forms?

Outline

1. Cut-elimination by resolution

2. Cut-elimination by proof search

Extending CERES

- First step: CERES-like method for classical first-order logic without clause normal form.
- Still, we work with Skolemized proofs (i.e. only weak quantifiers in the end-sequent).

Extending CERES

- Characteristic clause set $\mathrm{CL}(\pi) \rightsquigarrow$ Characteristic formula $\mathrm{CF}(\pi)$
- Resolution refutation of $\mathrm{CL}(\pi) \rightsquigarrow$ **LK**-proof of $\mathrm{CF}(\pi)$

Characteristic formulas

Definition

Let π be a proof of S. A formula F is a *characteristic formula* for π if there exists an elementary function e such that

1. F contains only weak quantifiers, and
2. $|F| \leqslant e(|\pi|)$, and
3. $\vdash F$ is provable, and
4. $(F \vdash) \circ S$ has a cut-free proof ψ such that $|\psi| \leqslant e(|\pi|)$.

Characteristic formulas

- If $S = \Gamma \vdash \Delta$ then $\bigwedge \Gamma \supset \bigvee \Delta$ is a trivial characteristic formula.
- Maybe: F is *good* if the shortest cut-free proof of F is smaller than the shortest cut-free proof of S.

Characteristic formulas

Theorem

Let π be a proof of S, and let F be a characteristic formula for π. Let ψ be a cut-free proof of $\vdash F$. Then there exists a cut-free proof φ of S such that $|\varphi|$ is elementary in $|\pi| * |\psi|$.

Proof.

By the definition of characteristic formula there exists a cut-free proof λ of $(F \vdash) \circ S$ such that $|\lambda| \leqslant e(|\pi|)$. Consider the proof φ':

$$\dfrac{\begin{array}{c}(\psi)\\ \vdash F\end{array} \qquad \begin{array}{c}(\lambda)\\ (F \vdash) \circ S\end{array}}{S}\ \mathit{cut}$$

Then φ' contains only the indicated cut. By definition F contains only weak quantifiers. φ can be obtained from φ' by cut-elimination with elementary blow-up (Hetzl 2010). □

Characteristic formulas

Theorem

Let π be a proof. Then there exists a characteristic formula for π.

Proof.

Let S be the end-sequent of π. Consider the following proof transformation on π: For inferences ρ operating on cut-formulas of π,

1. if ρ is a quantifier inference, omit it,
2. if ρ is a contr_l (contr_r) inference, replace it by $\wedge_l$ ($\vee_r$),
3. if ρ is a cut, replace it by $\supset_l$,
4. if ρ is a propositional inference, apply it.

This yields a cut-free proof of $(F_1, \ldots, F_n \vdash) \circ S$, where $F_1, \ldots, F_n$ are quantifier-free. Append $\wedge_l, \exists_l$ inferences to this proof to obtain a proof of $(\exists \bar{x} F \vdash) \circ S$, with F quantifier-free, where $\bar{x}$ are the free variables of F. It is easy to show, by induction on the construction, that $\vdash \exists \bar{x} F$ is provable. Hence $\exists \bar{x} F$ is a characteristic formula for π. $\square$

Characteristic formulas

- This algorithm often produces good characteristic formulas.
- In fact,

Conjecture

Any refutation for $\mathrm{CL}(\pi)$ gives rise to a proof of $\mathrm{CF}(\pi)$, and vice-versa.

Characteristic formulas

- We have found a CERES-like method for classical logic without CNF.
- It seems to simulate and speed-up the Gentzen method like CERES.
- Disadvantages:
  - It does not (directly) produce an ACNF, and
  - it relies on a restricted form of cut-elimination.
- Can we use this for intuitionistic logic?

Elementary cut-elimination

- To do so, we will use

Lemma

Let π be an **LJ***-proof of the form*

$$\dfrac{\begin{matrix}(\pi_1) \\ \vdash C\end{matrix} \qquad \begin{matrix}(\pi_2) \\ C, \Gamma \vdash \Delta\end{matrix}}{\Gamma \vdash \Delta}\ cut$$

such that $\Gamma \vdash \Delta$ does not contain strong quantifiers, C contains only weak quantifiers, and π_1, π_2 are cut-free. Then there exists a cut-free **LJ***-proof ψ of $\Gamma \vdash \Delta$ such that $|\psi|$ is elementary in $|\pi|$.*

Proof.

By doing an $\wedge\vee$-expansion of C, and extending the results of (Hudelmaier 1992) on propositional **LJ** to our setting. □

Unsuitability of the classical algorithm

- From this result, it follows immediatly that

Proposition

It is not the case that for all **LJ***-proofs there exists a characteristic formula* $\exists \bar{x} M$ *with* M *quantifier-free.*

- Hence we cannot directly use the previous construction.

A restricted class

Definition

We say that π *ends in a prenex closed cut chain* if there exist $n \geqslant 0$ and cut-free proofs $\psi_1, \ldots, \psi_n$ and closed prenex formulas $C_1, \ldots, C_{n-1}$ such that π is

$$
\dfrac{\dfrac{\dfrac{\overset{(\psi_1)}{\Gamma_1 \vdash C_1} \quad \overset{(\psi_2)}{C_1, \Gamma_2 \vdash C_2}}{\Gamma_1, \Gamma_2 \vdash C_2}\, cut}{\vdots}}{}
$$

$$
\dfrac{\Gamma_1, \ldots, \Gamma_{n-1} \vdash C_{n-1} \qquad \overset{(\psi_n)}{C_{n-1}, \Gamma_n \vdash \Lambda}}{\Gamma_1, \ldots, \Gamma_n \vdash \Lambda}\, cut
$$

and $\Gamma_1, \ldots, \Gamma_n, \Lambda$ do not contain strong quantifiers.

A partial result

Proposition

Let π be a **LJ**-*proof that ends in a prenex closed cut chain. Then there exists a characteristic formula for π.*

Proof.

The construction is again based on $\wedge\vee$-expansion of the cut-formulas. The expansions are then combined in a more involved way, putting quantifiers infix. $\square$

The extension is non-trivial

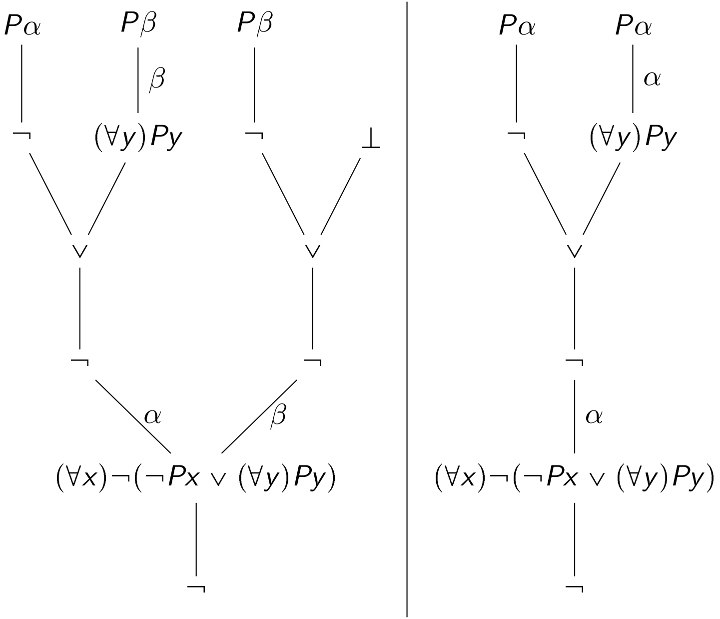
- In (Baaz, Leitsch 1999) a certain sequence of **LJ**-proofs (ψ_n) that end in prenex closed cut chains is used.
- For ψ_n, the classical algorithm yields a characteristic formula which is not intuitionistically valid!

Skolemization

- Like in the CERES method, we still use Skolemization.
- This is “due to” the fact that Skolemized proofs are more flexible:
- The eigenvariable condition is too strong a restriction.

Skolemization

- CERES in higher-order logic uses a sequent calculus with "less" eigenvariable conditions.
- Instead, it requires a global soundness condition.
- This is not new; e.g. expansion tree proofs (Miller 1983).


Pα
Pβ
Pβ
β
¬
(∀y)Py
¬
⊥
∨
∨
¬
¬
α
β
(∀x)¬(¬Px ∨ (∀y)Py)
¬
Pα
Pα
α
¬
(∀y)Py
∨
¬
α
(∀x)¬(¬Px ∨ (∀y)Py)
¬

Sequent calculi without eigenvariable conditions

- Skolemization can be regarded as the syntax-level encoding of this dependency relation.
- Acyclicity is guaranteed since terms cannot properly contain themselves.
- In intuitionistic logic, acyclicity does not suffice for soundness.
- Maybe it is possible to strengthen the condition to find a system for intuitionistic logic?

Sequent calculi without eigenvariable conditions

$$\dfrac{\dfrac{\dfrac{A\alpha \vdash A\alpha}{A\alpha \vdash (\forall x)Ax}\ \forall_r}{A\alpha \vdash (\forall x)Ax \lor B}\ \lor_r^1 \qquad \dfrac{B \vdash B}{B \vdash (\forall x)Ax \lor B}\ \lor_r^2}{\dfrac{A\alpha \lor B \vdash (\forall x)Ax \lor B}{(\forall x)(Ax \lor B) \vdash (\forall x)Ax \lor B}\ \forall_l}\ \lor_l$$

- Sound in classical logic, but not in intuitionistic logic.
- Forbid use of eigenvariable in instantiation according to propositional structure.

Dealing with Skolemization in **LJ**

- Develop/Use such a calculus for intuitionistic logic.
- Or: Use Skolemization for intuitionistic logic as developed in (Baaz, Iemhoff 2006 and 2008).
- Or: Use resolution calculus avoiding Skolemization (Mints 1981).

Conclusion

- Proof search is more flexible than syntactic cut-elimination.
- Used naively, it disregards much information from π.
- CERES
  - provides a way to use information from π during proof search and
  - allows application of results from proof search to cut-elimination.
- Extension to other logics is challenging.