Complete Inference Rules for the Cancellation Laws

—Extended Abstract—

Jieh Hsiang
Department of Computer Science
SUNY at Stony Brook
Stony Brook, NY 11794
U.S.A.

Michael Rusinowitch
CRIN
B.P. 239
54506 Vandoeuvre-les-Nancy
France

Ko Sakai
ICOT
Mita Kokusai Bldg, 2IF
1-4-28 Mita, Minato-ku
108 Tokyo, Japan

1. Introduction

In many cases, specialiied inference rules which incorporate certain axioms into the inference mechanism can produce fewer redundant consequences and more efficient proofs. The most notable example is *paramodulation.* Inference rules for inequalities, partial orerings, special binary relations have also been found ([BIH80], [S1N73], [MaW85]). Recently there has also been considerable interests in inference rules for the *cancellation law.* Stickel ((Sti84j) used it, with the Knuth-Bendix method, to prove that $x^3=x$ implies *xy =yx* in ring theory. [W0M86] introduced an inference rule called *negative paramodulation* to find useful consequences resulting from cancellation. However, these methods provide only *ad hoc* treatments of cancellation. These inference rules are not complete and cannot eliminate the cancellation axiom from the input set of clauses. In this paper we present some complete sets of inference rules, which can replace the cancellation axioms. Due to space limitation, we only outline the inference rules and state the main theorem without proofs. Only simple examples are given to illustrate how the rules are used. The proof and more examples will be given in the full paper.

2. Inference Rules for Cancellation Laws

We present inference rules for three types of cancellation laws, the basic cancellation, cancellation with identity, and cancellation except the null element.

2.1. Right Cancellation

A function / is *right cancellable* if it satisfies the *right cancellation law* $\forall x,y,z\,(f(y,x)=f(z,x)\supset y=z)$. For convenience we only consider right cancellation. Left cancellation is handled symmetrically. Although cancellation has only one axiom, it may lead to many resolvents and paramodulants in a resolution based theorem prover if simply treated as a clause. Replacing it with inference rules ensures that only those "relevant" ones are generated and kept. In the following we give a "rough-cut" version of the inference rules. A more efficient version involving *simplification orderings* is given later. We say two lists $(s_1,\ \cdots,s_n)$ and $(t_1,\ \cdots,t_n)$ **are unifiable with mgu** σ, **denoted** $(s_1,\ \cdots,s_n)\sigma=(t_1,\ \cdots,t_n)\sigma$, **if** σ **is the most general** unifier such that s, a=f$_t$ *a* for all 1.

$$\textbf{C1}\qquad \frac{(s=t)\vee C}{(y=z)\sigma\vee C\sigma}$$

where $(s,t)\sigma=(f(y,x),f(z,x))\sigma$

$$\textbf{C2}\qquad \frac{(s=t)\vee C,\ \ (l=r)\vee D}{(y=z)\sigma\vee C\sigma\vee D\sigma}$$

where $(s,t,l,r)\sigma=(f(y,x),u,f(z,x),u)\sigma$

The soundness of the rules is quite immediate. These two inference rules, with resolution and paramodulation, form a complete theorem proving strategy for first order predicate calculus with equality when some operators are right cancellable. The only extra axiom needed is reflexivity, $x=x$.

Here is a simple example. Given two clauses $c\,1$: $(b+y)+a=y$, **and** $c\,2$: $b+(a+a)\neq a$, **where + is right cancellable. The *only* inference applicable is rule C1 on clause c1, producing** $c\,3$: $b+(z+a)=z$. **Using resolution on** $c\,3$ **and** $c\,2$**, the contradiction is achieved.**

2.2. Cancellation with Identity

Similar inference rules can be designed for other types of cancellation laws. For example, in an algebraic theory with an identity *t* for an operator /, there is the *cancellation law with identity:* $\forall xy\,(f(y,x)=x\supset y=e)$. Although this law is a consequence of right cancellation and left identity, it may also be given as an independent axiom without the other two. The operator + in ring theory satisfies this law, and Stickel ([Sti84j) has demonstrated the power of incorporating this axiom intoinference rules.

With this axiom, we modify rule CI into:

$$\textbf{CI1}\qquad \frac{(s=t)\vee C}{\sigma(y)=e\vee C\sigma}$$

where $(s,t)\sigma=(f(y,x),x)\sigma$

It is interesting to note that this inference rule alone suffices to secure completeness, i.e., resolution and paramodulation, with CII for each operator satisfying this axiom, form a complete strategy for first order logic with equality when some operators are right cancellable with identity.

The rule C2 can also be modified into a rule

$$\textbf{CI2}\qquad \frac{(s=t)\vee C,\ \ (l=r)\vee D}{(y=e)\sigma\vee C\sigma\vee D\sigma}$$

where $(s,t,l,r)\sigma=(f(y,x),u,x,u)\sigma$

However, it is only needed for perhaps improving the efficiency, but not for completeness.

2.3. Cancellation Except the Null Element

In many richer algebraic theories, such as integral domains and field theory, the cancellation law holds for all elements except for the null element. Let f be such an operator and 0 its null element (i.e., $f(0,x)=0$ for all x), the law of *cancellation except the null element* is $\forall xyz\,(x\neq 0 \wedge f(y,x)=f(z,x) \supset y=z)$. By modifying the inference rules for basic cancellation to accommodate the $x\neq 0$ requirement, we obtain the following complete set of inference rules:

$$\textbf{CN1}\qquad \frac{(s=t)\vee C}{(y=z)\sigma\vee C\sigma\vee(z=0)\sigma}$$

where $(s,t)\sigma=(f(y,x),f(z,x))\sigma$

$$\textbf{CN2}\qquad \frac{(s=t)\vee C,\quad (l=r)\vee D}{(y=z)\sigma\vee C\sigma\vee D\sigma\vee(z=0)\sigma}$$

where $(s,t,l,r)\sigma=(f(y,x),u,f(z,x),u)\sigma$

As a simple example, we show that a commutative ring is an integral domain if $*$ is right cancellable except the null element. In other words, we want to prove that $\forall xy\,(x*y=0\supset x=0\vee y=0)$. After skolemizing the goal we have, as (part of the) inputs,

$c\,1$: $0*x=0$ $\quad$ $c\,2$: $a*b=0$
$c\,3$: $a\neq 0$ $\quad$ $c\,4$: $b\neq 0$

By applying $CN\,2$ on $c\,1$ and $c\,2$, we get $a=0\vee b=0$ which, with $c\,3$ and $c\,4$, immediately leads to the contradiction.

3. Inference Rules with Ground-Linear Simplification Orderings

The inference rules introduced in the above section can be improved substantially (with completeness preserved) and with more powerful equational inference rules such as *oriented paramodulatton* and *demodulation,* if a notion of *simplification orderings* ([Der82]) on the term structure is introduced.

Let *T(F* , X) be the set of terms and $A(P,F,X)$ be the set of atoms in the language. Also let *T (F*) be the set of ground terms *(Herbrand universe)* and $A(P,F)$l the *Herbrand base.* We also consider s — *t* and *t* — s as the same atom. An ordering $<$ on $T(F,X)\cup A(P,F,X)$ is a *simplification ordering* if it is a partial ordering which preserves the *substitution* property, is *monotonic* (if *t* <*s* t h $w[t]<w[s]$), d has the *subterm* property (any superterm of a term is larger than the term itself). A simplification ordering is a *ground-linear simplification ordering* if it is also total on $T(F)\cup A(P,F)$. The most important property of these orderings is that *they are well-founded.*

Variations of simplification orderings have appeared in [Der82], [Pla78], [Pet83], A comprehensive discussion is in [Der85]. A more detailed description of the version presented here is in [HsR86].

3.1. Inference Systems and Completeness

Ground-linear simplification orderings are used to compare literals within a clause, and to compare terms within an equational atom. Intuitively, they restrict inferences to be performed only on the larger items in the data. We first describe the second aspect, comparing terms.

If one side of an equation is bigger than the other, then an equation can be used as a *rule.* Only the left hand side of a rule can be considered for equational replacements. This includes both *reduction* and *paramodulation.* Let $s=t$ be an equation and $C[r]$ be a clause containing r as a subterm. $C[r]$ is *reducible using* $s=t$ if there is a unifier σ such that $s\sigma=r$ and $s\sigma>t\sigma$. We also say $s=t$ *reduces* $C[r]$ *to* $C[t\sigma]$. Note that if $s=t$ is oriented as a rule $s\rightarrow t$, which implies that $s>t$, then the condition $s\sigma>t\sigma$ is automatically satisfied. With this notion of reduction, we have the *reduction inference rule.*

$$\textbf{S1}\qquad \frac{C[r]\ \textit{is reduced to}\ C[t\sigma]\ \textit{by}\ s=t}{\textit{replace}\ C[r]\ \textit{by}\ C[t\sigma]}$$

Although the reduction rule is similar to *demodulation* ([WRC67|), there are some subtle differences. Reductions are based on a *well-founded* ordering, while demodulation may not be. Each reduction step reduces a clause to a "smaller" one. Reductions can be applied whenever applicable, as much as possible, without the risk of falling into an infinite loop.

Paramodulation can utilize this ordering on terms and be improved to the *oriented paramodulation inference rule:*

$$\textbf{SP}\qquad \frac{s=t\vee C,\ D[r]}{C\sigma\vee D[t]\sigma}$$

where $s\sigma=r\sigma$, $s\sigma\not< t\sigma$, *and* $(s=t)\sigma\not< L\sigma\,\forall L\in C$

where r is a non-variable subterm of *D* . Oriented paramodulation is different from paramodulation in the restriction of $s\sigma\not< t\sigma$ and that $s=t$ is not smaller than any other literal in *C*. This eliminates many potential paramodulants.

Using the ground-linear simplification ordering to compare literals within a clause also restricts the cancellation inference rules to be performed only on the literals among the largest in a clause. The rules *C* 1 and *C* 2 become:

$$\textbf{SC1}\qquad \frac{(s=t)\vee C}{(y=z)\sigma\vee C\sigma}$$

where $(s,t)\sigma=(f(y,x),f(z,x))\sigma$, $(s=t)\sigma\not< L\sigma\,\forall L\in C$

$$\textbf{SC2}\qquad \frac{(s_1=t_1)\vee C_1,\quad (s_2=t_2)\vee C_2}{(y=z)\sigma\vee C_1\sigma\vee C_2\sigma}$$

where $(s_1,t_1,s_2,t_2)\sigma=(f(y,x),u,f(z,x),u)\sigma$,
and $(s_i=t_i)\sigma\not< L\sigma\,\forall L\in C_i$

It is interesting to note that if a *pre dic ate-first* type ground-linear simplification ordering is used on the term structure (that is, atoms are compared lexicographically first by their predicate symbols, with = as the smallest predicate) then *no cancellation inference need be performed on any clause which contains a non-equality literal,* since all equality literals are smaller than any literal with non-equality predicate.

Even the resolution inference rule can be restricted by the ordering (into *oriented resolution).* For simplicity we give the binary resolution version here.

$$\textbf{SBR}\quad \frac{P_1 \vee C_1,\ \neg P_2 \vee C_2}{C_1\sigma \vee C_2\sigma}$$

$$\text{where } P_1\sigma = P_2\sigma,\ P_i\sigma \not< A\sigma\ \forall A \in C_i$$

Oriented resolution is different from ordered resolution or ordered predicate resolution (see [ChL73]) in that the ordering on literals are given in a natural way. For example, there is no oriented resolvents between clauses $P0$ and $\neg Px \vee Pgx$, because $Px < Pgx$ in *any* ground-linear simplification ordering.

These inference rules yield a complete strategy:

> Theorem Given a set of clauses S, *S* is unsatisfiable with respect to the equational axioms and the right cancellation law if and only if contradiction can be obtained from $S \cup \{x=x\}$ with the inference rules $SC1$–$SC3$, SP, $S1$, SBR, and factoring.

The proof of completeness, which involves a notion of transfinite semantic trees ((HsR86j), and a notion of inductively defined *C*-interpretations which incorporate the equality axioms and the cancellation law, is given in the full paper. The proof technique introduced in [HsR86] also enables us to eliminate the functional reflexive axioms.

The inference rules for the other cancellation axioms can be modified according to the ordering in a similar way. The completeness theorems are also similar.

4. Discussion

We presented several complete sets of inference rules which incorporated the cancellation laws into the inference mechanism. The major advantage of these specialized inference rules is that they may produce fewer redundant consequences and more direct proofs. We have also described ground-linear simplification orderings and how they can be use to improve inference rules in general.

The cancellation inference rules can also be used to speed up the completion process in Knuth-Bendix procedure ([Sti84]). In a prototype implementation these inference rules enable us to find the canonical set for groups after generating 14 critical pairs rather than the usual 17.

In [KnB70j another way of dealing with the basic cancellation axioms, by adding a new function symbol for each cancellable operator, is given. This method can be extended easily to first order theory. The completeness of their method is an easy corollary of our completeness theorem. However, their approach seems to produce more redundant consequences and does not seem to be efficient.

[WoM86] introduced *negative paramodulation* for handling cancellation. This inference rule cannot completely eliminate the cancellation axiom. A simple counterexample is the unsatisfiable set $\{a+c=b+c, h(a)\neq h(b)\}$, where $+$ is right cancellable. Neither negative paramodulation nor paramodulation/resolution is applicable to any of the clauses. However, negative paramodulation is compatible with the cancellation inference rules introduced here, and it provides for *backward chaining.* The inclusion of such an inference rule should further improve the efficiency of a refutational proving system involving the cancellation axioms.

5. References

[B1H80] W. W. Bledsoe and L. M. Hines, "Variable Elimination and Chaining in a Resolution-based Prover for Inequalities", *5th CADE,* 1980, 70-87.

[ChL73] C. L. Chang and C. T. Lee, *Symbolic Logic and Mechanical Theorem Proving,* Academic Press, 1973.

[Der82] N. Dershowitx, "Orderings for Term Rewriting Systems", *J.TCS,* 17, 3 (1982), 279-301.

[Der85j N. Dershowitz, "Termination", *1st RTA,* LNCS 202, May, 1985, 180-224.

[HsR86] J. Hsiang and M. Rusinowitch, "A New Method for Establishing Refutational Completeness in Theorem Proving", *8th CADE,* Oxford, England, 1986, 141-152.

[KnB70] D. E. Knuth and P. B. Bendix, "Simple Word Problems in Universal Algebras", in *Computational Algebra,* J. Leach, (ed.), Pergamon Press, 1970, 263-297.

[MaW85] Z. Manna and R. Waldinger, "Special Relations in Automated Deduction", *12th ICALP,* Nafplion, Greece, July, 1985.

[Pet83] G. E. Peterson, "A Technique for Establishing Completeness Results in Theorem Proving with Equality", *SIAM J. of Computing,* 12, 1 (1983), 82-100.

[Pla78| D. A. Plaisted, "A Recursively Defined Ordering for Proving Termination of Term Rewriting Systems", UIUCDCS-R-78-943, Univ. of Illinois, Urbana, IL, 1978.

[S1N73] J. Slagle and K. Norton, "Experiments with an Automatic Theorem Prover having Partial Ordering Inference Rules", *Comm. ACM,* 1973, 682-688.

[Sti84] M. Stickel, "A Case Study of Theorem Proving by Knuth-Bendix Method Discovering that $x*x*x=x$ Implies Ring Comutativity", *7th CADE,* 1984, 248-258.

[WRC67] L. Wos, G. A. Robinson, D. F. Carson and L. Shalla, "The Concept of Demodulation in Theorem Proving", *J. ACM,* 14, 4 (1967), .

[W0M86] L. Wos and W. McCune, "Negative Paramodulation", *8th CADE,* 1986, 229-239.