A Superposition Calculus for Divisible Torsion-Free Abelian Groups

Uwe Waldmann*

1 Introduction

Variable overlaps (via extended clauses) are one of the main sources for the inefficiency of AC or ACU superposition calculi. In the presence of the inverse axiom $x + (-x) \approx 0$ (Inv), or at least the cancellation axiom $x + y \approx x + z \Rightarrow y \approx z$ (K), ordering restrictions allow us to avoid some of these overlaps, but inferences with unshielded, i.e., potentially maximal, variables remain necessary (Waldmann [2]).

In non-trivial divisible torsion-free abelian groups (e.g., the rational numbers), the axioms ACUInv are extended by the torsion-freeness axiom $\forall k \in \mathbf{N}^{>0}$: $kx \approx ky \Rightarrow x \approx y$ (T), the divisibility axiom $\forall k \in \mathbf{N}^{>0}\ \forall x \exists y$: $ky \approx x$ (Div), and the non-triviality axiom $\exists y$: $y \not\approx 0$ (Nontriv). We show that in such structures every clause can be transformed into an equivalent clause without unshielded variables. This transformation is not necessarily a simplification in the superposition calculus: some ground instances of the transformed clause may be too large. It turns out, however, that all the critical instances can be handled by case analysis.

The resulting calculus requires neither extended clauses, nor variable overlaps, nor explicit inferences with the theory axioms. Furthermore, even AC unifications can be avoided, if abstractions are performed eagerly.

2 Preliminaries

We work in a many-sorted framework and assume that the function symbol $+$ is declared on a sort S_{G}. If t is a term of sort S_{G} and $n \in \mathbf{N}$, then nt is an abbreviation for the n-fold sum $t + \cdots + t$; in particular, $0t = 0$ and $1t = t$.

A function symbol is called free, if it is different from 0 and $+$. A term is called atomic, if it is not a variable and its top symbol is different from $+$. We say that a term t occurs at the top of s, if there is a position $o \in \mathrm{pos}(s)$ such that $s|_o = t$ and for every proper prefix o' of o, $s(o')$ equals $+$; the term t occurs in s below a free function symbol, if there is an $o \in \mathrm{pos}(s)$ such that $s|_o = t$ and $s(o')$ is a free function symbol for some proper prefix o' of o. A variable x is called shielded in a clause C, if it occurs at least once below a free function symbol in C, or if it does not have sort S_{G}. Otherwise, x is called unshielded.

We say that an ACU-compatible ordering has the multiset property, if whenever a ground atomic term u is greater than v_i for every i in a finite index set $I \neq \emptyset$, then $u \succ \sum_{i \in I} v_i$.

*Max-Planck-Institut für Informatik, Im Stadtwald, 66123 Saarbrücken, Germany, uwe@mpi-sb.mpg.de

From now on we will work *only* with ACU-congruence classes, rather than with terms. So *all* terms, equations, substitutions, inference rules, etc., are to be taken modulo ACU, i.e., as representatives of their congruence classes. The symbol $\succ$ will always denote an ACU-compatible ordering that has the multiset property and is total on ground ACU-congruence classes (Waldmann [2]).

Let e be a ground equation $nu + \sum_{i\in I} s_i \approx mu + \sum_{j\in J} t_j$, where u, s_i, and t_j are atomic terms, $n \geq m \geq 0$, $n \geq 1$, and $u \succ s_i$ and $u \succ t_j$ for all $i \in I$, $j \in J$. Then u is called the maximal atomic term of e.

The ordering $\succ_{\mathrm{L}}$ on literals compares lexicographically first the maximal atomic terms of the equations, then the polarities (negative $\succ$ positive), then the multisets of all non-zero terms occurring at the top of the equations, and finally the multisets consisting of the left and right hand sides of the equations. The ordering $\succ_{\mathrm{C}}$ on clauses is the multiset extension of the literal ordering $\succ_{\mathrm{L}}$.

The symbol $\models_{\mathrm{ACUKT}}$ denotes entailment modulo equality and ACUKT. In other words, $\{C_1, \ldots, C_n\} \models_{\mathrm{ACUKT}} C_0$ if and only if $\{C_1, \ldots, C_n\} \cup \mathrm{ACUKT} \models C_0$.

3 Cancellative Superposition

The inference system $\mathit{CS\text{-}Inf}_{\mathbf{N}^{>0}}$ of the cancellative superposition calculus (Waldmann [2]) consists of the inference rules *equality resolution*, *standard superposition*, *standard equality factoring*, *cancellation*, *negative cancellative superposition*, *positive cancellative superposition*, *abstraction*, and *cancellative equality factoring*. The first three rules are defined essentially as in the traditional superposition calculus (Bachmair and Ganzinger [1]), ground versions of the remaining ones are given below.

The following conditions are common to all the inference rules: Every literal involved in some inference must be maximal in the respective premise (except for the last but one literal in *equality factoring* inferences). A positive literal involved in a *superposition* or *abstraction* inference must be strictly maximal in the respective clause. In all *superposition* and *abstraction* inferences, the left premise is smaller than the right premise. *Standard superpositions* and *abstractions* take place only in maximal atomic subterms.

Cancellation

$$\frac{C' \vee [\neg]\, mu + s \approx m'u + s'}{C' \vee [\neg]\, (m - m')u + s \approx s'}$$

if $m \geq m' \geq 1$ and $u \succ s$, $u \succ s'$.

Neg. Canc. Superposition

$$\frac{D' \vee nu + t \approx t' \qquad C' \vee \neg\, mu + s \approx s'}{D' \vee C' \vee \neg\, \psi s + \chi t' \approx \chi t + \psi s'}$$

if $m \geq 1$, $n \geq 1$, $\psi = n/\mathrm{gcd}(m, n)$, $\chi = m/\mathrm{gcd}(m, n)$, and $u \succ s$, $u \succ s'$, $u \succ t$, $u \succ t'$.

Pos. Canc. Superposition

$$\frac{D' \vee nu + t \approx t' \qquad C' \vee mu + s \approx s'}{D' \vee C' \vee (m - n)u + s + t' \approx t + s'}$$

if $m \geq n \geq 1$ and $u \succ s$, $u \succ s'$, $u \succ t$, $u \succ t'$.

Abstraction

$$\frac{D' \vee nu + t \approx t' \qquad C' \vee [\neg]\, s[w] \approx s'}{C' \vee \neg\, y \approx w \vee [\neg]\, s[y] \approx s'}$$

if $n \geq 1$, $w = mu + q$ occurs in s immediately below some free function symbol, $m \geq 1$, $nu + t$ is not a subterm of w, and $u \succ t$, $u \succ t'$, $s[w] \succ s'$.

Canc. Eq. Factoring

$$\frac{C' \vee nu + t \approx n'u + t' \vee mu + s \approx s'}{C' \vee \neg\, \psi t + \chi s' \approx \chi s + \psi t' \vee nu + t \approx n'u + t'}$$

if $m \geq 1$, $n > n' \geq 0$, $\nu = n - n'$, $\psi = m/\gcd(m, \nu)$, $\chi = \nu/\gcd(m, \nu)$, and $u \succ s$, $u \succ s'$, $u \succ t$, $u \succ t'$.

The inference system $\mathit{CS}\text{-}\mathit{Inf}_{\mathbf{N}^{>0}}$ is sound with respect to ACUKT, i.e., for every inference with premises $C_1, \ldots, C_n$ and conclusion C_0, we have $\{C_1, \ldots, C_n\} \models_{\mathrm{ACUKT}} C_0$.

To make a saturation-based theorem proving technique practically useful, the inference system has to be complemented with a redundancy criterion. Given a set N of clauses, a clause is redundant with respect to N, if it follows from the equality and ACUKT axioms and smaller clauses in N. It can be deleted from the current set of clauses at any point of the saturation process. An inference is redundant, if its conclusion follows from the equality and ACUKT axioms and clauses in N that are smaller than the largest premise. It may be ignored during the saturation process without endangering the fairness of the derivation.

To lift the inference rules *equality resolution*, *standard superposition*, and *standard equality factoring* to non-ground premises, we proceed as in the standard superposition calculus: equality in the ground inference rule is replaced by unifiability.

As long as all variables in our clauses are shielded, the remaining inference rules can be lifted in a similar way: In a clause $C = C' \vee [\neg]\, e_1$, the maximal equation e_1 need no longer have the form $mu + s \approx s'$, where u is the unique maximal atomic term. Rather, it may contain several (distinct but ACU-unifiable) maximal atomic terms u_k with multiplicities m_k, where k ranges over some finite non-empty index set K. We obtain thus $e_1 = \sum_{k \in K} m_k u_k + s \approx s'$, where $\sum_{k \in K} m_k$ corresponds to m in the ground equation above. As in the standard superposition rule, the substitution σ that unifies all u_k (and the corresponding terms v_l from the other premise) is applied to the conclusion. For instance, the *negative cancellative superposition* rule has now the following form:

Negative Cancellative Superposition

$$\frac{D' \vee \sum_{l \in L} n_l v_l + t \approx t' \qquad C' \vee \neg \sum_{k \in K} m_k u_k + s \approx s'}{(D' \vee C' \vee \neg\, \psi s + \chi t' \approx \chi t + \psi s')\sigma}$$

if the following conditions are satisfied:

- $m = \sum_{k \in K} m_k \geq 1$, $n = \sum_{l \in L} n_l \geq 1$.
- $\psi = n/\gcd(m, n)$, $\chi = m/\gcd(m, n)$.
- σ is a most general ACU-unifier of all u_k and v_l $(k \in K, l \in L)$.
- $u_1\sigma \not\preceq s\sigma$, $u_1\sigma \not\preceq s'\sigma$, $u_1\sigma \not\preceq t\sigma$, $u_1\sigma \not\preceq t'\sigma$.

In the presence of unshielded variables, it is still possible to devise lifted inference rules that produce only finitely many conclusions for a given tuple of premises, but these rules are significantly more complicated than the rules given above. Furthermore, as unification is not an effective filter when one of the terms to be unified is a variable, clauses with unshielded variables lead to an enormous growth of the search space. In the sequel, we will show that the axioms DivInvNontriv allow us to eliminate unshielded variables completely. To this end we will construct a new inference system that is closed under clauses without unshielded variables.

4 Variable Elimination: The Logical Side

Let x be a variable. We define a noetherian binary relation $\rightarrow_x$ over clauses by

(CancelVar) $C' \vee [\neg]\, mx + s \approx m'x + s' \quad \rightarrow_x \quad C' \vee [\neg]\, (m{-}m')x + s \approx s'$
if $m \geq m' \geq 1$.

(ElimNeg) $C' \vee \neg\, mx + s \approx s' \quad \rightarrow_x \quad C'$
if $m \geq 1$ and x does not occur in C', s, s'.

(ElimPos) $C' \vee m_1 x + s_1 \approx s'_1 \vee \ldots \vee m_k x + s_k \approx s'_k \quad \rightarrow_x \quad C'$
if $m_i \geq 1$ and x does not occur in C', s_i, s'_i, for $1 \leq i \leq k$.

(Coalesce) $C' \vee \neg\, mx + s \approx s' \vee [\neg]\, nx + t \approx t'$
$\rightarrow_x \quad C' \vee \neg\, mx + s \approx s' \vee [\neg]\, \psi t + \chi s' \approx \psi t' + \chi s$
if $m \geq 1$, $n \geq 1$, $\psi = m/\gcd(m,n)$, $\chi = n/\gcd(m,n)$, and x does not occur at the top of s, s', t, t'.

The binary relation $\rightarrow_{\text{elim}}$ over clauses is defined in such a way that $C_0 \rightarrow_{\text{elim}} C_1$ if and only if C_0 contains an unshielded variable x and C_1 is a normal form of C_0 with respect to $\rightarrow_x$. The relation $\rightarrow_{\text{elim}}$ is noetherian; for a clause C, $\text{elim}(C)$ denotes some (arbitrary but fixed) normal form of C with respect to $\rightarrow_{\text{elim}}$. It is easy to check that $\text{elim}(C)$ contains no unshielded variables.

Lemma 4.1 *For every clause C, $\{\text{elim}(C)\} \models_{\text{ACUKT}} C$ and $\{C\} \cup \text{DivInvNontriv} \models_{\text{ACUKT}} \text{elim}(C)$. Furthermore, for every ground instance $C\theta$, $\{\text{elim}(C)\theta\} \models_{\text{ACUKT}} C\theta$.*

Proof. If $C_0 \rightarrow_x C_1$ by (CancelVar), the equivalence of C_0 and C_1 modulo ACUKT follows from cancellation; for (Coalesce), from cancellation and torsion-freeness. The soundness of (ElimNeg) follows from the divisibility and and inverse axiom, for (ElimPos) it is implied by torsion-freeness and non-triviality [2]. □

5 Variable Elimination: The Operational Side

Using the technique sketched above, every clause C can be transformed into a clause $\text{elim}(C)$ that contains no unshielded variables, implies C modulo ACUKT, and follows from C and ACUKT $\cup$ DivInvNontriv. However, these properties are not sufficient for a simplification in a superposition-based calculus: to make the simplified clause redundant, it is necessary that each of its ground instances follows from *smaller* instances of the simplifying clause. But this is not guaranteed for our variable elimination algorithm.

Let ι be an inference. We call the unifying substitution that is computed during ι and applied to the conclusion the pivotal substitution of ι. (For *abstraction* inferences and all ground inferences, the pivotal substitution is the identity mapping.) If u is the atomic term that is cancelled out in ι, or in which some subterm is replaced or abstracted out, and σ is the pivotal substitution of ι, then we call $u\sigma$ the pivotal term of ι. Finally, if $[\neg]\, e$

is the last literal of the last premise of ι, we call $[\neg]\, e\sigma$ the pivotal literal of ι.

Pivotal terms have two important properties: First, whenever an inference ι from clauses *without* unshielded variables produces a conclusion *with* unshielded variables, then all these unshielded variables occur in the pivotal term of ι. Second, no atomic term in the conclusion of ι can be larger than the pivotal term of ι.

LEMMA 5.1 *Let ι be a non-abstraction inference from clauses without unshielded variables with maximal premise C, conclusion C_0, pivotal literal $[\neg]\, e$, and pivotal term u; let $C_1 =$ $\mathrm{elim}(C_0)$. Let $\iota\theta$ be a ground instance of ι. If $C\theta \not\succ_{\mathrm{C}} C_1\theta$, then the multiset difference $C_1 \setminus C_0$ contains a literal $[\neg]\, e_1$, such that $[\neg]\, e_1$ has the same polarity as $[\neg]\, e$, an atomic term u_1 occurs at the top of $[\neg]\, e_1$, and for every minimal complete set U of* ACU*-unifiers of u and u_1, there is a $\rho \in U$ such that $C_0\theta$ is a ground instance of $C_0\rho$. Furthermore, for every $\rho \in U$, $C_0\rho$ has no unshielded variables. (A similar property holds for abstraction inferences.)*

We can now modify the inference system $\mathit{CS}\text{-}\mathit{Inf}_{\mathbf{N}^{>0}}$ in such a way that the new inference system is closed under clauses without unshielded variables: Whenever a $\mathit{CS}\text{-}\mathit{Inf}_{\mathbf{N}^{>0}}$-inference ι with pivotal term u produces a clause C_0 with unshielded variables, then we add $\mathrm{elim}(C_0)$ to the current set of clauses. Furthermore, for every literal $[\neg]\, e_1$ in the multiset difference $\mathrm{elim}(C_0) \setminus C_0$ with the same polarity as the pivotal literal of ι, and for every atomic term u_1 occurring at the top of $[\neg]\, e_1$, we add all clauses $C_0\rho$, where ρ ranges over a minimal complete set of ACU-unifiers of u and u_1. By the lemma above, this renders the inference ι redundant, so there is no need to add C_0.

For example, let $C = 3x \not\approx c \vee x + f(z) \approx 0 \vee f(x) + b \approx f(y)$. If a cancellation inference ι from C yields $C_0 = 3x \not\approx c \vee x + f(z) \approx 0 \vee b \approx 0$, then we add $\mathrm{elim}(C_0) =$ $c + 3f(z) \approx 0 \vee b \approx 0$, and, as the pivotal term $f(x)$ is unifiable with $f(z)$, the clause $C_0\rho = 3z \not\approx c \vee z + f(z) \approx 0 \vee b \approx 0$. The clause $\mathrm{elim}(C_0)$ makes all ground instances $\iota\theta$ redundant that satisfy $C\theta \succ_{\mathrm{C}} \mathrm{elim}(C_0)\theta$, that is, in particular, all ground instances with $x\theta \succ z\theta$. The only remaining ground instances are those where $x\theta = z\theta$; these are made redundant by $C_0\rho$.

A clause C is called fully abstracted, if no non-variable term of sort S_{G} occurs below a free function symbol in C. It is easy to check that the new inference system preserves full abstraction. If we abstract out all atomic terms of sort S_{G} in advance in the input of the inference system, then all terms that have to be unified during the saturation have the property that they do not contain the operator $+$. For such terms, ACU-unification and ordinary unification are equivalent. Therefore, our calculus allows us to avoid not only variable overlaps, but even ACU-unification completely.

Acknowledgments: Thanks to Harald Ganzinger for pointing out to me that abstraction allows us to avoid ACU-unification completely and to Jürgen Stuber for helpful comments on this paper.

References

[1] Leo Bachmair and Harald Ganzinger. Rewrite-based equational theorem proving with selection and simplification. *Journal of Logic and Computation*, 4(3):217–247, 1994.

[2] Uwe Waldmann. *Cancellative Abelian Monoids in Refutational Theorem Proving.* PhD thesis, Universität des Saarlandes, Saarbrücken, Germany, 1997. Submitted version: `http://www.mpi-sb.mpg.de/guide/staff/uwe/paper/PhDSubmitted.ps.gz`.