Superposition and Chaining for Totally Ordered Divisible Abelian Groups (Extended Abstract)

Uwe Waldmann

Max-Planck-Institut für Informatik, Stuhlsatzenhausweg 85,
66123 Saarbrücken, Germany, uwe@mpi-sb.mpg.de

Abstract. We present a calculus for first-order theorem proving in the presence of the axioms of totally ordered divisible abelian groups. The calculus extends previous superposition or chaining calculi for divisible torsion-free abelian groups and dense total orderings without endpoints. As its predecessors, it is refutationally complete and requires neither explicit inferences with the theory axioms nor variable overlaps. It offers thus an efficient way of treating equalities and inequalities between additive terms over, e. g., the rational numbers within a first-order theorem prover.

1 Introduction

Most real life problems for an automated theorem prover contain both uninterpreted function and predicate symbols, that are specific for a particular domain, and standard algebraic structures, such as numbers or orderings. General theorem proving techniques like resolution or superposition are notoriously bad at handling algebraical theories involving axioms like associativity, commutativity, or transitivity, since explicit inferences with these axioms lead to an explosion of the search space. To deal efficiently with such structures, it is therefore necessary that specialized techniques are built tightly into the prover.

AC-superposition (Bachmair and Ganzinger [1], Wertz [12]) is a well-known example of such a technique. It incorporates associativity and commutativity into the standard superposition calculus using AC-unification and extended clauses. In this way, inferences with the theory axioms and certain inferences involving variables are rendered unnecessary. Still, reasoning with the associativity and commutativity axioms remains difficult for an automated theorem prover, even if explicit inferences with the AC axioms can be avoided. This is not only due to the NP-completeness of the AC-unifiability problem, but it stems also from the fact that AC-superposition requires an inference between literals $u_1 + \cdots + u_k \approx s$ and $v_1 + \cdots + v_l \approx t$ (via extended clauses) whenever *some* u_i is unifiable with *some* v_j. Consequently, a variable in a sum can be unified with any part of any other sum – in this situation unification is completely unable to limit the search space.

The inefficiency inherent in the theory of associativity and commutativity can be mitigated by integrating further axioms into the calculus. In abelian

groups (or even in cancellative abelian monoids) the ordering conditions of the inference rules can be refined in such a way that summands u_i and v_j have to be overlapped only if they are *maximal* with respect to some simplification ordering $\succ$ (Ganzinger and Waldmann [4, 8], Marché [5], Stuber [7]). In this way, the number of variable overlaps can be greatly reduced; however, inferences with unshielded, i. e., potentially maximal, variables remain necessary.

In non-trivial divisible torsion-free abelian groups (e. g., the rational numbers and rational vector spaces), the abelian group axioms are extended by the torsion-freeness axiom $\forall k \in \mathbf{N}^{>0}\ \forall x, y\colon kx \approx ky \Rightarrow x \approx y$, the divisibility axiom $\forall k \in \mathbf{N}^{>0}\ \forall x\ \exists y\colon ky \approx x$, and the non-triviality axiom $\exists y\colon y \not\approx 0$. In such structures every clause can be transformed into an equivalent clause without unshielded variables. Integrating this variable elimination algorithm into cancellative superposition results in a calculus that requires neither extended clauses, nor variable overlaps, nor explicit inferences with the theory axioms. Furthermore, using full abstraction even AC unification can be avoided (Waldmann [10]).

When we want to work with a transitive relation $>$ in a theorem prover, we encounter a situation that is surprisingly similar to the one depicted above. Just as associativity and commutativity, the transitivity axiom is fairly prolific. It allows to derive a new clause whenever the left hand side of a literal $r > s$ overlaps with the right hand side of another literal $s' > t$. As such an overlap is always possible if s or s' is a variable, unification is not an effective filter to control the generation of new clauses. The use of the chaining inference rule makes explicit inferences with the transitivity axiom superfluous (Slagle [6]). Since this inference rule can be equipped with the restriction that the overlapped term s must be maximal with respect to a simplification ordering $\succ$, overlaps with shielded variables become again unnecessary. Only inferences with unshielded, i. e., potentially maximal, variables have to be computed.

Once more, the number of unshielded variables in a clause can be reduced if further axioms are available. In particular, in dense total orderings without endpoints, unshielded variables can be eliminated completely (Bachmair and Ganzinger [3]).

There are two facts that suggest to investigate the combination of the theory of divisible torsion-free abelian groups and the theory of dense total orderings without endpoints. On the one hand, the vast majority of applications of divisible torsion-free abelian groups (and in particular of the rationals or reals) requires also an ordering; so the combined calculus is likely to be much more useful in practice than the DTAG-superposition calculus on which it is based. On the other hand, these two theories are closely related: An abelian group $(G, +, 0)$ can be equipped with a total ordering that is compatible with $+$ if and only if it is torsion-free; furthermore divisibility and compatibility of the ordering imply that the ordering is dense and has no endpoints. One can thus assume that the two calculi fit together rather smoothly. We show in this paper that this is in fact true. The resulting calculus splits again into two parts: The first one is a base calculus, that works on clauses without unshielded variables, but whose rules may produce clauses with unshielded variables. This calculus has

the property that saturated sets of clauses are unsatisfiable if and only if they contain the empty clause, but it can not be used to effectively saturate a given set of clauses. The second part of the calculus is a variable elimination algorithm that makes it possible to get rid of unshielded variables, and thus renders the base calculus effective. The integration of these two components happens in essentially the same way as in the equational case (Waldmann [10]).

In this extended abstract, we can only sketch the main ideas of our work. The reader is referred to the full version [11] for the proofs.

2 The Base Calculus

2.1 Preliminaries

We work in a many-sorted framework and assume that the function symbol $+$ is declared on a sort G. If t is a term of sort G and $n \in \mathbf{N}$, then nt is an abbreviation for the n-fold sum $t + \cdots + t$; in particular, $0t = 0$ and $1t = t$. Analogously, $\sum_{i \in \{1,\ldots,n\}} t_i$ is an abbreviation for the sum $t_1 + \cdots + t_n$.

Without loss of generality we assume that the equality relation $\approx$ and the semantic ordering $>$ are the only predicates of our language. Hence a literal is either an equation $t \approx t'$, or a negated equation $t \not\approx t'$, where t and t' have the same sort, or an inequation $t > t'$, or a negated inequation $t \not> t'$, where t and t' have sort G. Occasionally we write $t' < t$ instead of $t > t'$. The symbol $\gtrless$ denotes either $>$ or $<$, the symbol $\sim$ stands for $\gtrless$ or $\approx$, and $\dot{\sim}$ denotes $\gtrless$ or $\approx$ or $\not\approx$. The equality symbol is supposed to be symmetric. Multiple occurrences of one of the symbols $\gtrless$, $\sim$, or $\dot{\sim}$ within a single inference rule denote consistently the same relation. A clause is a finite multiset of literals, usually written as a disjunction.

The clauses

$$
\begin{array}{rr}
(x + y) + z \approx x + (y + z) & \text{(Associativity (A))} \\
x + y \approx y + x & \text{(Commutativity (C))} \\
x + 0 \approx x & \text{(Identity (U))} \\
(-x) + x \approx 0 & \text{(Inverse (Inv))} \\
n \textit{ divided-by}_n(x) \approx x & \text{(Divisibility (Div))} \\
a_0 \not\approx 0 & \text{(Non-Triviality (Nt))} \\
x \not> x & \text{(Irreflexivity (Ir))} \\
x \not> y \vee y \not> z \vee x > z & \text{(Transitivity (Tr))} \\
x \not> y \vee x + z > y + z & \text{(Monotonicity (Mon))} \\
x > y \vee y > x \vee x \approx y & \text{(Totality (Tot))}
\end{array}
$$

plus the equality axioms[1] are the axioms ODAG of totally ordered divisible abelian groups.

[1] including the congruence axiom $x \not\approx y \vee y \not\gtrless z \vee x \gtrless z$ for the predicate $>$.

The following clauses are consequences of these axioms (for every $\psi \in \mathbf{N}^{>0}$):

$$x + z \not\approx y + z \vee x \approx y \qquad \text{(Cancellation (K))}$$
$$\psi x \not\approx \psi y \vee x \approx y \qquad \text{(Torsion-Freeness (T))}$$
$$x + z \not> y + z \vee x > y \qquad \text{(}>\text{-Cancellation (K}^{>}\text{))}$$
$$\psi x \not> \psi y \vee x > y \qquad \text{(}>\text{-Torsion-Freeness (T}^{>}\text{))}$$

We write OTfCAM for the union of the clauses A, C, U, Ir, Tr, Mon, K, T, $\mathrm{K}^{>}$, $\mathrm{T}^{>}$ and the equality axioms.

We denote the entailment relation modulo ODAG by $\models_{\mathrm{ODAG}}$, and the entailment relation modulo OTfCAM by $\models_{\mathrm{OTfCAM}}$. That is, $\{C_1, \ldots, C_n\} \models_{\mathrm{ODAG}} C_0$ if and only if $\{C_1, \ldots, C_n\} \cup \mathrm{ODAG} \models C_0$, and $\{C_1, \ldots, C_n\} \models_{\mathrm{OTfCAM}} C_0$ if and only if $\{C_1, \ldots, C_n\} \cup \mathrm{OTfCAM} \models C_0$.

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 G. Otherwise, x is called unshielded.

A clause C is called fully abstracted, if no non-variable term of sort G occurs below a free function symbol in C. Every clause C can be transformed into an equivalent fully abstracted clause $\mathrm{abs}(C)$ by iterated rewriting

$$C[f(\ldots, t, \ldots)] \quad \to \quad x \not\approx t \vee C[f(\ldots, x, \ldots)]\,,$$

where x is a new variable and t is a non-variable term of sort G occurring immediately below the free function symbol f in C.

We say that an ACU-compatible ordering $\succ$ has the multiset property, if whenever a ground atomic term u is greater than v_i for every i in a finite non-empty index set I, then $u \succ \sum_{i \in I} v_i$. Every reduction ordering over terms not containing + that is total on ground terms and for which 0 is minimal can be extended to an ordering that is ACU-compatible and has the multiset property (Waldmann [9]).[2]

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, is total on ground ACU-congruence classes, and satisfies $t \not\succ s[t]_o$ for every term $s[t]_o$.

Let A be a ground literal. Then the largest atomic term occurring on either side of A is denoted by $\mathrm{mt}(A)$.

[2] In fact, we use the extended ordering only as a theoretical device; as we work with fully abstracted clauses, the original reduction ordering is sufficient for actual computations.

The balance value of a ground literal A is 3, if $\mathrm{mt}(A)$ occurs on both sides of A, it is 2, if A is an inequation $[\neg]\ s > t$ and $\mathrm{mt}(A)$ occurs only in s, and otherwise it is 1. The ordering $\succ_{\mathrm{L}}$ on literals compares lexicographically first the maximal atomic terms of the literals, then the polarities (negative $\succ$ positive), then the kinds of the literals (inequation $\succ$ equation), then the balance values of the literals, then the multisets of all non-zero terms occurring at the top of the literals, and finally the multisets $\{\{s\},\{t\}\}$ (for equations $[\neg]\ s \approx t$) or $\{\{s,s\},\{t\}\}$ (for inequations $[\neg]\ s > t$). The ordering $\succ_{\mathrm{C}}$ on clauses is the multiset extension of the literal ordering $\succ_{\mathrm{L}}$. Both $\succ_{\mathrm{L}}$ and $\succ_{\mathrm{C}}$ are noetherian and total on ground literals/clauses.

2.2 Superposition and Chaining

We present the ground versions of the inference rules of the base calculus *OCInf*. The non-ground versions can be obtained by lifting in a rather straightforward way (see below).

Let us start the presentation of the inference rules with a few general conventions: Every term occurring in a sum is assumed to have sort G. The letters u and v, possibly with indices, denote atomic terms, unless explicitly said otherwise. In an expression like $mu + s$, m is a natural number, s may be zero.

If an inference involves a literal, then it must be maximal in the respective clause (except for the last but one literal in *factoring* inferences). A positive literal that is involved in a *superposition* or *chaining* inference must be strictly maximal in the respective clause. In all *superposition* or *chaining* inferences, the left premise is smaller than the right premise.

Cancellation

$$\frac{C' \vee mu + s \mathrel{\dot{\sim}} m'u + s'}{C' \vee (m - m')u + s \mathrel{\dot{\sim}} s'}$$

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

Equality Resolution

$$\frac{C' \vee u \not\approx u}{C'}$$

if u either equals 0 or does not have sort G.

Inequality Resolution

$$\frac{C' \vee 0 > 0}{C'}$$

Canc. Superposition

$$\frac{D' \vee nu + t \approx t' \qquad C' \vee mu + s \mathrel{\dot{\sim}} s'}{D' \vee C' \vee ns + mt' \mathrel{\dot{\sim}} ns' + mt}$$

if $n \geq 1$, $m \geq 1$, $u \succ s$, $u \succ s'$, $u \succ t$, $u \succ t'$.[3]

[3] If $\gcd(m,n) > 1$, then the conclusion of this inference can be simplified to $D' \vee C' \vee \psi s + \chi t' \mathrel{\dot{\sim}} \psi s' + \chi t$, where $\psi = n/\gcd(m,n)$ and $\chi = m/\gcd(m,n)$ (and similarly for the following inference rules). To enhance readability, we leave out this optimization in the sequel.

Canc. Chaining

$$\frac{D' \vee t' \gtreqless nu + t \qquad C' \vee mu + s \gtreqless s'}{D' \vee C' \vee ns + mt' \gtreqless ns' + mt}$$

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

Std. Superposition

$$\frac{D' \vee u \approx u' \qquad C' \vee s[u] \mathrel{\dot{\sim}} s'}{D' \vee C' \vee s[u'] \mathrel{\dot{\sim}} s'}$$

if u occurs in a maximal atomic subterm of s and does not have sort G, $u \succ u'$, $s[u] \succ s'$.

Canc. Eq. Factoring

$$\frac{C' \vee nu + t \approx t' \vee mu + s \approx s'}{C' \vee mt + ns' \not\approx mt' + ns \vee nu + t \approx t'}$$

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

Canc. Ineq. Factoring (I)

$$\frac{C' \vee nu + t \gtreqless t' \vee mu + s \gtreqless s'}{C' \vee mt + ns' \gtreqless mt' + ns \vee mu + s \gtreqless s'}$$

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

Canc. Ineq. Factoring (II)

$$\frac{C' \vee nu + t \gtreqless t' \vee mu + s \gtreqless s'}{C' \vee mt' + ns \gtreqless mt + ns' \vee nu + t \gtreqless t'}$$

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

Std. Eq. Factoring

$$\frac{C' \vee u \approx v' \vee u \approx u'}{C' \vee u' \not\approx v' \vee u \approx v'}$$

if u, u' and v' do not have sort G, $u \succ u'$, $u \succ v'$.

The inference rules of the calculus *OCInf* do not handle negative inequality literals. We assume that in the beginning of the saturation process every literal $s \not> t$ in an input clause is replaced by the two literals $t > s \vee t \approx s$, which are equivalent to $s \not> t$ by the totality, transitivity and irreflexivity axioms. Note that the inference rules of *OCInf* do not produce any new negative inequality literals.

Example 1. Let the ordering on constant symbols be given by $b \succ c \succ d$. We will use the inference rules of *OCInf* to show that the following three clauses are contradictory with respect to ODAG. (The maximal parts of every clause are underlined.)

$$\underline{3b} > 2d \tag{1}$$

$$\underline{b} > 2c \tag{2}$$

$$\underline{2b} \approx c + d \tag{3}$$

Cancellative superposition of (3) and (1) yields

$$\underline{3c} + 3d > 4d \tag{4}$$

Cancellative superposition of (3) and (2) yields

$$\underline{c} + d > \underline{4c} \tag{5}$$

By *cancellation* of (5) we obtain

$$d > \underline{3c} \tag{6}$$

Cancellative chaining of (6) and (4) produces

$$\underline{4d} > \underline{4d} \tag{7}$$

which yields the empty clause by *cancellation* and *inequality resolution*.

In the standard superposition calculus, lifting means replacing equality in the ground inference by unifiability. As long as all variables in our clauses are shielded, the situation is similar here: For instance, in the second premise $C' \vee A_1$ of a *cancellative superposition* inference the maximal literal A_1 need no longer have the form $mu + s \mathrel{\dot{\sim}} s'$ with a unique maximal atomic term u. 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 $A_1 = \sum_{k \in K} m_k u_k + s \mathrel{\dot{\sim}} s'$. In the inference rule, the substitution σ that unifies all u_k (and the corresponding terms v_l from the other premise) is applied to the conclusion. Consequently, the *cancellative superposition* rule has now the following form:

$$\frac{D' \vee \sum_{l \in L} n_l v_l + t \approx t' \qquad C' \vee \sum_{k \in K} m_k u_k + s \mathrel{\dot{\sim}} s'}{(D' \vee C' \vee ns + mt' \mathrel{\dot{\sim}} ns' + mt)\sigma}$$

where

(i) $m = \sum_{k \in K} m_k \geq 1$, $n = \sum_{l \in L} n_l \geq 1$.
(ii) σ is a most general ACU-unifier of all u_k and v_l $(k \in K, l \in L)$.
(iii) u is one of the u_k $(k \in K)$.
(iv) $u\sigma \not\preceq s\sigma$, $u\sigma \not\preceq s'\sigma$, $u\sigma \not\preceq t\sigma$, $u\sigma \not\preceq t'\sigma$.

The other inference rules can be lifted in a similar way, again under the condition that all variables in the clauses are shielded. As usual, the *standard superposition* rule is equipped with the additional restriction that the subterm of s that is replaced during the inference is not a variable. For clauses with unshielded variables, lifting would be significantly more complicated; however, as we will combine the base calculus with an algorithm that eliminates unshielded variables, we need not consider this case.

Theorem 2. *The inference rules of the calculus OCInf are sound with respect to* $\models_{\mathrm{ODAG}}$.

Definition 3. Let N be a set of clauses, let $\overline{N}$ be the set of ground instances of clauses in N. An inference is called *OCRed*-redundant with respect to N if for each of its ground instances with conclusion $C_0\theta$ and maximal premise $C\theta$ we have $\{ D \in \overline{N} \mid D \prec_{\mathrm{c}} C\theta \} \models_{\mathrm{OTfCAM}} C_0\theta$. A clause C is called *OCRed*-redundant with respect to N, if for every ground instance $C\theta$, $\{ D \in \overline{N} \mid D \prec_{\mathrm{c}} C\theta \} \models_{\mathrm{OTfCAM}} C\theta$.

2.3 Rewriting on Equations

To prove that the inference system described so far is refutationally complete we have to show that every saturated clause set that does not contain the empty clause has a model. The traditional approach to construct such a model is rewrite-based: First an ordering is imposed on the set of all ground instances of clauses in the set. Starting with an empty interpretation all such instances are inspected in ascending order. If a reductive clause is false and irreducible in the partial interpretation constructed so far, its maximal positive literal is turned into a rewrite rule and added to the interpretation. If the original clause set is saturated and does not contain the empty clause, then the final interpretation is a model of all ground instances, and thus of the original clause set (Bachmair and Ganzinger [2]).

In order to be able to treat cancellative superposition we have modified this scheme in [4] in such a way that the rewrite relation operates on equations rather than on terms. But if we also have to deal with inequations, a further extension is necessary: We need to be able to rewrite inequations *with inequations*; and unlike rewriting with equations, this does of course not produce logically equivalent formulae.

Definition 4. A ground equation or inequation e is called a cancellative rewrite rule with respect to $\succ$, if $\mathrm{mt}(e)$ does not occur on both sides of e.

We will usually drop the attributes "cancellative" and "with respect to $\succ$", speaking simply of "rewrite rules".

Every rewrite rule has either the form $mu + s \sim s'$, where u is an atomic term, $m \in \mathbf{N}^{>0}$, $u \succ s$, and $u \succ s'$, or the form $u \approx s'$, where $u \succ s'$ and u (and thus s') does not have sort G. This is an easy consequence of the multiset property of $\succ$.

Definition 5. Given a set R of rewrite rules, the four binary relations $\rightarrow_{\gamma,R}$, $\rightarrow_{\delta,R}$, $\rightarrow_{o,R}$, and $\rightarrow_{\kappa}$ on ground equations and inequations are defined (modulo ACU) as follows:[4]

(i) $mu + t \sim t' \;\rightarrow_{\gamma,R}\; s' + t \sim t' + s$,
if $mu + s \approx s'$ is a rule in R.

(ii) $t[s] \sim t' \;\rightarrow_{\delta,R}\; t[s'] \sim t'$,
if (i) $s \approx s'$ is a rule in R and (ii) s does not have sort G or s occurs in t below some free function symbol.

(iii) $mu + t \gtrless t' \;\rightarrow_{o,R}\; s' + t \gtrless t' + s$,
if $mu + s \gtrless s'$ is a rule in R.

(iv) $u + t \sim u + t' \;\rightarrow_{\kappa}\; t \sim t'$,
$u \approx u \;\rightarrow_{\kappa}\; 0 \approx 0$,
if u is atomic and different from 0.

[4] While we have the restriction $u \succ s$, $u \succ s'$ for the rewrite rules, there is no such restriction for the (in-)equations to which rules are applied.

The union of $\to_{\gamma,R}$, $\to_{\delta,R}$, $\to_{o,R}$, and $\to_{\kappa}$ is denoted by $\to_R$.[5]

If $e \to_R e'$ using a γ-, δ- or κ-step, then e and e' are equivalent modulo OTfCAM and the applied rewrite rule. If $s \gtrsim s' \to_{o,R} t \gtrsim t'$, then both $t \gtrsim t'$ and $t \approx t'$ imply $s \gtrsim s'$ modulo OTfCAM and the applied rewrite rule.

We say that an (in-)equation e is γ-reducible, if $e \to_\gamma e'$ (analogously for δ, o, and κ). It is called reducible, if it is γ-, δ-, o-, or κ-reducible.

Unlike o- and κ-reducibility, γ- and δ-reducibility can be extended to terms: A term t is called γ-reducible, if $t \approx t' \to_\gamma e'$, where the rewrite step takes place at the left-hand side (analogously for δ). It is called reducible, if it is γ- or δ-reducible.

Lemma 6. *The relation $\to_R$ is contained in $\succ_{\mathrm{L}}$ and thus noetherian.*

Definition 7. Given a set R of rewrite rules, the relation $\to_R^\circ$ is defined by $\to_R^\circ = (\to_R^* \circ \to_{o,R} \circ \to_R^*)$.

Definition 8. Given a set R of rewrite rules, the set $\mathrm{tr}(R)$ is the set of all (in-)equations $s \sim s'$ for which there exists a derivation $s \sim s' \to_R^* 0 \sim 0$. The truth set $\mathrm{tr}^\circ(R)$ of R is the set of all equations $s \approx s'$ for which there exists a derivation $s \approx s' \to_R^* 0 \approx 0$, and the set of all inequations $s \gtrsim s'$ for which there exists a derivation $s \gtrsim s' \to_R^\circ 0 \gtrsim 0$. The Ψ-truth set $\mathrm{tr}_\Psi^\circ(R)$ of R is the set of all equations or inequations $e = s \sim s'$, such that either $e \in \mathrm{tr}^\circ(R)$ and s does not have sort G, or $\psi s \sim \psi s' \in \mathrm{tr}^\circ(R)$ for some $\psi \in \mathbf{N}^{>0}$.

All (in-)equations in $\mathrm{tr}_\Psi^\circ(R)$ are logical consequences of the rewrite rules in R and the theory axioms OTfCAM.

2.4 Model Construction

Definition 9. A ground clause $C' \vee e$ is called reductive for e, if e is a cancellative rewrite rule and strictly maximal in $C' \vee e$.

Definition 10. Let N be a set of (possibly non-ground) clauses that does not contain the empty clause, and let $\overline{N}$ the set of all ground instances of clauses in N. Using induction on the clause ordering we define sets of rules R_C, R_C^Ψ, E_C, and E_C^Ψ, for all clauses $C \in \overline{N}$. Let C be such a clause and assume that R_D, R_D^Ψ, E_D, and E_D^Ψ have already been defined for all $D \in \overline{N}$ such that $C \succ_{\mathrm{C}} D$. Then the set R_C of primary rules and the set R_C^Ψ of secondary rules are given by

$$R_C = \bigcup_{D \prec_{\mathrm{C}} C} E_D \quad \text{and} \quad R_C^\Psi = \bigcup_{D \prec_{\mathrm{C}} C} E_D^\Psi .$$

[5] As we deal only with ground terms and as there are no non-trivial contexts around (in-)equations, this operation does indeed satisfy the definition of a rewrite relation, albeit in an unorthodox way.

E_C is the singleton set $\{e\}$, if C is a clause $C' \vee e$ such that (i) C is reductive for e, (ii) C is false in $\mathrm{tr}^\circ(R_C^\Psi)$, (iii) C' is false in $\mathrm{tr}^\circ_\Psi(R_C^\Psi \cup \{e\})$, and (iv) $\chi\,\mathrm{mt}(e)$ is $\gamma\delta$-irreducible with respect to R_C^Ψ for every $\chi \in \mathbf{N}^{>0}$. Otherwise, E_C is empty.

If $E_C = \{e\}$, then E_C^Ψ is the set of all rewrite rules $e' \in \mathrm{tr}^\circ_\Psi(R_C^\Psi \cup E_C)$ such that $\mathrm{mt}(e') = \mathrm{mt}(e)$ and e' is $\delta\kappa$-irreducible with respect to R_C^Ψ. Otherwise, E_C^Ψ is empty.

Finally, the sets R_∞ and R_∞^Ψ are defined by

$$R_\infty = \bigcup_{D \in \overline{N}} E_D \quad \text{and} \quad R_\infty^\Psi = \bigcup_{D \in \overline{N}} E_D^\Psi \,.$$

Our goal is to show that, if N is saturated with respect to *OCInf*, then $\mathrm{tr}^\circ(R_\infty^\Psi)$ is a model of the axioms of totally ordered divisible abelian groups and of the clauses in N.

2.5 Refutational Completeness of *OCInf*

The relations $\to_{R_C^\Psi}$ and $\to_{R_\infty^\Psi}$ are in general not confluent, not even in the purely equational case. One can merely show that that $\to_{R_C^\Psi}$ is confluent on equations in $\mathrm{tr}(R_C^\Psi)$, that is, that any two derivations starting from an equation e can be joined, provided that there is a derivation $e \to^+ 0 \approx 0$. But even this kind of restricted confluence does not hold for inequations, and in particular, not for o-rewriting. We can only prove that two derivations starting from the same inequation can be joined, if one of them leads to $0 > 0$ and if the other one does not use o-steps. This property will be sufficient for our purposes, however.

Definition 11. Let E be a set of equations and/or inequations. We say that the relation $\to_R$ is partially confluent on E, if for all equations $e_0 \in E$ and e_1, e_2 with $e_1 \leftarrow_R^* e_0 \to_R^* e_2$ there exists an equation e_3 such that $e_1 \to_R^* e_3 \leftarrow_R^* e_2$, and if for all inequations $e_0' \in E$ and e_1' with $e_1' \leftarrow^*_{\gamma\delta\kappa,R} e_0' \to_R^* 0 > 0$ or $e_1' \leftarrow^*_{\gamma\delta\kappa,R} e_0' \to_R^\circ 0 > 0$ there is a derivation $e_1' \to_R^* 0 > 0$ or $e_1' \to_R^\circ 0 > 0$, respectively.

There is one important technical difference between the equational case developed in (Waldmann [8]) and the inequational case that we consider here: In the equational case, one can show that $\to_{R_\infty^\Psi}$ is confluent on $\mathrm{tr}(R_\infty^\Psi)$, and hence that $\mathrm{tr}(R_\infty^\Psi)$ is a model of the theory axioms, without requiring that the set N of clauses is saturated. Saturation is only necessary to prove that $\mathrm{tr}(R_\infty^\Psi)$ is also a model of $\overline{N}$. In the inequational case, such a separation does not work: Proving partial confluence of $\to_{R_\infty^\Psi}$ is only possible if we require that *cancellative chaining* inferences are redundant. For this reason, the proof that $\to_{R_\infty^\Psi}$ is partially confluent and the proof that $\mathrm{tr}^\circ(R_\infty^\Psi)$ is a model of $\overline{N}$ must be combined within a single induction.

The following two lemmas are copied almost verbatim from (Waldmann [8]).

Lemma 12. *The relation* $\to_{R_C^\Psi}$ *is confluent on the equations in* $\mathrm{tr}^\circ(R_C^\Psi)$ *for every* $C \in \overline{N}$. *The relation* $\to_{R_\infty^\Psi}$ *is confluent on the equations in* $\mathrm{tr}^\circ(R_\infty^\Psi)$.

Corollary 13. *For every* $C \in \overline{N}$, $\mathrm{tr}^\circ(R_C^\Psi)$ *and* $\mathrm{tr}^\circ(R_\infty^\Psi)$ *satisfy* ACUKT *and the equality axioms (except the congruence axiom for the predicate* $>$*).*

In a similar way as Lemma 12, we obtain by a rather tedious case analysis over various kinds of critical pairs:

Lemma 14. *If for every pair of rules* $mu + s > s'$ *and* $nu + t < t'$ *from* $E_C \cup R_C$ *the inequation* $ns + mt' > ns' + mt$ *is contained in* $\mathrm{tr}^\circ(R_C^\Psi)$*, then* $\to_{R_C^\Psi \cup E_C^\Psi}$ *is partially confluent on* $\mathrm{tr}(R_C^\Psi \cup E_C^\Psi)$*.*

Using the same techniques as in (Waldmann [8]) and (Bachmair and Ganzinger [3]) we can now prove the following theorem. Note in particular that in the presence of the totality axiom *cancellative inequality factoring (I)/(II)* inferences are simplifications, hence clauses where the maximal atomic term occurs on the same side of two ordering literals do not produce primary rules.

Theorem 15. *Let* N *be a set of clauses without negative inequality literals and without unshielded variables; suppose that* N *is saturated up to redundancy and contains the theory axiom* Div, Inv, Nt, *and all ground instances of* Tot*. If all clauses of* N*, except the ground instances of* Tot*, are fully abstracted, and if* N *does not contain the empty clause, then we have for every ground clause* $C\theta \in \overline{N}$*:*

(i) $E_{C\theta} = \emptyset$ *if and only if* $C\theta$ *is true in* $\mathrm{tr}^\circ(R_{C\theta}^\Psi)$*.*

(ii) $C\theta$ *is true in* $\mathrm{tr}^\circ(R_\infty^\Psi)$ *and in* $\mathrm{tr}^\circ(R_D^\Psi)$ *for every* $D \succ_C C\theta$*.*

(iii) The relation $\to_{R_{C\theta}^\Psi}$ *is partially confluent on* $\mathrm{tr}(R_{C\theta}^\Psi)$ *and the relation* $\to_{R_{C\theta}^\Psi \cup E_{C\theta}^\Psi}$ *is partially confluent on* $\mathrm{tr}(R_{C\theta}^\Psi \cup E_{C\theta}^\Psi)$*.*

(iv) $\mathrm{tr}^\circ(R_{C\theta}^\Psi)$ *and* $\mathrm{tr}^\circ(R_{C\theta}^\Psi \cup E_{C\theta}^\Psi)$ *satisfy the axioms* Ir, Tr, Mon, $\mathrm{K}^>$, $\mathrm{T}^>$*, and the congruence axiom for the predicate* $>$*.*

(v) The relation $\to_{R_\infty^\Psi}$ *is partially confluent on* $\mathrm{tr}(R_\infty^\Psi)$ *and* $\mathrm{tr}^\circ(R_\infty^\Psi)$ *satisfies the axioms* Ir, Tr, Mon, $\mathrm{K}^>$, $\mathrm{T}^>$*, and the congruence axiom for the predicate* $>$*.*

Theorem 16. *Let* N *be a set of clauses without negative inequality literals and without unshielded variables; suppose that* N *is saturated up to redundancy and contains the theory axiom* Div, Inv, Nt, *and all ground instances of* Tot*. Suppose that all clauses of* N*, except the ground instances of* Tot*, are fully abstracted. Then* $N \cup \mathrm{ODAG}$ *is unsatisfiable if and only if* N *contains the empty clause.*

We may assume without loss of generality that the constant a_0 does not occur in non-theory input clauses and that the function symbols $-$ and *divided-by*$_n$ are eliminated eagerly from all non-theory input clauses. In this case, no inferences are possible with the axioms Div, Inv, and Nt. Furthermore, one can show that inferences with the totality axiom Tot are always redundant (analogously to Bachmair and Ganzinger [3]).

3 The Extended Calculus

3.1 Variable Elimination

As we have mentioned in the introduction, the calculus *OCInf* works on clauses without unshielded variables, but its inference rules may produce clauses with

unshielded variables. To make it effectively saturate a given set of clauses, it has to be supplemented by a variable elimination algorithm.

In the equational case, every clause with unshielded variables can be transformed into an equivalent clause without unshielded variables. However, in the presence of ordering literals, this does no longer hold.

Example 17. Consider the clause $C = x > a \vee x \approx b \vee x < c$. This clause is true for every value of x, if either $c > a$ or both $a \approx b$ and $c \approx b$. So C can be replaced by the clause normal form of $c > a \vee (a \approx b \wedge c \approx b)$, that is, by the two clauses $c > a \vee a \approx b$ and $c > a \vee c \approx b$, but C is not equivalent to a single clause without unshielded variables.

For any disjunction of conjunctions of literals F let $\mathrm{CNF}(F)$ be the clause normal form of F (represented as a multiset of clauses).

Let x be a variable of sort G. We define a binary relation $\to_x$ over multisets of clauses by

CancelVar
$$M \cup \{C' \vee mx + s \mathrel{\dot{\sim}} m'x + s'\} \to_x M \cup \{C' \vee (m-m')x + s \mathrel{\dot{\sim}} s'\}$$
if $m \geq m' \geq 1$.

ElimNeg
$$M \cup \{C' \vee mx + s \not\approx s'\} \to_x M \cup \{C'\}$$
if $m \geq 1$ and x does not occur in C', s, s'.

ElimPos
$$M \cup \Big\{C' \vee \bigvee_{i\in I} l_i x + r_i \approx r'_i \vee \bigvee_{j\in J} m_j x + s_j > s'_j \vee \bigvee_{k\in K} n_k x + t_k < t'_k\Big\} \to_x$$
$$M \cup \mathrm{CNF}\Big(C' \vee \bigvee_{j\in J}\bigvee_{k\in K}(n_k s_j + m_j t'_k > n_k s'_j + m_j t_k \vee \bigvee_{i\in I}(l_i s_j + m_j r'_i \approx l_i s'_j + m_j r_i \wedge l_i t_k + n_k r'_i \approx l_i t'_k + n_k r_i))\Big)$$
if $I \cup J \cup K \neq \emptyset$, $l_i \geq 1$, $m_j \geq 1$, $n_k \geq 1$ and x does not occur in $C', r_i, r'_i, s_j, s'_j, t_k, t'_k$, for $i \in I$, $j \in J$, $k \in K$.

Coalesce
$$M \cup \{C' \vee mx + s \not\approx s' \vee nx + t \mathrel{\dot{\sim}} t'\} \to_x M \cup \{C' \vee mx + s \not\approx s' \vee mt + ns' \mathrel{\dot{\sim}} mt' + ns\}$$
if $m \geq 1$, $n \geq 1$, and x does not occur in s, s', t, t'.

It is easy to show that $\to_x$ is noetherian. We define the relation $\to_{\mathrm{elim}}$ over multisets of clauses in such a way that $M \cup \{C\} \to_{\mathrm{elim}} M \cup M'$ if and only if C contains an unshielded variable x and M' is a normal form of $\{C\}$ with respect to $\to_x$.

The relation $\to_{\mathrm{elim}}$ is again noetherian. For a clause C, $\mathrm{elim}(C)$ denotes some (arbitrary but fixed) normal form of $\{C\}$ with respect to the relation $\to_{\mathrm{elim}}$.

Corollary 18. *For any C, the clauses in* $\mathrm{elim}(C)$ *contain no unshielded variables.*

Lemma 19. *For every C,* $\{C\} \models_{\mathrm{ODAG}} \mathrm{elim}(C)$ *and* $\mathrm{elim}(C) \cup \mathrm{Tot} \models_{\mathrm{OTfCAM}} C$. *For every ground instance $C\theta$,* $\mathrm{elim}(C)\theta \cup \mathrm{Tot} \models_{\mathrm{OTfCAM}} C\theta$.

3.2 Integration of the Elimination Algorithm

Using the technique sketched so far, every clause C_0 can be transformed into a set of clauses $\mathrm{elim}(C_0)$ that do not contain unshielded variables, follow from C_0 and the axioms of totally ordered divisible abelian groups, and imply C_0 modulo OTfCAM $\cup$ Tot. Obviously, we can perform this transformation for all initially given clauses *before* we start the saturation process. However, when clauses with unshielded variables are produced during the saturation process, then logical equivalence is not sufficient to eliminate them. We have to require that the transformed set of clauses $\mathrm{elim}(C_0)$ makes the inference ι producing C_0 redundant. Unfortunately, it may happen that the clauses in $\mathrm{elim}(C_0)$ or the instances of the totality axiom needed in Lemma 19 are too large, at least for some instances of ι. To integrate the variable elimination algorithm into the base calculus, it has to be supplemented by a case analysis technique.

Let $k \in \{1, 2\}$, let $C_1, \ldots, C_k$ be clauses without unshielded variables and let ι be an *OCInf*-inference

$$\frac{C_k \ \ldots \ C_1}{C_0\sigma}$$

We call the unifying substitution σ that is computed during ι and applied to the conclusion the pivotal substitution of ι. (For ground inferences, the pivotal substitution is the identity mapping.) If the last premise C_1 has the form $C_1' \vee A$ where A is maximal (and the replacement or cancellation takes place at A) then we call $A\sigma$ the pivotal literal of ι. Finally, if u_0 is the atomic term that is cancelled out in ι, or in which some subterm is replaced,[6] then we call $u_0\sigma$ the pivotal term of ι.

Two properties of pivotal terms are important for us: 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.

One can now show that, if the clauses in $\mathrm{elim}(C_0)$ or the instances of the totality axiom needed in Lemma 19 are too large to make the *OCInf*-inference ι redundant, then there must be an atomic term in some clause in $\mathrm{elim}(C_0)$ that is unifiable with the pivotal term. If we apply the unifier to the conclusion of the *OCInf*-inference, then the result does no longer contain unshielded variables, and moreover it subsumes the critical instances of ι. Using this result, we can now transform the inference system *OCInf* into a new inference system that operates on clauses without unshielded variables and produces again such clauses. The new system *ODInf* is given by two meta-inference rules:

Eliminating Inference

$$\frac{C_n \ \ldots \ C_1}{C'}$$

[6] More precisely, u_0 is the maximal atomic subterm of s containing u in *standard superposition* inferences, and the term u in all other inferences.

if the following conditions are satisfied:

(i) $\dfrac{C_n \quad \ldots \quad C_1}{C_0}$ is a *OCInf*-inference.

(ii) $C' \in \mathrm{elim}(C_0)$.

Instantiating Inference

$$\frac{C_n \quad \ldots \quad C_1}{C_0\tau}$$

if the following conditions are satisfied:

(i) $\dfrac{C_n \quad \ldots \quad C_1}{C_0}$ is a *OCInf*-inference with pivotal literal A and pivotal term u.

(ii) $\mathrm{elim}(C_0) \neq \{C_0\}$.

(iii) A literal A_1 with the same polarity as A occurs in some clause in $\mathrm{elim}(C_0)$.

(iv) An atomic term u_1 occurs at the top of A_1.

(v) τ is contained in a minimal complete set of ACU-unifiers of u and u_1.

We define the redundancy criterion for the new inference system in such a way, that an *ODInf*-inference is redundant, if the appropriate instances of its parent *OCInf*-inference are redundant. Then a set of clauses without unshielded variables that is saturated with respect to *ODInf* up to redundancy is also saturated with respect to *OCInf* up to redundancy. *ODInf* can thus be used for effective saturation of a given set of input clauses:

Theorem 20. *Let N_0 be a set of clauses without negative inequality literals and without unshielded variables; let N_0 contain the theory axiom* Div, Inv, Nt, *and all ground instances of* Tot. *Suppose that all clauses of N_0, except the ground instances of* Tot, *are fully abstracted. Let $N_0 \vdash N_1 \vdash N_2 \vdash \ldots$ be a fair ODInf-derivation. Let N_∞ be the limit of the derivation. Then $N_0 \cup$ ODAG is unsatisfiable if and only if N_∞ contains the empty clause.*

4 Conclusions

We have presented a superposition-based calculus for first-order theorem proving in the presence of the axioms of totally ordered divisible abelian groups. It is based on the DTAG-superposition calculus from (Waldmann [10]) and the ordered chaining calculus for dense total orderings without endpoints (Bachmair and Ganzinger [3]), and it shares the essential features of these two calculi: It is refutationally complete, it does not require explicit inferences with the theory clauses, and due to the integrated variable elimination algorithm it does not require variable overlaps. It offers thus an efficient way of treating equalities and inequalities between additive terms over, e. g., the rational numbers within a first-order theorem prover.

Acknowledgments: I would like to thank the anonymous IJCAR referees for helpful comments on this paper.

References

1. Leo Bachmair and Harald Ganzinger. Associative-commutative superposition. In Nachum Dershowitz and Naomi Lindenstrauss, eds., *Conditional and Typed Rewriting Systems, 4th International Workshop, CTRS-94*, Jerusalem, Israel, July 13–15, 1994, LNCS 968, pp. 1–14. Springer-Verlag.
2. Leo Bachmair and Harald Ganzinger. Rewrite-based equational theorem proving with selection and simplification. *Journal of Logic and Computation*, 4(3):217–247, 1994.
3. Leo Bachmair and Harald Ganzinger. Ordered chaining calculi for first-order theories of transitive relations. *Journal of the ACM*, 45(6):1007–1049, November 1998.
4. Harald Ganzinger and Uwe Waldmann. Theorem proving in cancellative abelian monoids (extended abstract). In Michael A. McRobbie and John K. Slaney, eds., *Automated Deduction – CADE-13, 13th International Conference on Automated Deduction*, New Brunswick, NJ, USA, July 30–August 3, 1996, LNAI 1104, pp. 388–402. Springer-Verlag.
5. Claude Marché. Normalized rewriting: an alternative to rewriting modulo a set of equations. *Journal of Symbolic Computation*, 21(3):253–288, March 1996.
6. James R. Slagle. Automatic theorem proving with built-in theories including equality, partial ordering, and sets. *Journal of the ACM*, 19(1):120–135, January 1972.
7. Jürgen Stuber. Superposition theorem proving for abelian groups represented as integer modules. In Harald Ganzinger, ed., *Rewriting Techniques and Applications, 7th International Conference, RTA-96*, New Brunswick, NJ, USA, July 27–30, 1996, LNCS 1103, pp. 33–47. Springer-Verlag.
8. Uwe Waldmann. *Cancellative Abelian Monoids in Refutational Theorem Proving*. Dissertation, Universität des Saarlandes, Saarbrücken, Germany, 1997. `http://www.mpi-sb.mpg.de/~uwe/paper/PhD.ps.gz`.
9. Uwe Waldmann. Extending reduction orderings to ACU-compatible reduction orderings. *Information Processing Letters*, 67(1):43–49, July 16, 1998.
10. Uwe Waldmann. Superposition for divisible torsion-free abelian groups. In Claude Kirchner and Hélène Kirchner, eds., *Automated Deduction – CADE-15, 15th International Conference on Automated Deduction*, Lindau, Germany, July 5–10, 1998, LNAI 1421, pp. 144–159. Springer-Verlag.
11. Uwe Waldmann. Superposition and chaining for totally ordered divisible abelian groups. Technical Report MPI-I-2001-2-001, Max-Planck-Institut für Informatik, Saarbrücken, Germany, 2001.
12. Ulrich Wertz. First-order theorem proving modulo equations. Technical Report MPI-I-92-216, Max-Planck-Institut für Informatik, Saarbrücken, Germany, April 1992.