The Equality Relation. Paramodulation

Temur Kutsia

RISC, JKU Linz

The Equality Relation

- Equality $\approx$: A very important relation
- Reflexive
- Symmetric
- Transitive
- Substitute equals by equals
- When equality is used in a theorem, we need extra axioms which describe the properties of equality

The Equality Relation

Example 1

Theorem: Let G be a group with the binary operation $\cdot$, the inverse $^{-1}$, and the identity e. If $x \cdot x = e$ for all $x \in G$, then G is commutative.

Axioms:

1. For all $x, y \in G$, $x \cdot y \in G$.
2. For all $x, y, z \in G$, $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$.
3. For all $x \in G$, $x \cdot e \approx x$.
4. For all $x \in G$, $x \cdot x^{-1} \approx e$.

The Equality Relation

Example 1 (Cont.)

Express the axioms and the theorem in first-order logic with equality:

(A1) $\forall x, y.\ \exists z.\ x \cdot y \approx z.$

(A2) $\forall x, y, z.\ (x \cdot y) \cdot z \approx x \cdot (y \cdot z).$

(A3) $\forall x.\ x \cdot e \approx x.$

(A4) $\forall x.\ x \cdot i(x) \approx e.$

(T) $\forall x.\ x \cdot x \approx e \Rightarrow \forall u, v.\ u \cdot v \approx v \cdot u.$

The Equality Relation

Example 1 (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \approx f(x, y)$.
2. $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$.
3. $x \cdot e \approx x$.
4. $x \cdot i(x) \approx e$.
5. $x \cdot x \approx e$
6. $\neg(a \cdot b \approx b \cdot a)$.

The Equality Relation

Example 1 (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \approx f(x, y)$.
2. $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$.
3. $x \cdot e \approx x$.
4. $x \cdot i(x) \approx e$.
5. $x \cdot x \approx e$
6. $a \cdot b \not\approx b \cdot a$.

The Equality Relation

Example 1 (Cont.)

Take the conjunction of axioms and the negation of the theorem and bring it to the Skolem normal form. We obtain the set consisting of the clauses:

1. $x \cdot y \approx f(x, y)$.
2. $(x \cdot y) \cdot z \approx x \cdot (y \cdot z)$.
3. $x \cdot e \approx x$.
4. $x \cdot i(x) \approx e$.
5. $x \cdot x \approx e$
6. $a \cdot b \not\approx b \cdot a$.

Using resolution alone, we can not derive the contradiction here.

The Equality Relation

Example 1 (Cont.)

We need extra axioms to describe the properties of equality:

$$
\begin{array}{lll}
S: & x \cdot y \approx f(x, y). & x \not\approx y \vee y \not\approx z \vee x \approx z. \\
& (x \cdot y) \cdot z \approx x \cdot (y \cdot z). & x \not\approx y \vee x \not\approx u \vee y \approx u. \\
& x \cdot e \approx x. & x \not\approx y \vee u \not\approx x \vee y \approx u. \\
& x \cdot i(x) \approx e. & x \not\approx y \vee f(z, x) \approx f(z, y). \\
& x \cdot x \approx e. & x \not\approx y \vee f(x, z) \approx f(y, z). \\
& a \cdot b \not\approx b \cdot a. & x \not\approx y \vee x \cdot z \approx y \cdot z. \\
K: & x \approx x. & x \not\approx y \vee z \cdot x \approx z \cdot y. \\
& x \not\approx y \vee y \approx x. & x \not\approx y \vee i(x) \approx i(y).
\end{array}
$$

The Equality Relation

Example 1 (Cont.)

We need extra axioms to describe the properties of equality:

$$
\begin{array}{lll}
S: & x \cdot y \approx f(x,y). & x \not\approx y \lor y \not\approx z \lor x \approx z. \\
 & (x \cdot y) \cdot z \approx x \cdot (y \cdot z). & x \not\approx y \lor x \not\approx u \lor y \approx u. \\
 & x \cdot e \approx x. & x \not\approx y \lor u \not\approx x \lor y \approx u. \\
 & x \cdot i(x) \approx e. & x \not\approx y \lor f(z,x) \approx f(z,y). \\
 & x \cdot x \approx e. & x \not\approx y \lor f(x,z) \approx f(y,z). \\
 & a \cdot b \not\approx b \cdot a. & x \not\approx y \lor x \cdot z \approx y \cdot z. \\
K: & x \approx x. & x \not\approx y \lor z \cdot x \approx z \cdot y. \\
 & x \not\approx y \lor y \approx x. & x \not\approx y \lor i(x) \approx i(y).
\end{array}
$$

Unsatisfiability of this set can be proved by resolution.

The Equality Relation

The described approach has several drawbacks:

- Every time equality is used, one has to provide axioms that specify reflexive, symmetric, transitive, substitutive properties of equality.
- clumsy approach.
- Generates large search space.
- Hopelessly inefficient.

The Equality Relation

The described approach has several drawbacks:

- Every time equality is used, one has to provide axioms that specify reflexive, symmetric, transitive, substitutive properties of equality.
- clumsy approach.
- Generates large search space.
- Hopelessly inefficient.

A solution: Use a dedicated inference rule for equality.

Paramodulation

- An inference rule to handle equality, introduced by G. A. Robinson and L. Wos in 1969.
- It can replace the axioms concerning symmetric, transitive, substitutive properties of equality.
- Combined with resolution, paramodulation can be used to prove theorems involving equality.
- Simple, natural, and more efficient than the naive approach described in the previous slide.
- Still, search space can be large. Various improvements have been proposed to improve efficiency.

Unsatisfiablity Under Special Class of Models

- The set S in Example 1 is not unsatisfiable.
- However, it is unsatisfiable in all models of the set K.
- Restriction to special classes of models.

Unsatisfiablity Under Special Class of Models

Definition 1

Given:

- S: a set of clauses,
- $\mathcal{I}$: the set of all interpretations of S,
- $\mathcal{J}$: a nonempty subset of $\mathcal{I}$.

S is said to be $\mathcal{J}$-unsatisfiable if S is false in every element of $\mathcal{J}$.

Unsatisfiablity Under Special Class of Models

How can $\mathcal{J}$ be given?

- If it is finite, just list them.
- Otherwise, it is usually defined by the axioms of a theory.
- When the axioms are axioms of the equality theory, $\mathcal{J}$-unsatisfiable sets are called also $\mathcal{E}$-unsatisfiable sets.

Unsatisfiablity Under Special Class of Models

- In Example 1, $\mathcal{J}$ is all models of K.
- Since K is the set of axioms of the equality theory, the set S is $\mathcal{E}$-unsatisfiable.

$\mathcal{E}$-Interpretation

Given:

- S: A set of clauses,
- I: A Herbrand interpretation of S,
- s, t, r: Terms from the Herbrand universe of S,
- L: A literal in I.

I is called an $\mathcal{E}$-interpretation of S if it satisfies the following conditions:

1. $s \approx s \in I$;
2. if $s \approx t \in I$, then $t \approx s \in I$;
3. if $s \approx t \in I$ and $t \approx r \in I$, then $s \approx r \in I$;
4. if $s \approx t \in I$, L contains s, and L' is the result of replacing of one occurrence of s in L by t, then $L' \in I$.

$\mathcal{E}$-Interpretation

Example 2

- Let $S := \{p(a),\ \neg p(b),\ a \approx b\}$.
- Then there are 16 Herbrand interpretations of S.
- Among them the following six are $\mathcal{E}$-interpretations:

$$
\begin{array}{llllll}
\{\ \ p(a) & \ \ p(b) & a \approx a & b \approx b & a \approx b & b \approx a\} \\
\{\neg p(a) & \neg p(b) & a \approx a & b \approx b & a \approx b & b \approx a\} \\
\{\ \ p(a) & \ \ p(b) & a \approx a & b \approx b & a \not\approx b & b \not\approx a\} \\
\{\ \ p(a) & \neg p(b) & a \approx a & b \approx b & a \not\approx b & b \not\approx a\} \\
\{\neg p(a) & \ \ p(b) & a \approx a & b \approx b & a \not\approx b & b \not\approx a\} \\
\{\neg p(a) & \neg p(b) & a \approx a & b \approx b & a \not\approx b & b \not\approx a\}
\end{array}
$$

- S is satisfiable, but $\mathcal{E}$-unsatisfiable.

Towards Herbrand's Theorem for $\mathcal{E}$-Unsatisfiable Sets

Definition 3

Let S be a set of clauses. The set of the equality axioms for S is the set consisting of the following clauses:

1. $x \approx x$.
2. $x \not\approx y \vee y \approx x$.
3. $x \not\approx y \vee y \not\approx z \vee x \approx z$.
4. $x \not\approx y \vee \neg p(x_1, \ldots, x, \ldots, x_n) \vee p(x_1, \ldots, y, \ldots, x_n)$, where x and y appear in the same position i, for all $1 \leq i \leq n$, for every n-ary predicate symbol p appearing in S.
5. $x \not\approx y \vee f(x_1, \ldots, x, \ldots, x_n) \approx f(x_1, \ldots, y, \ldots, x_n)$, where x and y appear in the same position i, for all $1 \leq i \leq n$, for every n-ary function symbol f appearing in S.

Towards Herbrand's Theorem for $\mathcal{E}$-Unsatisfiable Sets

Theorem 1

Let S be a set of clauses and E be the set of equality axioms for S. Then S is $\mathcal{E}$-unsatisfiable iff $S \cup E$ is unsatisfiable.

Proof.

($\Rightarrow$) Assume by contradiction that S is $\mathcal{E}$-unsatisfiable but $S \cup E$ is satisfiable. Then $I \models S \cup E$ for some Herbrand interpretation I. Then I satisfies E. Then I satisfies the conditions of $\mathcal{E}$-interpretation. Then I is an $\mathcal{E}$-model of S.
A contradiction.

Towards Herbrand's Theorem for $\mathcal{E}$-Unsatisfiable Sets

Theorem 1 (Cont.)

Let S be a set of clauses and E be the set of equality axioms for S. Then S is $\mathcal{E}$-unsatisfiable iff $S \cup E$ is unsatisfiable.

Proof.

($\Leftarrow$) Assume by contradiction that $S \cup E$ is unsatisfiable but S is $\mathcal{E}$-satisfiable. Then $I \models S$ for some $\mathcal{E}$-interpretation I. But then I satisfies E as well. Then I satisfies $S \cup E$.
A contradiction.

□

Herbrand's Theorem for $\mathcal{E}$-Unsatisfiable Sets

Theorem 2

A finite set S of clauses is $\mathcal{E}$-unsatisfiable iff there exists a finite set S' of ground instances of clauses in S such that S' is $\mathcal{E}$-unsatisfiable.

Proof.

($\Rightarrow$) Let E be the set of equality axioms of S. By Theorem 1, $S \cup E$ is unsatisfiable. By Herbrand's theorem, there is a finite set S' of ground instances of clauses in S such that $S' \cup E$ is unsatisfiable. Hence, by Theorem 1, S' is $\mathcal{E}$-unsatisfiable.

($\Leftarrow$) Since S' is $\mathcal{E}$-unsatisfiable, every $\mathcal{E}$-interpretation falsifies S'. Then every $\mathcal{E}$-interpretation falsifies S. Hence, S is $\mathcal{E}$-unsatisfiable.

□

Paramodulation

Example 2

Consider the clauses:

C_1: $p(a)$.

C_2: $a \approx b$.

We can substitute b for a in C_1 to obtain

C_3: $p(b)$.

Paramodulation

Example 2

Consider the clauses:

C_1: $p(a)$.

C_2: $a \approx b$.

We can substitute b for a in C_1 to obtain

C_3: $p(b)$.

Paramodulation is an inference rule that extends this equality substitution rule.

Paramodulation

Example 2

Consider the clauses:

C_1: $p(a)$.

C_2: $a \approx b$.

We can substitute b for a in C_1 to obtain

C_3: $p(b)$.

Paramodulation is an inference rule that extends this equality substitution rule.

Notation: $A[t]$ for A containing a term t.
A can be a clause, a literal, or a term.

Paramodulation for Ground Clauses

Definition 4

Given:

- A ground clause $C_1 = L[s] \vee C_1'$, where $L[s]$ is a literal containing a term s, and C_1' is a clause,
- a ground clause $C_2 = s \approx t \vee C_2'$, where C_2' is a clause.

Infer the following ground clause, called a paramodulant

$$L[t] \vee C_1' \vee C_2'.$$

Paramodulation for Ground Clauses

Example 5

C_1: $p_1(a) \vee p_2(b)$

C_2: $a \approx b \vee p_3(b)$

Paramodulant of C_1 and C_2: $p_1(b) \vee p_2(b) \vee p_3(b)$.

Binary Paramodulation for General Clauses

Definition 6

Given:

- A general clause $C_1 = L[r] \vee C_1'$, where $L[r]$ is a literal containing a term r, and C_1' is a clause,
- a general clause $C_2 = s \approx t \vee C_2'$, where C_2' is a clause, C_1 and C_2 have no variables in common, and s and r have an mgu σ.

Infer the following clause, called a binary paramodulant of the parent clauses C_1 and C_2:

$$L\sigma[t\sigma] \vee C_1'\sigma \vee C_2'\sigma.$$

The literals L and $s \approx t$ are called the literals paramodulated upon. Sometimes one also says that paramodulation has been applied from C_2 into C_1.

Binary Paramodulation for General Clauses

Example 7

- C_1: $p_1(g(f(x))) \vee p_2(x)$.
- C_2: $f(g(b)) \approx a \vee p_3(g(c))$.
- An mgu of $f(x)$ and $f(g(b))$: $\sigma = \{x \mapsto g(b)\}$.
- Paramodulant of C_1 and C_2: $p_1(g(a)) \vee p_2(g(b)) \vee p_3(g(c))$.
- The literals paramodulated upon are $p_1(g(f(x)))$ and $f(g(b)) \approx a$.

Putting Things Together: The Inference system $\mathcal{RP}$

Binary Resolution: $$\frac{A \lor C \quad \neg B \lor D}{(C \lor D)\sigma}, \qquad \sigma = mgu(A, B)$$

Positive Factoring: $$\frac{A \lor B \lor C}{(A \lor C)\sigma}, \qquad \sigma = mgu(A, B)$$

Binary Paramodulation: $$\frac{s \approx t \lor C \quad L[r] \lor D}{(L[t] \lor C \lor D)\sigma}, \qquad \sigma = mgu(s, r)$$

Reflexivity Resolution: $$\frac{s \not\approx t \lor C}{C\sigma}, \qquad \sigma = mgu(s, t)$$

A, B atomic formulas, C, D clauses, L literal, s, t, r terms.

Completeness of $\mathcal{RP}$

Theorem 3

If S is an $\mathcal{E}$-unsatisfiable set of clauses, then the empty clause can be generated from S using the rules in $\mathcal{RP}$.

Resolution and Paramodulation

Example 8

$$
\begin{array}{ll}
(1) & q(a) \\
(2) & \neg q(a) \vee f(x) \approx x \\
(3) & p(x) \vee p(f(a)) \\
(4) & \neg p(x) \vee \neg p(f(x))
\end{array}
$$

Resolution and Paramodulation

Example 8

(1)	$q(a)$	
(2)	$\neg q(a) \lor f(x) \approx x$	
(3)	$p(x) \lor p(f(a))$	
(4)	$\neg p(x) \lor \neg p(f(x))$	
(5)	$f(x) \approx x$	Resolution (1,2)

Resolution and Paramodulation

Example 8

(1)	$q(a)$	
(2)	$\neg q(a) \vee f(x) \approx x$	
(3)	$p(x) \vee p(f(a))$	
(4)	$\neg p(x) \vee \neg p(f(x))$	
(5)	$f(x) \approx x$	Resolution (1,2)
(6)	$\neg p(f(f(a)))$	Resolution (factor 3,4)

Resolution and Paramodulation

Example 8

(1)	$q(a)$	
(2)	$\neg q(a) \vee f(x) \approx x$	
(3)	$p(x) \vee p(f(a))$	
(4)	$\neg p(x) \vee \neg p(f(x))$	
(5)	$f(x) \approx x$	Resolution (1,2)
(6)	$\neg p(f(f(a)))$	Resolution (factor 3,4)
(7)	$\neg p(f(a))$	Paramodulation (5,6)

Resolution and Paramodulation

Example 8

(1)	$q(a)$	
(2)	$\neg q(a) \vee f(x) \approx x$	
(3)	$p(x) \vee p(f(a))$	
(4)	$\neg p(x) \vee \neg p(f(x))$	
(5)	$f(x) \approx x$	Resolution (1,2)
(6)	$\neg p(f(f(a)))$	Resolution (factor 3,4)
(7)	$\neg p(f(a))$	Paramodulation (5,6)

Resolution and Paramodulation

Example 8

(1)	$q(a)$	
(2)	$\neg q(a) \vee f(x) \approx x$	
(3)	$p(x) \vee p(f(a))$	
(4)	$\neg p(x) \vee \neg p(f(x))$	
(5)	$f(x) \approx x$	Resolution (1,2)
(6)	$\neg p(f(f(a)))$	Resolution (factor 3,4)
(7)	$\neg p(f(a))$	Paramodulation (5,6)
(8)	$\square$	Resolution (factor 3,7)

Restriction of Paramodulation

- Unrestricted use of paramodulation can make the inference system too inefficient.
- For instance, from an equation $f(a) \approx a$ it can generate infinitely many new equations:
  $f(f(a)) \approx a,\ f(f(f(a))) \approx a, \ldots.$
- History of paramodulation-based proving: Restrict applications of the paramodulation rule.
- Important restrictions:
  - Prohibit paramodulation into a variable.
  - The use of reduction orderings.
  - The basic strategy of paramodulation.
  - Simplification.