

Tau: A Web-Deployed Hybrid Prover for First-Order Logic with Identity, with Optional Inductive Proof

Jay Halcomb, Randall R. Schulz
H&S Information Systems
<http://hsinfosystems.com>
<mailto:hsis@hsinfosystems.com>

April 29, 2005

Abstract

We outline Tau, a practical and extensible hybrid theorem prover for first-order predicate calculus with identity. Tau is flexible and user-configurable, accepts the KIF Language, is implemented in Java, and has multiple user interfaces. Tau combines rule-based problem rewriting with Model Elimination, uses Brand's Modification Method to implement identity, and accepts user-configurable heuristic search to speed the search for proofs. Tau optionally implements mathematical induction. Formulas are input and output in KIF or infix FOPC, and other external forms can be added. Tau can be operated from a Web interface or from a command-line interface. Tau is implemented entirely in Java and can run on any system for which a current Java Virtual Machine is available.

Keywords: automated theorem proving (ATP), first-order logic (FOL), hybrid prover, Knowledge Interchange Format (KIF), web-based, interactive, model elimination (ME), resolution, rewriting, Java.

1 Introduction: How Tau Works

Consider the remarks of [Bachmair and Ganzinger, 1998] in the Handbook of Automated Reasoning, "Resolution Theorem Proving":

"It has been pointed out that **a weakness of resolution is its lack of goal orientation**. Simplification and clause elimination based on redundancy helps ameliorate the problem, but one might also consider possible combinations of resolution with such goal-oriented methods as the sequent calculus or semantic tableaux. Semantic tableaux and variants thereof, including the Davis-Putnam method, model elimination and SL-resolution can be viewed as tree-like theorem proving process in which the limits of the individual branches are saturated under (ordered) resolution with selection. **This view may serve as a basis for further investigations of the combination problem.**" P. 94, Vol. 1, emphasis added.

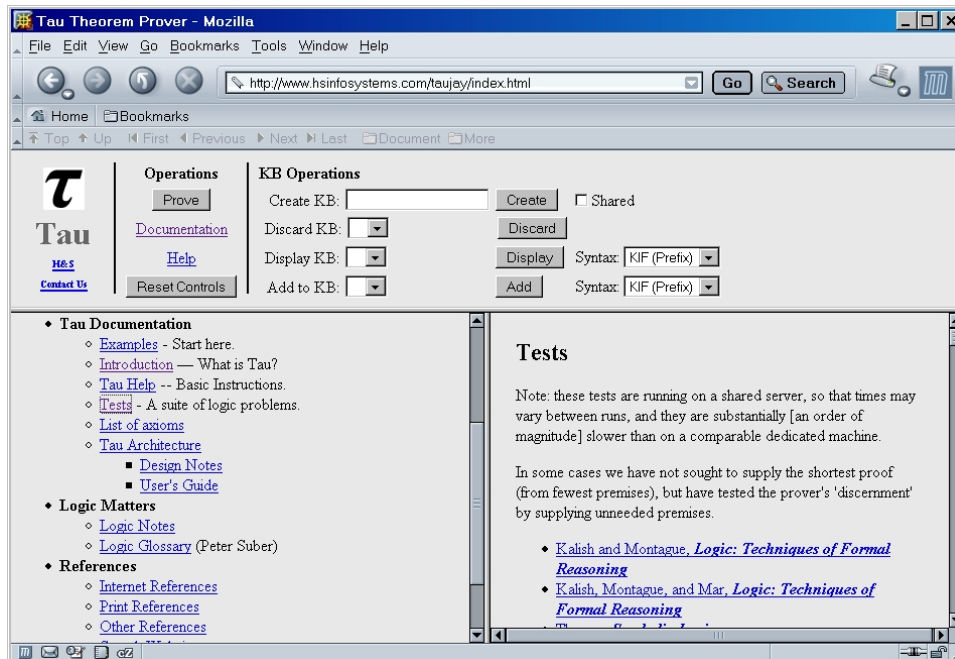


Figure 1: Initial Tau Screen

That was the spirit with which we approached the Tau project. It is perhaps as difficult to induce a computer to ‘reason logically’ as it is to induce a human to do so, but with the Tau theorem prover and knowledge base (eventually we hope Tau to be a formal theory repository), we are aiming to produce the first interactive, easy-to-use, and comprehensive prover of its kind on the Internet. Tau is sound and theoretically complete for the First Order Predicate Calculus with Identity – a phrase which can cover a multitude of sins, due to the general undecidability of FOPC. Tau’s syntax is full FOPC with sentential constants, relation symbols, function symbols, complex terms, and identity.

What you can presently do with Tau:

- Test the FOL validity of symbolic formulas
- Test the FOL validity of formal arguments (derive a conclusion from premises)
- Normalize formulas – command line interface only at this time.
- Construct a formal FOPC theory and make deductions from it. Examples already constructed are: theorems in Presburger and Peano arithmetic, both with and without mathematical induction; theorems in the theory of commutative ordered fields; theorems in graph theory.

Tau’s initial screen is shown in Figure 1. Use of Tau is quite simple: well-formed formulas of KIF can be typed or pasted into the browser window. Then (after perhaps selecting an option check box) press ‘Prove’.

| | |
|---|---|
| <p>2: To prove:</p> <pre>(<=> (forall ?X-3 (=> (F ?X-3) (H ?X-3))) (forall ?X-4 (=> (G ?X-4) (J ?X-4))))</pre> | <p>Split the equivalence, yielding:</p> <p>3:</p> <pre>(=> (forall ?X-3 (=> (F ?X-3) (H ?X-3))) (forall ?X-4 (=> (G ?X-4) (J ?X-4))))</pre> <p>4:</p> <pre>(=> (forall ?X-4 (=> (G ?X-4) (J ?X-4))) (forall ?X-3 (=> (F ?X-3) (H ?X-3))))</pre> |
|---|---|

Figure 2: An Example of Rewriting

Tau is written in the Java programming language ([Sun Microsystems]). Its Web interface uses the Tomcat servlet container ([Apache Jakarta Project]). The primary proof procedure employed by Tau is Loveland’s well-known Model Elimination algorithm ([Loveland, 1968], [Loveland, 1969], and [Loveland, 1978]) augmented with a selectable variety of search algorithms, including heuristic search guided by a user-supplied heuristic ranking function.

Prior to submission to the Model Elimination algorithm, problems are optionally subjected to a process of rewriting, in which the original conclusion is rewritten into logically equivalent formulas that are more tractable. The rewriting process is recursive in the sense that the result of a rewriting may itself be rewritten further. When the problem submitted includes use of the identity predicate, the Model Elimination prover stage applies the necessary transformations, using a variant of Brand’s Modification Method [Brand, 1975].

Tau is intended for experimentation and educational use. Tau can be used as a proof assistant and as a teaching aid.

Note: The URLs for test cases mentioned in this paper refer to a shared, commercial Internet hosting server with limited computational resources. As a result, problems run slowly there. Full performance of Tau can be witnessed on a dedicated host. Interested parties should contact the authors at their email address for access to this host. Also,

note that in some test cases we have not sought to supply the shortest proof (from fewest premises), but we have tested the prover's 'discernment' by supplying unneeded premises.

Tau proofs are based upon proof-by-contradiction using a linear restriction of resolution invented by Loveland called Model Elimination. Tau's implementation of Model Elimination also incorporates (by default) the so-called Set-of-Support restriction, in which the contradiction sought in the indirect proof must exist between the negated conclusion and the premises or within the negated conclusion itself. Tau proof displays, being based upon proof-by-contradiction using a resolution (Model Elimination) strategy, are not informative in the way a natural deduction style of presentation is. We intend later to expose in a more natural way some N.D. proof structure, and to provide further aid to using Tau as a semi-automated proof assistant. We do presently display some of the initial rewriting techniques used (see Figure 2).

Tau can prove either valid theorems or arguments. Other examples with which to try Tau are at the URLs:

- T260 <http://www.hsinfosystems.com/taujay/doc/samples/tests/T260.jsp>
- T265 <http://www.hsinfosystems.com/taujay/doc/samples/tests/T265.jsp>
- T327 <http://www.hsinfosystems.com/taujay/doc/samples/tests/T327.jsp>
- HOH <http://www.hsinfosystems.com/taujay/doc/samples/HeadOfAHorse.jsp>
- AssocAdd
<http://www.hsinfosystems.com/taujay/doc/samples/PrA.web/AssocAdd.html>

We've been using theorems from [Kalish and Montague, 1964], (through the chapter on identity) for many of our basic tests. The entire test directory (containing over 250 tests) is at:

<http://www.hsinfosystems.com/taujay/doc/samples/testsJSP.html>.

2 Tau and the KIF Language

Typical KIF looks like:

```
(<=>
  (exists ?Y
    (and
      (forall ?X (<=> (f ?X) (= ?X ?Y)))
      (g ?Y)))
  (and
    (exists ?Y
      (forall ?X (<=> (f ?X) (= ?X ?Y))))
    (forall ?X (=> (f ?X) (g ?X)))))
```

You can run a Tau proof of this theorem by clicking ‘Prove’ at:

<http://www.hsinfosystems.com/taujay/doc/samples/tests/T324.jsp>

After running that test you will see the trace of Tau’s proof of the theorem. That page will show a verbose trace of Tau’s actions in proving this theorem, displaying how the theorem was broken down into sub-proofs and how the formulas were rewritten and normalized to facilitate the proof. More concise proof display options are also available from running Tau in a command line mode.

KIF (Knowledge Interchange Format) is essentially a parenthesized prefix version of common first-order logical notation, which largely emanates from environs of Stanford University; KIF is also a part of the ISO (International Organization for Standardization) [Common Logic Standard] effort. Being a prefix form, it is efficient for many computer applications and for that reason we adopted KIF as Tau’s first internal language. Tau also has an infix syntax which is consistent with typical conventions used in ASCII computer settings. Both of these concrete syntaxes are intended for situations where no special logic symbols are available. Our architecture admits unlimited additional concrete syntaxes, including those which include proper mathematical and logical symbology such as TeX or MathML; we intend to incorporate graphical notations and I/O into Tau.

Tau accepts both a prefix version of FOL, called KIF (Knowledge Interchange Format), and a related infix form of FOL. Tau KIF is a Lisp-like, S-Expression prefix syntax based on the KIF 3 standard. Details of KIF 3 are available at the Knowledge Interchange Format home page, <http://ks1-web.stanford.edu/knowledge-sharing/kif/>. An HTML conversion of the TeX original from the preceding page is here: <http://logic.stanford.edu/kif/Hypertext/kif-manual.html>.

Variables in KIF are preceded by a ‘?’; individual constants, predicates, relations, and functions may be a single alphabetic character or a string of such. Computer generated individual constants appearing in our proofs are preceded by a ‘\$’.

For further details, please see:

- Knowledge Interchange Format (KIF) an HTML conversion of the TeX original from the preceding page <http://www-ks1.stanford.edu/knowledge-sharing/kif/>
- Knowledge Interchange Format, dpAns <http://logic.stanford.edu/kif/dpans.html>
- Knowledge Interchange Format <http://logic.stanford.edu/kif/specification.html>

3 The Logical Theory of Tau

The Tau prover is essentially an indirect prover that proves formulas by establishing the mutual unsatisfiability of the set of clauses that result from the Skolemized form of the original input problem’s formulas with the conclusion to prove first negated.

Before Skolemization, clausalization and the application of Model Elimination, the conclusion is subject to a process of rule-driven rewriting that replaces the original conclusion with other more tractable but (collectively) equivalent conclusions, each of which is proved independently. The result of any given rewriting is itself subject to rewriting.

This recursive decomposition process produces a tree of sub-proofs. Both conjunctive (all sub-proofs produced by a given rewriting must succeed) and disjunctive (only one of a rewriting's sub-proof need succeed) sub-proof combination rules are allowed. The system can optionally compute estimates of the proof complexity of each resulting sub-proof and then order the attempts to prove them so as to conclude the overall proof successfully (or fail) in the shortest time.

For some types of problems we have also implemented a direct instantiation method and an optional incremental satisfiability checker (based upon Davis-Putnam-Loveland); see [Hooker, 1993] and [Hooker, 1993a].

Tau is based on:

- normalization, (see, e.g., [Baaz et al, 2002]), and [Nonnengart and Weidenbach, 2002]
- reductio ad absurdum, or contradiction testing
- our version of Brand transformations
(see, e.g., [Brand, 1975], and [Degtyarev and Voronkov, 1999], "Equality reasoning in sequent-based calculi"), to implement identity rewriting strategies

Tau's use of a Model Elimination technique in conjunction with selection heuristics and proof strategizing helps overcome some of the difficulties resulting from a lack of goal-directedness.

Our primary emphasis is on the logical soundness of the proof method and the integrity of the software design. Principally via the command line interface we have a good deal of control and flexibility in choosing proof strategies, and over the presentations and annotations, and we are adding these options judiciously to the browser interface.

4 Algorithms

4.1 Resolution

Resolution proof was introduced in the classic papers [Robinson, 1965] and [Robinson, 1971]; the well-known [Chang and Lee, 1973] gave resolution further impetus. However, the resolution method requires considerable augmentation by efficient search techniques to be of practical use.

4.2 Model Elimination

The Model Elimination technique was introduced in [Loveland, 1968], [Loveland, 1969], and [Loveland, 1978], and is theoretically sound and complete. Interest in it was more lately revived with Stickel's work on the theorem prover PTTP, e.g. [Stickel, 1984]. Tau uses a version of Model Elimination with refinements to handle certain completeness issues which may arise from an uncareful application of search techniques; for example,

the Inoue problem (see below). In this regard, Tau also offers multiple search strategies, with selection heuristics (clausal weighting).

As with all automated theorem proving, search plays a central role. Tau's implementation of the Model Elimination procedure implements three kinds of search:

- Breadth-First Search
- Depth-First Search
- Heuristic Search
- Modified Search

In all cases, a user-specified depth-cutoff is applied.

Breadth-first search is guaranteed to find the shortest proof possible for the problem, but will typically examine far too many clauses in the process of finding that shortest proof. Breadth-first search also tends to consume excessive amounts of primary storage holding clauses at the frontier of the proof search tree.

Depth-first search requires the least amount of storage and depends strongly on the depth cutoff to prevent its becoming trapped in unbounded sub-trees of the proof tree.

Heuristic search is the default and almost always produces the best overall results. Each clause in the set of clauses produced by the conclusion and each clause (or *chain*, in Loveland's terminology) that arises by successful applications of the Model Elimination inference operations is evaluated by a user-specified *heuristic function* whose purpose is to estimate the distance from the specified clause to a successful proof (i.e., an empty clause). Pending clauses, those that occupy the current frontier of the Model Elimination proof search tree, are held in a priority queue that is ordered by the aforementioned heuristic function. At each cycle of the Model Elimination proof search, the clause with the lowest heuristic value (i.e., the one deemed closest to yielding a successful proof) is chosen for processing.

Modified search, as described in [Chang and Lee, 1973], is an option for any of the three basic proof search procedures mentioned above. Model Elimination includes three kinds of inference operation: Factorization, Reduction and Extension. Factorization and Reduction operate on single clauses, while Extension operates on pairs of clauses. Modified search differs from basic search only with respect to the pairs of clauses that participate in the Extension operation. Instead of computing all of the Extension operations possible for a given clause as a single operation, all potential Extension side (or *auxiliary*) clauses are determined and each of the resulting center-clause / side-clause Extension pairs are scheduled independently. This allows for a more refined heuristic to be computed than is possible if only the center clause is examined, because the heuristic function has access to both the center and the side clauses.

Factorization is itself optional at the user's discretion.

In most cases, modified search produces better performance than basic search.

4.3 Brand Transformations

Brand transformations are rewrites of standard clausal forms which contain identities. There is a transformation corresponding to the transitivity of identity, and one to the

symmetry of identity. These transformations were introduced in [Brand, 1975]; they are further discussed in [Degtyarev and Voronkov, 1999]. Apart from Brand’s *flattening* transform, which supplies the substitutivity of identity and is applied unconditionally to problems that include application of the identity predicate, the transitivity and symmetry properties of identity may be supplied either by introducing the pertinent axioms as additional premises or by the application of the corresponding Brand transformation.

4.4 Martelli and Montanari

Resolution theorem proving and all its derivatives and variants rely heavily on the use of unification between first-order expressions. The efficiency of the unifier bears heavily on the overall speed of the prover. In addition to the classic recursive “mesh” unification algorithm presented in many texts, papers and books, Tau implements the efficient unification algorithm discussed in [Martelli and Montanari, 1977] and in [Martelli and Montanari, 1982]. This unification algorithm treats the expressions to be unified, any number of them, as a system of simultaneous equations and solves that system. It has substantially improved typical and worst-case complexity by comparison with the classical mesh unification algorithm.

4.5 Stillman’s Subsumption Algorithm

Another time-consuming operation for resolution-based theorem provers is computing clause subsumption. In addition to the classic subsumption algorithm described in [Chang and Lee, 1973], Tau implements the better-performing subsumption algorithm invented by Stillman and described in [Gottlob and Leitsch, 1985].

5 Computational Results

The notion of an empirically successful theorem prover is difficult to define, and has a problematic history. As with human provers, it is not clear or uncontroversial exactly what to count as virtue in a prover. Is it: speed, some idea of completeness or comprehensiveness, ease of use, subtlety and originality, or some other factor, or some combination of these? In a practical sense, the idea is one of instrumental virtue, and thus relative to the various conceptions of good use of logic.

However, that may be, we shall give below some sample Tau statistics, after a discussion of some various types of problems.

5.1 Logic Theorems

There are at present 78 logical theorems available for testing in the Tau browser, derived from [Kalish and Montague, 1964] and [Montague, Kalish, and Mar, 1980].

A simple theorem which caused an incompleteness problem for some older resolution style provers was posed in [Inoue, 1992].

```
(=> (and
      (forall ?X) (or (not (Q ?X)) (P ?X) (P a))
      (not (P B))
      (Q B) )
(P a))
```

Tau handles such problems easily; a test run can be seen in Appendix 4.

The ‘Los theorem’ was considered a surprise in the early days of theorem proving, as no one seems to have thought it intuitive, and it was discovered first by a theorem prover. the theorem is:

```
(=> (and
      (forall (?X ?Y ?Z) (=> and (P ?X ?Y) (P ?Y ?Z)) (P ?X ?Z))
      (forall (?X ?Y ?Z) (=> (and (Q ?X ?Y) (Q ?Y ?Z)) (Q ?X ?Z)))
      (forall (?X ?Y) (=> (Q ?X ?Y) (Q ?Y ?X)))
      (forall (?X ?Y) (or (P ?X ?Y) (Q ?X ?Y))) )
(or (forall (?X ?Y) (P ?X ?Y)) (forall (?X ?Y) (Q ?X ?Y))))
```

Tau also handles this with dispatch; a test run can be seen in Appendix 3.

5.2 Identity Problems

As you have seen, Tau solves a variety of identity tests. However, there are two theorems involving identity from [Montague, Kalish, and Mar, 1980] which Tau has not yet been able to prove (except in simplified form) are T328 and T329:

T328

```
(forall (?A ?B ?C)
  (=>
    (and (=> (exists ?Z (forall ?X (<=> (f ?X) (= ?X ?Z)))) (f ?A))
          (=> (not (exists ?Z (forall ?X (<=> (f ?X) (= ?X ?Z)))) (= ?A ?C))
          (=> (exists ?Z (forall ?Y (<=> (f ?Y) (= ?Y ?Z)))) (f ?B))
          (=> (not (exists ?Z (forall ?Y (<=> (f ?Y) (= ?Y ?Z)))) (= ?B ?C)) )
    (= ?A ?B)))
```

T329

```
(forall (?A ?B ?C)
  (=>
    (and (=> (exists ?Y (forall ?X (<=> (f ?X) (= ?X ?Y)))) (f ?A))
          (=> (not (exists ?Y (forall ?X (<=> (f ?X) (= ?X ?Y)))) (= ?A ?C))
          (=> (exists ?Y (forall ?X (<=> (g ?X) (= ?X ?Y)))) (g ?B))
          (=> (not (exists ?Y (forall ?X (<=> (g ?X) (= ?X ?Y)))) (= ?B ?C))
          (forall ?X (<=> (f ?X) (g ?X))) )
    (= ?A ?B)))
```

For more discussion of identity handling in theorem provers, see [Bachmair and Ganzinger, 1998].

5.3 Theory of a Successor, Presburger and Peano Arithmetic

We denote the theory of a successor, Succ. It is a subtheory of Peano Arithmetic, expressed in KIF by:

```
(forall ?X (not (= 0 (succ ?X))))  
(forall ?X (forall ?Y (=> (= (succ ?X) (succ ?Y)) (= ?X ?Y))))
```

Tau tests in the theory Succ are at:

<http://www.hsinfosystems.com/taujay/doc/samples/testsJSP.html#Succ>

Presburger Arithmetic axioms (the theory PrA), is also a subtheory of Peano arithmetic, lacking multiplication; it is decidable, but already has difficult computational complexity. It is expressed in KIF by the axioms:

```
(forall ?X (not (= 0 (succ ?X))))  
(forall ?X (forall ?Y (=> (= (succ ?X) (succ ?Y)) (= ?X ?Y))))  
(forall ?X (= (+ ?X 0) ?X))  
(forall ?X (forall ?Y (= (+ ?X (succ ?Y)) (succ (+ ?X ?Y)))))
```

Tau tests in the theory PrA are at:

<http://www.hsinfosystems.com/taujay/doc/samples/testsJSP.html#Presburger>

Peano Arithmetic adds the multiplication axioms:

```
(forall ?X (forall ?Y (= (* 0 ?X) 0))  
(forall ?X (forall ?Y (= (* ?X (succ ?Y)) (+ (* ?X ?Y) ?X))))
```

Tau tests in simple Peano Arithmetic are at:

<http://www.hsinfosystems.com/taujay/doc/samples/testsJSP.html#Enderton>

and tests using induction at:

<http://www.hsinfosystems.com/taujay/doc/samples/testsJSP.html#PAI>.

Combinations and reductions of these sets of axioms (PA, PrA, and Succ), together with the introduction of definitions give us other theories. which we will denote below, while presenting some sample axioms of each theory. Each of these theories may also be extended by the use of induction. Some of the theories involve only ‘succ’, some involve addition and multiplication also. There are various courses possible with extension by definition and with axiomatization by primitives. For example, ‘<’ may be defined axiomatically in an extension of the theory Succ; alternatively, it may be defined in PrA. Tau also has sample problems which are extensions of PrA and PA: these involve various definitions of the predicates ‘even’, ‘odd’, ‘=<’, and others.

See [Enderton, 2001] for further discussion.

5.4 Mathematical Induction

Mathematical induction may be used (see the checkbox on the Tau website) in Tau (all instances of):

```
(=> (and (F 0) (forall ?X (=> (F ?X) (F (succ ?X)))) (forall ?X (F ?X))),
```

where F represents any formula with one free variable.

Note that some proofs in Peano arithmetic and Presburger arithmetic require that Tau apply mathematical induction or use results which haven been previously proved by induction, while others do not. It is a good exercise for the user or student to determine what the dependencies are.

A sample proof using induction is given in Appendix 1.

See, e.g.,: [Bundy, 2001]

5.5 Graph Theory

We have axiomatized in KIF several problems in finite graph theory. A sample can be seen in Appendix 2. These problems are over very small domains, so the universal quantifiers are equivalent to finite conjunctions of atomic sentences, and the existential quantifiers are equivalent to finite disjunction of atomic sentences. Accordingly, we have taken advantage of these equivalences to introduce corresponding proof rewrites into Tau, for such problems.

5.6 Commutative Ordered Fields

The Theory of Commutative Ordered Fields may be expressed in KIF by the axioms [Kalish and Montague, 1964]:

```
COF1:(forall (?X ?Y ?Z) (= (+ ?X (+ ?Y ?Z)) (+ (+ ?X ?Y) ?Z)))
COF2:(forall (?X ?Y) (= (+ ?X ?Y) (+ ?Y ?X)))
COF3:(forall ?X (= (+ ?X 0) ?X))
COF4:(forall ?X (= (+ ?X (neg ?X)) 0))
COF5:(forall (?X ?Y ?Z) (= (* ?X (* ?Y ?Z)) (* (* ?X ?Y) ?Z)))
COF6:(forall (?X ?Y) (= (* ?X ?Y) (* ?Y ?X)))
COF7:(forall ?X (= (* ?X 1) ?X))
COF8:(forall ?X (=> (not (= ?X 0)) (= (* ?X (recip ?X)) 1)))
COF9:(forall (?X ?Y ?Z) (= (* ?X (+ ?Y ?Z)) (+ (* ?X ?Y) (* ?X ?Z))))
COF10:(not (= 1 0))
COF11:(forall ?X (or (=< 0 ?X) (=< 0 (neg ?X))))
COF12:(forall ?X (=> (not (= ?X 0))
                    (or (not (=< 0 ?X)) (not (=< 0 (neg ?X))))))
COF13:(forall (?X ?Y) (=> (and (=< 0 ?X) (=< 0 ?Y) (=< 0 (+ ?X ?Y))))
COF14:(forall (?X ?Y) (=> (and (=< 0 ?X) (=< 0 ?Y) (=< 0 (* ?X ?Y))))
COF15:(forall (?X ?Y) (<=> (=< ?X ?Y) (=< 0 (+ ?Y (neg ?X)))))
```

The theory of commutative ordered fields has interesting relations to theoretical decidability questions, since it has as a decidable extension the theory of real numbers (first proved decidable by Tarski). With Tau, we have just begun to study proofs in COF.

5.7 Sample Statistics

Proof statistics can be calculated for each submitted problem, each sub-proof in a submitted problem, or collectively for batch runs of multiple problems. The sample statistics shown here are for a batch test suite of 233 problems. Note that the inferences

counted are complex Model Elimination inferences, including factorizations, subsumptions, reductions and extensions, not simply resolutions. Tau's speed of inference upon these problems runs from a few hundred per second up to tens of thousands per second, depending upon the logical complexity of the clausal forms, and upon the specific search mechanism invoked. The overall average for this test suite was about a thousand inferences per second.

- **Proved:** The number of problems successfully proved out of the total number of problems submitted followed by the total number of inference steps in the resulting proofs and lastly the average length of the proofs obtained over the entire test run.
- **Roots:** The number of root clauses used to prime the Model Elimination search tree. This number is greater than or equal to the number of problems attempted because each FOF in the conclusion in general produces multiple clauses, each of which must be used as a root for a Model Elimination proof search.
- **Inputs:** The total number of clauses submitted, whether they derive from conclusions to prove or from the premises.
- **Horn / Definite / Other:** Histogram of input clauses according to type. (Horn clauses have at most one positive literal, Definite clauses have exactly one literal.)
- **Root Literals:** The number of literals in the clauses used as Model Elimination proof search tree roots.
- **Side Literals:** The number of literals in clauses used as Model Elimination side or auxiliary clauses.
- **Generated:** The number of clauses produced before the proof attempt concluded, whether successfully or not.
- **Expanded:** The number of clauses processed by application of the Model Elimination inference operations.
- **Derivations:** The number of successful (new clause-producing) applications of Model Elimination inference operations.
- **Factorizations:** The number of successful applications of the Model Elimination factorization operation.
- **Reductions:** The number of successful applications of the Model Elimination reduction operation.
- **Extensions:** The number of successful applications of the Model Elimination extension operation.

Totals:

| | |
|--------------------------|---|
| Proved: | 216 of 233; 1755 inferences; 8.12 Inference/Proof |
| Elapsed Time: | 708.54 sec |
| Roots: | 977 |
| Inputs: | 8858 |
| Horn / Definite / Other: | 8101 / 6329 / 483 |
| Root Literals: | 4001 |
| Side Literals: | 30841 |
| Generated: | 320434 |
| Expanded: | 276289 |
| Derivations: | 319457 |
| Factorizations: | 1971 |
| Reductions: | 22414 |
| Extensions: | 295511 |
| Out-order: | 1.16 |
| Residual: | 1651309 |
| Too deep: | 0 |
| Unacceptable: | 30051 |
| XUnacceptable: | 1815 |
| Subsumed: | 106 |
| Vacuous: | 7542 |

6 Disproofs

Tau can in certain cases disprove theorems. A few of our tests are deliberate disproofs, as a check on soundness. These tests are positively proved invalid and are noted as such when they are run. The soundness of such disproof depends upon the prover's noticing in simple cases that it has exhausted all the possibilities for obtaining a proof by contradiction. A refinement on that which Tau uses in certain cases is to notice that a theorem has only a very small number of finite models, up to isomorphism.

7 User Interface

The browser version of Tau is implemented in HTML and CSS using a forms-based submission.

8 Next Extensions of Tau

“De l’audace, encore de l’audace, et toujours de l’audace!” - Danton

Tau is an ongoing project and its authors plan to follow several paths, including:

- Implementation of MathML notation

- Implementation of notation for the treatment of variable-binding operators in [Montague, Kalish, and Mar, 1980] (see Chapters X and XI), and of theorem schemata
- Persistent KB storage across browser sessions
- Formal language translation facilities
- Simplified English translation facilities
- Translation between systems of logic (i.e., intuitionistic and FOL)
- Formal definitions (work partially implemented)
- Implementing the use of metalogical expressions in deduction, as axiom schemata and, particularly, in forming inductive axioms (work now underway)
- Implementation of HOL and the use of theorem schemata
- Implementation of sequent style proofs (work now underway). For an introduction to, and discussion of sequent calculi, see, e.g., [Robinson and Voronkov (Eds.), 2002] or [Buss, 1998].
- TPTP testing (work now underway)
- Graphical notations

We hope that users will find Tau stimulating.

References

- [Apache Jakarta Project] The Tomcat servlet container, a product of the Apache Jakarta Project; <http://jakarta.apache.org/tomcat/index.html>.
- [Bachmair and Ganzinger, 1998] Bachmair, Leo and Harald Ganzinger. “Equational reasoning in saturation based theorem proving”, in Wolfgang Bibel and Peter H. Schmidt, editors, *Automated Deduction: A Basis for Applications. Volume I, Foundations: Calculi and Methods*, pages 353–398. Kluwer Academic Publishers, Dordrecht, 1998.
- [Baaz et al, 2002] Baaz, Matthias, Uwe and Leitsch, “Normal Form Transformations”, in Robinson and Voronkov (Eds), *Handbook of Automated Reasoning (2 vols)*, MIT Press, Cambridge, 2002.
- [Brand, 1975] Brand, Daniel. “Proving theorems with the modification method”, *SIAM Journal on Computing*, 4(4):412430, 1975.
- [Bundy, 2001] Bundy, Alan. “The Automation of Proof by Mathematical Induction”, *Handbook of Automated Reasoning 2001*: 845-911
- [Buss, 1998] Buss, Samuel R. (Ed.), *Handbook of Proof Theory*, Elsevier, New York, NY, 1998
- [Chang and Lee, 1973] Chang, C.L., and R. C. T. Lee, *Symbolic Logic and Mechanical Theorem Proving*, Academic Press, New York, 1973.
- [Common Logic Standard] Common Logic Standard, an ISO effort towards an international standard for Common Logic <http://philebus.tamu.edu/cl/>
- [Degtyarev and Voronkov, 1999] Degtyarev, Anatoli and Andrei Voronkov. “Equality reasoning in sequent-based calculi”. In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*, Elsevier Science Publishers, 1999.
- [Enderton, 2001] Enderton, Herbert B., *A Mathematical Introduction to Logic*, 2nd Ed., Harcourt Academic Press, New York, 2001
- [Gottlob and Leitsch, 1985] Gottlob, G. and L. Leitsch. “On the efficiency of subsumption algorithms”, *Journal of the ACM*, Volume 32, Issue 2, April 1985, pp. 280 - 295; <http://doi.acm.org/10.1145/3149.214118>
- [Hooker, 1993] Hooker, J.N. “Solving the incremental satisfiability problem”, *Journal of Logic Programming* 15 (1993) 177-186.
- [Hooker, 1993a] Hooker, J.N. “New methods for computing inferences in first order logic”, *Annals of Operations Research* (1993) 479-492.
- [Inoue, 1992] Inoue, K. “Linear resolution for consequence finding”, *Artificial Intelligence*, 56:301–353, 1992.

- [Loveland, 1968] Loveland, D.W. “Mechanical theorem-proving by model elimination,” *Journal of the ACM*, Volume 15, Issue 2, April 1968, pp. 236-251; <http://doi.acm.org/10.1145/321450.321456>, ACM DOI bookmark.
- [Loveland, 1969] Loveland, D.W. “A simplified format for the model elimination procedure”, *Journal of the ACM*, Vol. 15, Issue 2 1969, pp. 349-363; <http://doi.acm.org/10.1145/321526.321527>, ACM DOI bookmark.
- [Loveland, 1978] Loveland, D.W. *Automated Theorem Proving: A Logical Basis*, North-Holland, Amsterdam, 1978.
- [Martelli and Montanari, 1982] Martelli, Alberto and Ugo Montanari, “An Efficient Unification Algorithm”, *ACM Trans. Program. Lang. Syst.* 4(2): 258-282 (1982).
- [Martelli and Montanari, 1977] Martelli, A., and Montanari, U. “Theorem proving with structure sharing and efficient unification”, *Internal Rep. S-77-7*, Ist. di Scienze della Informazione, University of Pisa, Pisa, Italy; also in *Proceedings of the 5th International Joint Conference on Artificial Intelligence*, Boston, 1977, p. 543.
- [Kalish and Montague, 1964] Montague, Richard and Donald Kalish, *Logic, Techniques of Formal Reasoning*, New York, Harcourt, Brace and World, Inc., 1964.
- [Montague, Kalish, and Mar, 1980] Montague, Richard , Kalish, Donald, and Mar, Gary (Ed. Robert Fogelin), *Logic: Techniques of Formal Reasoning*, Harcourt Brace, New York, 1980.
- [Nonnengart and Weidenbach, 2002] Andreas Nonnengart, Christoph Weidenbach, “Computing Small Clause Normal Forms”, In Alan Robinson and Andrei Voronkov, editors, *Handbook of Automated Reasoning*. Elsevier Science Publishers, 1999.
- [Robinson, 1965] Robinson, J.A. “A machine-oriented logic based on the resolution principle”, *Jour. Assoc. for Comput. Mach.*, 1965, 23-41.
- [Robinson, 1971] Robinson, J.A., “Computational logic: The unification computation”, In *Machine Intelligence*, vol. 6, B. Meltzer and D. Michie (Eds.). Edinburgh Univ. Press, Edinburgh, Scotland, 1971, pp. 63-72.
- [Robinson and Voronkov (Eds.), 2002] Robinson and Voronkov (Eds), *Handbook of Automated Reasoning (2 vols)*, MIT Press, Cambridge, 2002.
- [Sun Microsystems] <http://java.sun.com/>.
- [Stickel, 1984] Stickel, M.E., “A Prolog technology theorem prover”, *New Generation Computing*, 1984, 371-383.

Appendix 1: Proof PrA02Ind, a problem using mathematical induction

Show:

```
(forall ?X
 (= (+ ?X 0) (+ 0 ?X)))
```

Given:

1. (forall ?X
 (not (= 0 (succ ?X))))
2. (forall ?X
 (forall ?Y
 (>=>
 (= (succ ?X) (succ ?Y))
 (= ?X ?Y))))
3. (forall ?X
 (forall ?Y
 (<=>
 (= (succ ?X) (succ ?Y))
 (= ?X ?Y))))
4. (forall ?X
 (= (+ ?X 0) ?X))
5. (forall ?X
 (forall ?Y
 (= (+ ?X (succ ?Y)) (succ (+ ?X ?Y)))))
6. (forall ?X
 (forall ?Y
 (<=>
 (= (+ ?X 0) ?Y)
 (= ?X ?Y))))
7. (forall ?X
 (forall ?Y
 (forall ?Z
 (<=>
 (= (+ ?X (succ ?Y)) ?Z)
 (= (+ (+ ?X ?Y) (succ 0)) ?Z))))))
8. (forall ?X
 (forall ?Y
 (>=>
 (= ?X ?Y)
 (= (succ ?X) (succ ?Y))))
9. (forall ?X
 (= (+ 0 ?X) ?X))

Proof Trace

| Proof Steps 1 2 3 | |
|--|--|
| 1: To prove: (forall ?X (= (+ ?X 0) (+ 0 ?X))) | Apply Mathematical Induction and prove both: 2: (= (+ 0 0) (+ 0 0)) 3: (= (+ (succ \$MVI-1) 0) (+ 0 (succ \$MVI-1))) |
| 2: Using the Model Elimination prover, Show: (= (+ 0 0) (+ 0 0)) The Model Elimination proof succeeded. Proved in 0 ME inference steps creating 0 clauses taking 0 seconds. | |
| 3: Using the Model Elimination prover, Show: (= (+ (succ \$MVI-1) 0) (+ 0 (succ \$MVI-1))) Given: • (= (+ \$MVI-1 0) (+ 0 \$MVI-1)) The Model Elimination proof succeeded. Proved in 3 ME inference steps creating 195 clauses taking 0.24 seconds. | |
| Conclusion Proved creating 195 clauses taking 0.24 seconds. | |
| Proof Steps 1 2 3 | |
| Result: proved | |

Appendix 2: Proof GM08d, a problem in Graph Theory

Show:

```
(or
 (forall ?Z
  (or
   (P ?Z)
   (and
    (not (R ?Z a))
    (not (R b ?Z))))))
 (forall ?Z
  (or
   (P ?Z)
   (and
    (not (R ?Z b))
    (not (R a ?Z))))))
```

Given:

1. (forall ?X
 (forall ?Y
 (forall ?Z
 (=>
 (and
 (R ?X ?Y)
 (R ?X ?Z))
 (= ?Y ?Z))))))
2. (forall ?X
 (forall ?Y
 (forall ?Z
 (=>
 (and
 (R ?Y ?X)
 (R ?Z ?X))
 (= ?Y ?Z))))))
3. (forall ?X
 (not (R ?X ?X)))
4. (R a b)
5. (R b c)
6. (R c d)
7. (R d a)
8. (P a)
9. (P b)
10. (not (P c))
11. (not (P d))
12. (not (= a b))
13. (not (= a c))
14. (not (= a d))
15. (not (= b c))
16. (not (= b d))
17. (not (= c d))

Proof Trace

| |
|--|
| Proof Steps <u>1</u> |
| 1: Using the Model Elimination prover, Show: <pre>(or (forall ?Z (or (P ?Z) (and (not (R ?Z a)) (not (R b ?Z)))))) (forall ?Z (or (P ?Z) (and (not (R ?Z b)) (not (R a ?Z))))))</pre> |
| The Model Elimination proof succeeded. Proved in 8 ME inference steps creating 1,264 clauses taking 0.621 seconds. |
| Conclusion Proved creating 1,264 clauses taking 0.621 seconds. |
| Proof Steps <u>1</u> |
| Result: proved |

Appendix 3: Argument Los001

Show:

```
(or
 (forall ?X
  (forall ?Y
   (P ?X ?Y)))
 (forall ?X
  (forall ?Y
   (Q ?X ?Y))))
```

Given:

```
1. (forall ?X
   (forall ?Y
    (forall ?Z
     (=>
      (and
       (P ?X ?Y)
       (P ?Y ?Z))
      (P ?X ?Z)))))
```

```
2. (forall ?X
   (forall ?Y
    (forall ?Z
     (=>
      (and
       (Q ?X ?Y)
       (Q ?Y ?Z))
      (Q ?X ?Z)))))
```

```
3. (forall ?X
   (forall ?Y
    (=>
     (Q ?X ?Y)
     (Q ?Y ?X))))
```

```
4. (forall ?X
   (forall ?Y
    (or
     (P ?X ?Y)
     (Q ?X ?Y))))
```

Proof Trace

| |
|--|
| Proof Steps 1 |
| 1: Using the Model Elimination prover, Show: <pre>(or (forall ?X (forall ?Y (P ?X ?Y))) (forall ?X (forall ?Y (Q ?X ?Y))))</pre> |
| The Model Elimination proof succeeded. Proved in 19 ME inference steps creating 391 clauses taking 0.735 seconds. |
| Conclusion Proved creating 391 clauses taking 0.735 seconds. |
| Proof Steps 1 |

Result: proved

Appendix 4: Inoue001

Show:

(P a)

Given:

1. (or
 (not (Q ?X))
 (P ?X)
 (P a))
2. (not (P B))
3. (Q B)

Proof Trace

| |
|--|
| Proof Steps 1 |
| 1: Using the Model Elimination prover, Show: (P a) |
| The Model Elimination proof succeeded. Proved in 3 ME inference steps creating 5 clauses taking 0.004 seconds. |
| Conclusion Proved creating 5 clauses taking 0.004 seconds. |
| Proof Steps 1 |

Result: proved