A Summary of New Results in Mathematics Obtained with Argonne's Automated Deduction Software

This page covers work up through 1995.

The results were obtained with various programs associated with Argonne's automated reasoning effort.

- The NIUTP/AURA series of the 1970s and early 1980s
- LMA/ITP of the 1980s
- Otter, our current prover
- EQP, an experimental AC prover for equational logic
- MACE, a model searcher

In all cases, the results were unknown (as far as we know) before the work, and one of the programs was used in a substantial way. The degree of contribution by the programs ranges from providing insight for a hand proof to finding a proof with no guidance from the user.

Contents

Algebraic Geometry

This section contains results obtained with Otter's implementation of Padmanabhan's inference rule `=(gL)=>'. This inference rule allows one to prove, within first-order equational logic, theorems about nonsingular cubic curves in the projective plane.

R. Padmanabhan and W. McCune, ``Automated Reasoning about Cubic Curves", *Computers and Mathematics with Applications* 29(2), 17-26 (1995).

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Cancellative Semigroups on a Cubic Curve

THEOREM (Otter). A cancellative semigroup operation on a cubic curve must be commutative.

In fact, Otter showed that associativity can be replaced with the (weaker) pair of equations $\{x(yx)=(xy)x,\ x(xy)=(xx)y\}$, or with any of several weaker forms of associativity such as $x(y(zu)) = ((xy)z)u$.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Uniqueness of the 5-ary Steiner Law

THEOREM (Otter). Given an inflection point e on a cubic curve G, there cannot be two distint 5-ary Steiner laws, both admitting e as an idempotent, defined on G. We state this formally as follows. Given the identities S=

$f(e,e,e,e,e)=e,\ f(f(x,y,e,e,e),y,e,e,e) = x,$ f is symmetric,
$g(e,e,e,e,e)=e,\ g(g(x,y,e,e,e),y,e,e,e) = x,$ g is symmetric

(symmetry means that the arguments can be permuted in any way). Then S =(gL)=> $f(x,y,z,u,v) = g(x,y,z,u,v)$.

A corollary of this theorem is the following. Consider the conic determined by 5 points on a cubic curve. Then the sixth point of intersection can be obtained by a simple ruler construction.

R. Padmanabhan and W. McCune, ``An Equational Characterization of the Conic Construction on Cubic Curves", preprint MCS-P517-0595, Argonne National Laboratory, 1995.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Cancellative Semigroups

A long-standing conjecture of Padmanabhan is the following. Let $A = \{a1,a2,...,an\}$ and $\{a\}$ be identities in the language of one binary operation. If A => a (modulo group theory), then A => a in cancellative semigroups as well. For example, in group theory, we can easily show

$\{xyzyx=yxzxy\}$ => $\{xyyx=yxxy\}$

by letting z be the identity. The statement holds also for cancellative semigroups, but the proof is more difficult.

In working on the conjecture and searching for a counterexample, we have used Otter to generalize many theorems in group theory to cancellative semigroups, for example,

$\{x\ y^3 = y^3\ x\}$ => $\{(xy)^9 = x^9\ y^9\}$, and
$\{xyyyxy = yyyyxx\}$ => $\{yxyyyx = xxyyyy\}$.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Lattice Theory

A Simpler Absorptive Basis for Lattice Theory

An absorption equality has a variable on one size of the equality symbol and a term with at least one other variable on the other side. An absorptive axiomatization consists entirely of absorption equalities. The simplest previously known absorptive axiomatization of lattice theory (in terms of meet and join) was Ralph McKenzie's:

L1. *(y join (x meet (y meet z))) = y*
L2. *(y meet (x join (y join z))) = y*
L3. *(((x meet y) join (y meet z)) join y) = y*
L4. *(((x join y) meet (y join z)) meet y) = y*

By examining many candidate sets with Otter, we found an alternative axiomatization in which the pair L1 and L4 are replaced with

L4'. *(((y join x) meet (y join z)) meet y) = y*.

W. McCune and R. Padmanabhan, ``Single Identities for Lattice Theory and for Weakly Associative Lattices", Algebra Universalis, to appear (preprint MCS-P493-0395).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

A New Schema for Single Axioms

Padmanabhan has a schema that can be used to build a single axiom for any theory that (1) admits a majority polynomial satisfying $p(x,y,y)=p(y,x,y)=p(y,y,x)=y$ and (2) can be axiomatized with absorption identities. The challenge was to find schemata that produce simpler axioms. With Otter, we built a large set of candidates, and with each, we ran an Otter search trying to prove it to be an acceptable schema. We discovered several schemata that produce simpler single axioms, including the following,

$p(p(x,y,y),p(x,p(y,z,F(y)),G(y)),u)=y$,

where $F(y)$ and $G(y)$ are to be replaced with absorption identities.

W. McCune and R. Padmanabhan, ``Single Identities for Lattice Theory and for Weakly Associative Lattices'', Algebra Universalis, to appear (preprint MCS-P493-0395).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

A Shorter Single Axiom for Lattice Theory

Padmanabhan's schema and McKenzie's absorptive basis for lattice theory (see the two preceding sections) produce an axiom with 7 variables and length 355. The new schema (preceding sections), a slightly different majority polynomial, and a new technique that relies on properties of the polynomial, allowing a weaker absorptive basis, produce an axiom of length 79 (also with 7 variables).

W. McCune and R. Padmanabhan, ``Single Identities for Lattice Theory and for Weakly Associative Lattices'', Algebra Universalis, to appear (preprint MCS-P493-0395).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

A Single Axiom for Weakly Associative Lattices

An absorption basis was found for weakly associative lattices (WAL) by giving many conjectures to Otter. With that basis, a single axiom was constructed using a majority reduction schema (similar to the lattice theory case above). The axiom has 6 variables and length 75. Similarly, a single axiom schema was found for all equational subvarieties of WAL.

W. McCune and R. Padmanabhan, ``Single Identities for Lattice Theory and for Weakly Associative Lattices'', Algebra Universalis, to appear (preprint MCS-P493-0395).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Quasilattice Theory

A *regular* identity has the same set of variables on each side of the equality symbol. Quasilattices satisfy the set of regular identities of lattice theory (and not necessarily, for example, *x meet (x join y) = x*).

With Otter, several results in lattice theory were proved for quasilattices:

- A distributive law implies its dual.
- Bowden's inequality, *x join (y meet z) >= (x join y) meet z*, implies distributivity.
- Self-dual forms of distributivity and modularity.

These theorems were previously known by model theoretic arguments; Otter's proofs are the first known equational proofs.

With MACE, a theorem in lattice theory was shown to fail for quasilattices:

- A quasilattice (but not a lattice) can have two distinct meet (dually, join) operations.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Uniqueness of Operations in Lattice-like Algebras

It was previously known that there does not exist a lattice with two distinct meet (dually join) operations. We found that

- (MACE) a quasilattice *can* have two meets;
- (Otter) a weakly associative lattice *cannot* have two meets;
- (MACE) a ternary near lattice *can* have two meets.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Self-dual Bases for Boolean Algebra

(Here, by duality we mean the ordinary meet-join duality.) Several independent self-dual 2- and 3- bases were found for Boolean algebra. These consist of big equations, because they were found with reduction schemas. We conjectured various combinations until Otter found appropriate proofs.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Self-dual 2-Basis for Group Theory

Is there an independent self-dual axiomatization, of size 2, for group theory in terms of product and inverse?

Here, a set *S* of equalities is self-dual if for each equality *E* in *S*, its mirror image *d(E)* is also in *S*. Size 2 was the only open case. A large set of candidate pairs was enumerated, and Otter answered *yes* by proving that the following pair axiomatizes groups.

((x y) z) (y z)' = x
(z y)' (z (y x)) = x

The analogous question for Abelian groups was also open, and Otter answered that question positively as well, with the following pair.

(z (x y)) (y z)' = x
(z y)' ((y x) z) = x

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Self-dual Bases for Group Varieties

Theorem. Let *E* be an equational subvariety of group theory. then there exists an independent self-dual *n*-basis for *E*, for *n*>1.

We conjectured various schemas, Otter proved cases *n*=2,3,4, and the rest was by hand (with induction).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear. (cases 2,3,4).

The full proof will be published separately.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Quasigroup Theory

We have several new results on consequences of (and relationships between) the Thomsen closure condition (TC), the Reidemeister closure condition (RC) and Padmanabhan's overlay condition. [[Get most significant examples from RP.]]

These proofs were obtained by Otter (without our guidance).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Quasigroup Design Problems

Several open questions on the existence of finite quasigroups were answered with the model searcher MACE. The questions were about Mendelsohn triple systems and self-orthogonal Latin squares. See the MACE quasigroup page for details.

W. McCune, ``A Davis-Putnam Program and Its Application to Finite First-Order Model Search: Quasigroup Existence Problems", Tech. Memo. ANL/MCS-TM-194, Argonne National Laboratory, 1994.

mccune@mcs.anl.gov

Single Axioms for Ternary Boolean Algebra

A single axiom for TBA (see standard axioms) was easily found (by hand) using a previous method of Padmanabhan; it has length 34. The challenge was to find a simpler one. We used Otter to generate about 1000 consequences of Padmanabhan's axiom, then ran an Otter search with each consequence, trying to prove Padmanabhan's axiom. Several single axioms of length 26 were discovered. As far as we know, these are the shortest single axioms for Boolean algebra using any set of operations.

R. Padmanabhan and W. McCune, ``Single Identities for Ternary Boolean Algebras", *Computers and Mathematics with Applications* 29(2), 13-16 (1995).

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Single Axioms for Groups

Ordinary Groups

Group theory can be axiomatized with different sets of operations, but there is not always a single axiom for a given set of operations (e.g., product, inverse, and identity). Our goal was to find simple single axioms for several sets suggested by B. H. Neumann. By examining large sets of candidate equalities, Otter proved that each of the following is a single axiom for group theory. In each case, it is either shorter than previously known axioms or the first known single axiom.

Product and inverse: $(x(y(((zz')(uy)')x))') = u$
Division and identity: $((e / (x / (y / (((x / x) / x) / z)))) / z) = y$
Division and inverse: $((x / x) / (y / ((z / (u / y)) / u'))) = z$
Double inversion and identity: $((x \# (((x \# y) \# z) \# (y \# e))) \# (e \# e)) = z$
Double inversion and inverse: $(x' \# ((x \# (y \# z))' \# (u \# (y \# u)))') = z$

Ken Kunen showed later that no axiom in terms of product and inverse is shorter than the one given above.

W. McCune, ``Single Axioms for Groups and Abelian Groups with Various Operations", *J. Automated Reasoning* 10(1), 1-13 (1993).

mccune@mcs.anl.gov

Abelian Groups

This work and the results are analogous to the case of ordinary groups summarized in the preceding section. As above, each of the following is either shorter than previously known axioms or the first known.

Product and inverse: *(((xy)z)(xz)')=y*
Division and identity: *((e / (((x / y) / z) / x)) / z) = y*
Division and inverse: *((x / (y / (x / z))') / z) = y*
Double inversion and identity: *((x # ((z # (x # y)) # (e # y))) # (e # e)) = z*
Double inversion and inverse: *(x # (((x # y) # z')' # y)') = z*

W. McCune, ``Single Axioms for Groups and Abelian Groups with Various Operations'', *J. Automated Reasoning* 10(1), 1-13 (1993).

mccune@mcs.anl.gov

Exponent Groups

A group of exponent *n* satisfies *x^n=e* (the identity element); such theories can be axiomatized with product alone. With Otter, we found single axioms for *n=3,5,7*, then noticed a pattern in the form of the axioms and in the proofs, then proved (by hand) that the pattern works for all odd *n*. We also found a pattern, in terms of product and identity, for odd exponents. Examples (terms are right associated):

xx(xxxyzzzz)z=y [exponent 5]
xxx(xxxxyzzzzzz)z=y [exponent 7]
xx(xx(xy)z)ezzzz=y [exponent 5, with e]
xxx(xxx(xy)z)ezzzzzz=y [exponent 7, with e]

We found that even exponents are much more difficult.

W. McCune and L. Wos, ``Application of Automated Deduction to the Search for Single Axioms for Exponent Groups'', *Proc. of LPAR*, Springer-Verlag LNCS #624, 131-136 (1992).

mccune@mcs.anl.gov, wos@mcs.anl.gov

Some Permutative Varieties

The goal was to find short single axioms for several types of permutative group. (By a result of B. H. Neumann, single axioms for the varieties in question can be constructed, but they are large.) By running Otter proof searches with large numbers of candidates, single axioms were discovered for several varieties:

xxy=yxx groups: *((xy')'((zz)(xu)))(u(zz))'=y*

xxyy=yyxx groups: *(((x(x(yy)))z)'u)(((y(y(xx)))(zv))'u)'=v*

From the second of these, Ken Kunen later derived a schema, much simpler than Neumann's, for building single axioms for varieties of groups.

Not published.

mccune@mcs.anl.gov

Ordinary Groups (Kunen)

K. Kunen, ``Single Axioms for Groups'', *J. Automated Reasoning* 9(3), 291-308 (1992).

ABSTRACT. We study equations of the form *(alpha = x)* which are single axioms for group theory. Earlier examples of such were found by Neumann and McCune. We prove some lower bounds on the complexity of these *alpha*, showing that McCune's examples are the shortest possible. We also show that no such *alpha* can have only two distinct variables. We do produce an *alpha* with only three distinct variables, refuting a conjecture of Neumann. Automated reasoning techniques are used both positively (searching for and verifying single axioms) and negatively (proving that various candidate *(alpha = x)* hold in some non-group and are hence not single axioms).

kunen@cs.wisc.edu

Groups of Exponent 4 (Kunen)

K. Kunen, ``The Shortest Single Axioms for Groups of Exponent 4", *Computers and Mathematics with Applications* 29(2), ??-?? (1995).

ABSTRACT. We study equations of the form *(alpha = x)* which are single axioms for groups of exponent 4, where *alpha* is a term in product only. Every such *alpha* must have at least nine variable occurrences, and there are exactly three such *alpha* of this size, up to variable renaming and mirroring. These terms were found by an exhaustive search through all terms of this form. Automated techniques were used in two ways: to eliminate many *alpha* by verifying that *(alpha = x)* is true in some non-group, and to verify that the group axioms do indeed follow from the successful *(alpha = x)*. We also present an improvement on Neumann's scheme for single axioms for varieties of groups.

kunen@cs.wisc.edu

Odd Exponent Groups (Hart and Kunen)

J. Hart and K. Kunen, ``Single Axioms for Odd Exponent Groups", *J. Automated Reasoning* 14(3), 383--412 (1995).

ABSTRACT. With the aid of automated reasoning techniques, we show that all previously known short single axioms for odd exponent groups are special cases of one general schema. We also demonstrate how to convert the proofs generated by an automated reasoning system into proofs understandable by a human.

jhart@math.wisc.edu, kunen@cs.wisc.edu

Simple Bases for Moufang Loops

Several simple axiomatizations were discovered (Otter) for Moufang loops, for example:

1x = x
x'x = 1
((xy)z)y = x(y(zy)) % Moufang-2

It was also found that Moufang-2 can be replaced with Moufang-3 (Otter), but not with Moufang-1 (MACE).

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Single Axioms for Inverse Loops and Subvarieties

A single axiom, in terms of product and inverse, was discovered for inverse loops:

$x((((xy')y)'z)(u'u)) = z$. % 2158

This was then generalized to a schema for equational subvarieties of inverse loops:

$x((((xy')y)'z)((\mathit{alpha}\ u)'(\mathit{beta}\ u))) = z$.

The terms *alpha* and *beta* specify the subvariety of interest. This gives us single axioms for Moufang loops, groups, Abelian groups, etc.

W. McCune and R. Padmanabhan, *Automated Deduction in Equational Logic and Cubic Curves*, Springer-Verlag LNAI, to appear.

mccune@mcs.anl.gov, padman@cc.umanitoba.ca

Left Group and Right Group Calculi

Group theory can be axiomatized without equality, using the division operation, with instantiation and the detachment rule:

If x/y is 1 and y is 1, then x is 1.

This is the left group calculus (for the right calculus, change x/y to y/x). No single axioms were previously known. Large sets (tens of thousands) of candidates were constructed, and an Otter search was run on each candidate, trying to show it to be a single axiom. Single axioms for each of the calculi were discovered, for example,

$(((x/y)/z)/((u/v)/(((w/v)/(w/u))/s)))/(z/((y/x)/s))$ [left],
$x/(x/((y/z)/((y/u)/(z/u))))$ [right].

W. McCune, ``Single Axioms for the Left Group and Right Group Calculi", *Notre Dame J. Formal Logic* 34(1), 132-139 (1993).

W. McCune, ``Automated Discovery of New Axiomatizations of the Left Group and Right Group Calculi", *J. Automated Reasoning* 9(1), 1-24 (1992).

mccune@mcs.anl.gov

Fixed Point Combinators

These problems focus on whether particular fragments of combinatory logic satisfy the weak or strong fixed point properties.

Weak -- all x exists y, $xy=y$ [every combinator has a fixed point].

Strong -- exists Q all x, $x(Qx) = Qx$ [Q is a fixed-point-finder].

Many fragments were shown (directly, with Otter) to satisfy the weak property or both of the properties, and many fragments and classes of fragments were shown (automatically with MACE, or by hand, with insight from failed Otter searches) to fail the strong property or both of the properties.

A specialized technique, the *kernel strategy*, was developed to search for fixed point combinators; many new results were obtained by using the strategy with Otter. (An important question that remains open is whether the fragment {*M,B*} satisfies the strong property.)

W. McCune and L. Wos, ``The Absence and the Presence of Fixed Point Combinators", *Theoretical Computer Science* 87, 221-228 (1991).

L. Wos ``The Kernel Strategy and Its Use for the Study of Combinatory Logic", *J. Automated Reasoning* 10(3), 287-343 (1993).

{mccune,wos}@mcs.anl.gov

Semigroup Structure (F3B2)

[[Get abstract from Lusk.]]

E. Lusk and R. McFadden.

lusk@mcs.anl.gov, rbmcfa01@ulkyvm.louisville.edu

Illative Combinatory Logic (Jech)

T. Jech, ``OTTER Experiments in a System of Combinatory Logic", *J. Automated Reasoning* 14(3), 413--426 (1995).

ABSTRACT. This paper describes some experiments involving the automated theorem-proving program Otter in the system TRC of illative combinatory logic. We show how Otter can be steered to find a contradiction in an inconsistent variant of TRC, and present some experimentally discovered identities in TRC.

jech@math.psu.edu

Robbins Algebra and Boolean Algebra

The Robbins problem has been solved. See the *Robbins Algebra Page*.

{swinker,wos,mccune}@mcs.anl.gov

Equivalential Calculus Single Axioms

Exactly seven length-11 theorems of the equivalential calculus (EC) were unclassified in regard to their being single axioms for EC. Two were shown to be single axioms by using the theorem prover AURA. Four were shown to be too weak to be single axioms; in these cases, the proofs were produced mostly by hand using insight gained from failed attempts at automated proofs.

L. Wos, S. Winker, R. Veroff, B. Smith, and L. Henschen, ``Questions Concerning Possible Shortest Single Axioms in Equivalential Calculus: An Application of Automated Theorem Proving to Infinite Domains", *Notre*

Dame J. Formal Logic 24(2), 205-223 (1983).

{wos,swinker}@mcs.anl.gov, veroff@cs.unm.edu

Semigroups, Antiautomorphisms, and Involutions

Does there exist a finite semigroup admitting a nontrivial antiautomorphism but no nontrivial involution?

The answer was shown to be *yes* by using one of the NIUTP/AURA theorem provers in nonstandard ways to search for models. Four models of order 7 were found, and it was shown that there are no others of size less than or equal to 7.

S. Winker, L. Wos, and E. Lusk, ``Semigroups, Antiautomorphisms, and Involutions: A Computer Solution to an Open Problem, I'', *Math. of Comp.* 37, 533-545 (1981).

{swinker,wos,lusk}@mcs.anl.gov

Independence of Ternary Boolean Algebra Axioms

The Grau axioms for ternary Boolean algebra (TBA) are

(1) *f(f(v,w,x),y,f(v,w,z)) = f(v,w,f(x,y,z))*
(2) *f(y,x,x) = x*
(3) *f(x,y,g(y)) = x*
(4) *f(x,x,y) = x*
(5) *f(g(y),y,x) = x*

It was previously known that (4) and (5) together are dependent on (1), (2), and (3). Using one of the NIUTP/AURA theorem provers in a nonstandard way to search for models, it was shown that each of (1), (2), and (3) is independent of the remaining four axioms.

S. Winker, ``Generation and Verification of Finite Models and Counterexamples Using an Automated Theorem Prover Answering Two Open Questions'', *J. ACM* 29, 273-284 (1982).

swinker@mcs.anl.gov

Two-valued Sentential Calculus

This area of logic was studied by using the Lukasiewicz axiom system

i(i(x,y),i(i(y,z),i(x,z)))
i(i(n(x),x),x)
i(x,i(n(x),y))

with the inference rule condensed detachment. A new axiom system was found with OTTER, consisting of theses 19, 37, and 60.

Other axiom systems had already been known, due to Church, Frege, Hilbert, and (an alternate of) Lukasiewicz. With a methodology relying on a variety of strategies, shorter proofs of the various axiom systems were found, using as hypothesis the three listed Lukasiewicz axioms.

L. Wos, ``Automated Reasoning and Bledsoe's Dream for the Field", *Automated Reasoning: Essays in Honor of Woody Bledsoe*, ed. R. S. Boyer, Kluwer Academic Publishers: Dordrecht, 1991.

wos@mcs.anl.gov

Many-valued Sentential Calculus

This area of logic can be axiomatized by using the four formulas

i(x,i(y,x))
i(i(x,y),i(i(y,z),i(x,z)))
i(i(i(x,y),y),i(i(y,x),x))
i(i(n(x),n(y)),i(y,x)

with the inference rule condensed detachment. The following formula, once thought by Lukasiewicz to be required as an axiom, is in fact dependent.

i(i(i(x,y),i(y,x)),i(y,x))

Otter was used to find the first unguided proof of this fact with condensed detachment as the inference rule. Further, Otter eventually was used to find a 34-step proof of this fact, a proof far shorter than previously known, and a proof in which no terms of the form *n(n(t))* are present, also conjectured to be unobtainable.

L. Wos, *The Automation of Reasoning: An Experimenter's Notebook with Otter Tutorial*, Academic Press, to appear.

wos@mcs.anl.gov

Short Proofs in Various Logic Calculi

For the two equivalential calculus single axioms XHK and XHN, far shorter proofs were obtained. Specifically, Winker's proof that XHN is a single axiom has length 159, and his proof for XHK has length 84. With the hot list strategy, OTTER produced proofs of respective lengths 24 and 27. The hot list strategy asks the researcher to choose clauses that are then included in the input and immediately visited with each newly-retained clause, thus rearranging sharply the order in which conclusions are drawn. A powerful variant of this strategy is the dynamic hot list strategy, which enables the program, based on a user-assigned threshold, to adjoin during the run new clauses to the hot list.

L. Wos, ``The Power of Combining Reasonance with Heat", *J. Automated Reasoning*, to appear (preprint P522.ps.Z).

wos@mcs.anl.gov

Pure Proofs in Equivalential Calculus

For the entire set of thirteen shortest single axioms for EC, a circle of pure proofs was produced with Otter. A circle of pure proofs for a set of *k* equivalent properties or definitions consists of *k* proofs such that (regarding the circle aspect) the first proves the second property or definition from the first, the second proof proves the third from the second, ..., the *k*-th proves the first from the *k*-th, and such that (regarding the pure aspect) for all *i* from 1 to *k* the *i*-th proof does not rely on any of the *k* properties or definitions other than the *i*-th and *i*+1st. To obtain the circle of thirteen pure proofs, Otter relied on a variety of strategies, including the dynamic hot list strategy.

L. Wos, ``Searching for Circles of Pure Proofs", *J. Automated Reasoning* 15, pp. 279-315, 1995 (preprint P479.ps.Z).

wos@mcs.anl.gov

These activities are projects of the Mathematics and Computer Science Division of Argonne National Laboratory.