Some Recent Results in Algebra & Logical Calculi Obtained Using Automated Reasoning

Branden Fitelson

Department of Philosophy
San José State University

Automated Reasoning Group
Mathematics & Computer Science Division
Argonne National Laboratory
http://www-unix.mcs.anl.gov/AR/

March 21, 2003

Results reported here are either the result of joint work, or the work of others associated with AR @ MCS @ ANL: Larry Wos, Bill McCune, Ken Kunen, Steve Winker, Bob Veroff, Ken Harris, Zac Ernst, John Slaney, Ted Ulrich, Bob Meyer, R. Padmanabhan et al.

Overview of Presentation

- Simple Equational Bases for Boolean Algebra
  - In the connectives + (disjunction) and \( n \) (negation)
  - In the connective \( \neg \) (Sheffer Stroke)
  - Pointers to recent work in other algebraic systems
- Simple Axiomatizations of Classical Propositional Logics
  - Classical Propositional Logic (in two sets of connectives)
  - Equivalential Fragment of Classical Propositional Logic
- Simple Axiomatizations of Non-Classical Propositional Logics
  - Strict Implicational fragments of modal logics S4, S5
  - Implicational fragments of relevance logics R, RM, E, Ł
- Time permitting: discussion of methods

Some recent results in algebra & logical calculi...
**Equational Bases for BA in $+$ and $\land$ III**

- It was thought that the (32-symbol) Robbins basis for BA was the simplest known, until I dug-up the following 23-symbol 2-basis for Boolean algebra reported (without proof) by Carew Meredith in 1968 [30, p. 228]:
  
  \[
  (\text{Meredith}_1) \quad n(n(x) + y) + x = x \\
  (\text{Meredith}_2) \quad n(n(x) + y) + (z + y) = y + (z + x)
  \]
- In 1966, Tarski [45] reported that BA does have single $+$, $\land$ axioms. Building on Tarski’s work, Padmanabhan and Quackenbush [33] gave a method for constructing such axioms. But, their method yields long single axioms [23].
- Recently, Bill McCune [26] discovered a 22-symbol single axiom for BA:
  
  \[
  (\text{DN}_1) \quad n(n(n(x) + y) + z) + n(x + n(n(z) + n(z + u))) = z 
  \]
- OPEN: do shorter single axioms (or bases!) for BA (in $+$ and $\land$) exist?

---

**Equational Bases for BA in Sheffer’s | II**

- The work of Tarski [45] and Padmanabhan & Quackenbush [33] also implies the existence of single axioms for BA in the Sheffer Stroke. But, as before, the $|-$single axioms generated by the methods of [33] are quite long [23].
- Recently, [53, 26] the following 15-symbol 1-bases were discovered.
  
  \[
  (\text{Sh}_1) \quad (x | (y | x) | x) | (y | (z | x)) = y \\
  (\text{Sh}_2) \quad ((y | x) | y) | (x | (z | y)) = x
  \]
- It is also known [53, 26] that these $|-$single axioms are the shortest possible.
- Elegant axioms for groups [13, 19], lattices [25], loops [14, 15, 12], and other algebraic structures [24] have been discovered by the extended Argonne team.

---

**Sheffer Stroke Single Axioms for Sentential Logic I**

- In 1913, Sheffer [42] gave the following 3-basis for Boolean algebra in terms of a single binary connective $|$ (Sheffer’s | is NAND: $x | y = n(x) + n(y)$).
  
  \[
  (\text{Sheffer}_1) \quad (x | x) | (x | x) = x \\
  (\text{Sheffer}_2) \quad x | (y | (y | y)) = x \\
  (\text{Sheffer}_3) \quad (x | (y | z)) | (x | (y | z)) = ((y | y) | x) | ((z | z) | x)
  \]
- Meredith [28] (again, in obscurity, and rediscovered by me) simplified matters in 1969 by presenting the following (23-symbol) 2-basis for the same theory.
  
  \[
  (\text{Meredith}_3) \quad (x | x) | (y | x) = x \\
  (\text{Meredith}_4) \quad x | (y | (x | z)) = ((z | y) | y) | x
  \]
- Recently, Bob Veroff [50] established the following (17-symbol) 2-basis:
  
  \[
  (\text{Commutativity}) \quad x | y = y | x \\
  (\text{Veroff}_26a) \quad (x | y) | (x | (y | z)) = x
  \]

---

\*Actually, Nicod’s original proofs are erroneous (as noted by Łukasiewicz in [17]). See Scharle’s [41] for a rigorous proof of the completeness of Nicod’s system.
**Sheffer Stroke Single Axioms for Sentential Logic II**

- Łukasiewicz’s student Mordchaj Wajsberg [51, pp. 37–39] later discovered the following organic\(^a\) 23-symbol single axiom for \(D\):
  \[ DDpDqrDDsrDDpDpsDpsDpsDpDpq \]

- Łukasiewicz later discovered another 23-symbol organic axiom:
  \[ DDpDqrDDDsrDDpsDpsDps \]
- Ken Harris and I have recently discovered many new 23-symbol single axioms, some of which are organic and have only 4 variables, e.g.,
  \[ DDpDqrDDpDqrDDsrDDrsDps \]
- We have also shown that 23 symbol axioms are the shortest possible.

\(^a\)A single axiom is organic if it contains no tautologous subformulae. (N) and (L) are non-organic, because they contain tautologous subformulae of the form \(DxDxx\).

**Single C-O Axioms for Classical Sentential Logic**

- Meredith [27, 29] reports two 19-symbol single axioms for classical sentential logic (using only the rule of condensed detachment, or modus ponens for \(C\)) in terms of implication \(C\) and the constant \(O\) (semantically, \(O\) is “The False”):
  
  \[
  \text{CCCCCpqCr0stCCtCpCp} \\
  \text{CCCCpqCORSsCCspCtCp}
  \]

- Meredith [27, page 156] claims to have “almost completed a proof that no single axiom of \((C,O)\) can contain less than 19 letters.” As far as we know, no such proof was ever completed (that is, until now…).

- We have performed an exhaustive search/elimination of all \((C,O)\) theorems with fewer than 19 symbols. We have proven Meredith’s conjecture: no single axiom of classical PL in \((C,O)\) can contain less than 19 letters.\(^2\)

\(^2\)The elimination of some \((C,O)\) candidates relied on matrices generated using **stochastic local search** techniques (as described by Ted Ulrich in his [47, 49] and by Cipra [2]). Stochastic local search is very powerful in the context of implicational logics. It has led to many useful (small) models.

**Single Axioms for The Equivalential Fragment of Classical Sentential Logic**

- In 1933, Łukasiewicz [46, 250–277] showed (lots of hand calculations!) that (with MP for \(E\) as the sole rule) the shortest single axioms for the equivalential (\(E\)) fragment of classical propositional logic contain 11 symbols. He found 2 such axioms.

- In the 1950’s, Meredith [29] discovered seven more 11-symbol single axioms for \(E\).

- John Kalman [11], and his student J. Peterson [36, 37], did extensive work on the problem in the 1970’s. They found one more 11-symbol single axiom, and they eliminated all but 7 of the remaining 640 11-symbol candidate single axioms.

- In 1977–1979, Wos, Winker, et al (all at Argonne) [55] worked on the remaining 7 candidates. They ruled-out all but three, and showed that two of these three were single axioms. This left the following (and last) remaining 11-symbol candidate:
  \[ EppEEEpqErqr \]

- About a year ago, we (Wos, Dolph Ulrich, Fitelson [54]) proved that XCB is a single axiom for the equivalential calculus. The proof contains substitution instances with over 2000 symbols. This completes a 70-year study initiated by Łukasiewicz.

**New Bases for C5**

- In their classic paper [16], Lemmon, Meredith, Meredith, Prior, and Thomas present several axiomatizations (assuming only the rule of condensed detachment, or *modus ponens* for \(C\)) of the system \(C5\), which is the strict-implicational fragment of the modal logic \(S5\).

- Bases for \(C5\) containing 4, 3, 2, and a single axiom are presented in [16]. The following 2-basis is the shortest of these bases. It contains 20 symbols, 5-variables, and 9 occurrences of the connective \(C\).
  \[
  \text{Ccpp} \\
  \text{CCCCpqqrqCCqsCtCp}
  \]

- The following 21-symbol (6-variable, 10-\(C\)) single axiom (due to C.A. Meredith) for \(C5\) is also reported in [16]:
  \[
  \text{CCCCCcppCrsCCspCstCp}
  \]
New Bases for C5 (Cont’d)

- We (Ernst, Fitelson, Harris, Wos) searched both for new (hopefully, shorter than previously known) single axioms for C5 and for new 2-bases for C5.
- We discovered the following new 2-basis for C5, which is shorter than any previously known basis (indeed, it is as short as any possible basis — see below). It has 18 symbols, 4 variables, and 8 occurrences of C:
  \[
  Cpp \\
  CCpqCCqCrsCpr
  \]
- Moreover, we discovered the following new 21-symbol (6-variable, 10-C) single axiom for C5 (as well as 5 others, not given here):
  \[
  CCCCCpqCCsCCqCpt
  \]
- No formula with fewer than 21 symbols is a single axiom for C5. And, no basis for C5 whatsoever has fewer than 18 symbols. Results to appear in [5].

New Bases for C4

- C4 is the strict-implicational fragment of the modal logic S4 (and several other modal logics in the neighborhood of S4 — see Ulrich’s [48]).
- As far as we know, the shortest known basis for C4 is due to Ulrich (see Ulrich’s [48]), and is the following 25-symbol, 11-C, 3-axiom basis:
  \[
  Cpp \\
  CCpqCrCpq \\
  CCpCqrCCpqCr
  \]
- Anderson & Belnap [1, p. 89] state the finding of a (short) single axiom for C4 as an open problem (as far as we know, this has remained open). The following is a 21-symbol (6-variable, 10-C) single axiom for C4:
  \[
  CCpCCqCrrCpsCCqCtCqCpt
  \]
- We have also the following 20-symbol 2-basis for C4:
  \[
  Cppq \\
  CCpCqCCpqCsrCPr
  \]
- No formula with fewer than 21 symbols is a single axiom for C4. And, no basis for C4 whatsoever has fewer than 20 symbols. Results to appear in [5].

New Bases for RM

- The “classical” relevance logic R-Mingle (RM) was first carefully studied by Dunn in the late 60’s (e.g., in [4]). Interestingly, the implicational fragment of R-Mingle (RM→) has an older history.
- RM→ was studied (albeit, unwittingly!) by Sobociński in the early 50’s. Sobociński [43] discusses a two-designated-value-variant of Łukasiewicz’s three-valued implication-negation logic (I’ll call Sobociński’s logic S). Sobociński leaves the axiomatization of S→, as an open problem.
- Rose [39, 40] solved Sobociński’s open problem, but his axiomatizations of S→ are very complicated and highly redundant (see Parks’ [34]).
- Meyer & Parks [31, 35] report: (i) an independent 4-basis for S→, (ii) that S→ = RM→ (thus, a 4-basis for RM→); and (iii) that RM→ can be axiomatized by adding the following “unintelligible” 21-symbol formula to R→:
  \[
  CCCCCpqCqCqCpqrr
  \]

New Bases for RM→ (Cont’d)

- In other words, Meyer & Parks gave the following 5-basis for RM→:
  \[
  Cpp \\
  CppCpq \\
  CCpqCCrqCrq \\
  CCpqCpq \\
  CCCCCpqCqCrq
  \]
- The reflexivity axiom Cpp is dependent in the above 5-basis. The remaining (independent) 4-basis is the Meyer-Parks basis for RM→.
- After much effort (and, with valuable assistance from Bob Veroff and Larry Wos), we (Ernst, Fitelson, Harris) discovered the following 13-symbol replacement for Parks’ 21-symbol formula (and there are none shorter [6]):
  \[
  CCCCCpqCrCqCqrr
  \]
- The contraction axiom CCpqCpCrqCq is dependent in our new 4-basis. The remaining (independent) 3-basis for RM→ contains 31 symbols and 14 C’s (the Meyer-Parks basis has 4 axioms, 48 symbols, and 22 C’s):
  \[
  CppCpq \\
  CCpqCCrqCrq \\
  CCCCCpqCqCqrr
  \]
result for this purpose is the Diamond-McKinsey theorem that no Boolean algebra can be axiomatized by formulas containing less than three distinct propositional letters [1, p. 83].

4. A set of formulas was selected from the list at random. Using either SEM [56] or a program written by the authors, we found a matrix that respects modus ponens, invalidates a known axiom-basis for the system, but validates the formulas selected from the list. Such a model suffices to show that the formulas are not single axioms for the system.

5. All the remaining formulas in the list were then tested against that matrix. Every formula validated by that matrix would be eliminated.

6. Steps 4 and 5 were repeated until the list of candidate formulas was down to a small number, or eliminated entirely.

7. We would then use Orrer [20] (+strategies!) to attempt to prove a known axiom basis from each of the remaining candidates.

References

Vanquishing the XCB question: The methodological discovery of the last

L. Wos, D. Ulrich, and B. Fitelson,

J. Zhang and H. Zhang,

A. Tarski,

S. Winker,

M. Wajsberg,

A. Rose,

W. McCune and R. Padmanabhan,

R. Vener,

R. Meyer and Z. Parks,

J. Łukasiewicz and A. Tarski,


J. Łukasiewicz and A. Tarski, Investigations into the sentential calculus, (1956), Appears as chapter IV in [44].


C. Meredith, Single axioms for the systems (C,N), (C,O) and (A,N) of the two-valued propositional calculi, J. Computing Systems 1 (1953), 155–164.