

SOME RECENT RESULTS IN ALGEBRA & LOGICAL CALCULI
OBTAINED USING AUTOMATED REASONING

BRANDEN FITELSON^a

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

^aResults 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.*

Equational Bases for BA in + and n I

- In 1933, E.V. Huntington presented the following 3-basis for BA [10, 9]:

(Commutativity+)

$$x + y = y + x$$

(Associativity+)

$$(x + y) + z = x + (y + z)$$

(Huntington)

$$n(n(x) + y) + n(n(x) + n(y)) = x$$

- BA is usually presented in terms of +, ·, n, 0, 1. From Huntington's basis, 0, 1, and ·, with appropriate properties, can be established (*easy* for OTTER [20]).
- Shortly thereafter, Herbert Robbins asked whether the Huntington equation can be replaced with the following equation (which is shorter by one "n"):
 - (Robbins)
$$n(n(x + y) + n(x + n(y))) = x$$
- The Robbins problem remained open for over 63 years, and attracted the attention of various people, including Tarski, and others [8], [2].

Equational Bases for BA in + and n II

- In 1979, Steve Winker, a student visiting Argonne, learned of the Robbins problem from Joel Berman. He and Larry Wos began to attack the problem.
- Larry Wos suggested looking for properties that force Robbins algebras to be Boolean. Winker [52] ingeniously found several such conditions (both "hand" and automated reasoning), including the following two relatively weak ones:
 - $\exists c \exists d (c + d = c)$
 - $\exists c \exists d (n(c + d) = n(c))$
- In 1996, Bill McCune [22] used an Argonne TP (EQP [21], a cousin of OTTER [20]) to prove that all Robbins algebras satisfy Winker's (2), above.
- This solved the long-standing Robbins problem. But, the machine proof of Winker's condition was not very easy for a human to follow or understand.
- Since McCune's discovery, several people (including myself [7]) have tried, in various ways, to make the EQP (and OTTER) proofs easier to digest [3].

Equational Bases for BA in + and n 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]:

(Meredith₁)

$$n(n(x) + y) + x = x$$

(Meredith₂)

$$n(n(x) + y) + (z + y) = y + (z + x)$$

- In 1966, Tarski [45] reported that BA does have *single* +, n 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:
 - (DN₁)
$$n(n(n(x + y) + z) + n(x + n(n(z) + n(z + u)))) = z$$
- OPEN: do shorter single axioms (or bases!) for BA (in + and n) exist?

Equational Bases for BA in Sheffer's | I

- In 1913, Sheffer [42] gave the following 3-basis for Boolean algebra in terms of a single binary connective | (Sheffer's | is just NAND: $x|y = n(x) + n(y)$).

$$\text{(Sheffer}_1) \quad (x|x)|(x|x) = x$$

$$\text{(Sheffer}_2) \quad x|(y|(y|y)) = x|x$$

$$\text{(Sheffer}_3) \quad (x|(y|z))|(x|(y|z)) = ((y|y)|x)|((z|z)|x)$$

- 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:

$$\text{(Commutativity |)} \quad x|y = y|x$$

$$\text{(Veroff}_{26a}) \quad (x|y)|(x|(y|z)) = x$$

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, we at Argonne [26] discovered the following 15-symbol 1-bases.

$$\text{(Sh}_1) \quad (x|((y|x)|x))|(y|(z|x)) = y$$

$$\text{(Sh}_2) \quad ((y|(x|y))|y)|(x|(z|y)) = x$$

- We [26] also proved that these |-single axioms are the *shortest possible*.^a
- 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.

^aWolfram [53, 801–818] suggests that *he* discovered these axioms (no citations to our work). He also reports McCune's 22-symbol (+, n) BA single axiom with no citation [53, 1175]. When Wolfram heard we had established these results (he had been working on such things independently), he put legal pressure on Argonne to prevent the publication of our paper [26] until his book [53] came out. He succeeded. But, the propriety of McCune *et al* was established publicly on Bob Boyer's QED archive.

Sheffer Stroke Single Axioms for Sentential Logic I

- In 1917, Nicod [32] showed^a that the following 23-symbol formula (in Polish notation) is a single axiom for classical sentential logic (D is interpreted semantically as NAND, *i.e.*, the Sheffer stroke):

$$\text{(N)} \quad DDpDqrDDtDttDDsqDDpsDps$$

- The only rule of inference for Nicod's single axiom system is the following, somewhat odd, detachment rule for D :

$$\text{(D-Rule)} \quad \text{From } DpDqr \text{ and } p, \text{ infer } r.$$

- Łukasiewicz [17, pp. 179–196] later showed that the following *substitution instance* (t/s) of Nicod's axiom (N) would suffice:

$$\text{(Ł}_1) \quad DDpDqrDDsDsDDsqDDpsDps$$

^aActually, Nicod's original proofs are erroneous (as noted by Łukasiewicz in [17]). See Schärle'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 :

$$\text{(W)} \quad DDpDqrDDDsrDDpsDpsDpDpq$$

- Łukasiewicz later discovered another 23-symbol organic axiom:

$$\text{(Ł}_2) \quad DDpDqrDDpDrpDDsqDDpsDps$$

- 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.*,

$$\text{(HF}_1) \quad DDpDqrDDpDqrDDsrDDrsDps$$

- We have also shown that 23 symbol axioms are the *shortest possible*.

^aA single axiom is *organic* if it contains no tautologous subformulae. (N) and (Ł) 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”):

$$\begin{aligned} &CCCCpqCrOstCCtpCrp \\ &CCcpqCCOrsCCspCtCup \end{aligned}$$

- 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.*^a

^aThe 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:
(XCB) $EpEEEpqErqr$
- 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 .

$$\begin{aligned} &Cp p \\ &CCCCpqrqCCqsCtCps \end{aligned}$$

- The following 21-symbol (6-variable, 10- C) single axiom (due to C.A. Meredith) for $C5$ is also reported in [16]:

$$CCCCCtppqCrsCCspCuCrp$$

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 :

$$\begin{aligned} &Cp p \\ &CCpqCCCCqrsrCpr \end{aligned}$$

- Moreover, we discovered the following new 21-symbol (6-variable, 10- C) single axiom for $C5$ (as well as 5 others, not given here):

$$CCCCpqrCCssqCCqtCuCpt$$

- 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:

$$Cp p \quad CCp q Cr C p q \quad CCp C q r CCp q C p r$$

- 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:

$$CCpCCqCrrCpsCCstCuCpt$$

- We have also the following 20-symbol 2-basis for C4:

$$CpCqq \quad CCpCqrCCpqCsCpr$$

- *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_→:

$$CCCCCpqqprCCCCCqppqrr$$

New Bases for RM_→ (Cont’d)

- In other words, Meyer & Parks gave the following 5-basis for RM_→:

$$Cp p \quad CpCCpqq \quad CCpqCCrpCrq \quad CCpCpqCpq \\ CCCCCpqqprCCCCCqppqrr$$

- The reflexivity axiom $Cp p$ 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 (& there are none shorter [6]):

$$CCCCCpqrCqpr$$

- The contraction axiom $CCpCpqCpq$ 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):

$$CpCCpqq \quad CCpqCCrpCrq \quad CCCCCpqrCqpr$$

(Long) Single Axioms for Some Non-Classical Logics

- It was shown by Rezuş [38] (building on earlier seminal work of Tarski and Łukasiewicz [18]) that the systems E_→, R_→, and L_→ have single axioms. However, applying the methods of [38] yields very long, *inorganic* single axioms. As far as we know, these axioms have never been explicitly written down. Here is a 69-symbol (17-variable!) single axiom for the implicational fragment of Łukasiewicz’s infinite-valued logic L_→ (obtained by Ken Harris, using the methods of [38]):

$$L_{\rightarrow}; \quad CCCfCg f CCCCCCCCdCCeCedCCaCbazzCCCCxyyCCyxwwCCCCtuCutCutssCCqCrpp$$

- Single axioms of comparable length (*i.e.*, containing fewer than 75 symbols) can also be generated for the relevance logics E_→ and R_→ (omitted). Here’s what we know about the shortest single axioms for the systems E_→, R_→, L_→, and RM_→:
 - The shortest single axiom for E_→ has between 23 and 75 symbols.
 - The shortest single axiom for R_→ has between 23 and 75 symbols.
 - The shortest single axiom for L_→ has at most 69 symbols.
 - The shortest single axiom for RM_→ (if there is one^a) has at least 23 symbols.

^aMethods of [18] and [38] do *not* apply to RM_→, so whether RM_→ has a single axiom remains open.

References

- [1] A. Anderson and N. Belnap, *Entailment: Volume I*, Princeton University Press, 1975.
- [2] B. Cipra, *As easy as EQP*, What's happening in the mathematical sciences (P. Zorn, ed.), AMS, 1999, pp. 59–72.
- [3] B. Dahn, *Robbins algebras are Boolean: A revision of McCune's computer-generated solution of Robbins problem*, J. Algebra **208** (1998), no. 2, 526–532.
- [4] J. Dunn, *Algebraic completeness results for R-mingle and its extensions*, J. Symbolic Logic **35** (1970), 1–13.
- [5] Z. Ernst, B. Fitelson, K. Harris, and L. Wos, *Shortest axiomatizations of implicational S4 and S5*, to appear in the *Notre Dame Journal of Formal Logic* (NDJFL).
- [6] ———, *A concise axiomatization of RM₁*, Bull. Sect. Logic Univ. Łódź **30** (2001), 191–194.
- [7] B. Fitelson, *Using mathematica to understand the computer proof of the Robbins conjecture*, Mathematica in Education and Research **7** (1998), 17–26.
- [8] L. Henkin, J. Monk, and A. Tarski, *Cylindric algebras, Part I*, North-Holland, 1971.
- [9] E. Huntington, *Boolean algebra. A correction*, Trans. AMS **35** (1933), 557–558.
- [10] ———, *New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's Principia Mathematica*, Trans. AMS **35** (1933), 274–304.
- [11] J. Kalman, *A shortest single axiom for the classical equivalential calculus*, NDJFL **19** (1978), no. 1, 141–144.
- [12] M. Kinyon, K. Kunen, and J. Phillips, *A generalization of Moufang and Steiner loops*, Algebra Universalis **48** (2002), 81–101.
- [13] K. Kunen, *Single axioms for groups*, J. Automat. Reason. **9** (1992), 291–308.

- [14] ———, *Quasigroups, loops, and associative laws*, J. Algebra **185** (1996), 194–204.
- [15] ———, *The structure of conjugacy closed loops*, Trans. Amer. Math. Soc. **352** (2000), 2889–2911.
- [16] E. Lemmon, C. Meredith, D. Meredith, A. Prior, and I. Thomas, *Calculi of pure strict implication*, in *Philosophical Logic* (J. Davis, ed.), D. Reidel, 1969.
- [17] J. Łukasiewicz, *Selected Works*, Noth Holland, 1970.
- [18] J. Łukasiewicz and A. Tarski, *Investigations into the sentential calculus*, (1956), Appears as chapter IV in [44].
- [19] W. McCune, *Single axioms for groups and Abelian groups with various operations*, J. Automated Reasoning **10** (1993), 1–13.
- [20] ———, *Otter 3.0 Reference Manual and Guide*, Tech. Report ANL-94/6, Argonne National Lab, 1994.
- [21] ———, *33 basic test problems: A practical evaluation of some paramodulation strategies*, Automated Reasoning and its Applications: Essays in Honor of Larry Wos (Robert Veroff, ed.), MIT Press, 1997, pp. 71–114.
- [22] ———, *Solution of the Robbins problem*, J. Automat. Reason. **19** (1997), no. 3, 263–276.
- [23] ———, *Single Axioms for Boolean Algebra*, Tech. Memo ANL/MCS-TM-243, MCS @ ANL, June 2000.
- [24] W. McCune and R. Padmanabhan, *Automated deduction in equational logic and cubic curves*, Lecture Notes in Computer Science (AI subseries), vol. 1095, Springer-Verlag, Berlin, 1996.
- [25] W. McCune, R. Padmanabhan, and R. Veroff, *Yet another single law for lattices*, to appear in *Algebra Universalis*.
- [26] W. McCune, R. Veroff, B. Fitelson, K. Harris, A. Feist, and L. Wos, *Short single axioms for Boolean algebra*, J. Automat. Reason. **29** (2002), no. 1, 1–16.
- [27] C. Meredith, *Single axioms for the systems (C, N), (C, O) and (A, N) of the two-valued propositional calculus*, J. Computing Systems **1** (1953), 155–164.

- [28] ———, *Equational postulates for the Sheffer stroke*, NDJFL **10** (1969), no. 3, 266–270.
- [29] C. Meredith and A. Prior, *Notes on the axiomatics of the propositional calculus*, NDJFL **4** (1963), 171–187.
- [30] ———, *Equational logic*, NDJFL **9** (1968), 212–226.
- [31] R. Meyer and Z. Parks, *Independent axioms for the implicational fragment of Sobociński's three-valued logic*, Z. Math. Logik Grundlagen Math. **18** (1972), 291–295.
- [32] J. Nicod, *A reduction in the number of primitive propositions of logic*, Proc. Camb. Phil. Soc. **19** (1917), 32–41.
- [33] R. Padmanabhan and R. W. Quackenbush, *Equational theories of algebras with distributive congruences*, Proc. AMS **41** (1973), 373–377.
- [34] Z. Parks, *Dependence of some axioms of Rose*, Z. Math. Logik Grundlagen Math. **18** (1972), 189–192.
- [35] ———, *A note on R-Mingle and Sobociński's three-valued logic*, NDJFL **13** (1972), 227–228.
- [36] J. Peterson, *Shortest single axioms for the classical equivalential calculus*, J. Automat. Reason. **17** (1976), 267–271.
- [37] ———, *The possible shortest single axioms for EC-tautologies*, Report 105, Dept. of Mathematics, University of Auckland, 1977.
- [38] A. Rezuş, *On a theorem of Tarski*, Libertas Math. **2** (1982), 63–97.
- [39] A. Rose, *A formalization of Sobociński's three-valued implicational propositional calculus*, J. Computing Systems **1** (1953), 165–168.
- [40] ———, *An alternative formalisation of Sobociński's three-valued implicational propositional calculus*, Z. Math. Logik. Grundlagen Math. **2** (1956), 166–172.
- [41] T. W. Scharle, *Axiomatization of propositional calculus with Sheffer functors*, NDJFL **6** (1965), 209–217.
- [42] H. Sheffer, *A set of five independent postulates for Boolean algebras, with application to logical constants*, Trans. AMS **14** (1913), no. 4, 481–488.

- [43] B. Sobociński, *Axiomatization of a partial system of three-value calculus of propositions*, J. Computing Systems **1** (1952), 23–55.
- [44] A. Tarski, *Logic, semantics, metamathematics. Papers from 1923 to 1938*, Oxford at the Clarendon Press, 1956.
- [45] ———, *Equational logic and equational theories of algebras*, Contributions to Math. Logic (Colloquium, Hannover, 1966), North-Holland, Amsterdam, 1968, pp. 275–288.
- [46] J. Łukasiewicz, *Selected works*, North-Holland, 1970, Edited by L. Borkowski.
- [47] D. Ulrich, *Local search*, mimeograph of unpublished lecture notes (private correspondence of 12 March 2001).
- [48] ———, *Strict implication in a sequence of extensions of S4*, Z. Math. Logik Grundlag. Math. **27** (1981), 201–212.
- [49] ———, *A legacy recalled and a tradition continued*, J. Automat. Reason. **27** (2001), 97–122.
- [50] R. Veroff, *Short 2-Bases for Boolean Algebra in Terms of the Sheffer Stroke*, Tech. Report TR-CS-2000-25, CS @ UNM, Albuquerque, NM, 2000.
- [51] M. Wajsberg, *Logical works*, Polish Academy of Sciences, 1977.
- [52] S. Winker, *Absorption and idempotency criteria for a problem in near-Boolean algebras*, J. Algebra **153** (1992), no. 2, 414–423.
- [53] S. Wolfram, *A new kind of science*, Wolfram Media, Inc., Champaign, IL, 2002.
- [54] L. Wos, D. Ulrich, and B. Fitelson, *Vanquishing the XCB question: The methodological discovery of the last shortest single axiom for the equivalential calculus*, J. Automated Reasoning **29** (2002), 107–124.
- [55] L. Wos, S. Winker, R. Veroff, B. Smith, and L. Henschen, *Questions concerning possible shortest single axioms for the equivalential calculus*, NDJFL **24** (1983), no. 2, 205–223.