Short Single Axioms for Boolean Algebra *

William McCune
Mathematics & Computer Science Division, Argonne National Laboratory

Robert Veroff
Computer Science Department, University of New Mexico

Branden Fitelson
Philosophy Department, University of Wisconsin-Madison, and
Mathematics & Computer Science Division, Argonne National Laboratory

Kenneth Harris
Madison, Wisconsin, and
Mathematics & Computer Science Division, Argonne National Laboratory

Andrew Feist
Mathematics Department, Duke University

Larry Wos
Mathematics & Computer Science Division, Argonne National Laboratory

Abstract. We present short single equational axioms for Boolean algebra in terms of disjunction and negation and in terms of the Sheffer stroke. Previously known single axioms for these theories are much longer than the ones we present. We show that there is no shorter axiom in terms of the Sheffer stroke than the ones we present. Automated deduction techniques were used for several different aspects of the work.

Keywords: Boolean algebra, Sheffer stroke, single axiom

1. Background & Introduction

In 1997, the following three equations were shown to be an axiomatization (a 3-basis) of Boolean algebra in terms of disjunction and negation [4].

$$x + y = y + x \qquad \text{(Commutativity+)}$$
$$(x + y) + z = x + (y + z) \qquad \text{(Associativity+)}$$
$$((x + y)' + (x' + y)')' = y \qquad \text{(Robbins)}$$

* This work was supported in part by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, U.S. Department of Energy, under Contract W-31-109-Eng-38, and in part by National Science Foundation grant no. CDA-9503064.

Less well known is the following (equivalent) 2-basis due to Meredith in 1968 [8, p. 221].

$$(x' + y)' + x = x \qquad \text{(Meredith}_1\text{)}$$
$$(x' + y)' + (z + y) = y + (z + x) \qquad \text{(Meredith}_2\text{)}$$

Boolean algebra can be axiomatized with other connectives, and in 1913, Sheffer [11] presented the following 3-basis for Boolean algebra in terms of a binary connective now known as the Sheffer stroke, or NAND, that is, $x|y = x' + y'$.

$$(x|x)|(x|x) = x \qquad \text{(Sheffer}_1\text{)}$$
$$x|(y|(y|y)) = x|x \qquad \text{(Sheffer}_2\text{)}$$
$$(x|(y|z))|(x|(y|z)) = ((y|y)|x)|((z|z)|x) \qquad \text{(Sheffer}_3\text{)}$$

Meredith [7] simplified matters in 1969 by presenting the following (equivalent) 2-basis for the same theory.

$$(x|x)|(y|x) = x \qquad \text{(Meredith}_3\text{)}$$
$$x|(y|(x|z)) = ((z|y)|y)|x \qquad \text{(Meredith}_4\text{)}$$

Recently, Veroff [12] further simplified matters by showing that the following pair of equations is a 2-basis for the same theory.

$$x|y = y|x \qquad \text{(Commutativity|)}$$
$$(x|y)|(x|(y|z)) = x \qquad \text{(26a)}$$

Researchers have known for some time that *single* equational axioms (i.e., 1-bases) exist for Boolean algebra, including representation in terms of disjunction and negation and in terms of the Sheffer stroke. In 1973, Padmanabhan and Quackenbush [10] presented a method for constructing a single axiom for any finitely based theory that has particular distributive and permutable congruences. Boolean algebra has these properties. However, straightforward application of the method usually yields single axioms of enormous length (sometimes with tens of millions of symbols). In [5], the construction method is used with a variety of automated deduction techniques to find single axioms of reasonable length for Boolean algebra with various sets of connectives. In particular, an axiom of length[1] 131, with six variables, was found for disjunction and negation, and an axiom of length 105, also with six variables, was found for the Sheffer stroke.

[1] The *length* of an equation counts the number of connectives, the variable occurrences, and the equal sign (but not the parentheses). For example, $(x + x) = x$ has length 5.

The shortest previously reported single equational axiom for Boolean algebra in any set of connectives is in terms of negation and a ternary operation f defined as

$$f(x, y, z) = (x \cdot y) + ((y \cdot z) + (z \cdot x)). \qquad \text{(TBA-op)}$$

The following axiom, found by Padmanabhan and McCune, has length 26 with 7 variables [9].

$$f(f(x, x', y), f(f(z, u, v), w, f(z, u, v_6))', f(u, f(v_6, w, v), z)) = y. \qquad \text{(TBA-ax)}$$

In this article, we show that the equation

$$(((x + y)' + z)' + (x + (z' + (z + u)')')')' \;=\; z \qquad (\mathrm{DN}_1)$$

is a 1-basis (i.e., single axiom) for Boolean algebra in terms of disjunction and negation, and we show that

$$(x \mid ((y \mid x) \mid x)) \mid (y \mid (z \mid x)) \;=\; y \qquad (\mathrm{Sh}_1)$$

is a 1-basis for Boolean algebra in terms of the Sheffer stroke.

Equation (DN_1) was found by automatically generating and semantically filtering a great number of equations, then sending the surviving candidates to the theorem prover OTTER [3, 2]. Equation (Sh_1) is a member of a list of 25 candidates sent to us by Stephen Wolfram [13], who asked whether OTTER could prove any of the candidates to be single axioms. OTTER could not do so automatically; we proved (Sh_1) to be a single axiom by first finding and investigating with OTTER many different 2-bases for the Sheffer stroke [12]. In both the disjunction/negation and Sheffer cases, OTTER deserves substantial credit for proving that the equations are indeed single axioms for the respective theories.

In addition, we show that (Sh_1) is a *shortest* single axiom in terms of the Sheffer stroke, and we construct a short list of Sheffer identities that contains all remaining single axioms of the same length as (Sh_1).

Rewriting Axioms. A frequently asked question:

> *If we take a single axiom in one set of operations and rewrite it to another set of operations, do we necessarliy get a single axiom in that second set of operations?*

Unfortunately, no. To see this, take any single axiom (or any basis) for Boolean algebra in terms of the Sheffer stroke, for example, (Sh_1). Now consider a 2-element model of (Sh_1), say,

$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1 & 1 \\ 1 & 1 & 0 \end{array}. \qquad (\mathcal{M}_0)$$

Next, rewrite (Sh_1) with the rule $x|y = x' + y'$ to obtain

$$(x' + ((y' + x')' + x')')' + (y' + (z' + x')')' = y. \qquad (\mathrm{Sh}_1\mathrm{a})$$

This equation is valid (with + as OR and $'$ as NOT), but it is not a single axiom: consider the 2-element interpretation of (Sh_1a) in which $x' = x$, and in which + is interpreted as in structure ($\mathcal{M}_0$). This interpretation is a model of (Sh_1a) (because removing the $'$ symbols from (Sh_1a) gives an equation just like (Sh_1)), but it is not a Boolean algebra with + as OR and $'$ as NOT.

Mirror Images. If we have a Boolean algebra basis $\mathcal{B}$ in terms of disjunction and negation or in terms of the Sheffer stroke, then the mirror image of $\mathcal{B}$, obtained by reversing arguments of all occurrences of the binary operation, is also a basis.

Pseudo Web Links. This article has a companion page on the World Wide Web, `http://www.mcs.anl.gov/~mccune/ba/sax`. That Web page contains links to OTTER input files and other data files related to the work presented here. In this article, we refer to those files with bold-faced underlined pseudolinks **<u>like this</u>**.

2. A Basis for Disjunction and Negation

Theorem 1. *Equation* (DN_1) *is a basis for Boolean algebra in terms of disjunction and negation.*

Proof. A straightforward calculation shows that (DN_1) holds in Boolean algebra. The following 57-step OTTER derivation shows that the Robbins 3-basis {(Commutativity+),(Associativity+),(Robbins)} follows from (DN_1). The justification $[m(i) \rightarrow n(j_1 \ldots j_n)]$ indicates paramodulation (equality substitution with unification) from the i-th argument of equation m into position $(j_1 \ldots j_n)$ of equation n.

3 $\quad (((x+y)'+z)'+(x+(z'+(z+u)')')')' = z$ $\quad$ [DN_1]

61 $\quad ((x+y)'+(((z+u)'+x)'+(y'+(y+v)')')')' = y$ $\quad$ [3 (1) → 3 (1.1.1.1.1)]

62 $\quad ((x+y)'+((z+x)'+(y'+(y+u)')')')' = y$ $\quad$ [61 (1) → 61 (1.1.2.1.1.1.1)]

63 $\quad ((x+x')'+x)' = x'$ $\quad$ [3 (1) → 61 (1.1.2)]

64 $\quad ((x+y)'+((z+x)'+(((y+y')'+y)'+(y+u)')')')' = y$ $\quad$ [63 (2) → 62 (1.1.2.1.2.1.1)]

65 $\quad ((x+y)'+((z+x)'+y)')' = y$ $\quad$ [3 (1) → 64 (1.1.2.1.2)]

66* $\quad ((x+y)'+(x'+y)')' = y$ $\quad$ [63 (1) → 65 (1.1.2.1.1)]

67 $\quad (((x+y)'+x)'+(x+y)')' = x$ $\quad$ [65 (1) → 64 (1.1.2)]

68	$(x+((x+y)'+x)')' = (x+y)'$	[67 (1) $\rightarrow$ 67 (1.1.1)]
69	$(((x+y)'+z)'+(x+z)')' = z$	[67 (1) $\rightarrow$ 65 (1.1.2.1.1)]
70	$(x+((y+z)'+(y+x)')')' = (y+x)'$	[69 (1) $\rightarrow$ 69 (1.1.1)]
71	$((((x+y)'+z)'+(x'+y)')'+y)' = (x'+y)'$	[66 (1) $\rightarrow$ 69 (1.1.2)]
72	$(x+((y+z)'+(z+x)')')' = (z+x)'$	[70 (1) $\rightarrow$ 70 (1.1.2.1.1)]
73	$((x+y)'+((z+x)'+(y'+(u+y)')')')' = y$	[70 (1) $\rightarrow$ 62 (1.1.2.1.2.1.2)]
74	$(x+y)' = (y+x)'$	[67 (1) $\rightarrow$ 72 (1.1.2)]
75	$(((x+y)'+(y+z)')'+z)' = (y+z)'$	[72 (1) $\rightarrow$ 74 (1)]
76	$((x+((x+y)'+z)')'+z)' = ((x+y)'+z)'$	[67 (1) $\rightarrow$ 75 (1.1.1.1.1)]
77	$(((x+y)'+x)'+y)' = (y+y)'$	[65 (1) $\rightarrow$ 76 (1.1.1)]
78	$(x'+(y+x)')' = x$	[70 (1) $\rightarrow$ 73 (1)]
79	$((x+y)'+y')' = y$	[74 (2) $\rightarrow$ 78 (1)]
80	$(x+(y+x')')' = x'$	[79 (1) $\rightarrow$ 69 (1.1.1)]
81	$(x+x)' = x'$	[79 (1) $\rightarrow$ 80 (1.1.2)]
83	$(((x+y)'+x)'+y)' = y'$	[77 (2) $\rightarrow$ 81 (1)]
85	$x'' = x$	[79 (1) $\rightarrow$ 83 (1)]
86	$((x+y)'+x)'+y = y''$	[83 (1) $\rightarrow$ 85 (1.1)]
87	$(x+y)'' = y+x$	[74 (2) $\rightarrow$ 85 (1.1)]
88	$x+((y+z)'+(y+x)')' = (y+x)''$	[70 (1) $\rightarrow$ 85 (1.1)]
89*	$x+y = y+x$	[85 (1) $\rightarrow$ 87 (1)]
90	$((x+y)'+x)'+y = y$	[85 (1) $\rightarrow$ 86 (2)]
91	$((x+y)'+y)'+x = x$	[89 (2) $\rightarrow$ 90 (1.1.1.1.1)]
92	$x+((y+x)'+y)' = x$	[89 (2) $\rightarrow$ 90 (1)]
93	$(x+y')'+(y'+y)' = (x+y')'$	[80 (1) $\rightarrow$ 92 (1.2.1.1)]
94	$(x+y)'+(y+y')' = (x+y)'$	[78 (1) $\rightarrow$ 92 (1.2.1.1)]
95	$(x+y)'+(y'+y)' = (x+y)'$	[89 (2) $\rightarrow$ 94 (1.2.1)]
96	$((x+y')''+y)' = (y'+y)'$	[93 (1) $\rightarrow$ 75 (1.1.1.1)]
97	$((x+y')+y)' = (y'+y)'$	[85 (1) $\rightarrow$ 96 (1.1.1)]
98	$((((x+y')+z)'+y)'+(y'+y)')' = y$	[97 (1) $\rightarrow$ 69 (1.1.2)]
99	$x+((y+z)'+(y+x)')' = y+x$	[85 (1) $\rightarrow$ 88 (2)]
100	$x+(y+((z+y)'+x)')' = (z+y)'+x$	[79 (1) $\rightarrow$ 99 (1.2.1.1)]
101	$x+((y+x)'+(y+z)')' = y+x$	[89 (2) $\rightarrow$ 99 (1.2.1)]
102	$((x+y)'+((x+y)'+(x+z)')')'+y = y$	[101 (1) $\rightarrow$ 91 (1.1.1.1.1)]
103	$(((x+y')+z)'+y)'' = y$	[95 (1) $\rightarrow$ 98 (1.1)]
104	$x+((y+x')+z)' = x$	[87 (1) $\rightarrow$ 103 (1)]
105	$x'+((y+x)+z)' = x'$	[85 (1) $\rightarrow$ 104 (1.2.1.1.2)]
107	$(x+y)'+x = x+y'$	[92 (1) $\rightarrow$ 100 (1.2.1)]
108	$(x+(x+y')')' = (x+y)'$	[107 (1) $\rightarrow$ 68 (1.1.2.1)]
109	$((x+y)'+(x+z))'+y = y$	[108 (1) $\rightarrow$ 102 (1.1)]
110	$(((x+y)'+z)'+(x'+y)')'+y = (x'+y)''$	[71 (1) $\rightarrow$ 85 (1.1)]
111	$(((x+y)'+z)'+(x'+y)')'+y = x'+y$	[85 (1) $\rightarrow$ 110 (2)]
112	$(x'+((y+x)''+(y+z))')'+(y+z) = (y+x)''+(y+z)$	

[109 (1) → 111 (1.1.1.1.1)]

113 $(x'+((y+x)+(y+z))')'+(y+z) = (y+x)''+(y+z)$ [85 (1) → 112 (1.1.1.2.1.1)]

114 $(x'+((y+x)+(y+z))')'+(y+z) = (y+x)+(y+z)$ [85 (1) → 113 (2.1)]

115 $x''+(y+z) = (y+x)+(y+z)$ [105 (1) → 114 (1.1.1)]

117 $(x+y)+(x+z) = y+(x+z)$ [85 (1) → 115 (1.1)]

118 $(x+y)+(x+z) = z+(x+y)$ [89 (2) → 117 (1)]

119 $x+(y+z) = z+(y+x)$ [117 (1) → 118 (1)]

120 $x+(y+z) = y+(z+x)$ [89 (2) → 119 (1.2)]

121* $(x+y)+z = x+(y+z)$ [89 (2) → 120 (1)]

Equation 66 is (Robbins), 89 is (Commutativity+), and 121 is (Associativity+). □

The preceding OTTER proof and the corresponding input file are available on line in the files **DN-1.proof** and **DN-1.in**.

In addition, we have found the following nine equations (excluding mirror images), all the same length as (DN_1), to be single axioms for Boolean algebra in terms of OR and NOT.

$$(((x+y)'+z')'+((u'+u)'+(z'+x))') = z \qquad \text{(DN-13345)}$$
$$(((x+y)'+z')'+(x+(z+(z'+u)')')') = z \qquad \text{(DN-20629)}$$
$$((x+y)'+((x+z)'+(y'+(y+u)')')')' = y \qquad \text{(DN-20775)}$$
$$((x+y')'+((x+z)'+(y+(y'+u)')')') = y \qquad \text{(DN-20787)}$$
$$((x+y)'+((y'+(z+y)')'+(x+u)')')' = y \qquad \text{(DN-24070)}$$
$$((x+y')'+((y+(z+y')')'+(x+u)')') = y \qquad \text{(DN-24086)}$$
$$((x+y)'+((y'+(z+y)')'+(u+x)')')' = y \qquad \text{(DN-24412)}$$
$$((x+y')'+((y+(z+y')')'+(u+x)')') = y \qquad \text{(DN-24429)}$$
$$(((x+y)'+z)'+((z'+(u+z)')'+y)')' = z \qquad \text{(DN-24970)}$$

OTTER input files and proofs for these equations can be found on line in the files **DN-*.in** and **DN-*.proof**.

3. A Basis for the Sheffer Stroke

Theorem 2. *Equation* (Sh_1) *is a basis for Boolean algebra in terms of the Sheffer stroke.*

Proof. A straightforward calculation shows that (Sh_1) holds in Boolean algebra when the Sheffer stroke is interpreted as NAND (or as NOR). The following 66-step OTTER derivation shows that the Sheffer 3-basis {($\mathrm{Sheffer}_1$),($\mathrm{Sheffer}_2$),($\mathrm{Sheffer}_3$)} follows from (Sh_1).

3	$(x\|((y\|x)\|x))\|(y\|(z\|x)) = y$	[Sh_1]
70	$((x\|(y\|z))\|(x\|(x\|(y\|z))))\|((z\|((x\|z)\|z))\|(u\|(x\|(y\|z)))) = z\|((x\|z)\|z)$	[3 (1) $\rightarrow$ 3 (1.1.2.1)]
71	$((x\|y)\|(((y\|((z\|y)\|y))\|(x\|y))\|(x\|y)))\|z = y\|((z\|y)\|y)$	[3 (1) $\rightarrow$ 3 (1.2)]
72	$(x\|((y\|x)\|x))\|(y\|(z\|((x\|z)\|z))) = y$	[71 (1) $\rightarrow$ 3 (1.2.2)]
73	$x\|((x\|((x\|x)\|x))\|(y\|(x\|((x\|x)\|x)))) = x\|((x\|x)\|x)$	[72 (1) $\rightarrow$ 70 (1.1)]
74	$x\|((x\|x)\|x) = x\|x$	[72 (1) $\rightarrow$ 73 (1.2)]
75	$(x\|((x\|x)\|x))\|(x\|x) = x$	[74 (1) $\rightarrow$ 3 (1.2)]
76	$(x\|x)\|(x\|(y\|x)) = x$	[74 (1) $\rightarrow$ 3 (1.1)]
77	$(x\|(((y\|y)\|x)\|x))\|y = y\|y$	[76 (1) $\rightarrow$ 72 (1.2)]
78	$((x\|y)\|(((x\|y)\|(x\|y))\|(x\|y)))\|((x\|y)\|(x\|y)) = y\|((((x\|y)\|(x\|y))\|y)\|y)$	[77 (1) $\rightarrow$ 71 (1.1.2.1)]
79	$x\|((((y\|x)\|(y\|x))\|x)\|x) = y\|x$	[75 (1) $\rightarrow$ 78 (1)]
80	$(x\|x)\|(y\|x) = x$	[79 (1) $\rightarrow$ 76 (1.2)]
83	$x\|(y\|(x\|x)) = x\|x$	[80 (1) $\rightarrow$ 80 (1.1)]
84	$((x\|y)\|(x\|y))\|y = x\|y$	[80 (1) $\rightarrow$ 80 (1.2)]
85	$x\|((y\|x)\|x) = y\|x$	[84 (1) $\rightarrow$ 79 (1.2.1)]
86	$(x\|y)\|(x\|(z\|y)) = x$	[85 (1) $\rightarrow$ 3 (1.1)]
88	$(x\|(y\|z))\|(x\|z) = x$	[80 (1) $\rightarrow$ 86 (1.2.2)]
89	$x\|((x\|y)\|(z\|y)) = x\|y$	[86 (1) $\rightarrow$ 88 (1.1)]
90	$((x\|(y\|z))\|z)\|x = x\|(y\|z)$	[88 (1) $\rightarrow$ 86 (1.2)]
91	$x\|((y\|x)\|x) = x\|y$	[3 (1) $\rightarrow$ 89 (1.2)]
93	$x\|y = y\|x$	[85 (1) $\rightarrow$ 91 (1)]
95*	$(x\|y)\|(x\|x) = x$	[91 (1) $\rightarrow$ 88 (1.1)]
97	$(x\|y)\|(y\|(z\|x)) = y$	[91 (1) $\rightarrow$ 3 (1.1)]
101	$(x\|(y\|z))\|(z\|x) = x$	[93 (1) $\rightarrow$ 88 (1.2)]
104	$(x\|y)\|(y\|(x\|z)) = y$	[93 (2) $\rightarrow$ 97 (1.2.2)]
105	$(x\|(y\|z))\|(y\|x) = x$	[93 (2) $\rightarrow$ 101 (1.1.2)]
106	$((x\|y)\|(x\|z))\|z = x\|z$	[104 (1) $\rightarrow$ 97 (1.2)]
108	$x\|(y\|(x\|(y\|z))) = x\|(y\|z)$	[105 (1) $\rightarrow$ 105 (1.1)]
109	$(x\|(y\|(x\|z)))\|y = y\|(x\|z)$	[105 (1) $\rightarrow$ 104 (1.2)]
110	$(x\|(y\|z))\|(x\|(u\|(y\|x))) = (x\|(y\|z))\|(y\|x)$	[105 (1) $\rightarrow$ 89 (1.2.1)]
114	$(x\|(y\|(x\|z)))\|y = y\|(z\|x)$	[93 (2) $\rightarrow$ 109 (2.2)]
115	$(x\|(y\|z))\|(x\|(u\|(y\|x))) = x$	[105 (1) $\rightarrow$ 110 (2)]
116	$x\|(y\|(x\|y)) = x\|x$	[86 (1) $\rightarrow$ 114 (1.1)]
117	$x\|(y\|z) = x\|(z\|y)$	[109 (1) $\rightarrow$ 114 (1)]
118	$x\|(y\|(x\|(z\|(y\|x)))) = x\|x$	[115 (1) $\rightarrow$ 90 (1.1)]
119	$(x\|(y\|z))\|((y\|x)\|x) = (x\|(y\|z))\|(x\|(y\|z))$	[105 (1) $\rightarrow$ 116 (1.2.2)]
120	$(x\|(y\|x))\|y = y\|y$	[93 (2) $\rightarrow$ 116 (1)]
121	$(x\|y)\|z = z\|(y\|x)$	[93 (2) $\rightarrow$ 117 (1)]
122	$x\|(y\|(z\|(x\|y))) = x\|(y\|y)$	[118 (1) $\rightarrow$ 108 (1.2)]

123	$((x\|y)\|y)\|(y\|(z\|x)) = (y\|(z\|x))\|(y\|(z\|x))$	[101 (1) → 120 (1.1.2)]
125	$(x\|y)\|(z\|u) = (u\|z)\|(y\|x)$	[117 (2) → 121 (1)]
126	$x\|(y\|((y\|x)\|z)) = x\|(y\|y)$	[121 (2) → 122 (1.2.2)]
127	$x\|(y\|x) = x\|(y\|y)$	[88 (1) → 122 (1.2.2)]
128	$(x\|y)\|y = y\|(x\|x)$	[93 (2) → 127 (1)]
130	$x\|(y\|y) = x\|(x\|y)$	[127 (1) → 117 (1)]
131	$(x\|(y\|y))\|(x\|(z\|y)) = (x\|(z\|y))\|(x\|(z\|y))$	[128 (1) → 123 (1.1)]
132	$(x\|(y\|z))\|(x\|(y\|y)) = (x\|(y\|z))\|(x\|(y\|z))$	[128 (1) → 119 (1.2)]
133	$x\|((y\|y)\|(z\|(x\|(x\|y)))) = x\|((y\|y)\|(y\|y))$	[130 (1) → 122 (1.2.2.2)]
134	$((x\|(y\|z))\|(x\|(y\|z)))\|(y\|y) = x\|(y\|y)$	[132 (1) → 106 (1.1)]
135	$x\|((y\|y)\|(z\|(x\|(x\|y)))) = x\|y$	[95 (1) → 133 (2.2)]
136	$(((x\|y)\|(x\|y))\|((z\|((x\|y)\|z))\|(x\|y)))\|(x\|x) = (z\|((x\|y)\|z))\|(x\|x)$	[120 (1) → 134 (1.1.1)]
137	$(x\|((y\|z)\|x))\|(y\|y) = (y\|z)\|(y\|y)$	[80 (1) → 136 (1.1)]
138	$(x\|((y\|z)\|x))\|(y\|y) = y$	[95 (1) → 137 (2)]
141	$x\|((y\|((x\|z)\|y))\|x) = y\|((x\|z)\|y)$	[138 (1) → 88 (1.1)]
142	$x\|((y\|(y\|(z\|x)))\|x) = y\|((x\|(y\|(x\|z)))\|y)$	[114 (1) → 141 (1.2.1.2)]
143	$x\|((y\|(y\|(z\|x)))\|x) = y\|(y\|(z\|x))$	[114 (1) → 142 (2.2)]
144	$x\|(y\|(z\|(z\|(u\|(y\|x))))) = x\|(y\|y)$	[143 (1) → 126 (1.2.2)]
145	$x\|(y\|(y\|(z\|(x\|y)))) = x\|(y\|(x\|x))$	[144 (1) → 108 (1.2)]
146	$x\|(y\|(y\|(z\|(x\|y)))) = x\|x$	[83 (1) → 145 (2)]
147*	$x\|(y\|(y\|y)) = x\|x$	[105 (1) → 146 (1.2.2.2)]
149	$x\|(((y\|(z\|x))\|(y\|(z\|x)))\|(z\|z)) = x\|(y\|(z\|x))$	[146 (1) → 135 (1.2.2)]
151	$x\|(y\|(z\|z)) = x\|(y\|(z\|x))$	[134 (1) → 149 (1.2)]
152	$x\|(y\|((z\|z)\|x)) = x\|(y\|z)$	[95 (1) → 151 (1.2.2)]
155	$(x\|(y\|y))\|(x\|(z\|((y\|y)\|x))) = (x\|(z\|y))\|(x\|(z\|y))$	[152 (2) → 131 (1.2)]
156	$(x\|(y\|y))\|(x\|(z\|(x\|(y\|y)))) = (x\|(z\|y))\|(x\|(z\|y))$	[121 (1) → 155 (1.2.2.2)]
157	$(x\|(y\|y))\|(x\|(z\|z)) = (x\|(z\|y))\|(x\|(z\|y))$	[151 (2) → 156 (1)]
158*	$((x\|x)\|y)\|((z\|z)\|y) = (y\|(x\|z))\|(y\|(x\|z))$	[125 (2) → 157 (1)]

Equation 95 is a generalization of (Sheffer_1), 147 is (Sheffer_2), and 158 (flipped, with variables renamed) is (Sheffer_3). □

The preceding OTTER proof and the corresponding input file are available on line in the files **Sh-1.proof** and **Sh-1.in**.

Excluding mirror images, we have proved one other length-15 equation to be a single axiom for Boolean algebra in terms of the Sheffer stroke, namely,[2]

$$(((y|(x|y))|y)|(x|(z|y))) = x. \qquad (\mathrm{Sh}_2)$$

[2] Axiom (Sh_2) is also a member of Wolfram's list of 25 Sheffer candidates.

A proof that (Sh_2) is a single axiom is in the file **Sh-2.proof**; the corresponding input file is **Sh-2.in**.

4. (Sh_1) is a Shortest 1-Basis for the Sheffer Stroke

Our proof that there is no single axiom for Boolean algebra in terms of the Sheffer stroke with fewer symbols than (Sh_1) begins along the lines of Kunen's proofs of similar properties for group axioms [1].

Lemma 1. *Any single axiom for the Sheffer stroke must be of the form $\tau = x$, where x is an individual variable.*

Proof. Consider any structure $\mathcal{M}$, containing at least 2 elements, in which $x|y$ is a constant. $\mathcal{M}$ is not Boolean. But, any equation of the form $\alpha = \beta$ in which neither α nor β is an individual variable will be true in $\mathcal{M}$. □

Lemma 2. *If $\tau = x$ is a single axiom for Boolean algebra in terms of the Sheffer stroke, then neither the leftmost nor the rightmost variable (ignoring parentheses) in τ is x.*

Proof. If the leftmost variable in τ is x, then $\tau = x$ is true in any structure in which $x|y = x$. Such projection models are not Boolean. The right-hand case is similar. □

Lemma 3. *No equation of the form $(y|\tau) = x$ or $(\tau|y) = x$ (where x and y are individual variables and τ is any term) can be a Boolean identity in terms of the Sheffer stroke.*

Proof. Consider the 2-element NAND interpretation of the Sheffer stroke. If y takes the value 0, then $(y|\tau)$ and $(\tau|y)$ both receive the value 1, regardless of the values any other variables take. □

Theorem 3. *Every single equational axiom for Boolean algebra in terms of the Sheffer stroke has length at least 15.*

Proof. We begin by noting that any equation (in the Sheffer stroke) of the form $\tau = x$, where x is an individual variable, must have an odd length. So, all we need to show is that no Boolean identity of the form $\tau = x$ with length 3, 5, 7, 9, 11, or 13 is a single axiom for the Sheffer stroke.

To this end, we note first that any equation of the form $\tau = x$ with length less than 15 must match exactly one of 64 templates. This exhaustive list of 64 templates can be reduced to the following 19 by Lemma 3.

$$\begin{array}{rr}
((_|_)|(_|_)) = _ & ((_|((_|_)|_))|(_|_)) = _ \\
(((_|_)|_)|(_|_)) = _ & ((_|(_|(_|_)))|(_|_)) = _ \\
((_|(_|_))|(_|_)) = _ & ((_|(_|_))|((_|_)|_)) = _ \\
((_|_)|((_|_)|_)) = _ & ((_|(_|_))|(_|(_|_))) = _ \\
((_|_)|(_|(_|_))) = _ & ((_|_)|(((_|_)|_)|_)) = _ \\
((((_|_)|_)|_)|(_|_)) = _ & ((_|_)|((_|(_|_))|_)) = _ \\
(((_|(_|_))|_)|(_|_)) = _ & ((_|_)|((_|_)|(_|_))) = _ \\
(((_|_)|(_|_))|(_|_)) = _ & ((_|_)|(_|((_|_)|_))) = _ \\
(((_|_)|_)|((_|_)|_)) = _ & ((_|_)|(_|(_|(_|_)))) = _ \\
(((_|_)|_)|(_|(_|_))) = _ &
\end{array}$$

We have written programs to implement the following procedure.

1. For each of the 19 templates,
   (a) generate all well-formed equations $\tau = x$ matching the template;
   (b) delete the equations with x as the leftmost or rightmost variable of τ;
   (c) delete equations that are not Boolean identities (BIs);
   (d) delete the BIs that are subsumed by other BIs for this template.
2. With the union of the BIs from all 19 templates, delete BIs that are subsumed by other BIs in the set.
3. Delete mirror images (allowing variable renaming).

We are left with the following eight equations.

$$\begin{aligned}
((y|x)|(x|(y|z))) &= x \\
((y|x)|(x|(z|y))) &= x \\
((y|x)|(x|(z|(x|z)))) &= x \\
((y|x)|(x|(z|(z|z)))) &= x \\
((y|x)|(x|((x|x)|z))) &= x \\
((y|x)|(x|((x|z)|z))) &= x \\
((y|x)|(x|((z|x)|z))) &= x \\
((y|x)|(x|((z|z)|z))) &= x
\end{aligned}$$

Every Boolean identity of length less than 15, except those excluded by Lemma 2, is an instance of one of these eight BIs. However, none of these can be a single axiom because each is true in the following non-Boolean structure (found by the model searching program SEM [15]).

$$\begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 2 & 0 & 2 \\ 1 & 0 & 2 & 0 & 2 \\ 2 & 1 & 3 & 1 & 3 \\ 3 & 1 & 3 & 1 & 3 \end{array} \qquad (\mathcal{M}_1)$$

This completes the proof of Theorem 3, and with it the demonstration that there is no single equational axiom for the Sheffer stroke shorter than (Sh_1), (Sh_2), and their mirror images. □

5. An Exhaustive List of Possible 15-Symbol Single Axioms

Using our programs for generating and filtering formulas, we show that all but 16 of the length-15 Boolean identities, excluding mirror images and the known single axioms, are not single axioms.

We begin our argument by noting, as we did in the less-than-length-15 cases, that all length-15 Boolean identities of the form $\tau = x$ must be an instance of exactly one of 48 length-15 templates. When all well-formed equations, Boolean identities, and most general Boolean identities are generated from these 48 templates using the same techniques as in the proof of Theorem 3, there remain a total of 772 most general Boolean identities on our initial, exhaustive list of length-15 candidate formulas (counting the 4 known single axioms). When this list is filtered, first by eliminating equations with x as leftmost or rightmost variable of the left side (by Lemma 2), and then by using the following 12 structures (found by SEM) all but 36 formulas (including mirrors and the 4 known single axioms) are eliminated.

$$\begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 2 & 0 & 2 \\ 1 & 0 & 2 & 0 & 2 \\ 2 & 1 & 3 & 1 & 3 \\ 3 & 1 & 3 & 1 & 3 \end{array} \; (\mathcal{M}_1) \qquad \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 2 & 0 & 3 \\ 1 & 0 & 3 & 1 & 2 \\ 2 & 3 & 0 & 2 & 1 \\ 3 & 2 & 1 & 3 & 0 \end{array} \; (\mathcal{M}_2)$$

	0	1	2	3	4
0	0	2	3	4	1
1	3	1	4	2	0
2	4	0	2	1	3
3	1	4	0	3	2
4	2	3	1	0	4

$(\mathcal{M}_3)$

	0	1	2	3	4
0	0	2	1	4	3
1	3	1	4	0	2
2	4	3	2	1	0
3	2	4	0	3	1
4	1	0	3	2	4

$(\mathcal{M}_4)$

	0	1	2	3	4	5
0	2	2	4	2	2	4
1	3	3	3	4	3	4
2	4	0	0	0	0	4
3	1	4	1	1	1	4
4	2	3	0	1	5	4
5	4	4	4	4	4	4

$(\mathcal{M}_5)$

	0	1	2	3	4	5
0	2	3	4	1	2	4
1	2	3	0	4	3	4
2	4	3	0	1	0	4
3	2	4	0	1	1	4
4	2	3	0	1	5	4
5	4	4	4	4	4	4

$(\mathcal{M}_6)$

	0	1	2	3	4	5
0	1	0	3	2	5	4
1	0	0	0	0	0	0
2	3	0	3	0	3	3
3	2	0	0	2	2	2
4	5	0	5	5	5	0
5	4	0	4	4	0	4

$(\mathcal{M}_7)$

	0	1	2	3	4	5	6	7
0	0	0	1	2	2	6	1	6
1	2	2	6	2	2	6	6	6
2	4	0	3	2	5	7	1	6
3	2	2	2	2	2	2	2	2
4	0	0	0	2	2	2	0	2
5	4	0	4	2	5	5	0	2
6	5	2	7	2	5	7	6	6
7	5	2	5	2	5	5	2	2

$(\mathcal{M}_8)$

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	2	0	1	5	8	6	3	4	7
2	1	2	0	6	7	3	5	8	4
3	4	7	8	0	3	2	1	6	5
4	3	6	5	4	0	8	7	1	2
5	7	8	4	1	6	0	2	5	3
6	8	4	7	2	5	1	0	3	6
7	5	3	6	8	2	7	4	0	1
8	6	5	3	7	1	4	8	2	0

$(\mathcal{M}_9)$

	0	1	2	3	4	5	6	7	8
0	0	2	1	4	3	7	8	5	6
1	1	0	2	5	8	3	7	6	4
2	2	1	0	6	7	8	3	4	5
3	3	7	8	0	4	6	5	1	2
4	4	6	5	3	0	2	1	8	7
5	5	4	6	8	1	0	2	7	3
6	6	5	4	7	2	1	0	3	8
7	7	8	3	2	6	5	4	0	1
8	8	3	7	1	5	4	6	2	0

$(\mathcal{M}_{10})$

	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	2	0	1	5	6	8	7	4	3
2	1	2	0	8	7	3	4	6	5
3	4	7	6	0	3	2	5	8	1
4	3	8	5	4	0	6	2	1	7
5	7	6	4	1	8	0	3	5	2
6	8	5	3	7	1	4	0	2	6
7	5	3	8	6	2	7	1	0	4
8	6	4	7	2	5	1	8	3	0

$(\mathcal{M}_{11})$

	0	1	2	3	4	5	6	7	8
0	0	2	1	8	6	7	4	5	3
1	3	4	5	0	1	2	7	6	8
2	8	7	6	3	5	4	2	1	0
3	5	3	4	1	2	0	8	7	6
4	1	0	2	6	7	8	3	4	5
5	6	8	7	5	4	3	0	2	1
6	2	1	0	7	8	6	5	3	4
7	4	5	3	2	0	1	6	8	7
8	7	6	8	4	3	5	1	0	2

$(\mathcal{M}_{12})$

By eliminating mirror images and the known single axioms, we have the following list of 16 length-15 candidates.[3]

$$((y|(y|(y|x)))|(x|(y|z))) = x \qquad (\mathcal{C}_1)$$
$$((y|(y|(x|y)))|(x|(z|y))) = x \qquad (\mathcal{C}_2)$$
$$((y|(y|(x|x)))|(x|(z|y))) = x \qquad (\mathcal{C}_3)$$
$$((y|(y|(x|z)))|(x|(z|y))) = x \qquad (\mathcal{C}_4)$$
$$((y|(y|(z|x)))|(x|(y|z))) = x \qquad (\mathcal{C}_5)$$
$$((y|((x|y)|y))|(x|(y|z))) = x \qquad (\mathcal{C}_6)$$
$$((y|(y|(y|x)))|(x|(z|y))) = x \qquad (\mathcal{C}_7)$$
$$((((y|x)|y)|y)|(x|(z|y))) = x \qquad (\mathcal{C}_8)$$
$$((((y|x)|z)|z)|(x|(y|z))) = x \qquad (\mathcal{C}_9)$$
$$(((y|(y|x))|y)|(x|(z|y))) = x \qquad (\mathcal{C}_{10})$$
$$(((y|(x|x))|y)|(x|(z|y))) = x \qquad (\mathcal{C}_{11})$$
$$((((y|x)|z)|z)|(x|(z|y))) = x \qquad (\mathcal{C}_{12})$$
$$((((y|x)|y)|y)|(x|(y|z))) = x \qquad (\mathcal{C}_{13})$$
$$(((y|(x|z))|y)|(x|(y|z))) = x \qquad (\mathcal{C}_{14})$$
$$(((y|(z|x))|y)|(x|(y|z))) = x \qquad (\mathcal{C}_{15})$$
$$(((y|(y|x))|y)|(x|(y|z))) = x \qquad (\mathcal{C}_{16})$$

The preceding argument constitutes our proof of the following.

Theorem 4. *Every length-15 single axiom for Boolean algebra in terms of the Sheffer stroke is a member of the set* $\{\mathrm{Sh}_1, \mathrm{Sh}_2, \mathcal{C}_1\text{–}\mathcal{C}_{16}\}$ *or is a mirror image of a member of that set.*

The most general Sheffer stroke identities constructed in the proof of Theorem 4 are summarized in Table I. Note that the list of most

[3] This list is a subset (modulo mirror images) of Wolfram's list of 25 candidates [13].

general identities of length ≤ 15 is not simply the union of the other four lists, because subsumption occurs across length boundaries. The lists are available on line in the named files.

Table I. Most General Sheffer Identities

Length	Number	Filename
9	4	**Sheffer-mgi-09**
11	24	**Sheffer-mgi-11**
13	104	**Sheffer-mgi-13**
15	772	**Sheffer-mgi-15**
9+11+13+15	712	**Sheffer-mgi**

Also, the list of interpretations $\mathcal{M}_1$–M_{12} is available on line in file **Sheffer-interpretations**.

6. Conclusion

Summary and Questions. Tables II and III summarize several properties of the disjunction/negation and Sheffer bases, respectively.

Table II. OR/NOT Bases

Basis	Axioms	Length	ORs	NOTs	Variables
(DN_1)	1	22	6	7	4
(Meredith)	2	9+15	7	4	3
(Robbins)	3	7+11+13	9	4	3

Table III. Sheffer Stroke Bases

Basis	Axioms	Length	Strokes	Variables
(Sh_1)	1	15	6	3
(Veroff)	2	7+11	6	3
(Meredith)	2	9+15	9	3
(Sheffer)	3	9+11+23	17	3

Three questions remain open.

1. Is there a single axiom in terms of disjunction and negation that has only three variables? (Any equational basis for Boolean algebra

must have at least three variables.) Note that in the case of group theory, the shortest single axiom has four variables, but there exist longer axioms with three variables [1].

2. Is there a single axiom in terms of disjunction and negation with length less than 22 (i.e., that is shorter than (DN_1))?

3. Which, if any, of the remaining length-15 candidates ($\mathcal{C}_1$) – ($\mathcal{C}_{16}$) are single axioms for the Sheffer stroke?

Circles of Pure Proofs. Given n equivalent (possibly assuming additional axioms) formulas, $F_1, \ldots, F_n$, a *circle of pure proofs* is a set of n proofs,

$$F_1 \to \ldots \to F_n \to F_1,$$

such that each proof $F_i \to F_j$ contains none of the $n-2$ other formulas. The existence problem for circles of pure proofs arose for a set of three (and later four) Moufang loop identities and for equivalential calculus single axioms [14]. We have applied techniques similar to the ones described in that paper to find a circle of proofs for the four known length-15 single axioms for the Sheffer stroke: (Sh_1), (Sh_2), and their mirror images. The OTTER input files and the corresponding proofs are available on line in files **circle-[1234].in** and **circle-[1234].proof**.

Soundness of Computer Proofs. Theorems produced by computers are always questionable. To check OTTER's proofs, we ran them through Ivy, an independent proof checker about which several soundness metatheorems have been proved [6]. Theorems proved by exhaustive enumeration are even more questionable, because explicit proofs are usually not produced. To check our proofs of Theorems 3 and 4, two of the authors independently wrote code, in different languages, to generate and filter formulas, and we have made the resulting sets of formulas available on line (see Table I).

References

1. Kunen, K.: 1992, 'Single Axioms for Groups'. *J. Automated Reasoning* **9**(3), 291–308.
2. McCune, W.: 1994a, 'Otter'. `http://www.mcs.anl.gov/AR/otter/`.
3. McCune, W.: 1994b, 'Otter 3.0 Reference Manual and Guide'. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL.
4. McCune, W.: 1997, 'Solution of the Robbins Problem'. *J. Automated Reasoning* **19**(3), 263–276.

5. McCune, W.: 2000, 'Single Axioms for Boolean Algebra'. Tech. Memo ANL/MCS-TM-243, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL.
6. McCune, W. and O. Shumsky: 2000, 'IVY: A Preprocessor and Proof Checker for First-Order Logic'. In: M. Kaufmann, P. Manolios, and J. Moore (eds.): *Computer-Aided Reasoning: ACL2 Case Studies.* Kluwer Academic. To appear.
7. Meredith, C. A.: 1969, 'Equational Postulates for the Sheffer Stroke'. *Notre Dame J. Formal Logic* **10**(3), 266–270.
8. Meredith, C. A. and A. N. Prior: 1968, 'Equational Logic'. *Notre Dame J. Formal Logic* **9**, 212–226.
9. Padmanabhan, R. and W. McCune: 1995, 'Single Identities for Ternary Boolean Algebras'. *Computers and Mathematics with Applications* **29**(2), 13–16.
10. Padmanabhan, R. and R. W. Quackenbush: 1973, 'Equational theories of algebras with distributive congruences'. *Proc. AMS* **41**(2), 373–377.
11. Sheffer, H.: 1913, 'A set of five independent postulates for Boolean algebras, with application to logical constants'. *Trans. AMS* **14**(4), 481–488.
12. Veroff, R.: 2000, 'Short 2-Bases for Boolean Algebra in Terms of the Sheffer Stroke'. Tech. Report TR-CS-2000-25, Computer Science Department, University of New Mexico, Albuquerque, NM.
13. Wolfram, S.: 2000. Correspondence by electronic mail.
14. Wos, L.: 1995, 'Searching for Circles of Pure Proofs'. *J. Automated Reasoning* **15**(3), 279–315.
15. Zhang, J. and H. Zhang: 1995, 'SEM: A System for Enumerating Models'. In: *Proceedings of the International Joint Conference on Artificial Intelligence.*