ARGONNE NATIONAL LABORATORY
9700 South Cass Avenue
Argonne, IL 60439

ANL/MCS-TM-244

A Short Sheffer Axiom for Boolean Algebra

by

Robert Veroff and William McCune

`http://www.cs.unm.edu/~veroff`
`http://www.mcs.anl.gov/~mccune`

Mathematics and Computer Science Division

Technical Memorandum No. 244

June 2000

This work was supported 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 by the National Science Foundation under Grant CDA-9503064.

Contents

A Short Sheffer Axiom for Boolean Algebra

by

Robert Veroff and William McCune

Abstract

A short Sheffer stroke identity is shown to be a single axiom for Boolean algebra. The axiom has length 15 and 3 variables. The proof shows that it is equivalent to Sheffer's original 3-basis for the theory. Automated deduction techniques were used to find the proof. The shortest single axiom previously known to us has length 105 and 6 variables.

1 Introduction

Logicians have long had an interest in finding simple axiom systems for various algebras and logics, where simplicity is characterized by the number of axioms in a system or by the lengths of the axioms in a system. In this report, we show that a short Sheffer stroke identity is a single axiom for Boolean algebra. The Sheffer stroke "|" can be interpreted as the "NOR" operation, $x|y = x' \wedge y'$.

In 1913, Sheffer [5] presented the following three-axiom equational basis (3-basis) for Boolean algebra.

$$(x|x)|(x|x) = x \tag{Sheffer-1}$$

$$x|(y|(y|y)) = x|x \tag{Sheffer-2}$$

$$(x|(y|z))|(x|(y|z)) = ((y|y)|x)|((z|z)|x) \tag{Sheffer-3}$$

In 1969, Meredith [3] presented the following 2-basis for the same theory.

$$(x|x)|(y|x) = x \tag{Meredith-1}$$

$$x|(y|(x|z)) = ((z|y)|y)|x \tag{Meredith-2}$$

Researchers have known for some time that single equational axioms (i.e., 1-bases) exist for Boolean algebra, including presentation in terms of the Sheffer stroke. In 1973, Padmanabhan and Quackenbush [4] presented a method for constructing a single axiom for any finitely based theory that has certain distributive and permutable congruences, and Boolean algebra has these properties. However, straightforward application of the method usually yields single axioms of enormous length. McCune [2] used the construction method with a variety of automated deduction techniques to find single axioms of reasonable length for Boolean algebra under a variety of treatments. In particular, an axiom of length 105, with six variables, was found for the Sheffer stroke.

Stephen Wolfram recently brought to our attention [6] a set of 25 Sheffer identities, all of length 15 with 3 variables, that he was investigating as being possible single axioms. His interest in finding simple bases for Boolean algebra arose in work on his project *A New Kind of Science* [7].

In this note, we show that the equation

$$((x|z)|y)|((x|(x|y))|x) = y \tag{BA-1}$$

is a single axiom for Boolean algebra in terms of the Sheffer stroke. As a simple corollary, we have that the mirror image of (BA-1),

$$(x|((y|x)|x))|(y|(z|x)) = y, \tag{BA-2}$$

is also a single axiom, because the mirror image of a Sheffer basis is also a Sheffer basis.

Equation (BA-2) is a member of Wolfram's set of 25 Sheffer identities.

2 The Proof

The proof of Theorem 1 below is presented by way of derivations obtained with the automated deduction system Otter [1]. The Otter proofs are by contradiction. The justification $[m \to n]$ indicates paramodulation from equation m into equation n.

The methods we used to find the Otter proofs involved heavy use of automated deduction techniques. A subsequent report will contain details of the work.

THEOREM 1 *Equation (BA-1) is a basis for Boolean algebra in terms of the Sheffer stroke.*

Proof. We show that (BA-1) is equivalent to the Sheffer 3-basis $\{$(Sheffer-1),(Sheffer-2),(Sheffer-3)$\}$ with two Otter proofs. First we show that (BA-1) is sound by proving it from the Sheffer 3-basis; then we show that it is complete by deriving the Sheffer 3-basis from it. The Sheffer stroke symbol is omitted to save space.

Part 1: $\{$(Sheffer-1),(Sheffer-2),(Sheffer-3)$\} \Longrightarrow$ (BA-1).

2	$(xx)(xx) = x$	[(Sheffer-1)]
3	$x(y(yy)) = xx$	[(Sheffer-2)]
4	$((yy)x)((zz)x) = (x(yz))(x(yz))$	[(Sheffer-3)]
5	$((AB)C)((A(AC))A) \neq C$	[denial of (BA-1)]
58	$x((yy)y) = xx$	$[3 \leftarrow 2]$
60	$(xx)(y(yy)) = x$	$[3 \leftarrow 2]$
67	$(xx)((yy)y) = x$	$[58 \leftarrow 2]$
70	$(xx)(x((yy)y)) = x$	$[58 \to 2]$
72	$(x((yy)y))(z(zz)) = x$	$[60 \leftarrow 58]$
80	$(x((yy)y))(x((zz)z)) = x$	$[70 \leftarrow 58]$
103	$(x((yy)z))(x((yy)z)) = (yx)((zz)x)$	$[4 \leftarrow 2]$
112	$(((xx)(xx))y)((xx)y) = y$	$[4 \leftarrow 80]$
116	$((x(yx))(x(yx)))(z(zz)) = (yy)x$	$[4 \to 72]$
117	$((x(yy))(x(yy)))((zz)z) = (yy)x$	$[4 \to 67]$
143	$(xy)((xx)y) = y$	$[112 \leftarrow 2]$
166	$((xx)y)(xy) = y$	$[143 \leftarrow 2]$
198	$x(yx) = (yy)x$	$[116 \leftarrow 60]$
209	$(xy)((xx)y) = (yy)(xy)$	$[198 \leftarrow 198]$
264	$(xx)(yx) = x$	$[209 \leftarrow 143]$
303	$(x(yx))x = yx$	$[264 \to 143]$
372	$x(yy) = (yy)x$	$[117 \leftarrow 264]$
386	$((xx)(xx))y = yx$	$[372 \leftarrow 264]$
403	$(xy)(yy) = y$	$[372 \leftarrow 264]$
435	$(x(yy))(yx) = x$	$[372 \to 166]$
458	$(x(y(zu)))(((zz)y)((uu)y)) = y(zu)$	$[403 \leftarrow 4]$

471	$(xy)((yy)x) = x$	$[435 \leftarrow 403]$
518	$(xy)((y(z(zz)))x) = x$	$[471 \leftarrow 3]$
558	$xy = yx$	$[386 \leftarrow 403]$
594	$(xx)(xy) = x$	$[386 \rightarrow 264]$
598	$(xy)(xx) = x$	$[386 \rightarrow 403]$
602	$((xx)y)(yx) = y$	$[386 \rightarrow 143]$
656	$(x(yz))(x(yz)) = ((yy)x)((zz)x)$	$[558 \leftarrow 4]$
681	$((xy)(xy))x = xy$	$[594 \leftarrow 471]$
713	$(xy)(x(z(zz))) = x$	$[598 \leftarrow 3]$
730	$((x(y(yy)))z)(zx) = z$	$[602 \leftarrow 3]$
1084	$((x(yz))(x(yz)))(((yy)x)((zz)x))$ $= (z((yy)x))((xx)((yy)x))$	$[103 \leftarrow 656]$
1110	$((xy)((zz)y))y = y((xx)z)$	$[103 \rightarrow 681]$
1239	$(x((yy)z))((zz)((yy)z)) = z(yx)$	$[1084 \leftarrow 458]$
1259	$(x((yy)z))z = z(yx)$	$[1239 \leftarrow 264]$
1362	$x((yy)z) = x(z(yx))$	$[1259 \leftarrow 1110]$
1504	$x((yz)(yx)) = xy$	$[1362 \leftarrow 594]$
1666	$(xy)((((y(z(zz)))x)u)x) = (xy)((y(z(zz)))x)$	$[1504 \leftarrow 730]$
1842	$(xy)(x(((y(z(zz)))(y(z(zz))))u)) = (xy)((y(z(zz)))x)$	$[1666 \leftarrow 1110]$
1847	$(xy)((y(z(zz)))x) = (xy)(x(yu))$	$[1842 \leftarrow 713]$
1856	$(xy)(x(yz)) = x$	$[1847 \leftarrow 518]$
1895	$(x(yz))(xy) = x$	$[1856 \leftarrow 1856]$
1972	$((xy)z)(zx) = z$	$[1895 \leftarrow 558]$
2142	$((xy)z)((x(zx))x) = z$	$[1972 \leftarrow 303]$
3223	$((xy)z)((x(xz))x) = z$	$[2142 \leftarrow 558]$
3224	$\square$	$[3223, 5]$

Part 2: (BA-1) $\Longrightarrow$ $\{$(Sheffer-1),(Sheffer-2),(Sheffer-3)$\}$.

2	$((xy)z)((x(xz))x) = z$	[(BA-1)]
3	$(AA)(AA) \neq A \quad \vee \quad A(B(BB)) \neq AA$ $\vee \quad ((BB)A)((CC)A) \neq (A(BC))(A(BC))$	[denial]
140	$(xy)((((zu)x)(((zu)x)y))((zu)x)) = y$	$[2 \leftarrow 2]$

141 $(((x(xy))x)z)((y((((xu)y)((x(xy))x))z))(((xu)y)((x(xy))x)))$
$\quad = z$ [$140 \leftarrow 2$]

142 $(xy)(((zx)((zx)y))(zx)) = y$ [$140 \rightarrow 2$]

143 $(((x(xy))x)z)((y(yz))(((xu)y)((x(xy))x))) = z$ [$141 \leftarrow 2$]

144 $(((x(xy))x)z)((y(yz))y) = z$ [$143 \leftarrow 2$]

145 $x((y(y((x(xx))x)))y) = (x(xx))x$ [$144 \leftarrow 2$]

146 $(((x(xx))x)(((x(xx))x)((x(xx))x)))((x(xx))x)$
$\quad = ((x(xx))x)((x((x(xx))x))x)$ [$145 \leftarrow 145$]

147 $((x(xx))x)((x((x(xx))x))x) = (((x(xx))x)x)((x(xx))x)$ [$146 \leftarrow 2$]

148 $((x(xx))x)((x((x(xx))x))x) = x$ [$147 \leftarrow 144$]

149 $(((x(xx))x)(((x(xx))x)((x(xx))x)))((x(xx))x) = x$ [$148 \leftarrow 146$]

150 $(((x(xx))x)(((x(xx))x)((x(xx))x)))((x(xx))x)$
$\quad = ((x(xx))x)((y(yx))y)$ [$149 \rightarrow 145$]

151 $(x(xx))x = xx$ [$149 \rightarrow 145$]

152 $((xy)x)(xx) = x$ [$151 \rightarrow 2$]

154 $(xx)(xx) = x$ [$152 \leftarrow 151$]

155 $x((y(y(xx)))y) = xx$ [$152 \rightarrow 144$]

156 $((x(xx))x)((y(yx))y) = x$ [$150 \leftarrow 149$]

157 $(xx)((y(yx))y) = x$ [$156 \leftarrow 151$]

158 $(x((y(yx))y))(((xx)x)(xx)) = (y(yx))y$ [$157 \rightarrow 142$]

159 $(x((y(yx))y))x = (y(yx))y$ [$158 \leftarrow 152$]

160 $(((x(xy))x)(((yy)y)(yy)))((x(xy))x)$
$\quad = ((yy)((yy)((x(xy))x)))(yy)$ [$159 \leftarrow 157$]

161 $((x(xy))x)(yy) = y$ [$159 \rightarrow 152$]

165 $(x(yy))((((x(xy))x)y)((x(xy))x)) = yy$ [$161 \rightarrow 142$]

166 $((xx)((xx)((y(yx))y)))(xx) = (((y(yx))y)x)((y(yx))y)$ [$160 \leftarrow 152$]

167 $(((x(xy))x)y)((x(xy))x) = ((yy)y)(yy)$ [$166 \leftarrow 157$]

168 $(((x(xy))x)y)((x(xy))x) = y$ [$167 \leftarrow 152$]

169 $(x(yy))y = yy$ [$168 \rightarrow 165$]

170 $(xy)(yy) = (yy)(yy)$ [$169 \leftarrow 154$]

177 $(xy)(yy) = y$ [$170 \leftarrow 154$]

178 $x(((yx)x)(yx)) = xx$ [$177 \rightarrow 155$]

179 $(x(xx))(((yx)x)(yx)) = xx$ [$177 \rightarrow 142$]

180 $(xx)((x(x(((yx)x)(yx))))x) = ((yx)x)(yx)$ [$179 \rightarrow 2$]

181 $(xx)((x(xx))x) = ((yx)x)(yx)$ [$180 \leftarrow 178$]

183	$((xy)y)(xy) = y$	$[181 \leftarrow 157]$
184	$(x(yx))(((yx)x)(yx)) = yx$	$[183 \leftarrow 183]$
185	$(x(yx))x = yx$	$[184 \leftarrow 183]$
187	$(xx)(((x(yx))(yx))(x(yx))) = x$	$[185 \rightarrow 157]$
192	$(xx)(yx) = x$	$[187 \leftarrow 183]$
193	$x(y(xx)) = xx$	$[192 \leftarrow 192]$
195	$((x(yy))y)(zy) = y$	$[192 \leftarrow 169]$
196	$(((xx)y)(zx))(((xx)x)(xx)) = zx$	$[192 \rightarrow 2]$
198	$((xy)(((z(yy))y)(xy)))(xy) = y$	$[195 \leftarrow 185]$
201	$(((xx)y)(zx))x = zx$	$[196 \leftarrow 183]$
202	$(x(xy))x = yx$	$[201 \leftarrow 2]$
205	$(xx)(xy) = x$	$[202 \rightarrow 157]$
206	$(xy)(xx) = x$	$[202 \rightarrow 161]$
207	$(xy)(y(zx)) = y$	$[202 \rightarrow 142]$
208	$((xy)z)(zx) = z$	$[202 \rightarrow 2]$
211	$x((xy)(z(xx))) = xy$	$[207 \leftarrow 205]$
212	$((xy)z)(zy) = z$	$[207 \leftarrow 198]$
213	$(x(xy))x = xy$	$[207 \leftarrow 206]$
214	$(xy)(y(xz)) = y$	$[208 \leftarrow 206]$
216	$xy = yx$	$[213 \leftarrow 202]$
221	$((xy)z)(xz) = z$	$[213 \rightarrow 2]$
222	$(x(yz))(zx) = x$	$[216 \leftarrow 207]$
224	$((x(xy))x)((xz)y) = y$	$[216 \leftarrow 2]$
225	$(x(yz))(xz) = x$	$[216 \rightarrow 212]$
226	$(x(yz))(xy) = x$	$[216 \rightarrow 208]$
227	$(xy)(x(zy)) = x$	$[216 \rightarrow 207]$
228	$(xy)((xz)y) = y$	$[214 \leftarrow 216]$
229	$((xy)(xz))z = xz$	$[214 \rightarrow 207]$
230	$x(y(x(yz))) = x(yz)$	$[221 \leftarrow 214]$
231	$x(y(x(zy))) = x(zy)$	$[221 \leftarrow 207]$
232	$(x(y(zx)))y = y(zx)$	$[222 \rightarrow 214]$
233	$x((yx)(zy)) = yx$	$[222 \rightarrow 212]$
234	$(x(y(xz)))y = y(xz)$	$[226 \rightarrow 207]$
235	$((xy)(zy))x = xy$	$[227 \leftarrow 227]$
236	$((x(yz))z)x = x(yz)$	$[227 \leftarrow 225]$

239 $(x(yz))(x(u(yx))) = (yx)(x(yz))$ $[233 \leftarrow 214]$

243 $(x(xy))y = yy$ $[224 \rightarrow 229]$

244 $(x(yx))y = yy$ $[243 \leftarrow 216]$

245 $x(y(yx)) = xx$ $[243 \leftarrow 216]$

251 $x(y(xy)) = xx$ $[244 \leftarrow 216]$

257 $x((yx)y) = xx$ $[245 \leftarrow 216]$

258 $(xx)((xy)(z(xz))) = z(xz)$ $[251 \rightarrow 228]$

259 $(xy)(x(x(zy))) = (xy)(xy)$ $[257 \leftarrow 225]$

266 $x(yy) = x(yx)$ $[230 \leftarrow 251]$

267 $x(yy) = x(xy)$ $[266 \leftarrow 216]$

268 $(xy)y = y(xx)$ $[266 \leftarrow 216]$

269 $x((xy)(z(xz))) = xy$ $[266 \rightarrow 211]$

270 $x(yx) = (yy)x$ $[266 \rightarrow 216]$

273 $(x(yy))x = yx$ $[266 \rightarrow 185]$

274 $x(x(yy)) = xy$ $[267 \leftarrow 206]$

275 $(xy)x = x(yy)$ $[267 \leftarrow 216]$

279 $((xy)(xy))(xx) = (xx)x$ $[270 \leftarrow 206]$

280 $x(x(yy)) = yx$ $[273 \leftarrow 216]$

286 $x(xy) = x(yy)$ $[274 \leftarrow 206]$

288 $((xy)(zy))(xx) = (xy)((xy)(zy))$ $[275 \leftarrow 235]$

290 $(x(y(xz)))y = y(zx)$ $[232 \leftarrow 216]$

291 $x(yz) = x(zy)$ $[290 \leftarrow 234]$

293 $(xy)z = z(yx)$ $[291 \leftarrow 216]$

294 $x(yz) = (zy)x$ $[291 \leftarrow 216]$

296 $(xy)(zu) = (uz)(yx)$ $[293 \leftarrow 291]$

297 $((xy)(xy))(xx) = x(xx)$ $[279 \leftarrow 294]$

298 $((xx)(xx))((xy)(z(xz))) = ((xy)(z(xz)))(z(xz))$ $[258 \rightarrow 270]$

299 $(x(y(zy)))(x(x(zz))) = (x(y(zy)))(x(y(zy)))$ $[259 \leftarrow 251]$

300 $(x(yz))(x(u(yx))) = x$ $[239 \leftarrow 214]$

302 $x(y(x(z(yx)))) = xx$ $[300 \rightarrow 236]$

303 $x(y(z(xy))) = x(yy)$ $[302 \rightarrow 230]$

304 $x((yy)(z(x(xy)))) = x((yy)(yy))$ $[303 \leftarrow 286]$

305 $x(y((yx)z)) = x(yy)$ $[303 \leftarrow 294]$

306 $(xy)((xy)(xy)) = x(xx)$ $[288 \leftarrow 297]$

307 $((x(xx))y)((xz)y) = y$ $[306 \rightarrow 221]$

317	$(x(xx))y = yy$	$[307 \to 229]$
319	$x(y(yy)) = xx$	$[317 \leftarrow 216]$
326	$(xy)(x(z(zz))) = x$	$[319 \to 206]$
327	$x((yy)(z(x(xy)))) = xy$	$[304 \leftarrow 206]$
328	$(x(y(zy)))(x(y(zy))) = (x(y(zy)))(xz)$	$[299 \leftarrow 274]$
329	$((xx)(xx))((xy)(z(xz))) = (z(xz))((xy)(xy))$	$[298 \leftarrow 268]$
330	$(x(yx))((yz)(yz)) = y((yz)(x(yx)))$	$[329 \leftarrow 206]$
331	$(x(yx))((yz)(yz)) = yz$	$[330 \leftarrow 269]$
332	$(x((yz)x))(y((yz)(y(u(uu))))) = (yz)(y(u(uu)))$	$[331 \leftarrow 326]$
335	$(x((yz)x))(yy) = (yz)(y(u(uu)))$	$[332 \leftarrow 326]$
336	$(x((yz)x))(yy) = y$	$[335 \leftarrow 326]$
337	$(x(x(yz)))(zz) = z$	$[336 \leftarrow 294]$
344	$x((y(y(zx)))x) = y(y(zx))$	$[337 \to 226]$
345	$x(y(z(z(u(yx))))) = x(yy)$	$[344 \to 305]$
346	$x(y(y(z(xy)))) = x(y(xx))$	$[345 \to 230]$
347	$x(y(y(z(xy)))) = xx$	$[346 \leftarrow 193]$
348	$(xx)(y(y(z(y(xy))))) = (xx)(xx)$	$[347 \leftarrow 270]$
350	$(xx)(y(y(z(y(xy))))) = x$	$[348 \leftarrow 206]$
351	$x(((y(x(zx)))(y(x(zx))))z) = x(y(x(zx)))$	$[350 \to 327]$
352	$x(((y(x(zx)))(yz))z) = x(y(x(zx)))$	$[351 \leftarrow 328]$
353	$x(y(x(zx))) = x(yz)$	$[352 \leftarrow 229]$
354	$x(y(x(xz))) = x(yz)$	$[353 \leftarrow 216]$
355	$x(y(x(zz))) = x(yz)$	$[353 \leftarrow 266]$
358	$x(y(zx)) = x(y(zz))$	$[354 \leftarrow 280]$
359	$(x(yz))(x(yz)) = (x(yz))(x(zz))$	$[358 \leftarrow 231]$
360	$(x(y(x(zz))))(x(zz)) = (x(yz))(x(yz))$	$[359 \leftarrow 355]$
361	$(x(yy))(x(z(x(yy)))) = (x(zy))(x(zy))$	$[360 \leftarrow 216]$
362	$(x(yy))(x(zz)) = (x(zy))(x(zy))$	$[361 \leftarrow 358]$
363	$((xx)y)((zz)y) = (y(xz))(y(xz))$	$[362 \leftarrow 296]$
364	$\square$	$[3, 206, 319, 363]$

Web Resources

`www.mcs.anl.gov/~mccune/ba-sheffer-15` contains Otter input files for the Otter proofs in Section 2.

`www.mcs.anl.gov/~mccune/ba-axioms` contains Otter input files, proofs, and other data related to paper [2].

`www.mcs.anl.gov/AR/otter/` contains information on Otter, including freely downloadable versions of Otter for Unix-like systems, Macintoshes, and Microsoft Windows systems.

References

[1] W. McCune. Otter 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994.

[2] W. McCune. Single Axioms for Boolean Algebra. Tech. Memo ANL/MCS-TM-243, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, June 2000.

[3] C. A. Meredith. Equational postulates for the Sheffer stroke. *Notre Dame J. Formal Logic*, 10(3):266–270, 1969.

[4] R. Padmanabhan and R. W. Quackenbush. Equational theories of algebras with distributive congruences. *Proc. of AMS*, 41(2):373–377, 1973.

[5] H. Sheffer. A set of five independent postulates for Boolean algebras, with application to logical constants. *Trans. AMS*, 14(4):481–488, 1913.

[6] S. Wolfram, Feb 4 2000. Correspondence by electronic mail.

[7] S. Wolfram. A New Kind of Science. `http://wolframscience.com`, 2000.