Single Axioms for the Left Group and Right Group Calculi *

William W. McCune
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4801
U.S.A.
phone: 708-972-3065, e-mail: mccune@mcs.anl.gov

March 30, 1995

1 Introduction

In [2], J. A. Kalman presents axiomatizations of the left group tautologies and the right group tautologies. In this paper we sharpen those results by showing that Kalman's axiomatizations are dependent and by giving other simpler axiomatizations, including ones that consist of single formulas.

A *left group formula* is an expression constructed from variables and a binary function symbol E. A left group formula α is a *left group tautology* iff $\alpha = 1$ is valid in (multiplicative) group theory when $E(x, y)$ is interpreted as $x^{-1} \cdot y$. The *left group calculus* consists of left group formulas and the inference rules variable instantiation and modus ponens, where E is treated as implication (i.e., from α and $E(\alpha, \beta)$ infer β). An *axiomatization of the left group calculus* is a finite set of left group tautologies from which every left group tautology

*This work was supported by the Applied Mathematical Sciences subprogram of the Office of Energy Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

is derivable in the left group calculus. A *single axiom for the left group tautologies* is a left group formula α such that $\{\alpha\}$ is an axiomatization of the left group calculus.

There are analogous definitions for the *right group calculus*, in which $E(x, y)$ is interpreted as $x \cdot y^{-1}$. (Ordinary modus ponens, rather than reverse modus ponens is used for the right group calculus. This is discussed in Section 3.)

The inference rule used for the proofs in this paper is C. A. Meredith's *condensed detachment* [5, 9], which uses unification to combine the operations of modus ponens and instantiation: consider premises α and $E(\gamma, \beta)$, in which variables have been renamed, if necessary, so that they have no variables in common; if α and γ unify, then infer the (most general) corresponding instance of β. Every formula that can be derived by modus ponens and instantiation either can be derived by condensed detachment or is a instance of a formula that can be derived by condensed detachment [4]. See the proof of Theorem 4 below for simple examples of the application of condensed detachment.

Section 2 contains condensed detachment proofs that three (L1, L4, and L5) of Kalman's five axioms for the left group calculus are dependent on the remaining two axioms. It is then shown that

$$E(E(E(E(x, y), z), E(E(u, v), E(E(E(w, v), E(w, u)), s))), E(z, E(E(y, x), s))) \qquad \text{(S1)}$$

is a single axiom for the left group calculus. Several other simple axiomatizations (which are not single axioms) are also given. Section 3 contains condensed detachment proofs that four (R1, R3, R4, and R5) of Kalman's five axioms for the right group calculus are dependent on the remaining axiom R2:

$$E(x, E(x, E(E(y, z), E(E(y, u), E(z, u))))). \qquad \text{(R2)}$$

Five other single axioms for the right group calculus are also given (without proof).

Single axioms are known for the equivalential calculus [11], in which $E(\alpha, \beta)$ can be interpreted as the $\alpha \cdot \beta$ in Boolean groups, and for the L-calculus [8] (respectively R-calculus [1]) in which $E(\alpha, \beta)$ can be interpreted as $\alpha^{-1} \cdot \beta$ (respectively $\alpha \cdot \beta^{-1}$) in Abelian

groups. Prior to the work reported in this paper, no single axioms for the left group or right group calculi were known to the author. The new single axioms answer questions raised by C. A. Meredith in [8, p. 222].

We made extensive use of the automated theorem-proving program OTTER [6] in obtaining the new axiomatizations. Theorem-proving programs have been used to study given candidate axiomatizations in related areas, for example, [3, 12, 10], but here, the goal was to *find* simpler axiomatizations. OTTER was used to generate candidate axiomatizations, to search for proofs that the candidates are in fact axiomatizations, and to search for dependencies in axiomatizations.

2 The Left Group Calculus

From here on, formulas are written in Polish notation. In the proofs that follow, the justification [m,n] indicates that formula m is the major premise $E\alpha\beta$ and that n is the minor premise, which unifies with α. The result is the corresponding instance of β. Variables are renamed starting with x, y, z, u, v, w, s, t. The formula numbers indicate position in the sequence of formulas retained by OTTER.

Kalman's axiomatization of the left group calculus consists of the following five axioms [2]:

$$EEExEEyyxzz \tag{L1}$$

$$EEEEExyExzEyzuu \tag{L2}$$

$$EEEEEExyExzuEEyzuvv \tag{L3}$$

$$EEEExyzuEEExvzEEyvu \tag{L4}$$

$$EEExEEyxzEEuxvEEEExyuzv \tag{L5}$$

Theorem 1. *The pair of formulas* {L2,L3} *axiomatizes the left group calculus.*

Proof (OTTER). The following condensed detachment proof derives L4, L5′, which is a generalization of L5, and L1 from {L2,L3}:

3		$EEEEExyExzEyzuu$	(L2)
4		$EEEEEExyExzuEEyzuvv$	(L3)
18	[4,4]	$EEExyzEEuyEExuz$	
21	[18,18]	$EExyEEEzuxEEvuEEzvy$	
22	[4,18]	$EExyEEEEzuEzvxEEuvy$	
23	[3,18]	$EExEyzEEEyuxEuz$	
25	[18,4]	$EExyEEEEEEzuEzvwEEuvwxy$	
34	[4,21]	$EEExyEEEzuEzvwEEsyEExsEEuvw$	
37	[21,4]	$EEExyEEEEEzuEzvwEEuvwsEEtyEExts$	
43	[3,22]	$EEEExyExzEEuvEuwEEyzEvw$	
46	[22,4]	$EEEExyExzEEEEEuvEuwsEEvwstEEyzt$	
48	[23,23]	$EEEEExyzuEzExvEuEyv$	
56	[23,18]	$EEEExyzEEuyvEzEEuxv$	
58	[23,3]	$EEExyEEEEzuEzvEuvExwEyw$	
139	[43,3]	$EEExyEEzxuEEzyu$	
366	[34,139]	$EExEEEyzuvEEEuEywxEEzwv$	
372	[23,139]	$EEEExyzEEuyEExuvEzv$	
375	[18,139]	$EExEEyzuEEEzvxEEyvu$	
385	[37,25]	$EExyEEEEEzuvEEwuEEzwvxy$	
1475	[46,22]	$EEEExyzuEEExvzEEyvu$	(L4)
2688	[56,18]	$ExEEyzEEzyx$	
3811	[48,2688]	$ExEyEEEEzuyEuzx$	
4814	[372,3811]	$ExEEEEyzEEzyuux$	
6608	[375,4814]	$EEExyzEEEEuvEEvuxyz$	
8757	[366,6608]	$EEExEEyzuEEvxwEEEEzyvuw$	(L5′)
19117	[58,385]	$EEExEEyyxzz$	(L1)

Theorem 2. *The pair of formulas* {L2,P1} *axiomatizes the left group calculus:*

$$EEEEExyExzEyzuu \tag{L2}$$

$$EEExyzEEuyEExuz \tag{P1}$$

Proof (OTTER). P1 is a left group tautology (which can be verified by rewriting $E\alpha\beta$ to $\alpha^{-1}\beta$ and reducing to 1). The following condensed detachment proof derives L3 from {L2,P1}:

3		$EEEExyExzEyzuu$	(L2)
4		$EExyzEEuyEExuz$	(P1)
32	[3,4]	$EExEyzEEEyuxEuz$	
35	[32,32]	$EEEExyzuEzExvEuEyv$	
38	[32,4]	$EEEExyzEEuyvEzEEuxv$	
44	[35,3]	$EEExyEEzxuEEzyu$	
61	[38,4]	$ExEEyzEEzyx$	
86	[32,44]	$EEEExyzEEuyEExuvEzv$	
93	[38,61]	$ExEEyzEEuyEEzux$	
116	[86,44]	$EEExyEEyxzz$	
161	[35,93]	$ExEyEEzuEEEEuvyEvzx$	
219	[32,116]	$EEExyEEzuEEuzExvEyv$	
221	[4,116]	$EExEEyzuEEEzyxu$	
1111	[221,221]	$EEExEyzExEEzyuu$	
1127	[4,1111]	$EExEyEEzuvEEEyEuzxv$	
1511	[219,161]	$ExEEEEyzEyuEzux$	
1522	[38,1511]	$ExEEEEyzEyuvEEvEzux$	
1524	[1127,1522]	$EEEEEExyExzuEEyzuvv$	(L3)

Theorem 3. *Formula* S1 *is a single axiom for the left group calculus:*

$$EEEExyzEEuvEEEwvEwusEzEEyxs \tag{S1}$$

Proof (OTTER). S1 is a left group tautology (which can be verified by rewriting $E\alpha\beta$ to $\alpha^{-1}\beta$ and reducing to 1). The following condensed detachment proof derives P1 and L2 from S1:

10 $EEEExyzEEuvEEEwvEwusEzEEyxs$ (S1)

23 [10,10] $EEExyEEEzyEzxuEEEvwEEsvEswu$

24 [10,23] $EEEExyExzEEEuEEvwEvsEuEwstEEyzt$

26 [24,10] $EEEExEEyzEyuExEzuEEEvwEvstEEwst$

32 [26,24] $EEExyzEEEuxEuyz$

33 [26,10] $EEEExyExzuEEyzu$

34 [32,32] $EEExEyzExuEEEvyEvzu$

41 [33,33] $EEExyzEEuyEExuz$ (P1)

331 [24,34] $EEEEExyExzEyzuu$ (L2)

Six other axiomatizations of the left group calculus were also discovered with the assistance of OTTER. The axiomatizations include formulas from the following list:

$EEEEExyExzEyzuu$ (L2)

$EEExyzEEuyEExuz$ (P1)

$ExEEEEyzEyuEzux$ (P4)

$ExEEyzEEzyx$ (Q1)

$EExyEEzxEzy$ (Q2)

$EEExyEEyxzz$ (Q3)

$EEExyExzEyz$ (Q4)

Each of the sets {L2,P4}, {L2,Q1,Q2}, {P1,Q3}, {P4,Q3}, {Q1,Q2,Q3}, {Q1,Q3,Q4} is an axiomatization of the left group calculus. Proofs can be found in [7].

3 The Right Group Calculus

Kalman's axiomatization of the right group tautologies consists of the following five axioms [2]:

$ExExEEyEzzy$ (R1)

$ExExEEyzEEyuEzu$ (R2)

$$ExExEEyEzuEyEEzvEuv \tag{R3}$$

$$EEExEyzEuEyvExEuEzv \tag{R4}$$

$$EExEyEzEuvEExEvzEEyEvuv \tag{R5}$$

Let the *mirror image* of a formula be obtained by rewriting each occurrence of $E\alpha\beta$ to $E\beta\alpha$. Note that each of the five axioms R1–R5 is the mirror image (after renaming variables) of the the corresponding axiom in L1–L5. When the inference rule used with the right group tautologies is *reverse* modus ponens, it is easy to see that the resulting calculus is isomorphic to the left group calculus. However, Kalman states (without proof) that ordinary modus ponens can also be used with R1–R5 to axiomatize the right group tautologies. We sketch a proof of this result here.

Theorem 4. *From formulas* R1–R5*, one can derive all right group tautologies with instantiation and ordinary modus ponens.*

Proof sketch (OTTER). We show that from R1–R5 (in fact, from just R2) and ordinary condensed detachment, we can derive reverse modus ponens. We do this by assuming $E\alpha\beta$ and β, for constants α and β, and deriving α. Once we have reverse modus ponens, we can derive all right group tautologies.

2		$E\alpha\beta$	
3		β	
4		$ExExEEyzEEyuEzu$	(R2)
6	[4,3]	$E\beta EExyEExzEyz$	
8	[6,3]	$EExyEExzEyz$	
9	[8,8]	$EEExyzEEExuEyuz$	
10	[8,2]	$EE\alpha xE\beta x$	
25	[9,10]	$EEE\alpha xEyxE\beta y$	
26	[9,8]	$EExyEzyEExuEzu$	
29	[9,25]	$EEEE\alpha xyEEzxyE\beta z$	
59	[26,26]	$EExyzEExyz$	
90	[29,59]	$E\beta\alpha$	

93 [90,3] α

For the right group calculus, we use ordinary modus ponens rather than reverse modus ponens in order to have a system that is substantially different from the left group calculus. In addition, it appears that the right group calculus has axiomatizations that are simpler than the left group calculus has.

Theorem 5. *Formula* R2 *is a single axiom for the right group calculus.*

Proof (OTTER). The following (ordinary) condensed detachment proof derives R3, R1, R4, and R5′, which is a generalization of R5, from R2:

3		$ExExEEyzEEyuEzu$	(R2)
21	[3,3]	$EExExEEyzEEyuEzuEEvwEEvsEws$	
22	[21,3]	$EExyEExzEyz$	
24	[22,22]	$EEExyzEEExuEyuz$	
25	[3,22]	$EEExyEExzEyzEEuvEEuwEvw$	
26	[22,3]	$EExyEExEEzuEEzvEuvy$	
27	[24,24]	$EEEExyzEuzEEExvEyvu$	
29	[3,24]	$EEEExyzEEExuEyuzEEvwEEvsEws$	
30	[24,22]	$EEExyEzyEExuEzu$	
31	[24,3]	$EEExyEzyEExzEEuvEEuwEvw$	
36	[26,22]	$EEExyEEzuEEzvEuvEExwEyw$	
40	[27,25]	$EEExyEzyExz$	
43	[27,29]	$EEEExyzEEuEyvzEExvu$	
57	[30,21]	$EEExEEyzEuzvEExEyuv$	
69	[22,40]	$EEEExyEzyuEExzu$	
74	[40,29]	$EEExyEzEyuEExuz$	
75	[40,21]	$EExEEyzEuzExEyu$	
93	[57,40]	$EEExEyzEuyExEuz$	
102	[69,69]	$EEExyzEExuEzEuy$	
124	[74,31]	$EEExyEEzuEyuExz$	

126 [69,75] $EExEyzEExEuzEyu$

135 [43,93] $EEExEEyyzzx$

142 [22,93] $EEEExEyzEuyvEExEuzv$

160 [24,102] $EEEExyzEuzEExvEuEvy$

161 [22,102] $EEEExyzuEEExvEzEvyu$

164 [102,74] $EEExyzEEExuvEzEvEyu$

181 [124,36] $EExEEyzEEyuEzux$

184 [126,126] $EEExEyzEuEyvEExEvzu$

378 [184,181] $EEExEEyzuEuEEyvEzvx$

382 [184,93] $EEExEyzEzyx$

542 [184,382] $EEEExEyzEuyEzux$

543 [164,382] $EEEExEyzuvExEvEEzyu$

544 [161,382] $EEExyEEzuEyEuzx$

836 [57,542] $EEEExEyEzuEEvuyEzvx$

876 [543,378] $ExExEEyEzuEyEEzvEuv$ (R3)

888 [543,135] $ExExEEyEzzy$ (R1)

1029 [160,544] $EEExEEyzEuEzyvExEvu$

1500 [543,836] $EExEyEzuExEEyEvuEzv$

1587 [142,1029] $EExEyEzEuvExEEyEvuz$

2210 [75,1500] $EEExEyzEuEyvExEuEzv$ (R4)

2276 [1500,1587] $EExEyEzEuvEExEwzEEyEvuw$ (R5′)

One might conjecture that a set of formulas axiomatizes the left group calculus if and only if its set of mirror images axiomatizes the right group calculus. On the contrary, although R2 is a single axiom for the right group calculus, L2 cannot be a single axiom for the left group calculus, because it does not (ordinary) condensed detach with itself.

Each of the following formulas is also a single axiom for the right group calculus (with ordinary modus ponens). Proofs can be found in [7].

$$EExEyzExEEyuEzu \tag{S2}$$

$$ExExEEEyzEuzEyu \tag{S3}$$

$$EExEyzEExEuzEyu \tag{S4}$$

$$EExEEyzEEyuEzux \tag{S5}$$

$$EExEEEyzEuzEyux \tag{S6}$$

4 The Role of OTTER

The program OTTER [6] is a general-purpose, resolution/paramodulation theorem prover for first-order logic with equality. The main consideration in the design of OTTER was the ability to quickly explore large search spaces rather than the use of heuristics to carefully control the searches.

We used OTTER in two ways to obtain these results. First, to find the multi-formula axiomatizations listed at the end of Section 2, we iterated as follows: take a known axiomatization, replace a complex axiom, say α, with a set of simpler tautologies, then search for a proof of α; if a proof is found, search for dependencies in the new axiomatization. Second, to find the single axioms, we generated large sets of tautologies, and with each, searched for a known axiomatization. The main method for generating the large sets of candidate single axioms was to enumerate tautologies not containing instances of $E(x, x)$. (Most tautologies contain instances of $E(x, x)$, but the interesting axiomatizations usually do not.) Approximately 10,000 OTTER searches were run, consuming about four days of computer time. Another paper [7] contains a detailed presentation of the use of OTTER to obtain the results presented in this paper.

Acknowledgments. I wish to thank Dana Scott for suggesting these calculi as challenges for OTTER, Larry Wos for collaborating on the formulation of search strategies applied by OTTER in related areas, John Kalman for discussions on the topic, and a referee for substantially improving to this paper.

References

[1] J. A. Kalman. Substitution-and-detachment systems related to Abelian groups. In *A Spectrum of Mathematics, Essays Presented to H. G. Forder*, pages 22–31. Auckland University Press, 1971.

[2] J. A. Kalman. Axiomatizations of logics with values in groups. *J. London Math. Society*, 2(14):193–199, 1975.

[3] J. A. Kalman. A shortest single axiom for the classical equivalential calculus. *Notre Dame J. Formal Logic*, 19:141–144, 1978.

[4] J. A. Kalman. Condensed detachment as a rule of inference. *Studia Logica*, LXII(4):443–451, 1983.

[5] E. J. Lemmon, C. A. Meredith, D. Meredith, A. N. Prior, and I. Thomas. Calculi of pure strict implication. Technical report, Canterbury University College, Christchurch, 1957. Reprinted in *Philosophical Logic*, Reidel, 1970.

[6] W. McCune. OTTER 2.0 Users Guide. Tech. Report ANL-90/9, Argonne National Laboratory, Argonne, IL, March 1990.

[7] W. McCune. Automated discovery of new axiomatizations of the left group and right group calculi. Preprint MCS-P220-0391, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, 1991.

[8] C. A. Meredith and A. N. Prior. Equational logic. *Notre Dame J. Formal Logic*, 9:212–226, 1968.

[9] D. Meredith. In memoriam Carew Arthur Meredith (1904–1976). *Notre Dame J. Formal Logic*, 18:513–516, 1977.

[10] J. G. Peterson. Shortest single axioms for the classical equivalential calculus. *Notre Dame J. Formal Logic*, 17(2):267–271, 1976.

[11] J. Łukasiewicz. *Selected Works*. North-Holland, 1970. Edited by L. Borkowski.

[12] 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.