Computer and Human Reasoning: Single Implicative Axioms for Groups and for Abelian Groups

W. McCune[*]
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60439-4844
U.S.A.

A. D. Sands
Department of Mathematics and Computer Science
University of Dundee
Dundee, DD1 4HN
Scotland
U.K.

May 31, 1996

The search for single axioms for groups has long interested mathematicians. In 1938, Tarski [7] presented the following single equational axiom (in terms of subtraction) for Abelian groups:

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

and in 1952, Higman and Neumann [1] presented the following single equational axiom (in terms of division) for ordinary groups:

$$(x/((((x/x)/y)/z)/(((x/x)/x)/z))) = y. \tag{2}$$

We use additive notation, $+$, 0, $'$, $-$, for Abelian groups, and multiplicative notation, $\cdot$, e, $^{-1}$, $/$, for ordinary groups. Throughout this note, $-$ and $/$ are binary operations rather than abbreviations for, e.g., $x + y'$ and $x \cdot y^{-1}$.

One might think it trivial, given (2), to obtain a single axiom in terms of product and inverse, by simply rewriting α/β to $\alpha \cdot \beta^{-1}$. Doing so gives a single axiom, but then $\cdot$ is not product, and $^{-1}$ is not inverse. The same situation holds for the Abelian case. Another curious fact is that there is no single equational axiom for groups or for Abelian groups in terms of the three standard operations of product, inverse, and

[*]Supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Computational and Technology Research, U.S. Department of Energy, under Contract W-31-109-Eng-38.

the identity element [8]. Single equational axioms in terms of product and inverse have been reported by Neumann [5] and others [3, 2].

In this note we consider single *implicative* axioms, that is, axioms of the form $\alpha = \beta \Rightarrow \gamma = \delta$. For Abelian groups, an axiom of this type with five variables was given by Sholander [6]. If we allow one of α and β to be a variable, it is trivial to obtain an implicative axiom from an equational one: select any term ζ in the equational axiom, replace it with a new variable v, and add the antecedent $\zeta = v$. Hence we restrict our attention to axioms in which neither α nor β is a variable.

Using a combination of human and computer reasoning—specifically, with the assistance of the automated deduction system Otter [4]—we obtained single implicative axioms for Abelian groups in terms of addition and inverse (4 variables) and in terms of subtraction (4 variables) and axioms for ordinary groups in terms of product and inverse (5 variables) and in terms of division (4 variables).

The axioms of Theorems 2 and 3 were found and proved to be single axioms by the second author, and those of Theorems 1 and 4 were found and proved to be single axioms by the Otter [4]. All of the proofs we present are adapted from proofs found (easily) by Otter.

Theorem 1 *Let G be a nonempty set with binary operation $+$ and unary operation $'$ such that for all $x, y, z, u \in G$,*

$$x + y = z + u \;\Rightarrow\; (y' + z) + u = x. \tag{3}$$

Then $\langle G; +, ' \rangle$ is an Abelian group.

Proof. We show the existence of an identity element and that the inverse, commutativity, and associativity properties hold for $\langle G; +, ' \rangle$. First, from (3) we obtain

$$(y' + x) + y = x. \tag{4}$$

Then, setting x to $z + w$, and applying (3) again, we have

$$(y' + z) + w = y' + (z + w). \tag{5}$$

(We no longer need (3), i.e., the pair (4) and (5) axiomatizes Abelian groups.)

$$\begin{array}{rcll} a' + a & = & ((b' + a') + b) + a & \text{[by (4)]} \\ & = & (b' + (a' + b)) + a & \text{[by (5)]} \\ & = & b' + ((a' + b) + a) & \text{[by (5)]} \\ & = & b' + b. & \text{[by (4)]} \end{array}$$

Thus, $a' + a$ is independent of a, and we may call it 0, and from (4), we have that 0 is a left identity: for all x,

$$x' + x = 0, \tag{6}$$

$$0 + x = x. \tag{7}$$

Commutativity:

$$\begin{aligned} a+b &= ((a'+a)+a)+b && [\text{by } (4)] \\ &= ((b'+b)+a)+b && [\text{by } (6)] \\ &= (b'+(b+a))+b && [\text{by } (5)] \\ &= b+a. && [\text{by } (4)] \end{aligned}$$

Associativity:

$$\begin{aligned} (a+b)+c &= (a+((c'+b)+c))+c && [\text{by } (4)] \\ &= (a+(c'+(b+c)))+c && [\text{by } (5)] \\ &= ((c'+(b+c))+a)+c && [\text{by commutativity}] \\ &= (c'+((b+c)+a))+c && [\text{by } (5)] \\ &= (c'+(a+(b+c)))+c && [\text{by commutativity}] \\ &= a+(b+c). && [\text{by } (4)] \end{aligned}$$

Therefore, $\langle G; +, ' \rangle$ is an Abelian group.

Theorem 2 *Let G be a nonempty set with a binary operation $-$ such that for all $x, y, z, u \in G$,*

$$x - y = z - u \;\Rightarrow\; u - (z - x) = y. \tag{8}$$

Then $\langle G; - \rangle$ is an Abelian group with $x - y = x + y'$ for all $x, y \in G$.

Proof. First note that (8) holds in Abelian groups when $-$ is interpreted as subtraction. The main part of the proof is to derive Tarski's axiom (1) from (8). By (8) we have

$$x - (y - y) = x = x - (z - z). \tag{9}$$

Applying (8) to (9) gives us $(z - z) - (x - x) = y - y$, which, by itself, yields $u - u = y - y$. Applying (8) to this, we have

$$y - (y - u) = u. \tag{10}$$

Let u be $v - w$, and apply (8) once again to obtain

$$w - (v - y) = y - (v - w). \tag{11}$$

In (10), let y be w and u be $v - y$, and substitute (11) to derive

$$w - (y - (v - w)) = v - y. \tag{12}$$

In (10), let y be v and u be y, and substitute (12) to obtain

$$v - (w - (y - (v - w))) = y,$$

which is Tarski's single axiom (1) for Abelian groups in terms of subtraction.

Theorem 3 *Let G be a nonempty set with binary operation $\cdot$ and unary operation $^{-1}$ such that for all $x, y, z, u \in G$,*

$$(x \cdot y) \cdot z = (x \cdot u) \cdot w \;\Rightarrow\; u \cdot (w \cdot z^{-1}) = y. \tag{13}$$

Then $\langle G; \cdot, ^{-1} \rangle$ is a group.

Proof. By (13) we have $x \cdot (y \cdot y^{-1}) = x = x \cdot (z \cdot z^{-1})$; hence $(x \cdot (y \cdot y^{-1})) \cdot u = (x \cdot (z \cdot z^{-1})) \cdot u$; hence by (13), $(z \cdot z^{-1}) \cdot (u \cdot u^{-1}) = (y \cdot y^{-1})$; hence $y \cdot y^{-1}$ is independent of y, and we name the element e, which is a right identity,

$$y \cdot y^{-1} = e, \tag{14}$$

$$x \cdot e = x. \tag{15}$$

We have $(e \cdot e) \cdot e = (e \cdot e^{-1}) \cdot e$, and by (13), $e^{-1} \cdot (e \cdot e^{-1}) = e$; hence

$$e^{-1} = e. \tag{16}$$

Next, we have $(e \cdot x) \cdot e = (e \cdot e) \cdot x$, and by (13), $e \cdot (x \cdot e^{-1}) = x$; hence

$$e \cdot x = x. \tag{17}$$

Now, we have $(e \cdot x) \cdot y = (e \cdot (x \cdot y)) \cdot e$, and by (13), $(x \cdot y) \cdot (e \cdot y^{-1}) = x$; hence

$$(x \cdot y) \cdot y^{-1} = x. \tag{18}$$

Finally, by (17) and (18), we have $(e \cdot ((x \cdot y) \cdot z)) \cdot z^{-1} = (e \cdot x) \cdot y$, and by (13), $x \cdot (y \cdot z^{-1-1}) = (x \cdot y) \cdot z$, and by (18), $x \cdot (((y \cdot z) \cdot z^{-1}) \cdot z^{-1-1}) = (x \cdot y) \cdot z$, and by (18) again,

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z. \tag{19}$$

Equations (14), (15), and (19) establish the result.

The proof of the following theorem is in the form produced by the theorem prover Otter. The justification $m \to n$ indicates substitution of an instance of the right side of equation m for an instance of a term in the left side of n, and $: i, j, \cdots$ indicates simplification with $i, j, \cdots$. Variables are automatically renamed by the program, and the numbering of the equations reflects the sequence of equations retained by the program.

Theorem 4 *Let G be a nonempty set with a binary operation $/$ such that for all $x, y, z, u \in G$,*

$$x/y = z/u \;\Rightarrow\; y/(((z/z)/z)/((x/x)/x)) = u. \tag{20}$$

Then $\langle G; / \rangle$ is a group with $x/y = x \cdot y^{-1}$ for all $x, y \in G$.

Proof. First Otter shows that x/x is independent of x. Terms of the form $(v/v)/v$ are abbreviated as $f(v)$.

2	$x = x$	
3	$x/y = z/u \;\to\; y/(f(z)/f(x)) = u$	
5	$x/(f(y)/f(y)) = x$	[3,2]
6	$(f(x)/f(x))/(f(y)/(((y/z)/(y/z))/(y/z))) = z$	[3,5]
10	$f(x)/f(x) = f(y)/f(y)$	[5 → 6 :5,5,5]
11	$(f(x)/f(x))/((f(y)/f(y))/f(y)) = f(y)$	[5 → 6 :5,5]
19	$(f(x)/f(x))/((((y/y)/(y/y))/(y/y))/((f(z)/f(z))/f(y))) = y$	[10 → 6]

22	$x/(((f(y)/f(y))/f(z))/((f(z)/f(z))/f(z))) = x$	[10 → 5]
25	$(f(x)/f(x))/((f(y)/f(y))/f(z)) = f(z)$	[10 → 11]
29	$(((x/x)/(x/x))/(x/x))/((f(y)/f(y))/f(x)) = f(x)$	[18 → 6 :5,5,19,19,25]
31	$(f(x)/f(x))/f(y) = y$	[19 :29]
36	$x/(y/y) = x$	[22 :31,31]
40	$(x/x)/f(y) = y$	[10 → 31 :31,31]
54	$x/x = y/y$	[36 → 40 :36,36]

We now introduce the element e and use $x/x = e$ to prove the Higman-Neumann single axiom (2). We assert that there are elements A, B, and C for which (2) fails to hold and Otter derives a contradiction.

1	$x = x$	
2	$x/y = z/u \rightarrow y/(((z/z)/z)/((x/x)/x)) = u$	
4	$x/x = e$	
5	$A/((((A/A)/B)/C)/(((A/A)/A)/C)) \neq B$	
6	$A/(((e/B)/C)/((e/A)/C)) \neq B$	[5 :4,4]
7	$x/y = z/u \rightarrow y/((e/z)/(e/x)) = u$	[2 :4,4]
9	$x/e = x$	[7,1 :4]
10	$e/((e/x)/(e/(x/y))) = y$	[7,9]
12	$((e/x)/(e/(x/(y/z))))/(e/y) = z$	[7,10 :4,9]
17	$(e/x)/(e/(x/y)) = e/(e/(e/y))$	[10 → 10 :4]
19	$e/(e/x) = x$	[4 → 10 :4,9]
20	$(e/(x/y))/(e/x) = y$	[12 :17,19]
24	$(e/x)/((e/y)/(x/(y/z))) = z$	[7,20 :19]
28	$(e/((e/x)/y))/x = y$	[19 → 20]
30	$x/((e/y)/((e/x)/(y/z))) = z$	[19 → 24]
103	$x/(((e/y)/z)/((e/x)/z)) = y$	[28 → 30 :19]
105	$\square$	[103,6]

Because (20) holds for groups when / is interpreted as division, and because the Higman-Neumann axiom can be derived, the proof is complete.

The main open question remaining is whether there exists a four-variable single implicative axiom in terms of product and inverse for ordinary groups. Also, for the non-Abelian cases, we do not know whether there exist implicative axioms shorter than ours.

Each of the four proofs we have presented arises from a different amount of translation (by hand) from an Otter-generated proof, and each is in a different style. The proof of Theorem 1 has had the most translation and is probably the most transparent (also it is the easiest theorem). Theorem 4's proof is nearly in the form produced by Otter and is probably opaque to most readers (it certainly is to us). Translating proofs found by computers into human-readable forms is an important problem in automated deduction.

The Otter input files and proofs for these four theorems are available on the World Wide Web through `http://www.mcs.anl.gov/home/mccune/ar/imply/`.

References

[1] G. Higman and B. H. Neumann. Groups as groupoids with one law. *Publicationes Mathematicae Debrecen*, 2:215–227, 1952.

[2] K. Kunen. Single axioms for groups. *Journal of Automated Reasoning*, 9(3):291–308, 1992.

[3] W. McCune. Single axioms for groups and Abelian groups with various operations. *Journal of Automated Reasoning*, 10(1):1–13, 1993.

[4] W. McCune. OTTER 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994. See also `http://www.mcs.anl.gov/home/mccune/ar/otter/`.

[5] B. H. Neumann. Another single law for groups. *Bull. Australian Math. Soc.*, 23:81–102, 1981.

[6] M. Sholander. Postulates for commutative groups. *Amer. Math. Monthly*, 66:93–95, 1959.

[7] A. Tarski. Ein Beitrag zur Axiomatik der Abelschen Gruppen. *Fundamenta Mathematicae*, 30:253–256, 1938.

[8] A. Tarski. Equational logic and equational theories of algebras. In K. Schütte, editor, *Contributions to Mathematical Logic*, pages 275–288. North-Holland, Amsterdam, 1968.