Levi's Commutator Theorems for Cancellative Semigroups

R. Padmanabhan* **W. McCune†** **R. Veroff‡**

Abstract

A conjecture of Padmanabhan, on provability in cancellative semigroups, is addressed. Several of Levi's group theory commutator theorems are proved for cancellative semigroups. The proofs, found by automated deduction, support the conjecture.

Key words and phrases: cancellative semigroup, commutator, automated theorem proving.

2000 Mathematics Subject Classification: 20M07, 20A05, 68T15.

1 Introduction

The following conjecture (apparently still open) was formulated by the first author in the 1980s and published in [4].

Conjecture. Let Σ be a nonempty set of equations of type $\langle 2 \rangle$, and let σ be an equation of the same type. If every group satisfying Σ also satisfies σ, then every cancellative semigroup satisfying Σ must satisfy σ as well. To put it more formally, let GT be the axioms of group theory and CS be the axioms for cancellative semigroups, that is, the associative law and the two cancellation laws. Then

$$\text{if } (\Sigma, \mathrm{GT} \Rightarrow \sigma), \text{ then } (\Sigma, \mathrm{CS} \Rightarrow \sigma).$$

From the deductive point of view, this conjecture says that if one uses the richer language of group theory (i.e., with inverse and identity) to derive σ from Σ, then one can do the same thing within the limited language of just one binary operation that is associative and cancellative.

For example, the statement

$$xyzyx = yxzxy \quad \Rightarrow \quad xyyx = yxxy.$$

*Supported by an operating grant from NSERC of Canada (OGP8215).

†Supported by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, Office of Science, U.S. Department of Energy, under Contract W-31-109-ENG-38.

‡Supported by the U.S. National Science Foundation grant CDA-9503064.

supports the conjecture. It satisfies the conditions of the conjecture, it has a proof in GT (trivial, by letting z be the identity), and the following proof shows it to hold for CS.

$$\begin{aligned}(xyyx)(xyx) &= (xy)(yxx)(yx) \\ &= (yx)(yxx)(xy) \quad \text{[by the assumed identity with } z = xyx\text{]} \\ &= (yx)(yx)x(xy) \\ &= (yx)(xy)x(yx) \quad \text{[by the assumed identity with } z = x\text{]} \\ &= (yxxy)(xyx) \\ xyyx &= yxxy \quad \text{[by canceling } (xyx)\text{]} \quad \square\end{aligned}$$

Unfortunately, the proof in GT does not seem to tell us much about how to prove it in CS. Many such examples supporting the conjecture can be found in [4].

Here we do not directly address the conjecture; rather, we provide further intuitive support for it by considering several theorems about commutators in GT and the corresponding statements in CS. Automated theorem proving was used to find proofs for the GT and the CS theorems. Apart from being generalizations, these proofs are strictly first order (e.g., avoiding quotient constructions) and hence may be construed as providing new equational proofs of the well known theorems in GT.

2 Commutator Theorems in GT and in CS

In GT, let the commutator operation be defined as

$$[x, y] = x^{-1}y^{-1}xy. \tag{C1}$$

The following three statements about commutators,

$$\begin{aligned}[x, y]z &= z[x, y] && \text{(nilpotency of class 2)} && \text{(N)} \\ [[x, y], z] &= [u, [v, w]] && \text{(“associativity” of commutator)} && \text{(A)} \\ [xy, z] &= [x, z][y, z] && \text{(distributivity),} && \text{(D)}\end{aligned}$$

are well known to be equivalent in GT [1, p. 99]. We refer to this fact as Levi's theorem on commutators. See the Web page [5] for equational proofs found by a theorem-proving program.

Consider the analogous problem in CS. We cannot use (C1) to define the commutator because the inverse operation is not in the language. Instead, we simply state the following property of the new operation:

$$yx[x, y] = xy. \tag{C2}$$

Indeed, such an element $[x, y]$ is unique by the cancellation law.

In the following section, we show informally that given (C2), the equations (N), (A), and (D) are equivalent in CS. In group theory, these three properties

are equivalent to the group being nilpotent of class 2. This is the essence of Levi's theorem on commutators. Thus, to capture the full scenario of Levi, we need to define the concept of nilpotence class 2 in a manner meaningful in CS, that is, with no mention of the inverse operation. This is precisely the role played by the identity

$$xyzyx = yxzxy. \qquad \text{(CS essence of (N))} \qquad \text{(E)}$$

This was first discovered by A. I. Malcev in [2]. In fact, he proved that any cancellative semigroup satisfying the property (E) is embeddable in a group of nilpotence class 2.

Note that these equations are outside the hypotheses of the conjecture on cancellative semigroups. First, there is an additional operation. Second, the CS versions use property (C2) instead of the definition (C1), giving slightly stronger theorems (which hold obviously for GT as well). Also, if a cancellative semigroup satisfies (C2), there is a left and right identity element for the semigroup operation (see Section 4), which allows the CS proofs to be a bit more grouplike.

3 Proof Sketch

By Malcev's discovery, the class of all cancellative semigroups satisfying (E) is identical to the class of all subsemigroups of nilpotent groups of class 2. Combining this with the proofs given by Kurosh of Levi's theorems on commutators [1, p. 91], we have a model-theoretic proof that property (E) is equivalent to (N), (A), and (D) in the class of all cancellative semigroups.

By the completeness theorem of first-order logic with equality, there must be proofs of this equivalence within the first-order theory of CS. The automated theorem-proving program Otter [3] has found such proofs, and we show one of the longer proofs in the following section. The other Otter proofs showing all of the equivalences can be found on the Web page associated with this paper [5].

4 Computer Proof of $(E) \Rightarrow (D)$

Here we give a formal equational proof that property (E) implies the distributivity property (D) in CS. The proof was found by Otter. (Notes on the proofs are given below.) First, Otter shows the existence of a constant $[x, x]$.

2	$x = x$	[]
3	$xy = z,\ xu = z \rightarrow y = u$	[left cancellation]
4	$xy = z,\ uy = z \rightarrow x = u$	[right cancellation]
5	$(xy)z = xyz$	[associativity of $\cdot$]
7	$xy[y, x] = yx$	[commutator property]
11	$x[x, x] = x$	[3,2,7]
21	$x[x, x]y = xy$	[11 $\rightarrow$ 5]
31	$[x, x]y = y$	[3,2,21]

33	$[x,x] = [y,y]$	[4,31,31]

Now Otter proves that (E) ⇒ (D) in CS.

2	$x = x$	[]
3	$xy = z,\ xu = z \rightarrow y = u$	[left cancellation]
4	$xy = z,\ uy = z \rightarrow x = u$	[right cancellation]
5	$(xy)z = xyz$	[associativity of .]
7	$xy[y,x] = yx$	[commutator property]
10	$xyzyx = yxzxy$	[property (E)]
11	$[x,x] = e$	[constant e]
15	$xe = x$	[3,2,7:11]
17	$xyz[yz,x] = yzx$	[5 → 7:5]
19	$xyz[z,xy] = zxy$	[5 → 7]
21	$xy[y,x]z = yxz$	[7 → 5:5,5]
24	$xey = xy$	[15 → 5]
30	$xy[xy,x] = yx$	[3,2,17]
36	$ex = x$	[3,7,24:11,15]
39	$xy[y,yx] = yx$	[3,2,19]
44	$x[x,e] = x$	[3,7,36:15]
49	$x[e,x] = x$	[36 → 7:36]
51	$[x,e] = e$	[3,15,44]
56	$xyxz = x[x,z]yzx$	[3,10,21]
57	$x[x,y]z = zx[x,yz]$	[3,21,19]
63	$[x,y]yx = xy[[x,y],yx]$	[19 → 21]
65	$[e,x] = e$	[3,15,49]
67	$x[yx,y] = x[x,y]$	[3,7,30]
75	$x[x,xy] = x[x,y]$	[3,7,39]
77	$[xy,x] = [y,x]$	[3,2,67]
89	$[xyz,xy] = [z,xy]$	[5 → 77]
91	$[x,xy] = [x,y]$	[3,2,75]
111	$[xy,xyz] = [xy,z]$	[5 → 91]
151	$[xy,yx] = [[x,y],yx]$	[7 → 89]
156	$[x,y]zyx = zxy$	[3,2,56]
157	$xyz = [y,z]xzy$	[3,56,2]
158	$[x,[x,y]zyx] = [x,zxy]$	[56 → 91:91]
160	$[x,yxz] = [x,[x,z]yzx]$	[158]
167	$[[x,y],yx] = [xy,[y,x]]$	[7 → 111:151]
169	$[xy,[y,x]] = [[x,y],yx]$	[167]
170	$x[x,y][y,zx] = [y,z]x$	[3,21,57]
180	$xy[[x,y],yx] = xy$	[3,2,156:63]
182	$[x,y]yx = xy$	[63:180]
196	$[[x,y],zxy] = [[x,y],zyx]$	[156 → 91]
210	$[x,yz]yzx = xyz$	[5 → 182]
225	$[xy,[x,y]] = [yx,[x,y]]$	[182 → 77]
226	$[x,y]yxz = xyz$	[182 → 5:5,5]

229	$[xy,[y,x]] = [yx,[y,x]]$	[225]
280	$xy[[x,y],zyx] = xy$	[3,19,157:5,21]
286	$[x,yz]zyx = xzy$	[156 → 157:5,226]
384	$x[[y,x],xy] = x$	[3,2,180]
387	$[[x,y],yx] = e$	[3,15,384]
391	$[xy,[y,x]] = e$	[169:387]
399	$[xy,[x,y]] = e$	[229:391]
1669	$[x,y][y,zx] = [y,z][[y,z],x]$	[3,170,7]
1670	$x[x,y][y,x] = x$	[36 → 170:51,36]
1755	$[x,y][y,x] = e$	[3,15,1670]
1797	$[x,y][y,x]z = z$	[1755 → 17:65,15,1755,15]
1998	$[[x,y],z][y,x]z[x,y] = z$	[157 → 1797]
2689	$[[x,y],z]xy = xy$	[196 → 170:399,36,5,280]
3280	$[x,yz] = [x,zy]$	[4,210,286]
3373	$[x,[y,z]uzy] = [x,yzu]$	[157 → 3280:5]
3428	$[x,yxz] = [x,zy]$	[160:3373,91]
3429	$[x,yz] = [x,zxy]$	[158:3373,91]
5622	$[[x,y],z] = e$	[4,36,2689]
5644	$[x,y]z[y,x] = z$	[1998:5622,36]
5646	$[x,y][y,zx] = [y,z]$	[1669:5622,15]
5968	$[x,yxz] = [x,yz]$	[3428 → 3429:5,91]
6186	$[x,y][x,z] = [x,yz]$	[3,5644,5646]
6243	$[x,yz][z,yx] = [xz,y]$	[89 → 5646:5968,77]
6516	$[x,yz]u = [x,y][x,z]u$	[6186 → 5]
6522	$[x,y][z,y] = [xz,y]$ (property (D))	[6243:6516,5646] □

In the preceding proof, the justification $i \rightarrow j$ indicates equality substitution between an instance of i and an instance of j, and the justification : $i, j, \ldots$ indicates simplification with $i, j, \ldots$.

The proof, found by Otter in several seconds, is in nearly the form output by Otter, and there is much room for improvement of the presentation. Inferences are frequently hard to follow, because the instances of the premises are not given, simplification is applied, and variables are renamed. In addition, Otter proofs are usually longer than necessary.

Otter can accept various forms and degrees of guidance from the user when searching for a proof. For these proofs, we simply specified an ordering on the symbols (which affects how derived identities are used as simplification rules) and a limit on the complexity of derived identities.

Automated theorem proving has been very useful in testing other instances of the CS conjecture [4], and we are using the resulting proofs to seek insights into the relationships between CS proofs and the corresponding GT proofs.

References

[1] A. G. Kurosh. *The Theory of Groups*, Volume 1. Chelsea, New York, 1956.

[2] A. I. Malcev. Nilpotent semigroups. *Ivanov. Gos. Ped. Inst. Zap. Fiz.-Mat. Nauki*, 4:107–111, 1953. In Russian.

[3] W. McCune. Otter 3.3 Reference Manual. Tech. Memo ANL/MCS-TM-263, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, IL, August 2003.

[4] W. McCune and R. Padmanabhan. *Automated Deduction in Equational Logic and Cubic Curves*, volume 1095 of *Lecture Notes in Computer Science (AI subseries)*. Springer-Verlag, Berlin, 1996.

[5] R. Padmanabhan, W. McCune, and R. Veroff. Levi's commutator theorems for cancellative semigroups: Web support. `http://www.mcs.anl.gov/~mccune/papers/cs-commutator/`, 2003.

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba R3T 2N2, Canada
padman@cc.umanitoba.ca

Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, Illinois 60419, USA
mccune@mcs.anl.gov

Department of Computer Science
University of New Mexico
Albuquerque, New Mexico 87131, USA
veroff@cs.unm.edu