First-Order Theorem Proving with Power Maps in Semigroups*

Yi Lin[1,†], Ranganathan Padmanabhan[2,†] and Yang Zhang[3,*,†]

[1]Department of Mathematics, The Ohio State University, Ohio, USA
[2]Department of Mathematics, University of Manitoba, Winnipeg, MB, Canada
[3]Department of Mathematics, University of Manitoba, Winnipeg, MB, Canada

Abstract

This paper deals with automated deduction techniques to prove and generalize some well-known theorems in group theory that involve power maps, i.e., functions of the form $f(x) = x^n$. Here, the main obstacle is that if n is interpreted as an integer variable, then these results are not expressible in first-order logic with equality. The strategy followed here is to look at the classical proofs, involving the integer variable n, and see what specific first-order properties of power maps that are needed in the proofs. Then we implement these first-order properties of power maps in a theorem prover Prover9 and demonstrate that a well-designed reformulation makes specific mathematical theories accessible to the modern first-order theorem-proving software, allowing even for generalizations of the classical results.

Keywords

Semigroup, Prover9, Power maps

1. Introduction

The theory of groups and that of semigroups are very closely related. In fact, every group is a cancellation semigroup and, by a classical theorem of O. Ore [14], every cancellation semigroup satisfying some nontrivial identity, say $f(x, y) = g(x, y)$, is embeddable in a group. Also, there are several examples of identities $f = g$ which are preserved during this process of expansion. The most well-known example of a semigroup law that is transferable to groups is, of course, the commutative law. A.I. Mal'cev [8] and B.H. Neumann [12] have shown independently that nilpotent semigroup laws are transferable. However, it is also known that not all semigroup laws are preserved under the Ore extension. This raises the important question of finding more (and possibly all) transferable semigroup laws. This problem was raised by G.M. Bergman ([1, 2]).

There are several transferability theorems in semigroups that involve power maps $f(x) = x^n$. For example, it is known that every cancellation semigroup satisfying $x^n \cdot y^n = y^n \cdot x^n$ can be embedded in a group satisfying the same identity. Such statements belong to first-order logic with equality and hence provable, in principle, by any first-order theorem prover. However, because of the presence of an arbitrary integer parameter n in the exponent, they are outside the scope of any first-order theorem prover. In particular, one cannot use such an automated reasoning system to prove theorems involving power maps. Here we focus just on the needed properties of power map $f(x) = x^n$ and show how one can easily avoid having to reason explicitly with integer exponents. Implementing these new equational rules of power maps, we show how a theorem prover can be a handy tool for quickly proving or confirming the truth of such theorems involving power maps without explicitly mentioning the integer variable n.

Following Macedonska [7], a positive semigroup law is said to be transferable if being satisfied in a cancellative semigroup S it must be satisfied in SS^{-1}, the group of right quotients of S. The most well-

SCSS 2024: The 10th International Symposium on Symbolic Computation in Software Science, August 28–30, Tokyo, Japan
*Corresponding author.
†These authors contributed equally.
yilinmaths@gmail.com (Y. Lin); Ranganathan.Padmanabhan@umanitoba.ca (R. Padmanabhan); Yang.Zhang@umanitoba.ca (Y. Zhang)

known example of a transferable law is, of course, the commutative law. A. I. Malcev, B. H. Neumann and others ([8, 12]) have shown that nilpotent identities are transferable. Macedonska [7] has proved the transferablity of several two-variable semigroup laws. These identities are defined by using power maps $f(x) = x^n$ in semigroups.

Here we will replace the power map by power-like functions and prove their transferability. The transferability of identities is first order problem but first-order theorem provers cannot handle power-maps because of the presence of an integer variable "n". Here we demonstrate that computers can prove these semigroup implications, thus generalizing what is known classically.

A motivating example: It is well-known that in groups, the commutators $[x,\ y]$ can be expressed in a product of three squares, that is,

$$[x,\ y] = x^{-1}y^{-1}xy = (x^{-1})^2 \cdot (xy^{-1})^2 \cdot y^2,$$

and hence $x^2y = yx^2$ implies $[x,\ y]$ is central, which is equivalent to the semigroup implication

$$x^2y = yx^2 \implies xyzyx = yxzxy.$$

Definition 1.1. A cancellation semigroup $(G, \cdot)$ is a semigroup with the two-sided cancellative properties, i.e., for all $x, y, z \in G$, the following are true:

(i) $x \cdot y = x \cdot z$ implies $y = z$,
(ii) $x \cdot y = z \cdot y$ implies $x = z$.

Some properties of cancellation semigroup can be found in, for example, [4, 5, 13, 7, 16, 17]. Here we show that the above implication is valid in cancellation semigroups:

$$\begin{aligned} y \cdot yxzxy \cdot x &= y^2xzxyx \\ &= xzy^2xyx \\ &= xzy \cdot (yx)^2 \\ &= (yx)^2xzy \\ &= yxyx^2zy \\ &= yxyzyx^2 \\ &= y \cdot xyzyx \cdot x. \end{aligned}$$

Canceling y and x, we have $xyzyx = yxzxy$.

Next we present the proof by using Prover9 [9].

```
%% INPUT file
%% In groups, squares are central ==> commutators are also central
(x * y) * z = x * (y * z).
x * e = x.
x * x' = e.
x * y = (y * x) * [x, y]. %% commutators defined
x * (y * y) = (y * y) * x. %% squares are central
%% goal to prove that commutators are central
x * [y, z]  =  [y, z] * x.
=============== PROOF ================================
1 x * [y,z] = [y,z] * x # label(non_clause) # label(goal).
2 (x * y) * z = x * (y * z).  [].
3 x * e = x.  [].
4 x * x' = e.  [].
5 x * y = (y * x) * [x,y].  [].
```

```
6 x * (y * [y,x]) = y * x.  [5,2].
7 x * (y * y) = (y * y) * x.  [].
8 x * (y * y) = y * (y * x).  [7,2].
9 [c2,c3] * c1 != c1 * [c2,c3].  [1].
10 x * (e * y) = x * y.  [3,2].
11 x * (x' * y) = e * y.  [4,2].
12 x * (y * (x * y)') = e.  [4,2].
13 x * (y * ([y,x] * z)) = y * (x * z).  [6,2,2,2].
14 x * (y * (z * [z,x * y])) = z * (x * y).  [6,2].
15 x * (y * (z * [y * z,x])) = y * (z * x).  [2,6,2].
16 x * (y * (y * z)) = y * (y * (x * z)).  [8,2,2,2,2].
20 e * x = x.  [3,8,3,10].
21 x * (x' * y) = y.  [11,20].
29 x'' = x.  [4,21,3].
31 x * [x,y'] = y * (x * y').  [6,21].
33 x * (y * (x' * x')) = x' * y.  [8,21].
35 x' * x = e.  [29,4].
36 x' * (x * y) = y.  [29,21].
40 x * (y * [x,y]') = y * x.  [4,13,3].
41 x * (y * (z * [z,[x,y]])) = y * (x * (z * [x,y])).[6,13].
43 x * (y * (z * (z * [y,x]))) = y * (x * (z * z)). [8,13].
55 x' * (y * x) = y * [y,x].  [6,36].
58 x * (y * x)' = y'.  [12,36,3].
66 x * (y * [y,z' * x]) = z * (y * (z' * x)).  [14,21].
80 x*(y *(z*(u*[y*(z*u),x])))=y*(z*(u*x)).[2,15,2,2].
98 (x * y)' = y' * x'.  [58,36].
112 x * (y * (z * (z * u))) = z * (z * (x * (y * u))).[16,2,2].
115 x * (x * (y * x')) = y * x.  [4,16,3].
127 x * (y * (x' * (x' * z))) = x' * (y * z).  [16,21].
128 x * (x * (y * (x' * z))) = y * (x * z).  [21,16].
189 x * (x * (y * (z * x'))) = y * (z * x).  [2,115,2].
190 x' * (y * x) = x * (y * x').  [115,21,29].
206 x * [x,y] = y * (x * y').  [55,190].
326 x' * (y * (x * z)) = x * (y * (x' * z)).  [190,2,2,2,2].
467 x * (y' * [y,x]) = y' * x.  [33,13,33].
481 x * [y,x]' = y * (x * y').  [40,36,190].
512 x * (y * (x' * y')) = [x',y'].  [31,21].
516 [x',y'] = [x,y'].  [31,36,326,512].
543 x * (y * (x' * y')) = [x,y'].  [512,516].
547 [x',y] = [x,y'].  [206,21,543].
551 [x,y'] = [x,y].  [206,36,326,543].
552 x' * (y * [y,x]) = y * x'.  [206,36].
569 x * [y,x] = y * (x * y').
    [206,190,98,29,2,36,98,29,2,36].
584 [x',y] = [x,y].  [547,551].
585 x * (y * (x' * y')) = [x,y].  [543,551].
592 x' * (y * ([y,x] * z)) = y * (x' * z).  [551,13].
605 x * (y * [x,y]) = y * x.  [569,8,8,115].
606 [x,y] = [y,x].  [569,21,585,551].
754 x * (y' * [x,y]) = y' * x.  [551,605].
1004 [x,y]' = [y,x].  [481,21,585,551].
1049 x * [y,[x,y]] = x.  [21,41,584,754,21].
```

```
1095 [x,[y,x]] = e.  [1049,21,4,584].
1157 [x,y' * (y' * x')] = e.
     [35,43,98,98,2,98,98,2,606,2,2,326,36,36,21].
1383 [x,x * (y * y)] = e.  [1157,551,98,98,29,29,29,2].
1387 [x,y * (y * x)] = e.  [8,1383].
1400 [x * y,x' * y] = e.  [21,1387,606].
1534 [x * (y * z),x * (y' * z)] = e.  [13,1400,592].
1861 x * (y * (x' * (y' * z))) = [x,y] * z.  [585,2,2,2].
1863 x * (y * (z * (x' * (z' * y')))) = [x,y * z].[2,585,98].
1874 x * ([y,z] * (x' * [z,y])) = [x,[y,z]].  [1004,585].
1903 [x,y' * x] = [y,x].  [66,21,190,585,584].
2118 [x,y * x] = [y,x].  [29,1903,584].
2121 [x,x * y] = [x,y].  [36,1903,606,2118].
2148 [x' * y,[x,y]] = e.  [1903,1095].
2195 [x * y,[x,y]] = e.  [2118,1095].
2365 [x * y,y * x] = e.  [2195,2121,2,605].
2384 [x * y,x' * y'] = e.  [2365,551,98].
2592 [x,y] * (y' * x) = x * y'.
     [2148,467,98,29,3,98,29,2,552].
2674 x' * (y' * (z * (x * (z' * y)))) = [x,z * y].
     [2384,80,98,3,2,2,326,98,1863].
3912 x*(y*(z*(x'*(x'*u))))=x'*(y*(z*u)).[112,21].
4517 [x,[y,z]] * ([z,y] * x) = x * [z,y]. [1004,2592,1004].
8121 x*(y*(x'*(z*(x'*z'))))=x'*(y*[x,z]). [206,127,584].
8175 x'*(y*(z*(x*u)))=x*(y*(z*(x'*u))). [128,127,29].
8179 x'*(y*(z*(u*x)))=x*(y*(z*(u*x'))). [189,127,29].
8223 [x,y * z] = [x,z * y].  [2674,8179,8175,1863].
8383 [x * (y * z),y' * (z * x)] = e.  [8223,1534,2].
13972 [x,[y,z]] = e.  [8383,585,98,98,2,98,98,29,2,2,2,8179,
                      2,2,3912,8121,2,2,1861,1874].
14283 [x,y] * z = z * [x,y].  [4517,13972,20].
14284 $F.  [14283,9].
====================== end of proof ==========================
```

Coda: In the human proof above, we already "knew" that commutators are expressible as a product of squares in the group and hence the human proof was almost trivial. But in the above machine proof of the same fact, the Prover9 is not even "aware" of the fact that commutators are products of squares. Still, the software did prove the centrality of commutators as explicitly shown in line #14283 above (proved with the Knuth-Bendix option). Dr. William McCune, the author of Prover9, has done a great job.

In this paper, we first consider the implication $(xy)^n = (yx)^n$ in cancellation semigroups. In Section 2, we prove that this implication is equivalent to the identity $xy^n = y^n x$ in all cancellation semigroups by replacing the power-map x^n by a weaker power-like function $f(x)$. Furthermore, we discuss a general extension. In Section 3, we prove that $xy^n = y^n x$ is transferable.

2. Power map properties

We first list some properties of power maps. We refer the readers to [11, 15] for more details.

Lemma 2.1. *Let $(S;\cdot)$ be a cancellation semigroup and let $f : S \to S$ be the usual power map $f(x) = x^n$, for some $n > 1$. Assume that $f(x \cdot y) = f(y \cdot x)$. Then the function $f(x)$ satisfies the following:*

(1) $x \cdot f(x) = f(x) \cdot x$.
(2) $x \cdot f(y \cdot x) = f(x \cdot y) \cdot x$.

(3) x and $f(f(x))$ commute.
(4) If x and y commute then $f(x \cdot y) = f(x) \cdot f(y)$.
(5) x and $f(y \cdot x)$ commute.
(6) x and $f(f(x) \cdot y)$ commute.

Proof. (1) is obvious since both sides are equal to x^{n+1}.
(2) $x \cdot f(y \cdot x) = x \cdot (y \cdot x)^n = (x \cdot y)^n \cdot x = f(x \cdot y) \cdot x$.
(3) follows that $f(f(x))$ is just a power of x and hence commutes with x.
(4) is obvious thanks to associativity and commutativity.
(5) $x \cdot f(y \cdot x) = f(x \cdot y) \cdot x = f(y \cdot x) \cdot x$ since $f(x \cdot y) = f(y \cdot x)$.
(6)

$$\begin{aligned} f(f(x) \cdot y) \cdot x &= f(g(x) \cdot x \cdot y) \cdot x && \text{where } g(x) = x^{n-1} \\ &= f(x \cdot y \cdot g(x)) \cdot x && \text{since } f(x \cdot y) = f(y \cdot x) \\ &= x \cdot f(y \cdot g(x) \cdot x) && \text{by (2) above} \\ &= x \cdot f(y \cdot f(x)) && \text{since } f(x) = g(x) \cdot x \\ &= x \cdot f(f(x) \cdot y) && \text{since } f(x \cdot y) = f(y \cdot x) \end{aligned}$$

Hence the two elements x and $f(f(x) \cdot y)$ commute. In particular, the two terms $y \cdot x$ and $f(f(y \cdot x) \cdot x)$ commute. □

Following the terminology of [11, 15], we call the unary functions $f(x)$ satisfying first-order properties (1) to (4) of Lemma 2.1 as *power-like functions*.

Theorem 2.2. *Let S be a cancellation semigroup and let $f : S \to S$ be a power-like function and assume that $f(x \cdot y) = f(y \cdot x)$. Then $f(x)$ is a central element in S.*

We can prove this theorem by using our method and Prover9. Here we list the a few lines of output of Prover9 which include the conditions and the final result.

```
========================== prooftrans ============================
Prover9 (32) version Dec-2007, Dec 2007.
Process 916 was started by yangzhang
on yangzhangsimac2.ad.umanitoba.ca,
Tue Mar 19 12:26:28 2024
The command was "/Users/yangzhang/Desktop/Prover9-Mace4-v05B.app/
Contents/Resources/bin-mac-intel/prover9".
============================ end of head ===========================
============================ end of input ==========================
========================== PROOF =================================
% -------- Comments from original proof --------
% Proof 1 at 0.84 (+ 0.02) seconds.
% Length of proof is 24.
% Level of proof is 6.
% Maximum clause weight is 29.
% Given clauses 117.

1 f(x) * y = y * f(x) # label(non_clause) # label(goal).  [goal].
2 (x * y) * z = x * (y * z).  [assumption].
3 x * y != x * z | y = z.  [assumption].
4 x * y != z * y | x = z.  [assumption].
5 f(x * y) = f(y * x).  [assumption].
6 f(x * y) * x = x * f(y * x).  [assumption].
7 f(x) * x = x * f(x).  [assumption].
```

```
8 f(f(x) * y) * x = x * f(f(x) * y).  [assumption].
9 x * y != y * x | f(x * y) = f(x) * f(y).  [assumption].
10 f(c1) * c2 != c2 * f(c1).  [deny(1)].
..........
..........
3645 f(f(x)) * x = x * f(f(x)).  [hyper(351,a,139,a),flip(a)].
3699 f(x)*(f(x)*(y*f(f(f(x)*y))))=f(x)*(y*(f(x)*f(f(f(x)*y)))).
[back_rewrite(395),rewrite([3645(8),2(8)])].
3700 $F.  [resolve(3699,a,67,a)].

======================== end of proof ==========================
```

Next, we give the human proof as follows:

$$
\begin{aligned}
& f(x)\cdot y\cdot x\cdot f(f(y\cdot x)) && \\
&= f(x)\cdot f(f(y\cdot x))\cdot y\cdot x && \text{since } u \text{ and } f(f(u)) \text{ commute} \\
&= f(x\cdot f(y\cdot x))\cdot y\cdot x && \text{since } x \text{ and } f(y\cdot x) \text{ commute} \\
&= f(f(\cdot x)\cdot x)\cdot (y\cdot x) && \text{since } f(x\cdot y)=f(y\cdot x) \\
&= (y\cdot x)\cdot f(f(y\cdot x)\cdot x) && \text{since } y\cdot x \text{ and } f(f(y\cdot x)\cdot x) \text{ commute.} \\
&= y\cdot x\cdot f(x\cdot f(y\cdot x)) && \text{since } f(x\cdot y)=f(y\cdot x) \\
&= y\cdot x\cdot f(x)\cdot f(f(y\cdot x)) && \text{since } x \text{ and } f(y\cdot x) \text{ commute} \\
&= y\cdot f(x)\cdot x\cdot f(f(y\cdot x)) && \text{since } x \text{ and } f(x) \text{ commute}
\end{aligned}
$$

Hence, we have

$$f(x)\cdot y\cdot x\cdot f(f(y\cdot x)) = y\cdot f(x)\cdot x\cdot f(f(y\cdot x)).$$

Finally, cancelling the common term $x\cdot f(f(y\cdot x))$ from the right sides, we get $f(x)\cdot y = y\cdot f(x)$.

Corollary 2.3. *In a cancellation semigroup $(S,\cdot)$, for $x,y\in S$ and $n\in\mathbb{Z}^+$, $(x\cdot y)^n=(y\cdot x)^n$ implies $x^n\cdot y = y\cdot x^n$.*

Proof. Simply take $f(x)=x^n$. The power map $f(x)=x^n$ satisfies all the six properties mentioned in Lemma 2.1 and hence the proof of Theorem 2.2 applies. Therefore, the n-th powers are central in the semigroup, i.e., $x^n\cdot y = y\cdot x^n$. □

Next we consider the following more general case.

Theorem 2.4. *In a cancellation semigroup S, if there exist $k\geq 2, n\in\mathbb{Z}^+$ such that $(a_1a_2\cdots a_k)^n = (a_k\cdots a_2a_1)^n$ for any $a_i\in S$ holds, then x^n is central in S for any $x\in S$.*

Proof. When $n=1$, all the situations can be reduced to $k=2$ or $k=3$.

In case of $n=1$ and $k=2$, we have $a_1a_2=a_2a_1$, and then S is commutative.

In case of $n=1$ and $k=3$, we have $a_1a_2a_3=a_3a_2a_1$. Then, for any $x,y,z,u\in S$,

$$xyzu = uzxy = yzxu.$$

Cancelling u from the right sides, we obtain $xyz=yzx$. By the condition, $yzx=xzy$. Then $xyz=xzy$, and thus $yz=zy$. Hence S is commutative.

Next, we consider $n\geq 2$. Note that

$$
\begin{aligned}
x\cdot(xy^{k-1})^n &= x\cdot(x\cdot y\cdots y)^n \\
&= x\cdot(y\cdots y\cdot x)^n \\
&= x\cdot(y^{k-1}\cdot x)^n \\
&= (xy^{k-1})^n x,
\end{aligned}
$$

that is, x and $(xy^{k-1})^n$ commute, and thus $(xy^{k-1})^n = (y^{k-1}x)^n$.

Pick up $m \in \mathbb{Z}^+$ such that $mn \geq k-1$. Now we claim the following identity holds

$$x^n y[(xy^{k-1})^{mn}]^n = yx^n[(xy^{k-1})^{mn}]^n.$$

We will combine suitable x's and y's together and apply above commutative properties:

$$\begin{aligned}
x^n y[(xy^{k-1})^{mn}]^n &= x^n y[(xy^{k-1})^{mn-1}(xy^{k-2})y]^n \\
&= x^n[y(xy^{k-1})^{mn-1}(xy^{k-2})]^n y \\
&= x^n[y(xy^{k-1})^{mn-1}x\underbrace{y\cdots y}_{k-2}]^n y \\
&= x^n[\underbrace{y\cdots y}_{k-2}\cdot x\cdot y(xy^{k-1})^{mn-1}]^n y \\
&= x^n(y^{k-2}xy(xy^{k-1})^{mn-1})^n y \\
&= x^n[y^{k-2}xy\underbrace{(xy^{k-1})\cdot(xy^{k-1})\cdots(xy^{k-1})^{mn+2-k}}_{k-2}]^n y \\
&\quad (\text{ since } mn \geq k-1, mn+2-k \geq 1) \\
&= x^n[\underbrace{(xy^{k-1})^{mn+2-k}(xy^{k-1})\cdots(xy^{k-1})}_{k-2}\cdot xy\cdot y^{k-2}]^n y \\
&= x^n[(xy^{k-1})^{mn}]^n y \\
&= [x\cdot(xy^{k-1})^{mn}]^n y \\
&\quad (\text{since } x \text{ commutes with } (xy^{k-1})^n \text{ and } (xy^{k-1})^{mn}).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
yx^n[(xy^{k-1})^{mc}]^n &= y[x\cdot(xy^{k-1})^{mn}]^n \text{ (since } x \text{ and } (xy^{k-1})^{mn} \text{ commute)} \\
&= y\cdot[x(xy^{k-1})^{mn-1}\cdot xy^{k-2}\cdot y]^n \\
&= [y\cdot x(xy^{k-1})^{mn-1}\cdot xy^{k-2}]^n y \\
&= [yx(xy^{k-1})^{mn-1}\cdot x\underbrace{y\cdots y}_{k-2}]^n y \\
&= [\underbrace{y\cdots y}_{k-2}\cdot x\cdot yx(xy^{k-1})^{mn-1}]^n y \\
&= [\underbrace{y\cdots y}_{k-2}\cdot(xy)\cdot x(xy^{k-1})^{mn-1}]^n y \\
&= [x(xy^{k-1})^{mn-1}\cdot(xy)\cdot\underbrace{y\cdots y}_{k-2}]^n y \\
&= [x(xy^{k-1})^{mn}]^n y
\end{aligned}$$

Therefore, cancelling $[(xy^{k-1})^{mc}]^n$ from the right sides of $x^n y[(xy^{k-1})^{mn}]^n = yx^n[(xy^{k-1})^{mc}]^n$, we have $x^n y = yx^n$. □

3. Transferability of $(xy)^n = (yx)^n$

Let $(S, \cdot)$ be a cancellation semigroup satisfying the law $(xy)^n = (yx)^n$. Then, by Corollary 2.3, we know that all the powers of n are central in S, i.e., S satisfies the identity $x^n \cdot y = y \cdot x^n$. We now use the Ore principle resulting from this identity to construct the actual group of quotients. Thus we will have an explicit formula for the group multiplication. We show that this group multiplication satisfies the semigroup law $x^n \cdot y = y \cdot x^n$. This will prove the transferability of $x^n \cdot y = y \cdot x^n$ from S to its Ore group of right quotients SS^{-1}. Since $(xy)^n = (yx)^n$ and $x^n \cdot y = y \cdot x^n$ are equivalent in cancellation semigroups, we get that the semigroup law $(xy)^n = (yx)^n$ is also transferable.

Since the semigroup satisfies a non-trivial identity, it obviously satisfies the Ore left multiple principle (the property Mv in Ore [14]), the group of right quotients SS^{-1} exists. What is not obvious is that the group also satisfies the identity.

Theorem 3.1. *The semigroup law $(xy)^n = (yx)^n$ is transferable in a semigroup $(S, \cdot)$.*

Proof. We first define the multiplication and the equality of quotients. Let $\frac{a}{b}$ and $\frac{c}{d}$ be two right quotients in the group SS^{-1}. Thus the elements a, b, c, d are in S. We follow the idea of Ore and define the product and equality of two right quotients. Note that

$$\frac{a}{b} \cdot \frac{c}{d} = ab^{-1}cd^{-1} = ab^{n-1-n}cd^{n-1-n} = ab^{n-1}cd^{n-1}b^{-n}d^{-n} = \frac{ab^{n-1}cd^{n-1}}{b^n d^n}.$$

Thus we can define the product

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ab^{n-1}cd^{n-1}}{b^n d^n}.$$

Also, here

$$\frac{a}{b} \sim \frac{c}{d} \text{ if and only if } ab^{n-1}d = b^n c.$$

Hence, the identity is $\frac{a_0}{a_0}$ and the inverse $\left(\frac{a}{b}\right)^{-1} = \frac{b^n}{ab^{n-1}}$.

Next we define the embedding map as following: for any $a \in S$,

$$\phi : S \to SS^{-1}, \quad \phi(a) = \frac{aa_0}{a_0}. \quad \text{for some } a_0 \in S.$$

For any $a, b \in S$, we have

$$\phi(ab) = \frac{aba_0}{a_0} = \frac{aba_0^n b_0^n}{a_0^n b_0^n} = \frac{aa_0}{a_0}\frac{bb_0}{b_0} = \phi(a)\phi(b).$$

Hence ϕ is an isomorphism.

Now we prove that $\frac{a}{b} = \phi(a)\phi(b)^{-1}$ for any $a, b \in S$.

$$\phi(a)\phi(b)^{-1} = \frac{aa_0}{a_0}\left(\frac{bb_0}{b_0}\right)^{-1} = \frac{aa_0}{a_0}\frac{b_0^n}{bb_0^n} = \frac{aa_0^n b_0^n (bb_0^n)^{n-1}}{a_0^n (bb_0^n)^n}.$$

Thus

$$\begin{aligned}
\frac{a}{b} &= \frac{aa_0^n b_0^n (bb_0^n)^{n-1}}{a_0^n (bb_0^n)^n} \\
&\iff aa_0^n b_0^n (bb_0^n)^{n-1} b^n = ab^{n-1} a_0^n (bb_0^n)^n \\
&\iff aa_0^n b_0^n (bb_0^n)^{n-1} b^n = aa_0^n b^{n-1} (bb_0^n)(bb_0^n)^{n-1} \\
&\iff aa_0^n b_0^n b^n (bb_0^n)^{n-1} = aa_0^n b_0^n b^n (bb_0^n)^{n-1} \text{ (since } a_0^n, b^n, b_0^n \text{ are central).}
\end{aligned}$$

Hence $\frac{a}{b} = \phi(a)\phi(b)^{-1}$. Therefore, we have the following two formats for the group of quotients:

$$SS^{-1} = \left\{\frac{a}{b} \mid a, b \in S\right\} = \{\phi(a)\phi(b)^{-1} \mid a, b \in S\}.$$

For any $a, b \in S$, we can verify the following four identities:

$$\phi(a)^n\phi(b) = \phi(a^n b) = \phi(ba^n) = \phi(b)\phi(a)^n.$$

$$\phi(a)^n\phi(b)^{-1} = \phi(b)^{-1}\phi(b)\phi(a)^n\phi(b)^{-1} = \phi(b)^{-1}\phi(a)^n\phi(b)\phi(b)^{-1} = \phi(b)^{-1}\phi(a)^n.$$

$$\begin{aligned}
(\phi(a)^{-1})^n\phi(b) &= (\phi(a)^{-1})^n\phi(b)\phi(a)^n(\phi(a)^{-1})^n \\
&= (\phi(a)^{-1})^n\phi(a)^n\phi(b)(\phi(a)^{-1})^n \\
&= \phi(b)(\phi(a)^{-1})^n. \\
(\phi(a)^{-1})^n\phi(b)^{-1} &= \phi(b)^{-1}\phi(b)(\phi(a)^{-1})^n\phi(b)^{-1} \\
&= \phi(b)^{-1}(\phi(a)^{-1})^n\phi(b)\phi(b)^{-1} \\
&= \phi(b)^{-1}(\phi(a)^{-1})^n.
\end{aligned}$$

Since every element in SS^{-1} has the form $\phi(a)\phi(b)^{-1}$, we can conclude that both $\phi(a)^n$ and $(\phi(a)^{-1})^n$ are central in SS^{-1} for all $a \in S$.

Next, we prove that for any $a, b \in S$, $\left(\frac{a}{b}\right)^n = [\phi(a)\phi(b)^{-1}]^n$ is central in SS^{-1}. For any $g \in SS^{-1}$, we have

$$\begin{aligned}
[\phi(a)\phi(b)^{-1}]^n g &= [\phi(a)\phi(b)^{-1}][\phi(a)\phi(b)^{-1}]^{n-1} g \\
&= \phi(a)^n[\phi(a)^{-1}]^{n-1}\phi(b)^{-1}[\phi(a)\phi(b)^{-1}]^{n-1} g \\
&= \phi(ba^{n-1})^{-1}[\phi(a)\phi(b)^{-1}]^{n-1} g \cdot \phi(a)^n \\
&= [\phi(ba^{n-1})^{-1}]^n\phi(ba^{n-1})^{n-1} \cdot [\phi(a)\phi(b)^{-1}]^{n-1} g \cdot \phi(a)^n \\
&= [\phi(ba^{n-1})^{n-1}] \cdot [\phi(a)\phi(b)^{-1}]^{n-1} g \cdot \phi(a)^n[\phi(ba^{n-1})^{-1}]^n \\
&= (\phi[(ba^{n-1})^{n-1} \cdot a]\phi(b)^{-1}) \cdot [\phi(a)\phi(b)^{-1}]^{n-2} g[\phi(a)\phi(b)^{-1}] \\
&\quad \cdot [\phi(ba^{n-1})^{n-1}]^{-1} \\
&= (\phi[(ba^{n-1})^{n-1} a]\phi(b)^{-1}) \cdot [\phi(a)\phi(b)^{-1}]^{n-2} g[\phi(a)\phi(b)^{-1}] \\
&\quad \cdot [\phi(ba^{n-1})^{n-1}]^{-1} \\
&\qquad (\text{Let } a' = (ba^{n-1})^{n-1} a) \\
&= [\phi(a')\phi(b)^{-1}] \cdot [\phi(a)\phi(b)^{-1}]^{n-2} g[\phi(a)\phi(b)^{-1}][\phi(a')\phi(a)^{-1}]^{-1}.
\end{aligned}$$

Using the deduction above again, we have

$$\begin{aligned}
&(\phi[(b(a')^{n-1})^{n-1} a]\phi(b)^{-1} \cdot [\phi(a)\phi(b)^{-1}]^{n-3} g[\phi(a)\phi(b)^{-1}][\phi(a')\phi(a)^{-1}]^{-1} \\
&\cdot [\phi(a')\phi(b)^{-1}] \cdot [\phi(b(a'))^{n-1})^{n-1}]^{-1} \\
= \; &(\phi[(b(a')^{n-1})^{n-1} a]\phi(b)^{-1} \cdot [\phi(a)\phi(b)^{-1}]^{n-3} g[\phi(a)\phi(b)^{-1}]^2 \\
&\cdot [\phi(b(a'))^{n-1})^{n-1}]^{-1}.
\end{aligned}$$

Define

$$a_1 = a, \; a_2 = a' = (ba^{n-1})^{n-1} a, \ldots, a_{k+1} = (ba_k^{n-1})^{n-1} a.$$

Then

$$\begin{aligned}
&[\phi(a)\phi(b)^{-1}]^n g \\
&= [\phi(a_1)\phi(b)^{-1}] \cdot [\phi(a)\phi(b)^{-1}]^{n-1} g \\
&= [\phi(a_2)\phi(b)^{-1}] \cdot [\phi(a)\phi(b)^{-1}]^{n-2} g [\phi(a)\phi(b)^{-1}] \cdot [\phi(a_2)\phi(a)^{-1}]^{-1} \\
&= \cdots \\
&= [\phi(a_k)\phi(b)^{-1}] \cdot [\phi(a)\phi(b)^{-1}]^{n-k} g [\phi(a)\phi(b)^{-1}]^{k-1} \cdot [\phi(a_2)\phi(a)^{-1}]^{-1} \\
&= \cdots \\
&= [\phi(a_n)\phi(b)^{-1}] \cdot g [\phi(a)\phi(b)^{-1}]^{n-1} \cdot [\phi(a_n)\phi(a)^{-1}]^{-1}
\end{aligned}$$

If $\phi(a_n)\phi(b)^{-1}$ is central, then we have

$$\begin{aligned}
&g[\phi(a)\phi(b)^{-1}]^{n-1} \cdot [\phi(a_n)\phi(a)^{-1}]^{-1}[\phi(a_n)\phi(b)^{-1}] \\
&= g[\phi(a)\phi(b)^{-1}]^{n-1} \cdot [\phi(a)\phi(b)^{-1}] \\
&= g[\phi(a)\phi(b)^{-1}]^{n}.
\end{aligned}$$

Hence, the proof is completed. Therefore, we will show that $\phi(a_n)\phi(b)^{-1}$ is central as follows.

Let $y_k = \phi(a_k)\phi(b)^{-1}$. Then

$$y_1 = \phi(a)\phi(b)^{-1},\ a_{k+1} = (ba_k^{n-1})^{n-1}a,$$

$$\phi(a_{k+1}) = \phi[(ba_k^{n-1})^{n-1}] \cdot \phi(a) = [\phi(b)\phi(a_k)^{n-1}]^{n-1} \cdot \phi(a).$$

Thus

$$\phi(a_{k+1})\phi(b)^{-1} = [\phi(b)\phi(a_k)^{n-1}]^{n-1} \cdot \phi(a)\phi(b)^{-1}.$$

That is,

$$\begin{aligned}
y_{k+1} &= [\phi(b)[y_k\phi(b)]^{n-1}]^{n-1} \cdot \phi(a)\phi(b)^{-1} \\
&= [[y_k\phi(b)]^n \cdot y_k^{-1}]^{n-1}\phi(a)\phi(b)^{-1} \\
&= [y_k\phi(b)]^{n(n-1)}(y_k^{-1})^n y_k\phi(a)\phi(b)^{-1}.
\end{aligned}$$

Continue the same deduction, and use y_{k-1} to represent y_k, we have

$$y_{k+1} = [y_k\phi(b)]^{n(n-1)}(y_k^{-1})^n[y_{k-1}\phi(b)]^{n(n-1)}(y_{k-1}^{-1})^n y_{k-1}[\phi(a)\phi(b)^{-1}]^2.$$

Thus

$$\begin{aligned}
y_n &= [y_{n-1}\phi(b)]^{n(n-1)}(y_{n-1}^{-1})^n y_{n-1}\phi(a)\phi(b)^{-1} \\
&= x_1^n x_2^n x_3^n x_4^n y_{n-2}[\phi(a)\phi(b)^{-1}]^2 \\
&= \cdots \\
&= x_1^n x_2^n \cdots x_{2n-2}^n y_1[\phi(a)\phi(b)^{-1}]^{n-1} \\
&= x_1^n x_2^n \cdots x_{2n-2}^n y_1[\phi(a)\phi(b)^{-1}]^{n},
\end{aligned}$$

where $x_i \in S, i = 1, \ldots, 2n-2$. Since all $x^n, x \in S$ are central, y_n is central as desired. Therefore, $\left(\frac{a}{b}\right)^n$ is central, and thus the emdedding ϕ is perfect embedding. □

Acknowledgments

This project is partially supported by Mitacs Globalink Research Internship Canada NSERC.

References

[1] G. Bergman, *Hyperidentities of groups and semigroups.* Aequat. Math. 23 (1981), 55–65.

[2] G. Bergman, *Questions in Algebra.* Preprint, Berkeley, U.D. 1986.

[3] B. M. Green and J. R. Isbell, *Problems and Solutions: Solutions of Elementary Problems: E2259. Commuting powers in a group.* The American Mathematical Monthly, 78(8)(1971): 909–910.

[4] S. V. Ivanov, A. M. Storozhev, *On identities in groups of fractions of cancellative semigroups*, Proc. Amer. Math. Soc. 133 (2005), 1873–1879.

[5] J. Krempa and O. Macedonska, *On identities of cancellation semigroups*, Contemporary Mathematics, Vol 131, 1992

[6] F. W. Levi, *Notes on group theory. I, II*, J. Indian Math. Soc. 8 (1944), 1–9.

[7] O. Macedonska and P. Slanina. *On identities satisfied by cancellative semigroups and their groups of fractions,* (Preprint).

[8] A.I. Mal'cev, *Nilpotent Groups*, Ivanov Gos.Ped.Ins.Uc.zap (1953).

[9] W. McCune, Prover9, https://www.cs.unm.edu/~mccune/mace4/.

[10] G. I. Moghaddam and R. Padmanabhan, *Commutativity theorems for cancellative semigroups,* Semigroup Forum 95 (2017), no. 3, 448–454.

[11] G. I. Moghaddam, R. Padmanabhan, and Yang Zhang, *Automated reasoning with power maps.* Journal of Automated Reasoning, 64(4)(2020), 689–697.

[12] B.H. Neumann and T. Taylor, *Subsemigroups of Nilpotent Groups,* Proc. Roy. Soc. Ser. A274(1963), pp 1-4.

[13] T. Nordahi, *Semigroups satisfying* $(xy)^m = x^m y^m$, Semigroup Forum 8(4) (1974), 332–346.

[14] O. Ore, Linear Equations in Non-Commutative Fields Annals of Mathematics, Jul., 1931, Second Series, Vol. 32, pp.463-477.

[15] R. Padmanabhan, and Yang Zhang, *C*ommutativity theorems in groups with power-like maps, J. Formaliz. Reason. 12(1) (2019), 1–10.

[16] Chen-Te Yen, *Note on the commutativity of cancellative semigroups.* Bulletin of the Institute of Mathematics Academia Sinica, 10(2)(1982), 149-153.

[17] Chen-Te Yen, *On the commutativity of rings and cancellative semigroups.* Chinese Journal of Mathematics, 11(2)(1983), 99–113.