Formalization of some inverse semigroup theory in Coq

Weiyun Lu
Department of Mathematics & Statistics, University of Ottawa

December 2, 2014

Contents

Introduction

Writing mathematics in a completely formal language is an idea that dates back to David Hilbert's programme in the 1930s. Hilbert had some lofty goals of being able to formalize all of mathematics in a system so that it was *consistent* (no contradictions derivable), *decidable* (every statement's truth or untruth could be checked by some finite algorithm) and *complete* (every true mathematical statement should be provable). Unfortunately for him, Gödel's incompleteness theorems a few years later proved that this was not possible — every formal system containing first-order logic and enough axioms to derive the basic properties of arithmetic necessarily also contain a statement which can be neither proven nor refuted, and even more strangely, a *true* statement which is not only impossible to prove, but one can *prove* that it *cannot* be proven!

Fast forward to modern day — the advent of computer proof assistants like Coq (among others, like Agda and Isabelle) have spurred renewed interest in the formalization of mathematics. With proofs of major theorems becoming incredibly long and technical, it becomes impractical to check them by hand. Some major results that have been formalized in Coq include the *Feit-Thompson theorem* (finite group theory) and the *Four Color theorem* (graph theory) — both of these done by Georges Gonthier and his team at Microsoft. In the case of the former, some errors in the proof (nobody checked the 200+ page print proof line-by-line carefully enough to find them) were discovered during the formalization process.

During 2012-2013 at the Institute for Advanced Study in Princeton, homotopy type theory (HoTT) was developed by Voevodsky, Awodey, and others, which shook the foundations of mathematics. The HoTT book was, perhaps the first of its kind, developed in Coq *before* being turned into a regular print book — the opposite direction of how things usually go in this business.

In this project, we formalize some inverse semigroup theory in Coq. Inverse semigroups are to partial symmetries what groups are to global symmetries. They are used in *coordinatization* theorems for MV/effect algebras (these are the algebraic semantics for, respectively, classical and quantum fuzzy logics), which I intend to investigate in my thesis. Our source material comes from Chapter 1 of Mark Lawson's book ([5]). The HoTT book ([6]) was helpful as a general reference for understanding set-theoretic foundations vs. type-theoretic foundations from mathematicians' viewpoint.

The documents [3] and [4] were useful in learning about various commands and tactics for Coq. Some useful tips were also gleamed from various posts and discussions on stackexchange which we will not individually mention. The *Ensembles* library was used for the material of Section 3. Especially in the beginning, user contributions on the Coq website, in particular Groups ([1]) and GroupTheory ([2]), were useful for learning by example.

With the exception of Section 2 describing our use of the *Ensembles* library for the remainder of the formalization, this report is primarily an informal account of the mathematics so that the reader may follow a more human-readable version of what has been implemented in Coq. Comments and remarks about the implementation, tactics and commands used, etc, can be found as comments in the Coq script itself.

1 Two equivalent axiomatizations

In the first section, we begin with a weaker notion of *regular semigroup* and prove that from this, there are two equivalent ways of defining an inverse semigroup — this theorem was originally due to Wagner and Preston.

Definition 1.1 (Regular semigroup, pseudoinverse)**.** A *regular semigroup* is a pair $(X, *)$ where X is a set and $*$ is a binary operation, satisfying:

- Closure — for all $x, y \in X$, $x * y$ is also in X.
- Associativity — for all $x, y, z \in X$, $(x * y) * z = x * (y * z)$.
- Pseudoinverse — for all $x \in X$, there exists $y \in X$ such that $x * y * x = x$ and $y * x * y = y$. We say that y is *pseudoinverse* to x.

As a common abuse of notation, we will often simply say "X is a regular semigroup" and leave the operation $*$ implicit, and write xy for $x * y$. We also write x^n, for some $n \in \mathbb{N}$, to mean $\underbrace{x * \ldots * x}_{n \text{ times}}$.

For the rest of this section we fix X to be an arbitrary regular semigroup.

Definition 1.2 (Idempotent, commute)**.** An element $e \in X$ that satisfies $e^2 = e$ is called *idempotent*. Two elements $x, y \in X$ *commute* if $xy = yx$.

Lemma 1.3. *Every idempotent element is pseudoinverse to itself.*

Proof. If $e \in X$ is idempotent, then clearly we have $eee = (ee)e = ee = e$. □

Lemma 1.4. *Let $x, y \in X$ and let e be a pseudoinverse of xy. Then yex is idempotent.*

Proof. As e is pseudoinverse to xy, this means $xyexy = xy$ and $exye = e$. We have, in particular, $(yex)(yex) = y(exye)x = yex$. □

Lemma 1.5. *If $x, y \in X$ are idempotents, then xy has an idempotent pseudoinverse.*

Proof. Let e be a pseudoinverse of xy, so that we have $xyexy = xy$ and $exye = e$. Now consider the element yex. By Lemma 1.4, yex is idempotent. Now to see that it is also pseudoinverse to xy, observe that on one hand we have

$$(xy)(yex)(xy) = x(y^2ex^2)y = xyexy = xy,$$

and on the other hand we have

$$(yex)(xy)(yex) = ye(x^2y^2)ex = yexyex = yex.$$

□

Theorem 1.6. *In a regular semigroup, the following conditions are equivalent:*

(1) All pairs of idempotent elements commute.

(2) Pseudoinverses are unique (i.e. each element has one and only one pseudoinverse).

Proof. (1) ⇒ (2): Suppose that all idempotents commute. Let $x \in X$ be an arbitrary element. Suppose z, z' are pseudoinverses of x, that is, we have the equations

$$\begin{aligned} xzx &= x, & zxz &= z, \\ xz'x &= x, & z'xz' &= z'. \end{aligned}$$

We must show $z = z'$. We claim first that $xz, xz', zx, z'x$ are all idempotents. Indeed we have

$$\begin{aligned} (xz)(xz) &= (xzx)z = xz, & (xz')(xz') &= (xz'x)z' = xz', \\ (zx)(zx) &= z(xzx) = zx, & (z'x)(z'x) &= z'(xz'x) = z'x. \end{aligned}$$

Then using the fact that the above elements are idempotent, the hypothesis that idempotents commute, and noting also that $xzx = x = xz'x$, we have

$$\begin{aligned} z = zxz &= z(xz) = z(xz)(xz) = z(xzx)z \\ &= z(xz'x)z = z(xz')(xz) = z(xz)(xz') = z(xzx)z' \\ &= z(xz'x)z' = (zx)(z'x)z' = (z'x)(zx)z' = z'(xzx)z' \\ &= z'(xz'x)z' = (z'x)(z'x)z' = (z'x)z' = z'. \end{aligned}$$

Thus, x has only one pseudoinverse. As x was arbitrary, we conclude all elements have a unique pseudoinverse.

(2) ⇒ (1): Suppose that pseudoinverses are unique. Let x, y be idempotent, so that $x^2 = x$ and $y^2 = y$. We must show $xy = yx$. By Lemma 1.5, we know xy has a (now unique) idempotent pseudoinverse e. So we have the equations

$$e^2 = e, (xy)e(xy) = xy, e(xy)e = e.$$

Now, we know from Lemma 1.3 that e is pseudoinverse to itself. But as e is pseudoinverse also to xy, uniqueness implies $e = xy$. That is, xy is idempotent and pseudoinverse to itself. Following similar lines of reasoning, yx is idempotent as well. Observe that

$$(xy)(yx)(xy) = (xy)(yxyx)(xy) = x(y^2)xy(x^2)y = (xy)(xy)(xy) = (xy)(xy) = xy,$$

and also

$$(yx)(xy)(yx) = (yx)(xyxy)(yx) = y(x^2)yx(y^2)x = (yx)(yx)(yx) = (yx)(yx) = yx.$$

These equations imply that yx is also pseudoinverse to xy, whence uniqueness implies $xy = yx$ as desired. As x, y were arbitrary idempotents, we conclude all idempotents commute.

□

A regular semigroup where the above conditions hold is called an *inverse semigroup*.

2 The *Ensembles* library

An interesting distinction between set-theoretical and type-theoretical foundations for mathematics is that the distinction between sets and logical propositions is blurry in type theory. Traditionally, if we have $x \in X$, this is written $x : X$ in type theory — the *typing judgement* that x is a term of the type X. However, a proof ϕ of a proposition P is also written $\phi : P$. That is, a proposition is also a type, and the terms are proofs of the type. Intuitively, we identify propositions with their sets of proofs, and a proposition is provable precisely when its type is *inhabited*. So, giving an explicit proposition of a proof is no different from exhibiting an explicit element of a set.

In Section 1, whenever we needed a set X, we simply let X : Set. However, in the material to come, we need to work with set-theoretical ideas like subsets, intersection, equality of sets, and so on. The problem is that terms of the type Set in Coq do not behave like mathematical sets. For instance, two different types are necessarily disjoint. Set theoretically, we have $3 \in \mathbb{N}$ and $3 \in \mathbb{R}$, and $\mathbb{N} \subseteq \mathbb{R}$, so we are in fact talking about the same 3. On the other hand, in type theory, if we have 3 : Nat and 3 : Real, these are necessarily different and incomparable versions of "3". (Defining the real numbers at all is no trivial task — there is an entire chapter in [6] devoted to this construction).

A clever way to work set theory into type theory is present in the *Ensembles* library, which is part of the standard Coq libraries. We will now discuss the parts of it that we will use. The first few lines are

```
Variable U : Type.
Definition Ensemble := U → Prop.
Definition In (A:Ensemble) (x:U) : Prop := A x.
Definition Included (B C:Ensemble) : Prop := forall x:U, In B x → In C x.
```

Intuitively what is going on here is that we specify some universe U in which all elements of the sets we are interested in reside. Then, a set is an Ensemble on U, which is actually a function U → Prop. So we are in some sense doing the opposite from what was described in the first paragraph of this section — by declaring X : Ensemble U we are identifying a set of elements X from the universe U with the unary predicate telling us whether any particular element of U is in X!

Any possible element x that we work with must be of the type of the universe, that is, x : U, and to say that $x \in X$ is to declare In X x. This allows us then to define what a subset is; given two sets B, C (B C : Ensemble U), to express $B \subseteq C$ is to declare Included B C; that is, for any x : U such that In B x, we also have In C x.

We can then also express equality of sets, $B = C$, by proving $B \subseteq C$ and $C \subseteq B$ with the definition

```
Definition Same_set (B C:Ensemble) : Prop := Included B C /\ Included C B.
```

Many set theoretical constructions like singletons, unions, intersections, complements, can now be defined *inductively*. The one we will use later is intersections. This is given by

```
Inductive Intersection (B C:Ensemble) : Ensemble :=
Intersection_intro : forall x:U, In B x → In C x → In (Intersection B C) x.
```

This is a (constructive) inductive definition with a single introduction rule. So this is saying that for any x : U, if both In B x and In C x, we can apply the rule to conclude In (Intersection B C) x, and conversely, if any x : U satisfies In (Intersection B C) x, then the only way this could be is via the sole introduction rule, so that In B x and In C x. This is exactly how the familiar set-theoretic construction of intersections behave.

3 Inverse semigroups

We begin by recalling the definition of an inverse semigroup.

Definition 3.1 (Inverse semigroup)**.** An *inverse semigroup* is a regular semigroup (see Definition 1.1) satisfying the additional equivalent conditions (see Theorem 1.6) that idempotents commute, and that pseudoinverses are unique.

For the remainder of this section, we fix X (following the same abuse of notation as before) to be an arbitrary inverse semigroup. Since pseudoinverses are unique, then for any $x \in X$ we can safely write "x^{-1}" for the element which is pseudoinverse to x.

3.1 Properties of pseudoinverses and idempotents

We now establish some useful properties that hold in an arbitrary inverse semigroup.

Proposition 3.2. *The following hold in an inverse semigroup X:*

(a) For all $x \in X$, the elements $x^{-1}x$ and xx^{-1} are idempotent.

(b) For all $x \in X$, we have $(x^{-1})^{-1} = x$.

(c) For any idempotent $e \in X$ and any element $x \in X$, the element $x^{-1}ex$ is idempotent.

(d) If $e \in X$ is idempotent, then $e = e^{-1}$.

(e) For all $x_1, x_2 \in X$, we have $(x_1x_2)^{-1} = x_2^{-1}x_1^{-1}$.

(f) If $e, f \in X$ are idempotent, then ef is also idempotent.

Proof. (a) We have that

$$(x^{-1}x)(x^{-1}x) = (x^{-1}xx^{-1})x = x^{-1}x$$

and

$$(xx^{-1})(xx^{-1}) = (xx^{-1}x)x^{-1} = xx^{-1}.$$

(b) Fix $x \in X$ and consider the following equations where y is a variable,

$$x^{-1}yx^{-1} = x^{-1}, yx^{-1}y = y.$$

Obviously, x for y is a solution, implying x is pseudoinverse to x^{-1}, whence by uniqueness $(x^{-1})^{-1} = x$.

(c) Using the result from (a) that xx^{-1} is idempotent and the fact that idempotents commute, we have

$$(x^{-1}ex)(x^{-1}ex) = x^{-1}(exx^{-1})ex = x^{-1}(xx^{-1}e)ex = (x^{-1}xx^{-1})e^2x = x^{-1}ex.$$

(d) This follows directly from Lemma 1.3 and uniqueness of pseudoinverses.

(e) From (a) we know $x_1^{-1}x_1$ and $x_2x_2^{-1}$ are idempotent and hence commute. So on one hand we have

$$\begin{aligned}(x_2^{-1}x_1^{-1})(x_1x_2)(x_2^{-1}x_1^{-1}) &= (x_2^{-1})(x_1^{-1}x_1)(x_2x_2^{-1})(x_1^{-1})\\ &= (x_2^{-1})(x_2x_2^{-1})(x_1^{-1}x_1)(x_1^{-1})\\ &= (x_2^{-1}x_2x_2^{-1})(x_1^{-1}x_1x_1^{-1})\\ &= x_2^{-1}x_1^{-1},\end{aligned}$$

and on the other,

$$\begin{aligned}(x_1x_2)(x_2^{-1}x_1^{-1})(x_1x_2) &= x_1(x_2x_2^{-1})(x_1^{-1}x_1)x_2\\ &= x_1(x_1^{-1}x_1)(x_2x_2^{-1})x_2\\ &= (x_1x_1^{-1}x_1)(x_2x_2^{-1}x_2)\\ &= x_1x_2\end{aligned}$$

Hence, the pseudoinverse of x_1x_2 is $x_2^{-1}x_1^{-1}$.

(f) We have

$$(ef)(ef) = e(fe)f = e(ef)f = e^2f^2 = ef.$$

□

Lemma 3.3. *For any idempotent $e \in X$ and any element $x \in X$, we have the following.*

(a) There is an idempotent $f \in X$ such that $ex = xf$.

(b) There is an idempotent $g \in X$ such that $xe = gx$.

Proof. (a) Put $f = x^{-1}ex$, which is idempotent by Proposition 3.2c. Then,

$$xf = x(x^{-1}ex) = (xx^{-1})ex = e(xx^{-1})x = e(xx^{-1}x) = ex.$$

(b) Put $g = xex^{-1} = (x^{-1})^{-1}ex^{-1}$, which is idempotent by Proposition 3.2c. Then,

$$gx = (xex^{-1})x = xe(x^{-1}x) = x(x^{-1}x)e = (xx^{-1}x)e = xe.$$

□

3.2 Ideals and generators

In this subsection we introduce a certain kind of subset of an inverse semigroup called an *ideal* and prove some structural properties of principal ideals.

Definition 3.4 ((Left/right) ideal)**.** Let $I \subseteq X$ be a subset of an inverse semigroup X.

(a) If for all $a \in I$ and for all $x \in X$, we have that $xa \in I$, then I is a *left ideal* of X (that is, I is invariant under left "multiplication" by X).

(b) If for all $a \in I$ and for all $x \in X$, we have that $ax \in I$, then i is a *right ideal* of X (that is, I is invariant under right "multiplication" by X).

Definition 3.5 ((Left/right) principal ideal)**.** Let $r \in X$ be a fixed element of an inverse semigroup X. We can then define the *left principal ideal* of X generated by r to be

$$Xr = \{xr \mid x \in X\},$$

or equivalently,

$$a \in Xr \Leftrightarrow \exists x \in X \text{ such that } a = xr.$$

Similarly, the *right principal ideal* of X generated by r is

$$rX = \{rx \mid x \in X\},$$

or equivalently,

$$a \in rX \Leftrightarrow \exists x \in X \text{ such that } a = rx.$$

For the remainder of this subsection, we will only consider right principal ideals. Similar statements can be made for left principal ideals and have similar proofs (in fact, they are the same, modulo changing the order of some symbols in the only way that makes sense.)

Remark 3.6. A right principal ideal is, in particular, a right ideal. Indeed, if $x \in X$ and $r_0 \in rX$, then $r_0 = ry$ for some $y \in X$, and we have that $r_0x = (ry)x = r(xy) \in rX$. An element is also always in the right principal ideal it generates, as $r = rr^{-1}r = r(r^{-1}r) \in rX$.

Theorem 3.7. *Every right principal ideal has a unique idempotent generator. In particular, let $r \in X$ be a fixed element of an inverse semigroup. Then the following hold.*

(a) - (Existence). As sets, $rX = (rr^{-1})X$ (recall that rr^{-1} is idempotent by Lemma 3.2a.).

(b) - (Uniqueness). If $e \in X$ is an idempotent and $eX = rX$, then $e = rr^{-1}$.

Proof. (a) First let $y \in rX$. Then $y = rx_0$ for some $x_0 \in X$. We have

$$y = rx_0 = (rr^{-1}r)x_0 = (rr^{-1})(rx_0) \in (rr^{-1})X.$$

This proves $rX \subseteq (rr^{-1})X$.

Now let $z \in (rr^{-1})X$. So $z = rr^{-1}x_1$ for some $x_1 \in X$. We have

$$z = rr^{-1}x_1 = r(r^{-1}x_1) \in rX.$$

This proves $(rr^{-1})X \subseteq rX$.

Thus, $rX = (rr^{-1})X$, and indeed every principal ideal has an idempotent generator.

(b) If $eX = rX$, then by part (a) we also have $eX = (rr^{-1})X$. By Remark 3.6, we know $e \in eX = rr^{-1}X$ and $rr^{-1} \in (rr^{-1})X = eX$. Thus we can write

$$rr^{-1} = ep, e = rr^{-1}t$$

for some $p, t \in X$. We claim $rr^{-1}e = e$ and $err^{-1} = rr^{-1}$. Indeed, we have

$$rr^{-1}e = rr^{-1}(rr^{-1}t) = (rr^{-1})(rr^{-1})t = (rr^{-1})t = e,$$

and

$$err^{-1} = e(rr^{-1})(rr^{-1}) = e(ep)rr^{-1} = (e^2p)rr^{-1} = (ep)rr^{-1} = (rr^{-1})(rr^{-1}) = rr^{-1}.$$

Combining these equalities with the fact that idempotents commute yields

$$rr^{-1} = err^{-1} = e(rr^{-1}) = (rr^{-1})e = e.$$

Therefore, together with part (a), we have that every principal ideal has a unique idempotent generator.

□

Proposition 3.8. *Let $e, f \in X$ be idempotent. Then, $eX \cap fX = efX$.*

Proof. Let $x_0 \in eX \cap fX$. Then, $x_0 \in eX$ and $x_0 \in fX$ so that we can write

$$x_0 = ex_1, \quad x_0 = fx_2$$

for some $x_1, x_2 \in X$. We have

$$e(x_0) = e(ex_1) = e^2x_1 = ex_1 = x_0$$

and

$$f(x_0) = f(fx_2) = f^2x_2 = fx_2 = x_0.$$

Therefore,

$$x_0 = ex_0 = e(fx_0) = (ef)x_0 \in efX.$$

As x_0 was arbitrary, this proves $eX \cap fX \subseteq efX$.

Now let $x_0 \in efX$. So we can write $x_0 = efx_1$ for some $x_1 \in X$. Thus,

$$x_0 = e(fx_1) \in eX.$$

But as idempotents commute, we also have

$$x_0 = (ef)x_1 = (fe)x_1 = f(ex_1) \in fX.$$

Thus $x_0 \in eX \cap fX$. As x_0 was arbitrary, this proves $efX \subseteq eX \cap fX$.

Therefore, $eX \cap fX = efX$. □

3.3 The natural partial order

We now show that there is a natural way to endow an inverse semigroup with the structure of a poset. Moreover, we will show that the subset of idempotents can be realized as a meet semilattice.

Definition 3.9 ($\leq$)**.** For any inverse semigroup X, we define a binary relation $\leq$ on the elements of X by

$$s \leq t \Leftrightarrow \exists \text{ idempotent } e \text{ such that } s = te.$$

Lemma 3.10. *Let s, t be elements of an inverse semigroup X. Then, the following are equivalent.*

(1) $s \leq t$.

(2) $s = ft$ *for some idempotent* f *(i.e. the side on which the idempotent appears doesn't matter).*

(3) $s^{-1} \leq t^{-1}$.

(4) $s = ss^{-1}t$.

(5) $s = ts^{-1}s$.

Proof.

(1) ⇒ (2): If $s \leq t$, then we have $s = te$ for some idempotent $e \in X$. Then, by Lemma 3.3, we have

$$s = te = ft$$

for some idempotent $f \in X$.

(2) ⇒ (3): If $s = ft$ for some idempotent f then using Proposition 3.2e and 3.2d we have

$$s^{-1} = (ft)^{-1} = t^{-1}f^{-1} = t^{-1}f$$

and hence $s^{-1} \leq t^{-1}$.

(3) ⇒ (4): If $s^{-1} \leq t^{-1}$ then we can write $s^{-1} = t^{-1}e$ for some idempotent $e \in X$. Then,

$$s = (s^{-1})^{-1} = (t^{-1}e)^{-1} = e^{-1}(t^{-1})^{-1} = et,$$

so that

$$ess^{-1} = e(et)s^{-1} = e^2ts^{-1} = (et)s^{-1} = ss^{-1}.$$

Thus,

$$(ss^{-1})t = (ess^{-1})t = (e)(ss^{-1})t = (ss^{-1})et = ss^{-1}s = s.$$

(4) ⇒ (5): If $s = ss^{-1}t$, then as ss^{-1} is idempotent we have by Lemma 3.3 that $s = (ss^{-1})t = tf$ for some idempotent $f \in X$. Then,

$$s^{-1}sf = s^{-1}(tf)f = s^{-1}tf^2 = s^{-1}(tf) = s^{-1}s.$$

Hence,

$$ts^{-1}s = t(s^{-1}sf) = t(s^{-1}s)f = tf(s^{-1}s) = ss^{-1}s = s.$$

(5) ⇒ (1): Immediately follows from the definition of $\leq$. □

Definition 3.11 (Partial order, poset)**.** Let R be a binary relation on a set S. Then, R is a *partial order* if it satisfies:

(a) *Reflexivity* - for all $x \in X$, we have xRx.

(b) *Antisymmetry* - for all $x, y \in X$, if xRy and yRx, then $x = y$.

(c) *Transitivity* - for all $x, y, z \in X$, if xRy and yRz, then xRz.

A set equipped with a partial order is called a *poset*.

Theorem 3.12. *Given an inverse semigroup X, the relation $\leq$ is a partial order on the (underlying set of) X.*

Proof. (Reflexivity): For any $x \in X$, we have $x = xx^{-1}x = x(x^{-1}x)$, so $x \leq x$.

(Antisymmetry): Suppose $x \leq y$ and $y \leq x$. Then by Lemma 3.10 (equivalent condition 5), we have that $x = yx^{-1}x$ and $y = xy^{-1}y$. Therefore,

$$x = yx^{-1}x = (xy^{-1}y)x^{-1}x = x(y^{-1}y)(x^{-1}x) = x(x^{-1}x)(y^{-1}y) = xx^{-1}x(y^{-1}y) = xy^{-1}y = y.$$

(Transitivity): Let $x \leq y$ and $y \leq z$. Then, $x = ye$ and $y = zf$ for some idempotents $e, f \in X$. Then,

$$x = ye = (zf)e = z(fe).$$

Moreover, fe is idempotent by Proposition 3.2f. Thus, $x \leq z$.

Therefore, $\leq$ is a partial order, giving (the underlying set of) X the structure of a poset. □

Proposition 3.13. *The following hold in an inverse semigroup X.*

(a) If $e, f \in X$ are idempotent, then $e \leq f$ if and only if $e = ef = fe$.

(b) If $s \leq t$ and $u \leq v$, then $su \leq tv$.

(c) If $s \leq t$, then $s^{-1}s \leq t^{-1}t$ and $ss^{-1} \leq tt^{-1}$.

Proof. (a) If $e \leq f$, then $e = fi$ for some idempotent $i \in X$. Then,

$$fe = f(fi) = f^2i = fi = e$$

and $ef = fe$ since idempotents commute. The converse is obvious.

(b) If $s \leq t$ and $u \leq t$, we can write $s = te$ and $u = vf$ for some idempotents $e, f \in X$. By Lemma 3.3, we have $ev = vi$ for some idempotent $i \in X$. Hence,

$$su = (te)(vf) = t(ev)f = t(vi)f = tv(if),$$

so that $su \leq tv$.

(c) If $s \leq t$, then we know $s^{-1} \leq t^{-1}$ by Proposition 3.10. The result then follows from part (b).

□

Definition 3.14 (Meet, meet semilattice)**.** Let $(X, \leq)$ be a poset. For any elements $x, y \in X$, the *meet* of x, y (which we denote $x \wedge y$), if it exists, is an element $z \in X$ such that $z \leq x$, $z \leq y$ with the property that if any other $w \in X$ satisfies that $w \leq x$ and $w \leq y$, then $w \leq z$. If the meet of all pairs of elements of X exists, we say X is a *meet semilattice.*

Remark 3.15. It is easy to see that, when it exists, the meet of a pair of elements is unique. This follows from the fact that if we have two meets, then antisymmetry forces them to be equal.

Definition 3.16 (Subset of idempotents)**.** Let $(X, *)$ be an inverse semigroup. We define $\operatorname{Idems}(X)$ to be the subset of X consisting of all of its idempotents.

Theorem 3.17. *Let X be an inverse semigroup. Define on* $\operatorname{Idems}(X)$ *a relation $\leq$ by*

$$e \leq f \Leftrightarrow e = ef.$$

Then $\leq$ is a partial order on $\operatorname{Idems}(X)$*, which in particular, endows it with the structure of a meet semilattice.*

Proof. (Reflexivity): For any $e \in \operatorname{Idems}(X)$, we have $e = e^2$ so $e \leq e$.

(Antisymmetry): If $e \leq f$ and $f \leq e$ we have $e = ef$ and $f = fe$. Thus $e = ef = fe = f$.

(Transitivity): If $e \leq f$ and $f \leq g$, then $e = ef$, $f = fg$, so $e = ef = e(fg) = (ef)g = eg$. Thus $e \leq g$.

(Existence of meets): We claim $e \wedge f = ef$. First $ef = eef = efe = ef(e)$, so $ef \leq e$. As $ef = ef^2 = ef(f)$, we have $ef \leq f$. Now suppose some i satisfies $i \leq e$, $i \leq f$. So we have $i = ie$ and $i = if$. Then, $i(ef) = (ie)f = if = i$, so $i \leq ef$. So indeed $e \wedge f = ef$.

Thus, $\operatorname{Idems}(X)$ equipped with $\leq$ is a meet semilattice. □

Remark 3.18. If X is an inverse semigroup where every element is idempotent, then $X = \operatorname{Idems}(X)$ so by the construction of Theorem 3.17, we can turn X into a meet semilattice. Conversely, given a meet semilattice $(Y, \leq)$, it is a routine application of the definitions to verify that $(Y, \wedge)$ has the structure of an inverse semigroup where every element is idempotent. For the sake of the limited timeframe of the project, I did not formalize the reverse construction and will, as mathematicians love to say, "leave it as an exercise to the reader". However, the fact that it does work shows that the notions of "meet semilattice" and "inverse semigroup where every element is idempotent" are the same!

3.4 Homomorphisms

Whenever studying mathematical objects, we are not just interested in the set-theoretic structure, but also the maps between the objects that preserve the structure. We now define the notion of a homomorphisms of inverse semigroups and prove some properties of homomorphisms.

Definition 3.19 (Homomorphism)**.** Let $(X, *)$ and $(Y, \bullet)$ be two inverse semigroups. Then, a *homomorphism* from X to Y is a function of sets $\phi\colon X \to Y$ which satisfies, for all $x_1, x_2 \in X$,

$$\phi(x_1 * x_1) = \phi(x_1) \bullet \phi(x_2).$$

Proposition 3.20. *Let $\phi\colon X \to Y$ be a homomorphism. Then, the following hold.*

(a) ϕ preserves pseudoinverses in the sense that for every $x \in X$, $\phi(x^{-1}) = \phi(x)^{-1}$.

(b) ϕ preserves idempotents in the sense that for any idempotent $e \in X$, $\phi(e)$ is an idempotent in Y.

(c) ϕ preserves the order relation in the sense that if $x_1, x_2 \in X$ such that $x_1 \leq x_2$, then $\phi(x_1) \leq \phi(x_2)$.

Proof. (a) We have

$$\phi(x)\phi(x^{-1})\phi(x) = \phi(xx^{-1}x) = \phi(x),$$

and

$$\phi(x^{-1})\phi(x)\phi(x^{-1}) = \phi(x^{-1}xx^{-1}) = \phi(x^{-1}).$$

The result then follows from uniqueness of pseudoinverses.

(b) For any idempotent $e \in X$ we have $\phi(e)\phi(e) = \phi(e^2) = \phi(e)$, so that $\phi(e)$ is idempotent.

(c) If $x \leq y$ then $x = ye$ for some idempotent $e \in X$. Then, $\phi(x) = \phi(ye) = \phi(y)\phi(e)$, and $\phi(e)$ is idempotent by part (b). Hence $\phi(x) \leq \phi(y)$.

□

Proposition 3.21. *Let $\phi\colon X \to Y$ be a homomorphism. Then the following hold.*

(a) ϕ reflects idempotents in the sense that if $x \in X$ and $\phi(x)$ is idempotent in Y, then there is an idempotent $e \in X$ such that $\phi(e) = \phi(x)$.

(b) ϕ reflects the order relation in the sense that if $x_1, x_2 \in X$ such that $\phi(x_1) \leq \phi(x_2)$, then there exists $x_0 \in X$ such that $x_0 \leq x_2$ and $\phi(x_0) = \phi(x_1)$.

Proof. (a) Suppose $\phi(x)$ is idempotent. We claim the idempotent $e \in X$ satisfying the statement is xx^{-1}. Indeed, we have

$$\phi(xx^{-1}) = \phi(x)\phi(x^{-1}) = \phi(x)\phi(x)^{-1} = \phi(x)\phi(x) = \phi(x).$$

(b) Suppose $\phi(x_1) \leq \phi(x_2)$. Then, $\phi(x_1) = \phi(x_2)f$ for some idempotent $f \in Y$. Put $x_0 = x_2 x_1^{-1} x_1 = x_2(x_1^{-1}x_1)$; we have that $x_0 \leq x_2$. Now, we have that

$$\begin{aligned}\phi(x_0) &= \phi(x_2 x_1^{-1} x_1) = \phi(x_2)\phi(x_1^{-1}x_1) = \phi(x_2)\phi(x_1)^{-1}\phi(x_1) \\ &= \phi(x_2)[\phi(x_2)f]^{-1}[\phi(x_2)f] = \phi(x_2)f^{-1}\phi(x_2)^{-1}\phi(x_2)f \\ &= \phi(x_2)[f\phi(x_2^{-1}x_2)]f = \phi(x_2)[\phi(x_2^{-1}x_2)f]f \\ &= \phi(x_2 x_2^{-1} x_2)f^2 = \phi(x_2)f = \phi(x_1).\end{aligned}$$

□

Concluding remarks

This project has been an interesting experience. Formalizing mathematics really does force one to be very careful and thorough with one's definitions and proofs. There were a few times where some steps of a proof were omitted in the original material from Lawson's book and I filled in the details incorrectly at first — and only caught myself when trying to make the proof go through in Coq.

In a lecture given by J.P. Serre titled "How to write mathematics badly", (see [7]), Serre discusses several annoying things that mathematicians do when writing papers. I paraphrase from his talk some of these:

Theorem. *(blah blah blah)*

Proof. See [8] for details. □

... and then [8] is a six or seven hundred page book, with no further instructions on where the proof actually is. Another thing that people will do is:

Theorem. *(blah blah blah)*

Proof. It follows from Euler's theorem. □

... which one of Euler's dozens (if not hundreds) of theorems??? And the worst offender of all, which I have actually encountered myself when trying to read a paper by a researcher well-respected in his field:

Theorem. *(blah blah blah)*

Proof. □

Of course, when using a formal proof assistant, one cannot get away with these kinds of things. Certainly the amount of mathematical knowledge and the length of proofs have become so enormous that one cannot possibly reprove everything every time and expect to get anywhere, but if things are done in formal proof assistants then we can always trace every result back to a proof somewhere. As it stands now, there are many things "left to the reader" in papers that are incredibly difficult to find the proof of anywhere (if it exists at all), or poorly referenced as in the above examples — so how can we *really* be sure that they are actually correct?

Furthermore, the sheer amount of reading one needs to do to get to the frontiers of mathematical knowledge has reached a bewildering level. It is possible (presently I'm not sure how it works, but it can apparently be done with Gonthier's proof of the Feit-Thompson theorem) to simply press a button and see a tree of every definition, lemma, and result needed to prove a particular theorem. This way, one does not have to, for instance, read *all* of Serge Lang's *Algebra* to understand Feit-Thompson, but just the parts that are actually directly necessary for the proof.

Whether or not it will really be the norm to write mathematical papers in proof assistants, as Vladimir Voevodsky and the HoTT folks hope, is left to be seen. While Gonthier's SSReflect has formalized large parts of algebra, and the Univalent Foundations program has formalized large parts of topology and category theory, it will take time for the average working mathematician to embrace formalization (if they do at all). It does, after all, take an incredibly long time to write formal proofs - something I've come to appreciate after doing this project!

I had hoped initially to cover *all* of Chapter 1 of Lawson's book (40 pages long), but I underestimated the amount of work involved and ended up doing around 30% of it (the stuff I didn't get to: partial bijections on a set are a canonical example of inverse semigroups, applications to local structures in differential geometry/topology, more stuff on lattices, the Wagner-Preston representation theorem which says every inverse semigroup embeds faithfully into the set of partial bijections on its underlying set). I had also hoped to study the HoTT libraries, but they seemed a bit much to be able to get anywhere with in the timeframe of the project. I now see how Feit-Thompson took six years, and how people are able to do their entire PhD on the formalization of their master's thesis!

References

[1] Coq community user contributions. Groups. Available at: http://www.lix.polytechnique.fr/coq/pylons/coq/pylons/contribs/view/Groups/v8.4.

[2] Coq community user contributions. GroupTheory. Available at: http://www.lix.polytechnique.fr/coq/pylons/coq/pylons/contribs/view/GroupTheory/v8.4.

[3] The Coq development team. Coq reference manual. Available at: https://coq.inria.fr/distrib/current/refman/.

[4] H. Herbelin, F. Kirchner, B. Monate, and J. Narboux. Coq version 8.0 for the clueless. 2012. Available at: http://flint.cs.yale.edu/cs428/coq/doc/faq.html.

[5] Mark Lawson. *Inverse Semigroups: The Theory of Partial Symmetries*. World Scientific Pub Co Inc, Singapore, second edition, 1998.

[6] Univalent Foundations Program. *Homotopy Type Theory: Univalent Foundations of Mathematics*. Independently published, Princeton, first edition, 2013.

[7] J.P. Serre. How to write mathematics badly (lecture). Available at: https://www.youtube.com/watch?v=tJZpdXWm4Gg.