Are all substitutions invertible; are all monoids groups?

Murdoch J. Gabbay and Peter Kropholler

Thanks to Dan Ghica and Birmingham CS department

September 23, 2011

Describing the issue

Suppose you are a fresher at Birmingham Uni and you have some system and collection of operations on that system. For instance:

1. A typewriter with a sheet of paper in it. Your operations are ‘a’, ‘b’, . . . , ‘z’ and whitespace.
2. A bank account. Your operations are ‘withdraw money’.
3. A Rubiks cube. Your operations are various twists and turns.
4. A bottle of beer. Your operations are ‘drink beer’ and (for some of the rougher ones) ‘smash bottle’.

Q. Which of these systems is reversible? ε ɹǝqɯnN ·∀

Which of these systems would you like to be reversible?
∀. Numbers 1,2,3, and 4

Describing the issue

Reversibility is useful. That's why word-processors have an 'undo' function. Similarly for version control (subversion, CVS, git). In proof-search the difference between asynchronous and synchronous proof-rules is important:

Asynchronous $\dfrac{\Gamma, A \wedge B \vdash C}{\Gamma, A, B \vdash C}\,(\wedge\mathbf{L})$ *Synchronous* $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\vee\mathbf{R})$

($\wedge\mathbf{L}$) just rearranges connectives; ($\vee\mathbf{R}$) irreversibly eliminates B.

Reversible computation has physical importance for heat-dissipation. Quantum computation is reversible (until you take a measurement). The laws of physics are time-reversible.

Reversibility is real, useful, and important.

Monoids and groups

Consider the following axioms:

(**assoc**)	$x \circ (x' \circ x'') = (x \circ x') \circ x''$
(**id**)	$\mathrm{id} \circ x = x \circ \mathrm{id} = x$
(**inv**)	$x \circ x^{-1} = x^{-1} \circ x = \mathrm{id}$

- A group G is a tuple $(|G|, \circ, \mathrm{id}, ^{-1})$ of a carrier set $|G|$, a composition $\circ$ mapping $|G| \times |G|$ to $|G|$, an element $\mathrm{id} \in |G|$, and an inverse map $^{-1}$ mapping $|G|$ to $|G|$, satisfying (**assoc**), (**id**), and (**inv**).
- A monoid M is a tuple $(|M|, \circ, \mathrm{id})$ as above, satisfying (**assoc**) and (**id**).

Groups and monoids are an abstract mathematical representation of reversible/irreversible operations on some system.

Not every monoid can be homomorphically injected into a group

Consider the two-element monoid $\{0, 1\}$ with

$$1 \circ 0 = 0 \quad 1 \circ 1 = 1 \quad 0 \circ 0 = 0 \quad 0 \circ 1 = 0$$

Try to adjoin an inverse 0^{-1}.

$0 = 0 \circ 0$ and so (applying 0^{-1} to both sides) $0 = 1$.

We lose injectivity; if $M = \{0, 1\}$ then its 'natural' corresponding group is trivial.

It can't be done

It's impossible. You can't inject a monoid into a group.

But impossibility shouldn't stop us; it can only slow us down a little. You just have to re-frame the question a little.

It only took me two years to see how. One-and-a-half years to understand the question. Six months to find the proof.

So let's try something else

A (compatible) order on a monoid M is a partial order $\leq \subseteq |\mathrm{M}| \times |\mathrm{M}|$ such that $x \leq y$ implies $x \circ z \leq y \circ z$ and $z \circ x \leq z \circ y$.

- A partially ordered monoid is a pair $(\mathrm{M}, \leq)$ of a monoid M and a compatible order on M.
- A partially ordered group is a pair $(\mathrm{G}, \leq)$ of a group G and a compatible order on G, considered as a monoid.

We are most interested in the case that $\leq_{\mathrm{M}}$ is trivial (so $m \leq_{\mathrm{M}} m'$ implies $m = m'$). The reason we care about partial orders will become clear; for the proofs, it is easier to consider the general case.

Lax homomorphisms

Call $f : (\mathrm{M}, \leq) \to (\mathrm{M}', \leq)$ a lax homomorphism when:

- $\mathrm{id}_{\mathrm{M}'} \leq_{\mathrm{M}'} f(\mathrm{id}_{\mathrm{M}})$.
- $f(x \circ_{\mathrm{M}} y) \leq_{\mathrm{M}'} f(x) \circ_{\mathrm{M}'} f(y)$ (laxness).
- $x \leq_{\mathrm{M}} y$ implies $f(x) \leq_{\mathrm{M}'} f(y)$ (monotonicity).

If $f(x \circ_{\mathrm{M}} y) = f(x) \circ_{\mathrm{M}'} f(y)$ then f is a homomorphism.

Lax homomorphisms seem to be new. The idea comes from lax functors in category theory.

What does a lax homomorphism mean?

Think of $\leq$ as some notion of computation or reduction.

$f(x \circ y) \leq f(x) \circ f(y)$ means that $f(x) \circ f(y)$ evaluates, reduces, rewrites, or computes to $f(x \circ y)$.

For example:

- $H_2O \leq H_2 + O$. The 'computation' is the chemical reaction.
- $2 + 3 \to 5$. Here $\leq$ is $\leftarrow$ and represents rewriting.
- Traditional married couple $\leq$ Man + Woman. I leave the 'computation' involved to your imagination.

Note that these are not necessarily reversible. $x \leq y$ does not imply $y \leq x$.

So a lax homomorphism from M to M′ is a notion of "map M to M′, but M′ may have a more fine-grained notion of computation".

The (free) group for a monoid

For X a set write $X^{\pm}$*string* for the inductive set

$$s ::= () \mid s{+}x \mid s{-}x$$

() is empty string, concatenation is $s{\cdot}t$. We may elide $\cdot$ and ().

E.g. $\mathbb{N}_{+}^{\pm}$*string* is the set of lists of nonzero integers.

Given a partially ordered monoid $(\mathrm{M}, \leq_{\mathrm{M}})$ define $\leq$ a relation on $|\mathrm{M}|^{\pm}$*string* by:

1. (**Group**) $()+m-m \leq () \leq ()-m+m$ (standard).
2. (**Cong**) If $s \leq s'$ and $t \leq t'$ then $s{\cdot}t \leq s'{\cdot}t'$ (standard).
3. (**Lax**) $+(m \circ_{\mathrm{M}} +m') \leq +m+m'$ (non-standard).

If we quotient $\mathrm{M}^{\pm}$*string* by the greatest equivalence relation in $\leq$—we'll see what that is in a moment—then we get a partially ordered group $(\mathrm{M}^{\pm}, \leq_{\mathrm{M}^{\pm}})$.

That's our candidate reversible version of M!

Examples (without proof)

Suppose M is the monoid of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ under addition (so 0 is the identity). Then $\mathsf{M}^{\pm}$ is not isomorphic to the integers. For instance, $+3+4 \in |\mathsf{M}^{\pm}|$ is not equal to $+7$, though $+7 \leq_{\mathsf{M}^{\pm}} +3+4$. Proof later.

Suppose M is the one-element monoid with underlying set $\{*\}$ and monoid composition $* \circ * = *$. Then $\mathsf{M}^{\pm}$ is isomorphic to the integers under addition: the unit is (); the number 1 corresponds to $+*$; the number 2 corresponds to $+*+*$; the number -1 corresponds to $-*$, and so on.

So $\mathsf{M}^{\pm}$ is resource sensitive. Note, however, that resources can be destroyed if we interpret $\geq$ as 'entailment'; $+*+* \geq +*$. In logical terminology, we have contraction on the right but not on the left.

Time for a theorem: M injects into $\mathrm{M}^{\pm}$

You see, we built $\leq$ on $\mathrm{M}^{\pm}\mathit{string}$ using some rules. There is no guarantee that we do not accidentally overgenerate and make e.g. $s \leq t$ for every s and t, so that $\mathrm{M}^{\pm}$ (which is $\mathrm{M}^{\pm}\mathit{string}$ quotiented by the reflexive kernel of $\leq$) is the trivial group.

This happened to us before—recall the example of adding inverses to $\{0, 1\}$.

This time, we got it right:

Theorem 1. $+n \leq_{\mathrm{M}^{\pm}} +m$ if and only if $n \leq_{\mathrm{M}} m$.

Theorem 2. $+n \leq_{\mathrm{M}^{\pm}} +m_1 + m_2$ if and only if $n \leq_{\mathrm{M}} m_1 \circ_{\mathrm{M}} m_2$.

Intuitive corollary. The monoid M lives laxly inside the group $\mathrm{M}^{\pm}$.

How does the proof work?

In the rest of this talk, I want to give just a sketch of the key ideas behind proving Theorems 1 and 2.

Definition 0. Suppose $m \in |\mathrm{M}| \setminus \{\mathrm{id}_{\mathrm{M}}\}$. Define index functions $i(s)_m$ and $i(s)$ on $|\mathrm{M}|^{\pm}$*string* as follows:

$$i(())_m = 0$$

$$i(s{+}m')_m = i(s)_m \quad (m' \neq m) \qquad i(s{-}m')_m = i(s)_m \quad (m' \neq m)$$

$$i(s{+}m)_m = i(s)_m{+}1 \qquad i(s{-}m)_m = i(s)_m{-}1$$

$$i(s) = \Sigma_{m \in |\mathrm{M}|} i(s)_m$$

$i(s)_p$ 'counts' m in s. $i(s)$ counts all m and takes the sum.

Three technical lemmas

Lemma 1. If $() \leq_{\mathrm{M}^{\pm}} p$ and $i(p) = 0$ then every proof that $() \leq_{\mathrm{M}^{\pm}} p$, does not mention (**Lax**).

Corollary 2. If $() \leq_{\mathrm{M}^{\pm}} p$ and $i(p)_m = 0$ for all m, then $p = ()$.

Lemma 3.

1. If $() \leq_{\mathrm{M}^{\pm}} p$ then $i(p) \geq 0$.
2. If $p \leq_{\mathrm{M}^{\pm}} q$ then $i(p) \leq i(q)$.

Example application of the three technical lemmas

Corollary 4. Take M to be the monoid of natural numbers $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ under addition (so 0 is the identity). Then $+3{+}4 \in |\mathrm{M}^{\pm}|$ is not equal to $+7$.

Proof. $i(+3{+}4) = 2$ and $i(+7) = 1$. We note that $1 \neq 2$ and we use Lemma 3.

The key technical result

Proposition 5. Suppose $p \in |\mathrm{M}^{\pm}|$ and $i(p) = 0$. Suppose $i(p)_m > 0$. Then there exists some $\leq_{\mathrm{M}}$-least $n \leq_{\mathrm{M}} m$ such that $i(p)_n < 0$.

Proposition 5 might seem formidable, but it is common sense:

Suppose the index of p is 0, so that for every $+m$ in p there is a corresponding $-n$. Suppose there are more $+m$s in p than $-m$s, so that there is a surfeit of ms in p and $i(p)_m > 0$. For balance, there must be n such that $i(p)_n < 0$—that is, there is a deficit of ns—and since p is a finite structure we can find an $\leq$ least such n in the partial order on M.

Proof of Theorem 1

Theorem 1. $+n \leq_{\mathrm{M}^{\pm}} +m$ if and only if $n \leq_{\mathrm{M}} m$.

Proof. The right-to-left implication is by construction.

For the left-to-right implication we reason as follows: If $m = n$ then $n \leq_{\mathrm{M}} m$ is a fact, so suppose $m \neq n$ and $+n \leq_{\mathrm{M}^{\pm}} +m$.

We note that $i(+m{-}n) = 0$ and $i(+m{-}n)_m > 0$. Using Proposition 5 it follows that $n \leq_{\mathrm{M}} m$.

Significance of these results

I have exhibited part of an adjunction between two categories: the category of partially ordered monoids and lax homs, and the category of partially ordered groups and homs.

Yes. The groups have homomorphisms (not lax). Only the monoids need lax homs.

The functor of interest is left adjoint to the forgetful functor that forgets inverses to obtain a monoid from a group.
imag : PoMonX $\rightarrow$ PoGrp is left adjoint to
forg : PoGrp $\rightarrow$ PoMonX. In symbols:

$$\text{imag} \dashv \text{forg} : \text{PoGrp} \rightarrow \text{PoMonX}$$

Significance of these results

Our main results express intuitively that the unit of the adjunction, mapping M to $\mathrm{M}^{\pm}$ considered forgetfully as a monoid, is injective.

The index function $i(p)$ corresponds via the adjunction to the function mapping $m \in |\mathrm{M}|$ to 1. (Note that the components $i(p)_m$ are not monotone.)

Speculative examples

Substitution forms a monoid, so we can form a corresponding group. I believe that from this we obtain a notion of unification with σ, and generalises nominal unification, in which problems have most general solutions (not decidable). Connection to higher-order unification.

Boolean algebra forms a monoid under conjunction. We obtain a new kind of algebra with antiformulae. Cf. database theory and substructural logics.

Rewrites on strings form a partially ordered monoid. We obtain an extended rewrite system in which every token has an inverse.

Models of the λ-calculus form an applicative structure under application (not a monoid, because not associative). I believe that these results are robust—we never really use associativity in the proofs. One could build a new non-associative structure with e.g. left inverses to all functions. . . . more. . .

Mathematical implications

Perhaps partially ordered monoids and lax homomorphisms are an interesting thing to start proving theorems about.

In a somewhat unexpected sense, these seem to be a computational analogue to groups.

Thank you.