Exercise Sheet 2

Please send me your solutions in English or French by email by December 9, 2024, including executable Isabelle files.

Exercises 2.1–2.3 and parts of Exercise 2.5 and 2.6 require Isabelle. Please provide detailed human-readable Isar proofs if suitable, as you would normally write them on paper. Some other exercises are not too hard with Isabelle either (I indicate which ones), but Isabelle proofs are optional. Of course, Isabelle may still help checking your reasoning.

To find Isabelle/HOL's theory for natural numbers with the relevant syntax and functions you can, for instance, type a simple expression using a natural number type into Isabelle (e.g. asking for the value of $5 :: nat$), press command, hover over nat and click. Likewise, you can access the Isabelle/HOL theory for functional lists asking e.g for the value of $[a] :: 'a\ list$.

Question 2.1 In Isabelle's theory for natural numbers, using in particular its type class *nat* and its addition and multiplication functions, (re)prove that multiplication is associative, commutative and has a unit.

Question 2.2 The *list_map* function discussed in class is called *map* in Isabelle's list theory. Using this theory, give step-by-step Isar proofs showing that

(i) $map\ f\ (xs \cdot ys) = (map\ f\ xs) \cdot (map\ f\ ys)$ (where here I write $\cdot$ for list concatenation),

(ii) $map\ (f \circ g) = (map\ f) \circ (map\ g)$,

(iii) $map\ id = id$.

Question 2.3 Use Isabelle to check that $\mathcal{P}X^*$, the powerset of the free monoid X^* on the set X, forms a Kleene algebra. You can proceed by a series of instantiation proofs:

(i) The first shows that Isabelle's functional lists (polymorphic and without a carrier set) form multiplicative monoids with respect to list concatenation/append and the empty list, using Isabelle's *monoid_mult* type class.

(ii) The second shows that for each multiplicative monoid M (again without carrier sets), $\mathcal{P}M$ forms a multiplicative monoid. The instantiation proof that powersets form semilattices in the file *My_Algebras.thy* yields a template for this proof.

(iii) The third shows, incrementally to the second, that $\mathcal{P}M$ forms a dioid, using the dioid type class in *My_Algebras.thy*.

(iv) The fourth shows, incrementally to the third, that $\mathcal{P}M$ forms a Kleene algebra, using the Kleene algebra type class in *My_Algebras.thy*. Some auxiliary lemmas may be helpful for this proof. You can instruct Isabelle to use such lemmas in apply-style proof steps by adding them to the simplifier in a proof writing *simp_add*: $\langle name{-}of{-}lemma \rangle$ or *unfolding* $\langle name{-}of{-}lemma \rangle$. You can also suggest to Isabelle to use a particular lemma writing *using* with the name of the lemma before calling *auto*, *blast*, *force* etc or Sledghammer. The file *My_Algebras.thy*, in particular he interpretation proof that relations form Kleene algebras, shows several examples for this.

(v) Finally, try a simple Isabelle proof on $P\Sigma^*$ to test that Isabelle now "understands" that $\mathcal{P}\Sigma^*$ forms indeed a Kleene algebra.

Alternatively, you can give interpretation proofs instead of instantiation proofs, using the examples in *My_Algebras.thy* as a template. The Isabelle documentation on type classes and locales gives further guidance.

Question 2.4 Let $(P, \leq, \bot)$ be a poset with least element $\bot$ in which each pair of elements has a sup $\sqcup$, that is, for all $x, y, z \in P$,

$$x \sqcup y \leq z \Leftrightarrow x \leq z \wedge y \leq z.$$

Show that the algebraic laws for semilattices are derivable: for all $x, y, z \in P$,

$$x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z, \qquad x \sqcup y = y \sqcup x, \qquad x \sqcup x = x, \qquad x \sqcup \bot = x.$$

If you want to use Isabelle to derive these identities, start with extending Isabelle's type class for partial orders to one for semilattices-as-orders.

Question 2.5 A *modal semiring* is a dioid (an additively idempotent semiring) $(S, +, \cdot, 0, 1)$ with domain and codomain operations $dom, cod : S \to S$ that satisfy, for all $x, y, z \in S$,

$$\begin{gathered} dom(x) \cdot x = x, \qquad dom(x \cdot dom(y)) = dom(x \cdot y), \qquad dom(x) \leq 1, \\ dom(0) = 0, \qquad dom(x + y) = dom(x) + dom(y), \\ x \cdot cod(x) = x, \qquad cod(cod(x) \cdot y) = cod(x \cdot y), \qquad cod(x) \leq 1, \\ cod(0) = 0, \qquad cod(x + y) = cod(x) + cod(y), \\ cod(dom(x)) = dom(x), \qquad dom(cod(x)) = cod(x). \end{gathered}$$

Hence the domain and codomain axioms are the same as for modal quantales discussed in class, up-to notation. Show that

(i) $dom(dom(x)) = dom(x)$ and $cod(cod(x)) = cod(x)$;

(ii) $x \in dom(S)$ (the image of S under dom) if and only if x is a fixpoint of dom;

(iii) the set S_d of fixpoints of dom equals the set of fixpoints of cod;

(iv) S_d forms a distributive lattice with least element 0 and greatest element 1 in which $\cdot$ coincides with binary inf;

(v) there are domain semirings in which the set of all subidentities (elements below 1) strictly includes S_d. Define a type class for modal semirings extending the dioid class from *My_Algebras.thy* and refute a suitable statement using Nitpick.

The first three parts of this exercise are easy with Isabelle as well, if you want to try. Part four is harder, but you can still easily check individual properties (individual closure conditions etc) leading to this fact with Isabelle without fully formalising it (this would probably require a subtype and other heavy machinery).

Question 2.6 Recall that a Kleene algebra is a dioid $(K, +, \cdot, 0, 1)$ with a star operation $(-)^* : K \to K$ such that, for all $x, y, z \in K$,

$$1 + x \cdot x^* \leq x^*, \qquad z + x \cdot y \leq y \Rightarrow x^* \cdot z \leq y, \qquad 1 + x^* \cdot x \leq x^*, \qquad z + y \cdot x \leq y \Rightarrow z \cdot x^* \leq y.$$

Using relevant properties from *My_Algebras.thy*, show (on paper or using Isabelle), that

(i) $x^{**} = x^*$,

(ii) $(x \cdot y)^* \cdot x = x \cdot (y \cdot x)^*$,

(iii) $(x + y)^* = x^* \cdot (y \cdot x^*)^*$.

(iv) Refute the generalised confluence property $x^* \cdot y^* \leq y^* \cdot x^*$ using Nitpick; show the multiplication tables.

Show detailed Isar proof if you choose to use Isabelle.

Question 2.7 Recall that a *catoid* is a structure $(C, \odot, s, t)$ consisting of a set C, a multioperation $\odot : C \times C \to \mathcal{P}C$ and source and target maps $s, t : C \to C$ such that, for all $x, y, z \in C$,

$$\bigcup_{v \in x \odot z} x \odot v = \bigcup_{u \in x \odot y} u \odot z, \qquad x \odot y \neq \emptyset \Rightarrow t(x) = s(y), \qquad s(x) \odot x = \{x\}, \qquad x \odot t(x) = \{x\}.$$

Show that, for all $x, y \in C$,

(i) $s \circ s = s$, $t \circ t = t$, $s \circ t = t$ and $t \circ s = s$,

(ii) $s(x) = x$ if and only if $t(x) = x$,

(iii) $s(x) \odot s(x) = \{s(x)\}$ and $t(x) \odot t(x) = \{t(x)\}$,

(iv) $s(x) \odot t(y) = t(x) \odot s(y)$,

(v) $s(s(x) \odot y) = s(x) \odot s(y)$ and $t(x \odot t(y)) = t(x) \odot t(y)$,

(vi) $s(x \odot y) \subseteq s(x \odot s(y))$ and $t(x \odot y) \subseteq t(t(x) \odot y)$,

(vii) $s(x \odot y) = \{s(x)\}$ and $t(x \odot y) = \{t(y)\}$ whenever $x \odot y \neq \emptyset$.

Note that images of domain and codomain maps are taken tacitly in some statements. If a statement is the opposite of another, in the sense that the arguments of $\odot$ are swapped and s and t exchanged, then it suffices to write "proof by opposition". Once again, it is not very hard to do Isar proofs, starting from a type class for catoids.

Question 2.8 Suppose you have constructed a modal powerset quantale $\mathcal{P}C$ on a catoid C, with $X * Y = \bigcup\{x \odot y \mid x \in X, y \in Y\}$ for all $X, Y \subseteq C$, with *dom* the image of s, *cod* the image of t and with monoidal identity C_0 (the set of all fixpoints of s/t). Show that the singleton sets in $\mathcal{P}C$ give rise to a catoid on the set C, defining

$$x \in y \odot z \Leftrightarrow \{x\} \subseteq \{y\} * \{z\}.$$

Question 2.9 The *shuffle operation* $\| : X^* \times X^* \to \mathcal{P}X^*$ on the free monoid X^* on the set X is the multioperation defined, for all letters $a, b \in X$, words $v, w \in X^*$ and empty word ε, as

$$v \| \varepsilon = \{v\} = \varepsilon \| v, \qquad (a \cdot v) \| (b \cdot w) = \{a\} \cdot (v \| (b \cdot w)) \cup \{b\} \cdot ((a \cdot v) \| w),$$

where the complex product $\cdot : \mathcal{P}X^* \times \mathcal{P}X^* \to \mathcal{P}X^*$ is tacitly used in the right-hand side of the second equation. Show that $(X^*, \|, s, t)$ forms a catoid. What are the source and target maps? Extend the shuffle operation to sets and use it in the proof if helpful.

If you are planning to formalise this example with Isabelle, note that the simple induction proofs we saw in class might not suffice. You can check the induction heuristics section of the Isabelle document *Programming and Proving in Isabelle/HOL* for more advanced uses of induction.

The shuffle operation allows interleaving concurrent processes in computing systems, where actions of concurrent processes are scheduled sequentially in time.

Question 2.10 We have defined functors as homomorphisms of single-set categories in class (see also Chapter XII of Mac Lane's book). How would you define natural transformations?