Quotients in Simple Type Theory

Bart Jacobs[1]

June 1994

We introduce a syntax for quotient types in a predicate logic over a simply type theory. To illustrate its usefulness we construct in purely type theoretic terms (a) the free abelian group on a commutative monoid H, as quotient of $H \times H$; a special instance is the construction of $\mathbb{Z}$ from $\mathbb{N}$; (b) the quotient poset of a preorder, (c) the abelian quotient of an arbitrary group, and (d) tensor products and sums of abelian groups.

The syntax we use comes from a categorical analysis, in which quotients are described as certain adjunctions. This gives us introduction and elimination rules as transposes, and the associated (β)- and (η)-conversions. A brief discussion of this matter is included.

1 Introduction

Quotients are used throughout mathematics for constructing new objects from old, by collapsing part of the structure, see for example any textbook on algebra or topology. Here we give a completely general description of such quotients in a type theoretic language. We assume a simple type theory, together with a predicate logic to reason about types and terms. Then quotients can be described as a left adjoint to a certain equality-predicate functor. This gives us all the rules we need: formation, introduction, elimination and (β)- and (η)-conversions for quotients. These will be described in the next section below. Subsequently, the new syntax is put to use in constructing $\mathbb{Z}$ from $\mathbb{N}$, a poset from a preorder, the abelianization of a group, and tensor products $\otimes$ and sums $\oplus$ of abelian groups. All these constructions involve taking a suitable quotient. They will be described in purely type theoretic terms. The syntax for quotients turns out to be rather close to the ordinary mathematical vernacular. In the final section 4 we briefly describe (for cognoscienti) the categorical considerations underlying the syntax that we put forward here.

We like to emphasize the fundamental role played by adjunctions in logic. The most important occurrences are:

$$\begin{array}{rcl}
\exists & \dashv & \text{weakening} \\
\text{weakening} & \dashv & \forall \\
\text{equality} & \dashv & \text{contraction} \\
\text{truth} & \dashv & \text{separation (subsets)} \\
\text{quotients} & \dashv & \text{equality.}
\end{array}$$

Here we concentrate on the latter one. The formalization of quotients that we achieve may be of use in the verification of pieces of mathematics or software on a computer. Also it may be useful for reasoning directly in some mathematical structure, using type theory as internal language.

[1] Written while at Mathematical Institute, University of Utrecht. Current address: CWI, Kruislaan 413, 1098 SJ Amsterdam. `bjacobs@cwi.nl`

There are other investigations of quotient types in type theory, for example in NUPRL [1], and in the forthcoming thesis of Hofmann (see [3] for some information). But these deal with quotients in *dependent* type theory, which are much more difficult for the following reasons.

- The description of quotient types involves equality. Categorically this is very clear via the adjunction mentioned above. Equality types in dependent type theory however, are not well-understood, because there are many versions around. This complicates the description of quotients. Below we use quotient types in a predicate logic over simple type theory. And in such a (standard) predicate logic, equality is well-understood.

- In dependent type theory one does not distinguish between propositions and types. This is confusing, and complicates matters. In contrast, in the logic that we use, there are separate syntactic categories for propositions and for types. This enables us to use propositions without proof-terms. As a result, types cannot depend on propositions. In particular, the equality proposition that needs to hold in the elimination rule for quotients (see below) does not involve a proof-term. And hence, also the resulting elimination term does not dependend on a proof-term. This enables us to use quotients like in ordinary mathematics.

  In contrast, in dependent type theory one gets a quotient elimination term depending on a proof. But the outcome should be independent of which proof one has. This is like the problem in dependent type theory where one needs a proof p of the propositions $x \geq 0$ in $\mathbb{R}$ before one can form the square root $\sqrt{x}$; but the outcome of $\sqrt{x}$ should not depend on which particular proof p one uses. In the present set-up, such problems don't exist.

Finally we should emphasize that it is our intention to present a syntax for quotients in simple type theory, based on a categorical axiomatization of quotients, and show its usefulness by presenting some examples. We totally ignore the proof-theoretic aspects, like confluence or normalization, of adding this feature.

2 Syntax for quotients

We will be working in a many-typed predicate logic. Types will be written as $\sigma, \tau, \rho, \ldots \colon \mathsf{Type}$. They are built up from certain constants, products $\times$, function space $\rightarrow$, and possibly also coproducts $+$. Type contexts $\Gamma = x_1\colon \sigma_1, \ldots, x_n\colon \sigma_n$ are sequences of (term) variable declarations. There is a usual calculus of terms $\Gamma \vdash M\colon \tau$, with λ-abstraction $\lambda x\colon \sigma.\, M$, application PQ, tupling $\langle M, N\rangle$ and projections $\pi P, \pi' P$. We will use these with the (η)-rules.

On top of this (simple) type theory, there is a logic. It has propositions $\varphi(\vec{x})\colon \mathsf{Prop}$, containing term variables $\vec{x}$. A bit formally these propositions will be written as

$$x_1\colon \sigma_1, \ldots, x_n\colon \sigma_n \vdash \varphi\colon \mathsf{Prop}$$

Like type theoretic assumptions $x_i\colon \sigma_i$ may be put in a type context Γ, also logical assumptions may be put in a proposition context $\Theta = \varphi_1, \ldots, \varphi_m$. Then one can have entailments like

$$\varphi_1, \ldots, \varphi_m \vdash \psi$$

expressing that ψ follows from $\varphi_1, \ldots, \varphi_m$. Often it is better, but a bit more cumbersome, to have such entailments with all the term variable declarations explicit, like in

$$x_1 \colon \sigma_1, \ldots, x_n \colon \sigma_n \mid \varphi_1, \ldots, \varphi_m \vdash \psi \qquad \text{or simply} \qquad \Gamma \mid \Theta \vdash \psi$$

where $\mid$ is a symbol that separates contexts. It has no logical meaning; it is like $\mid$ in $\{x \in X \mid \varphi(x)\}$ where it separates the set-theoretic, from the logical part.

The logic that we use will have the familiar propositional connetives $\wedge$, $\top$, $\vee$, $\bot$ and $\supset$; the latter for implication. Sometimes we write $\varphi \supset\subset \psi$ for $(\varphi \supset \psi) \wedge (\psi \supset \varphi)$. Also there are univeral and existential quantifiers $\forall x \colon \sigma.\, \varphi$ and $\exists x \colon \sigma.\, \varphi$ with the standard rules. Additionally there will be an equality predicate $=_\sigma$ for each type σ, with formation rule,

$$\frac{\Gamma \vdash M \colon \sigma \qquad \Gamma \vdash M' \colon \sigma}{\Gamma \vdash M =_\sigma M' \colon \mathsf{Prop}}$$

These equality predicates are required to be reflexive, symmetric and transitive; to contain conversion:

$$\frac{\Gamma \vdash M \colon \sigma \qquad \Gamma \vdash M' \colon \sigma \qquad M = M'}{\Gamma \mid \emptyset \vdash M =_\sigma M'}$$

and further to be substitutive: if $M =_\sigma M'$ and $N(x) =_\tau N'(x)$ for $x \colon \sigma$, then $N[M/x] =_\tau N'[M'/x]$. For convenience, we sometimes omit the subscript σ in $=_\sigma$. But it is important to be aware of the difference between 'internal' or 'propositional' equality $=_\sigma$ and 'external' equality (i.e. conversion).

What we have described is first order predicate logic. It may be extended to higher order by requiring that Prop is a type, i.e. $\vdash \mathsf{Prop} \colon \mathsf{Type}$. Then one can quantify over propositions and over predicates, like in

$$\forall \alpha \colon \mathsf{Prop}.\, \alpha \supset \alpha \qquad \text{or} \qquad \exists p \colon \sigma \to \mathsf{Prop}.\, \forall x \colon \sigma.\, px \supset \bot.$$

In three of our examples in Section 3 we will use higher order predicate logic. In higher order logic, the equality predicate $=_\sigma$ may be defined as Leibniz equality:

$$x \colon \sigma, y \colon \sigma \vdash (x =_\sigma y) \overset{\text{def}}{=} \forall p \colon \sigma \to \mathsf{Prop}.\, px \supset py \colon \mathsf{Prop}.$$

Finally, we sometimes write $M \colon \sigma \to \tau$ if we mean that $M = M(x)$ is a term $x \colon \sigma \vdash M(x) \colon \tau$. The arrow notation is justified here, since one can form a category of types and terms in this way, see Example 4.3 (iv). Along the same lines, $\sigma \cong \tau$ means that there is an invertible term $\sigma \to \tau$.

We come to the syntax of quotient types.

Formation

$$\frac{x \colon \sigma, y \colon \sigma \vdash R(x, y) \colon \mathsf{Prop}}{\vdash \sigma/R \colon \mathsf{Type}}$$

Thus, given a type σ with a (binary) relation R on σ, we can form the quotient type σ/R. Notice that we don't require that R is an equivalence relation. Set theoretically, one can think of σ/R as the quotient by the equivalence relation generated by R. This is made precise in Remark 3.2 (iv) below.

Introduction

$$\frac{\Gamma \vdash M\colon \sigma}{\Gamma \vdash [M]_R\colon \sigma/R} \qquad \text{with} \qquad \frac{\Gamma \vdash M\colon \sigma \qquad\qquad \Gamma \vdash M'\colon \sigma}{\Gamma \mid R(M, M') \vdash [M]_R =_{\sigma/R} [M']_R}$$

This yields the equivalence class $[M]_R$ associated with an inhabitant M of σ. Often we write $[M]$ for $[M]_R$ if the relation R is understood. The associated equality rule tells that if terms are related by R, then their classes are equal. We thus get the "canonical" map $[\bot]_R\colon \sigma \to \sigma/R$.

Elimination

$$\frac{\Gamma, x\colon \sigma \vdash N\colon \tau \qquad \Gamma, x\colon \sigma, y\colon \sigma \mid R(x,y) \vdash N(x) =_\tau N(y)}{\Gamma, a\colon \sigma/R \vdash \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N(x) : \tau}$$

The intuition is as follows: by assumption, $N(x)$ is constant on equivalence classes of R. Hence we may define a new term $\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N(x)$ which, given a class $a\colon \sigma/R$, picks a representant x from the class a, and uses it in $N(x)$. The outcome does not depend on which x we pick. Notice that the variable x thus becomes bound in the elimination term $\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N(x)$. By α-conversion, this term is then the same as $\mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ N(y)$.

The associated conversions are

$$\begin{array}{lrcl} (\beta) & \mathsf{pick}\ x\ \mathsf{from}\ [M]_R\ \mathsf{in}\ N & = & N[M/x] \\ (\eta) & \mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ N[\,[x]_R/a] & = & N[Q/a]. \end{array}$$

In the (η)-conversion it is assumed—as usual—that the variable x does not occur free in N. In the calculations below, (η) turns out to be very useful, especially in 'expansion' form: from right to left.

For completeness we should still mention the behaviour of the new terms under substitution:

$$\begin{array}{rcl} [\,M\,]_R[P/z] & \equiv & [\,M[P/z]\,]_R \\ (\mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ N)[P/z] & \equiv & \mathsf{pick}\ x\ \mathsf{from}\ Q[P/z]\ \mathsf{in}\ N[P/z] \end{array}$$

The latter if x does not occur free in P. And also the compatibility rules:

$$\frac{\Gamma \mid \Theta \vdash M =_\sigma M'}{\Gamma \mid \Theta \vdash [M]_R =_{\sigma/R} [M']_R}$$

$$\frac{\Gamma, x\colon \sigma \mid \Theta \vdash N =_\tau N'}{\Gamma, a\colon \sigma/R \mid \Theta \vdash (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N) =_\tau (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N')}\ (x \text{ not free in } \Theta)$$

where in the latter case it is implicitly understood that both N and N' are constant on equivalence classes.

In the special case where the relation R that we started from is an equivalence relation (provable in the logic), then we say that σ/R is an **effective quotient** if one also has the rule

$$\frac{\Gamma \vdash M\colon \sigma \qquad\qquad \Gamma \vdash M'\colon \sigma}{\Gamma \mid [M]_R =_{\sigma/R} [M']_R \vdash R(M, M')}$$

Thus effectiveness says that inhabitants of σ forming the same classes must be related by R.

2.1. Remark. In the above description of quotients we have restricted the relation $R = R(x, y)$ on σ in such a way that it contains only the variables $x, y\colon \sigma$. If we drop this restriction, we get a formation rule

$$\frac{\Gamma, x\colon \sigma, y\colon \sigma \vdash R(x, y)\colon \mathsf{Prop}}{\Gamma \vdash \sigma/R\colon \mathsf{Type}}$$

involving a context Γ of term variables. This leads to *type dependency*: the newly formed quotient type σ/R may contain term variables z in R declared in Γ. A typical example is the group $\mathbb{Z}_n$ of integers modulo n, obtained as quotient type $\mathbb{Z}/n\mathbb{Z}$, for $n\colon \mathbb{N}$. This leads in an obvious way to what one can call "dependent predicate logic". It is a predicate logic over a dependent type theory, as described for example in [7] and [4]. Although we think this to be a very natural (and expressive) logic, we don't wish to complicate matters unnecessarily at this stage. Therefore we have restricted the formation rules for quotients, so that we stay within simple type theory.

By the way, the same thing happens with separation (or subtypes) in the formation rule:

$$\frac{\Gamma, x\colon \sigma \vdash \varphi\colon \mathsf{Prop}}{\Gamma \vdash \{x\colon \sigma \mid \varphi\}\colon \mathsf{Type}}$$

like in the example $p\colon \mathbb{N} \vdash \{n\colon \mathbb{N} \mid \ltimes < \imath\}\colon \mathsf{Type}$. There are some formal similarities between quotients and subtypes: in the first case one collapses $\sigma \twoheadrightarrow \sigma/R$ and in the second case one takes a subpart $\{x\colon \sigma \mid \varphi\} \rightarrowtail \sigma$.

The presence of quotient types has some consequences for equality in the logic. The following observation is due to Martin Hofmann.

2.2. Lemma. *In the presence of quotient types (and (η) for $\rightarrow$), propositional equality on functions is extensional: one has*

$$f\colon \sigma \rightarrow \tau, g\colon \sigma \rightarrow \tau \mid \forall x\colon \sigma.\, fx =_\tau gx \vdash f =_{\sigma\rightarrow\tau} g.$$

Proof. Consider the following relation on the arrow type $\sigma \rightarrow \tau$,

$$f\colon \sigma \rightarrow \tau, g\colon \sigma \rightarrow \tau \vdash f \sim g \stackrel{\text{def}}{=} \forall x\colon \sigma.\, fx =_\tau gx : \mathsf{Prop}.$$

and form the associated quotient type $\sigma \Rightarrow \tau \stackrel{\text{def}}{=} (\sigma \rightarrow \tau)/{\sim}$, with canonical map $[\perp]\colon (\sigma \rightarrow \tau) \rightarrow (\sigma \Rightarrow \tau)$. There is a term P in the reverse direction, obtained via

$$\cfrac{\cfrac{x\colon \sigma, f\colon \sigma \rightarrow \tau \vdash fx\colon \tau \qquad x\colon \sigma, f\colon \sigma \rightarrow \tau, g\colon \sigma \rightarrow \tau \mid f \sim g \vdash fx =_\tau gx}{x\colon \sigma, a\colon (\sigma \Rightarrow \tau) \vdash \mathsf{pick}\ f\ \mathsf{from}\ a\ \mathsf{in}\ fx\colon \tau}}{a\colon (\sigma \Rightarrow \tau) \vdash P(a) \stackrel{\text{def}}{=} \lambda x\colon \sigma.\, \mathsf{pick}\ f\ \mathsf{from}\ a\ \mathsf{in}\ fx\colon \sigma \rightarrow \tau}$$

Obviously, for $f\colon \sigma \to \tau$,

$$P([f]) = \lambda x\colon \sigma.\, fx = f,$$

by first using (β) for quotients, and then (η) for $\to$. Thus if $f \sim g$, then $[f] =_{\sigma \Rightarrow \tau} [g]$, and so $f =_{\sigma \to \tau} g$. This completes the proof. Notice by the way, that one also has that $[P(a)] = a$, so that we have an isomorphy of types $(\sigma \to \tau) \cong (\sigma \Rightarrow \tau)$. □

2.3. Lemma. *In the presence of (β)-conversion, the (η)-conversion is equivalent to the combination of*

$$\begin{array}{llcl} \text{(commutation)} & P[(\mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ N)/z] & = & \mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ P[N/z] \\ (\eta') & \mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ [x]_R & = & Q. \end{array}$$

The interest of this result is two-fold. Firstly, the commutation rule will turn out the be extremely useful in computations. Secondly, if one wishes to use non-extensional quotients, one probably wants do away with (η') and keep (commutation).

There are similar results for other 'colimits' like coproduct $+$ and dependent sum Σ.

Proof. Assuming (η) as above, (η') obviously holds. For (commutation), we use (η)-expansion:

$$\begin{array}{rcl} P[(\mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ N)/z] & = & P[(\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N)/z][Q/a] \\ & \overset{(\eta)}{=} & (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ P[(\mathsf{pick}\ x\ \mathsf{from}\ [x]\ \mathsf{in}\ N)/z])[Q/a] \\ & \overset{(\beta)}{=} & (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ P[N/z])[Q/a] \\ & = & \mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ P[N/z]. \end{array}$$

And conversely, given (commutation) plus (η') we get (η) by

$$\begin{array}{rcl} \mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ N[\,[x]/a] & \overset{\text{(comm)}}{=} & N[(\mathsf{pick}\ x\ \mathsf{from}\ Q\ \mathsf{in}\ [x])/a] \\ & \overset{(\eta')}{=} & N[Q/a]. \end{array}$$

□

2.4. Abbreviation. We shall conveniently write

$$\mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ N(x, y)$$

for

$$\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ y\ \mathsf{from}\ b\ \mathsf{in}\ N(x, y))$$

whenever the latter expression makes sense.

This may be generalized to n variables in $\mathsf{pick}\ x_1, \ldots, x_n\ \mathsf{from}\ a_1, \ldots, a_n\ \mathsf{in}\ N(x_1, \ldots, x_n)$.

The next result is also useful in computations.

2.5. Lemma. (i) *In case the term $\Gamma \vdash N\colon \tau$ that we apply elimination to, does not contain a variable x of type σ, then we get in context $\Gamma, a\colon \sigma/R$ a conversion,*

$$\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N \quad = \quad N.$$

(ii) *And in case we have two variables* $\Gamma, x, y{:}\,\sigma \vdash N(x,y){:}\,\tau$ *and equalities*

$$\Gamma, x{:}\,\sigma, y, y'{:}\,\sigma \mid R(y,y') \vdash N(x,y) =_\tau N(x,y') \quad \textit{and} \quad \Gamma, x, x'{:}\,\sigma, y{:}\,\sigma \mid R(x,x') \vdash N(x,y) =_\tau N(x',y)$$

then in context $\Gamma, a{:}\,\sigma/R$ *we have a conversion,*

$$\mathsf{pick}\ x,y\ \mathsf{from}\ a,a\ \mathsf{in}\ N(x,y) \quad = \quad \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N(x,x).$$

The intuition behind the last one is clear: if we pick both x and y from the same class $a{:}\,\sigma/R$, then x and y must be related. And since N is constant on equivalence classes, we may replace y by x.

Proof. (i) Because one can introduce a dummy variable $b{:}\,\sigma/R$, as in,

$$\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N \ = \ \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ N[[x]/b] \ \overset{(\eta)}{=} \ N[a/b] \ = \ N.$$

(ii) First, the term $\mathsf{pick}\ x,y\ \mathsf{from}\ a,a\ \mathsf{in}\ N(x,y) = \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ N(x,y))$ is well-defined: by the first of the above equations we can form $\mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ N(x,y)$. By substituting x' for x we also get $\mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ N(x',y)$. We now obtain

$$\frac{\dfrac{\Gamma, x, x'{:}\,\sigma, y{:}\,\sigma \mid R(x,x') \vdash N(x,y) = N(x',y)}{\Gamma, x, x'{:}\,\sigma \mid R(x,x') \vdash \mathsf{pick}\ y\ \mathsf{from}\ b\ \mathsf{in}\ N(x,y) = \mathsf{pick}\ y\ \mathsf{from}\ b\ \mathsf{in}\ N(x',y)}}{\Gamma, a{:}\,\sigma/R \vdash \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ y\ \mathsf{from}\ b\ \mathsf{in}\ N(x,y)){:}\,\tau}$$

in which the second step is compatibility of the pick operation.

We now get the required conversion by starting with an (η)-expansion and unravelling:

$$\begin{array}{rcl}
\mathsf{pick}\ x,y\ \mathsf{from}\ a,a\ \mathsf{in}\ N(x,y) & = & \mathsf{pick}\ z\ \mathsf{from}\ a\ \mathsf{in}\ ((\mathsf{pick}\ x,y\ \mathsf{from}\ a,a\ \mathsf{in}\ N(x,y))[[z]/a]) \\
& = & \mathsf{pick}\ z\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ x,y\ \mathsf{from}\ [z],[z]\ \mathsf{in}\ N(x,y)) \\
& = & \mathsf{pick}\ z\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ x\ \mathsf{from}\ [z]\ \mathsf{in}\ (\mathsf{pick}\ y\ \mathsf{from}\ [z]\ \mathsf{in}\ N(x,y))) \\
& = & \mathsf{pick}\ z\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ x\ \mathsf{from}\ [z]\ \mathsf{in}\ N(x,z)) \\
& = & \mathsf{pick}\ z\ \mathsf{from}\ a\ \mathsf{in}\ N(z,z).
\end{array}$$

□

We close this section with a technical distributivity result. It is like distributivity for other 'colimits' like $(\sigma \times \tau) + (\sigma \times \rho) \perp\!\xrightarrow{\cong} \sigma \times (\tau + \rho)$ for coproducts $+$, or $\exists x{:}\,\sigma.\,(\varphi \wedge \psi(x)) \supset\!\subset \varphi \wedge (\exists x{:}\,\sigma.\,\psi(x))$ if x not free in φ, for existential quantifiers $\exists$. In the latter case one also speaks of 'Frobenius' distributivity.

2.6. Proposition. *Let types* σ, ρ *and a relation* $x, y{:}\,\sigma \vdash R(x,y){:}\,\mathsf{Prop}$ *be given. Form a new relation* $\rho^*(R)$ *on* $\rho \times \sigma$ *by*

$$u{:}\,\rho \times \sigma, v{:}\,\rho \times \sigma \vdash \rho^*(R)(u,v) \overset{\text{def}}{=} (\pi u =_\rho \pi v) \wedge R(\pi' u, \pi' v) : \mathsf{Prop}$$

Then the canonical map

$$(\rho \times \sigma)/\rho^*(R) \perp\!\!\longrightarrow \rho \times (\sigma/R)$$

given by

$$a\colon (\rho\times\sigma)/\rho^*(R) \vdash P(a) \stackrel{\mathrm{def}}{=} \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ \langle \pi u, [\pi' u]_R\rangle : \rho\times(\sigma/R)$$

is invertible.

Proof. An inverse Q of the canonical term P is obtained as follows.

$$\cfrac{\cfrac{y\colon\rho, x, x'\colon\sigma \mid R(x,x') \vdash \rho^*(R)(\langle y,x\rangle, \langle y,x'\rangle)}{y\colon\rho, x, x'\colon\sigma \mid R(x,x') \vdash [\langle y,x\rangle]_{\rho^*(R)} = [\langle y,x'\rangle]_{\rho^*(R)}}}{y\colon\rho, b\colon\sigma/R \vdash \mathsf{pick}\ x\ \mathsf{from}\ b\ \mathsf{in}\ [\langle y,x\rangle]_{\rho^*(R)}\colon (\rho\times\sigma)/\rho^*(R)}$$

Hence we can put for $w\colon \rho\times(\sigma/R)$,

$$Q(w) \stackrel{\mathrm{def}}{=} \mathsf{pick}\ x\ \mathsf{from}\ \pi' w\ \mathsf{in}\ [\langle \pi w, x\rangle]_{\rho^*(R)} : (\rho\times\sigma)/\rho^*(R)$$

These P and Q are then each others inverses:

$$\begin{array}{rcl}
P(Q(w)) & = & P[(\mathsf{pick}\ x\ \mathsf{from}\ \pi' w\ \mathsf{in}\ [\langle \pi w, x\rangle]_{\rho^*(R)})/a] \\
& = & \mathsf{pick}\ x\ \mathsf{from}\ \pi' w\ \mathsf{in}\ P[[\langle \pi w, x\rangle]_{\rho^*(R)}/a] \\
& = & \mathsf{pick}\ x\ \mathsf{from}\ \pi' w\ \mathsf{in}\ (\mathsf{pick}\ u\ \mathsf{from}\ [\langle \pi w, x\rangle]_{\rho^*(R)}\ \mathsf{in}\ \langle \pi u, [\pi' u]_R\rangle) \\
& = & \mathsf{pick}\ x\ \mathsf{from}\ \pi' w\ \mathsf{in}\ \langle \pi w, [x]_R\rangle \\
& = & \langle \pi w, \pi' w\rangle \\
& = & w. \\
Q(P(a)) & = & Q[(\mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ \langle \pi u, [\pi' u]_R\rangle)/w] \\
& = & \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ Q[\langle \pi u, [\pi' u]_R\rangle/w] \\
& = & \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ x\ \mathsf{from}\ [\pi' u]_R\ \mathsf{in}\ [\langle \pi u, x\rangle]_{\rho^*(R)}) \\
& = & \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\langle \pi u, \pi' u\rangle]_{\rho^*(R)} \\
& = & b.
\end{array}$$

□

3 Examples

This section consists of four subsections 3.1 – 3.4 containing examples of familiar constructions using quotients: turning a commutative monoid into an abelian group; turning a preorder into a poset; turning an arbitrary group into an abelian one; and constructing tensor products ⊗ and sums ⊕ for abelian groups. The point is to show how smoothly these constructions can be described in purely type theoretic terms with the syntax for quotients from the previous section. In the end, we present some observations on quotient types in higher order logic.

3.1 Turning a commutative monoid into an abelian group

Recall that the set of integers $\mathbb{Z}$ can be constructed from the naturals $\mathbb{N}$ by considering a pair of naturals (n, m) as representation for the integer $m \perp n$. Then one identifies two pairs (n_1, m_1) and (n_2, m_2) of naturals if $m_1 \perp n_1 = m_2 \perp n_2$. Or equivalently, if $n_1 + m_2 = n_2 + m_1$. Thus one takes a quotient of $\mathbb{N} \times \mathbb{N}$. One can then define plus $+\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, zero $0 \in \mathbb{Z}$ and minus $\perp\colon \mathbb{Z} \to \mathbb{Z}$ via representatives. For example, one takes for $a \in \mathbb{Z}$,

$$\perp a \stackrel{\text{def}}{=} [m, n] \qquad \text{if} \qquad a = [n, m].$$

This construction of $\mathbb{Z}$ form $\mathbb{N}$ can be described in a slightly more abstract way as the formation of the free abelian group on a commutative monoid. Indeed, $(\mathbb{Z}, 0, +, \perp(\cdot))$ is the free abelian group on $(\mathbb{N}, 0, +)$.

In our predicate logic over simple type theory we now assume that we have a commutative monoid $(H, 0, +)$, consisting of a type $H\colon \mathsf{Type}$ with constants 0, $+$ in

$$\vdash 0\colon H \qquad \text{and} \qquad x\colon H, y\colon H \vdash x + y\colon H$$

satisfying the commutative monoid equations

$$x\colon H \mid \emptyset \vdash 0 + x = x, \qquad\qquad x, y\colon H \mid \emptyset \vdash x + y = y + x,$$
$$x, y, z\colon H \mid \emptyset \vdash x + (y + z) = (x + y) + z$$

where $=$ is the equality predicate $=_H$ on H.

We then consider the relation $\sim$ on $H \times H$,

$$u\colon H \times H, v\colon H \times H \vdash u \sim v \stackrel{\text{def}}{=} (\pi u + \pi' v =_H \pi' u + \pi v) : \mathsf{Prop}$$

which corresponds to the identification of pairs (n_1, m_1), (n_2, m_2) via $n_1 + m_2 = n_2 + m_1$ above. We write

$$\widehat{H} = (H \times H)/{\sim} \qquad \text{and} \qquad [x, y] \text{ for } [\langle x, y\rangle] \qquad \text{in} \qquad [\perp]\colon H \times H \perp\!\!\!\to \widehat{H}$$

The next step is to provide $\widehat{H}$ with an abelian group structure $\widehat{0}$, $\widehat{+}$ and inverse $\perp$. This is done, as in the set-theoretic construction, via representatives. And the syntax we have allows us to reason conveniently with these representatives inside $\mathsf{pick}\ldots$ terms.

The neutral element is easily obtained as

$$\widehat{0} \stackrel{\text{def}}{=} [0, 0] : \widehat{H}$$

The inverse operation $\perp(\cdot)$ is

$$\perp a \stackrel{\text{def}}{=} \mathsf{pick}\ w\ \mathsf{from}\ a\ \mathsf{in}\ [\pi' w, \pi w],$$

which is very much like the set-theoretic minus $\perp(\cdot)$ mentioned above. Notice that this term is well-defined because from $u \sim v$ one obtaines $\langle \pi' u, \pi u\rangle \sim \langle \pi' v, \pi v\rangle$.

Finally, the addition $\widehat{+}$ of $\widehat{H}$ is then

$$\begin{aligned} a \mathbin{\widehat{+}} b &\overset{\text{def}}{=} \mathsf{pick}\ u, v\ \mathsf{from}\ a, b\ \mathsf{in}\ [\pi u + \pi v, \pi' u + \pi' v] \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ [\pi u + \pi v, \pi' u + \pi' v]). \end{aligned}$$

This operation is well-defined, by an argument like in (ii) in the proof of Lemma 2.5, since we have

$$\begin{gathered} u_1, u_2 \colon H \times H, v \colon H \times H \mid u_1 \sim u_2 \vdash \langle \pi u_1 + \pi v, \pi' u_1 + \pi' v \rangle \sim \langle \pi u_2 + \pi v, \pi' u_2 + \pi' v \rangle \\ u \colon H \times H, v_1, v_2 \colon H \times H \mid v_1 \sim v_2 \vdash \langle \pi u + \pi v_1, \pi' u + \pi' v_1 \rangle \sim \langle \pi u + \pi v_2, \pi' u + \pi' v_2 \rangle \end{gathered}$$

Then $\widehat{0}$ is neutral element, since

$$\begin{aligned} a \mathbin{\widehat{+}} \widehat{0} &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ [0,0]\ \mathsf{in}\ [\pi u + \pi v, \pi' u + \pi' v]) \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\pi u + 0, \pi' u + 0] \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\pi u, \pi' u] \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [u] \\ &= a. \end{aligned}$$

Notice how closely this calculation follows the ordinary fashion in which one would establish this equation.

Further $\widehat{+}$ is commutative, by commutation and by commutativity of + on H:

$$\begin{aligned} a \mathbin{\widehat{+}} b &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ [\pi u + \pi v, \pi' u + \pi' v]) \\ &= \mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\pi u + \pi v, \pi' u + \pi' v]) \\ &= \mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\pi v + \pi u, \pi' v + \pi' u]) \\ &= b \mathbin{\widehat{+}} a. \end{aligned}$$

For associativity we have to make essential use of commutation, see Lemma 2.3.

$$\begin{aligned} a \mathbin{\widehat{+}} (b \mathbin{\widehat{+}} c) &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ z\ \mathsf{from}\ b \mathbin{\widehat{+}} c\ \mathsf{in}\ [\pi u + \pi z, \pi' u + \pi' z]) \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ z\ \mathsf{from}\ (\\ &\qquad \mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\mathsf{pick}\ w\ \mathsf{from}\ c\ \mathsf{in}\ [\pi v + \pi w, \pi' v + \pi' w])) \\ &\qquad\quad \mathsf{in}\ [\pi u + \pi z, \pi' u + \pi' z]) \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\\ &\qquad \mathsf{pick}\ z\ \mathsf{from}\ (\mathsf{pick}\ w\ \mathsf{from}\ c\ \mathsf{in}\ [\pi v + \pi w, \pi' v + \pi' w])) \\ &\qquad\quad \mathsf{in}\ [\pi u + \pi z, \pi' u + \pi' z]) \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\mathsf{pick}\ w\ \mathsf{from}\ c\ \mathsf{in} \\ &\qquad \mathsf{pick}\ z\ \mathsf{from}\ [\pi v + \pi w, \pi' v + \pi' w]\ \mathsf{in}\ [\pi u + \pi z, \pi' u + \pi' z])) \\ &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ v\ \mathsf{from}\ b\ \mathsf{in}\ (\mathsf{pick}\ w\ \mathsf{from}\ c\ \mathsf{in} \\ &\qquad [\pi u + (\pi v + \pi w), \pi' u + (\pi' v + \pi' w)])). \end{aligned}$$

In a similar way one gets

$$\begin{aligned}(a \mathbin{\widehat{+}} b) \mathbin{\widehat{+}} c \;\; &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } (\textsf{pick } v \textsf{ from } b \textsf{ in } (\textsf{pick } w \textsf{ from } c \textsf{ in} \\ &\qquad\qquad [(\pi u + \pi v) + \pi w, (\pi' u + \pi' v) + \pi' w])))\end{aligned}$$

so that we are done by associativity of + on H.

Finally, we have a group $\widehat{H}$, since $\perp(\cdot)$ is inverse:

$$\begin{aligned}a \mathbin{\widehat{+}} (\perp a) \;\; &= \;\; \textsf{pick } u, v \textsf{ from } a, \perp a \textsf{ in } [\pi u + \pi v, \pi' u + \pi' v] \\ &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } (\textsf{pick } v \textsf{ from } (\\ &\qquad\quad \textsf{pick } w \textsf{ from } a \textsf{ in } [\pi' w, \pi w]) \textsf{ in } [\pi u + \pi v, \pi' u + \pi' v]) \\ &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } (\textsf{pick } w \textsf{ from } a \textsf{ in } (\\ &\qquad\quad \textsf{pick } v \textsf{ from } [\pi' w, \pi w] \textsf{ in } [\pi u + \pi v, \pi' u + \pi' v])) \\ &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } (\textsf{pick } w \textsf{ from } a \textsf{ in } [\pi u + \pi' w, \pi' u + \pi w] \\ &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } [\pi u + \pi' u, \pi' u + \pi u] && \text{by Lemma 2.5 (ii)} \\ &= \;\; \textsf{pick } u \textsf{ from } a \textsf{ in } [0, 0] && \text{since } \langle \pi u + \pi' u, \pi' u + \pi u \rangle \sim \langle 0, 0 \rangle \\ &= \;\; \widehat{0} && \text{by Lemma 2.5 (i).}\end{aligned}$$

We conclude that $\widehat{H}$ is an abelian group. Next we show that it has the appropriate universal property. First, we have a map $c: H \to \widehat{H}$ by $c(x) = [0, x]$. This is a monoid homomorphism, since by definition $c(0) = [0, 0] = \widehat{0}$, and

$$\begin{aligned}c(x) \mathbin{\widehat{+}} c(y) \;\; &= \;\; \textsf{pick } u, v \textsf{ from } [0, x], [0, y] \textsf{ in } [\pi u + \pi v, \pi' u + \pi' v] \\ &= \;\; [0 + 0, x + y] \\ &= \;\; c(x + y).\end{aligned}$$

Further, if we are given an abelian group $(G, \bullet, 1, (\cdot)^{-1})$ toghether with a monoid homorphism $M: H \to G$, then there is a unique homorphism $\widehat{M}: \widehat{H} \to G$ with $\widehat{M} \circ c = M$ in,

$$\begin{tikzcd} H \arrow[r, "c"] \arrow[dr, "M"'] & \widehat{H} \arrow[d, dashed, "\overline{M}"] \\ & G\text{, abelian group} \end{tikzcd}$$

Therefore write

$$N(u) \;=\; M(\pi' u) \bullet M(\pi u)^{-1} : G, \qquad \text{for } u : H \times H$$

To see that the term

$$\widehat{M}(a) \;\overset{\text{def}}{=}\; \textsf{pick } u \textsf{ from } a \textsf{ in } N(u) : G, \qquad \text{for } a : \widehat{H}\ (= (H \times H)/{\sim})$$

is well-defined we need to have

$$u, v\colon H \times H \mid u \sim v \vdash N(u) = N(v)$$

But this follows because G is an abelian group: if $u \sim v$, then by definition $\pi u + \pi' v = \pi' u + \pi v$. Hence $M(\pi u) \bullet M(\pi' v) = M(\pi u + \pi' v) = M(\pi' u + \pi v) = M(\pi' u) \bullet M(\pi v)$, and so $N(u) = M(\pi' u) \bullet M(\pi u)^{-1} = M(\pi' v) \bullet M(\pi v)^{-1} = N(v)$. Then indeed,

$$(\widehat{M} \circ c)(x) \;=\; \mathsf{pick}\ u\ \mathsf{from}\ [0, x]\ \mathsf{in}\ N(u) \;=\; N(\langle 0, x\rangle) \;=\; M(x) \bullet M(0)^{-1} \;=\; M(x) \bullet 1^{-1} \;=\; M(x).$$

We leave it to the reader to verify that $\widehat{M}$ is a homomorphism. And if another term (-homomorphism) $P\colon \widehat{H} \to G$ satisfies $P(c(x)) = M(x)$, then $N(u) = M(\pi' u) \bullet M(\pi u)^{-1} = P(c(\pi' u)) \bullet P(c(\pi u))^{-1} = P([0, \pi' u]) \bullet P(\perp[0, \pi u]) = P([0, \pi' u] \mathbin{\widehat{+}} [\pi u, 0]) = P([\pi u, \pi' u]) = P([u])$. So that

$$\widehat{M}(a) \;=\; \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ N(u) \;=\; \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ P([u]) \;=\; P(a).$$

Thus we have established that $\widehat{H}$ is the free abelian group on the commutative monoid H. In particular, we can now put $\mathbb{Z} \overset{\text{def}}{=} \widehat{\mathbb{N}}$ for the type of integers, assuming we have a type $\mathbb{N}$ of natural numbers (which is a commutative monoid). It can then be shown that $\mathbb{Z}$ is a commutative ring with unit (with multiplication inherited from $\mathbb{N}$). One can go further and construct the type of rationals $\mathbb{Q}$ as quotient of $\mathbb{Z} \times \mathbb{N}$, where the pair (a, n) represents the rational $\frac{a}{n+1}$.

3.2 The quotient poset of a preorder

In a preorder $X = (X, \leq)$, the ordering $\leq$ is reflexive and transitive. It can be turned into a poset $X/{\sim}$ in a canonical way by taking as (equivalence) relation $x \sim y \;\Leftrightarrow\; x \leq y \;\&\; y \leq x$. Then one can put a (well-defined) order $\sqsubseteq$ on $X/{\sim}$ via representatives: $[x] \sqsubseteq [y] \;\Leftrightarrow\; x \leq y$ in X. We have forced this order $\sqsubseteq$ to be anti-symmetric. Thus we have a poset $(X/{\sim}, \sqsubseteq)$. It additionally has a universal property.

In the type theoretic version of this construction we shall need $\mathsf{Prop}\colon \mathsf{Type}$, in the formation of $\sqsubseteq$ below. Thus we need higher order logic. Further we assume the following **extensionality principle** for predicates

$$\frac{\Gamma \vdash P, Q\colon \sigma \to \mathsf{Prop} \qquad \Gamma, x\colon \sigma \mid \Theta, Px \vdash Qx \qquad \Gamma, x\colon \sigma \mid \Theta, Qx \vdash Px}{\Gamma \mid \Theta \vdash P =_{\sigma \to \mathsf{Prop}} Q}\ (x \text{ not in } \Theta)$$

As a result we have for $P\colon \sigma \to \mathsf{Prop}$ that Px holds if and only if $P =_{\sigma \to \mathsf{Prop}} \lambda x\colon \sigma.\, \top$.

Since we'll be using quotient terms of the form $\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \varphi(x)$ where $\varphi(x)$ is a proposition, we first need to know a bit more about terms of this form. We notice that pick preserves finite conjunctions $\top, \wedge$ in the sense that

$$\begin{array}{rcl}
\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \top & = & \top \\
\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\varphi(x) \wedge \psi(x)) & = & (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \varphi(x)) \wedge (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \psi(x))
\end{array}$$

The first of these follows directly from Lemma 2.5 (i). For the second we use commuation twice and Lemma 2.5 (ii), in:

$$\begin{array}{ll} \multicolumn{2}{l}{(\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \varphi(x)) \wedge (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \psi(x))} \\ = & (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\varphi(x) \wedge (\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \psi(x)) \\ = & \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\mathsf{pick}\ x'\ \mathsf{from}\ a\ \mathsf{in}\ \varphi(x) \wedge \psi(x')) \\ = & \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ (\varphi(x) \wedge \psi(x)). \end{array}$$

As a consequence we have that if φ implies ψ, then $\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \varphi(x)$ implies $\mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \psi(x)$. This is because φ implies ψ if and only if $\varphi \wedge \psi =_{\mathsf{Prop}} \psi$.

We can now start the quotient poset construction in type theory. Therefore we assume a type σ with an ordering $\leq$ which is reflexive and transitive:

$$x{:}\,\sigma \mid \emptyset \vdash x \leq x \qquad \text{and} \qquad x, y, z{:}\,\sigma \mid x \leq y, y \leq z \vdash x \leq z$$

In order to turn $(\sigma, \leq)$ into a poset, we define a relation $\sim$ as above, by

$$x, y{:}\,\sigma \vdash (x \sim y) \stackrel{\text{def}}{=} (x \leq y \wedge y \leq x) : \mathsf{Prop}$$

and form the quotient type $\sigma/{\sim}$, with canonical map $[\bot]{:}\,\sigma \to \sigma/{\sim}$. We can put an order on $\sigma/{\sim}$, exactly as in the set theoretic description above, by

$$a{:}\,\sigma/{\sim}, b{:}\,\sigma/{\sim} \vdash a \sqsubseteq b \stackrel{\text{def}}{=} \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ x \leq y : \mathsf{Prop}$$

Then

$$\begin{array}{rcll} a \sqsubseteq a & = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, a\ \mathsf{in}\ x \leq y & \\ & = & \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ x \leq x & \text{by Lemma 2.5 (ii)} \\ & = & \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ \top & \\ & = & \top & \end{array}$$

and

$$\begin{array}{rcl} a \sqsubseteq b \wedge b \sqsubseteq c & = & (\mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ x \leq y) \wedge (\mathsf{pick}\ w, z\ \mathsf{from}\ b, c\ \mathsf{in}\ w \leq z) \\ & = & \mathsf{pick}\ x, y, w, z\ \mathsf{from}\ a, b, b, c\ \mathsf{in}\ x \leq y \wedge w \leq z \\ & = & \mathsf{pick}\ x, y, z\ \mathsf{from}\ a, b, c\ \mathsf{in}\ x \leq y \wedge y \leq z \\ & \supset & \mathsf{pick}\ x, y, z\ \mathsf{from}\ a, b, c\ \mathsf{in}\ x \leq z \\ & = & \mathsf{pick}\ x, z\ \mathsf{from}\ a, c\ \mathsf{in}\ x \leq z \\ & = & a \sqsubseteq c. \end{array}$$

The new order $\sqsubseteq$ is then anti-symmetric by construction:

$$\begin{array}{rcl}
a \sqsubseteq b \wedge b \sqsubseteq a & = & (\mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ x \leq y) \wedge (\mathsf{pick}\ v, u\ \mathsf{from}\ b, a\ \mathsf{in}\ v \leq u) \\
& = & \mathsf{pick}\ x, y, v, u\ \mathsf{from}\ a, b, b, a\ \mathsf{in}\ x \leq y \wedge v \leq u \\
& = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ x \leq y \wedge y \leq x \\
& = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ x \sim y \\
& \supset & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ [x] = [y] \\
& = & (a = b).
\end{array}$$

The canonical map $[\perp]\colon \sigma \to \sigma/{\sim}$ satisfies

$$[x] \sqsubseteq [y] \;=\; \mathsf{pick}\ u, v\ \mathsf{from}\ [x], [y]\ \mathsf{in}\ u \leq v \;=\; x \leq y.$$

so that $[\perp]$ preserves and reflects the order.

We have the usual universal property: if $(\tau, \preceq)$ is a poset, and $M\colon \sigma \to \tau$ is order preserving (i.e. monotone: $x, y\colon \sigma \mid x \leq y \vdash M(x) \preceq M(y)$), then there is a unique order preserving $\overline{M}\colon \sigma/{\sim} \to \tau$ making the following diagram commute.

$$\begin{tikzcd}
\sigma \arrow[r, "{[\perp]}"] \arrow[dr, "M"'] & \sigma/{\sim} \arrow[d, dashed, "\overline{M}"] \\
 & \tau\text{, poset}
\end{tikzcd}$$

Since $x \sim y$ means $x \leq y \wedge y \leq x$, it implies $M(x) \preceq M(y) \wedge M(y) \preceq M(x)$, and so $M(x) = M(y)$ since $\preceq$ is anti-symmetric. Thus we can define

$$\overline{M}(a) \overset{\text{def}}{=} \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ M(x)$$

We leave it to the reader to verify that $\overline{M}$ is order preserving, but we do notice that $\overline{M}([x]) = \mathsf{pick}\ x\ \mathsf{from}\ [x]\ \mathsf{in}\ M(x) = M(x)$. And if $P\colon \sigma/{\sim} \to \tau$ also satisfies $P \circ [\perp] = M$, then $P(a) = \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ P([x]) = \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ M(x) = \overline{M}(a)$.

3.3 The abelian quotient of an arbitrary group

In our third example we will give a type theoretic version of the construction of an abelian group from an arbitrary group. The usual group theoretic recipe is as follows. Let G be a group and consider the subset $C = \{x + y \perp x \perp y \mid x, y \in G\}$ of commutators; take G^{c} to be the subgroup generated by C. This is then a normal subgroup, so one can form the quotient (or factor) group G/G^{c}. This is the required abelian group, with an appropriate universal property.

The type theoretic construction we use will be slightly different: we consider equivalence relations on G which are congruences, and need therefore make essential use of higher order quantification. In this example we only sketch the essential points, and leave details (especially of the computations) to the reader.

Let G: Type be a type which carries a group structure $(0, +, \perp(\cdot))$. Consider the following relation $\sim$ on G,

$$\begin{aligned} u, v{:}\, G \vdash u \sim v \ \overset{\text{def}}{=}\ & \forall R{:}\, G \times G \to \mathsf{Prop}.\, \text{Equiv}(R) \wedge \text{Cong}(R) \\ & \qquad \wedge \forall x, y{:}\, G.\, R(x+y, y+x) \supset R(u, v) : \mathsf{Prop} \end{aligned}$$

where the predicates Equiv(R) and Cong(R) express that R is an equivalence relation, and is a congruence. They are described by

$$\begin{aligned} \text{Equiv}(R) \ &\overset{\text{def}}{=}\ \forall x{:}\, G.\, R(x, x) \wedge \forall x, y{:}\, G.\, R(x, y) \supset R(y, x) \\ & \qquad\qquad \wedge \forall x, y, z{:}\, G.\, R(x, y) \wedge R(y, z) \supset R(x, z) \\ \text{Cong}(R) \ &\overset{\text{def}}{=}\ \forall x_1, x_2, y_1, y_2{:}\, G.\, R(x_1, x_2) \wedge R(y_1, y_2) \supset R(x_1 \perp y_1, x_2 \perp y_2) \end{aligned}$$

It is then easy to see that if we have $\text{Equiv}(R) \wedge \text{Cong}(R)$ then $R(0, 0)$, and $R(x, y) \supset R(\perp x, \perp y)$. Also, with some elementary reasoning one gets $\text{Equiv}(\sim) \wedge \text{Cong}(\sim)$, where $\sim$ is the relation on G defined above.

We now put $\dot{G} \overset{\text{def}}{=} G/\!\sim$, with canonical map $x{:}\, G \vdash [x]{:}\, \dot{G}$. Then we can define for $a, b{:}\, \dot{G}$,

$$\begin{aligned} \dot{0} \ &\overset{\text{def}}{=}\ [0] \\ a \dot{+} b \ &\overset{\text{def}}{=}\ \textsf{pick } u, v \textsf{ from } a, b \textsf{ in } [u + v] \\ \dot{\perp} a \ &\overset{\text{def}}{=}\ \textsf{pick } u \textsf{ from } a \textsf{ in } [\perp u] \end{aligned}$$

so that we get operations on $\dot{G}$ via representatives. We then get an abelian group, by computations like in Subsection 3.1. Again we have that $[\perp]{:}\, G \to \dot{G}$ is a univeral group homomorphism: for any homorphism $M{:}\, G \to H$ into an abelian group H, we get a unique homomorphism $\overline{M}$ in

$$\begin{tikzcd} G \arrow[r, "{[\perp]}"] \arrow[dr, "M"'] & \dot{G} \arrow[d, dashed, "\overline{M}"] \\ & H, \text{ abelian} \end{tikzcd}$$

One puts $\overline{M}(a) \overset{\text{def}}{=} \textsf{pick } u \textsf{ from } a \textsf{ in } M(u)$, which is well-defined: form the kernel relation $x, y{:}\, G \vdash R(x, y) \overset{\text{def}}{=} (M(x) = M(y)){:}\, \mathsf{Prop}$. This is a congruence and an equivalence relation, which satisfies $R(x+y, y+x)$: one has $M(x+y) = M(x) \bullet M(y) = M(y) \bullet M(x) = M(y+x)$, since the group operation $\bullet$ of H is commutative. Thus if $u \sim v$, then $R(u, v)$ and so $M(u) = M(v)$. It is not hard to verify that $\overline{M}$ is a homomorphism. Uniqueness of is straightforward.

3.4 Tensor products and sums of abelian groups

A familiar construction in (abelian) group theory is the tensor product $G \otimes H$ of two abelian groups G, H. It comes equipped with a universal bi-homomorphism $\otimes{:}\, G \times H \to G \otimes H$. Recall that $f{:}\, G \times H \to K$ is a bi-homomorphism if f is a homomorphism in each coordinate separately, i.e. if

$$f(x \perp x', y) = f(x, y) \perp f(x', y) \qquad \text{and} \qquad f(x, y \perp y') = f(x, y) \perp f(x, y').$$

The universal property of this bi-homomorphism $\otimes$ is then: for each bi-homomorphism $f\colon G \times H \to K$ there is a unique homomorphism $\overline{f}\colon G \otimes H \to K$ with $\overline{f} \circ \otimes = f$.

Set-theoretically, one describes $G \otimes H$ as a suitable quotient of the free abelian group $(G \times H)^{+}$ on $G \times H$. We are going to give a type theoretic description (using higher order logic). We therefore assume that we have for each type σ the free abelian group σ^{+} on σ with universal map $\eta_{\sigma}\colon \sigma \to \sigma^{+}$. The set-theoretic construction of σ^{+} involves all maps $\sigma \to \mathbb{Z}$, which are 0 almost everywhere, see e.g. [6, I,9], with abelian group structure inherited pointwise from $\mathbb{Z}$. This does not work type theoretically, because the unit $\eta(x)$ is $y \mapsto \mathsf{if}\ x = y\ \mathsf{then}\ 1\ \mathsf{else}\ 0$, and involves an equality test. Instead, one can obtain σ^{+} via two successive quotients from the free monoid $\sigma^{*} = \mathsf{list}(\sigma)$ on σ, by first making the monoid commutative (like in Subsection 3.3) and then an abelian group (like in Subsection 3.1). At this stage, we are not so much interested in the construction of σ^{+}, and we simply assume it to be given, with appropriate universal property, given by $\eta\colon \sigma \to \sigma^{+}$.

Assume now that two types σ, τ are given, both carrying an abelian group structure. We form the product type $\sigma \times \tau$, and put the following relation $\sim$ on the free abelian group $(\sigma \times \tau)^{+}$ on $\sigma \times \tau$:

$$\begin{aligned} u\colon (\sigma \times \tau)^{+}, v\colon (\sigma \times \tau)^{+} \vdash u \sim v \quad \stackrel{\text{def}}{=} \quad & \forall R\colon (\sigma \times \tau)^{+} \times (\sigma \times \tau)^{+} \to \mathsf{Prop}.\, \mathrm{Equiv}(R) \wedge \mathrm{Cong}(R) \\ & \wedge \forall x, x'\colon \sigma.\, \forall y\colon \tau.\, \eta(x \perp x', y) R (\eta(x, y) \perp \eta(x', y)) \\ & \wedge \forall x\colon \sigma.\, \forall y, y'\colon \tau.\, \eta(x, y \perp y') R (\eta(x, y) \perp \eta(x, y')) \\ & \supset\ R(u, v). \end{aligned}$$

Notice that the congruence requirement $\mathrm{Cong}(R)$ is with respect to the (free) abelian group structure of $(\sigma \times \tau)^{+}$. The second and third line in this definition, impose the bi-homomorphism conditions.

We then form the quotient type,

$$\sigma \otimes \tau \stackrel{\text{def}}{=} \left((\sigma \times \tau)^{+}\right) /\!\sim$$

which comes with a quotient map $[\perp]\colon (\sigma \times \tau)^{+} \to \sigma \otimes \tau$. For variables $x\colon \sigma, y\colon \tau$, we can then write

$$x \otimes y \stackrel{\text{def}}{=} [\eta(x, y)] : \sigma \otimes \tau.$$

We first have to show that $\sigma \otimes \tau$ is an abelian group again. It inherits its structure from $(\sigma \times \tau)^{+}$, much like in the previous subsection:

$$\begin{aligned} 0 &= [0] \\ \perp a &= \mathsf{pick}\ u\ \mathsf{from}\ a\ \mathsf{in}\ [\perp u] \\ a + b &= \mathsf{pick}\ u, v\ \mathsf{from}\ a, b\ \mathsf{in}\ [u + v]. \end{aligned}$$

The canonical map $[\perp]$ then becomes a homomorphism. Further, by construction we have

$$\eta(x \perp x', y) \sim (\eta(x, y) \perp \eta(x', y))$$

and so

$$(x \perp x') \otimes y = [\eta(x \perp x', y)] = [\eta(x, y) \perp \eta(x', y)] = [\eta(x, y)] \perp [\eta(x', y)] = (x \otimes y) \perp (x' \otimes y).$$

Hence $\otimes\colon \sigma \times \tau \to \sigma \otimes \tau$ is a bi-homomorphism. It is universal by a two-step argument:

$$\begin{tikzcd}
\sigma \times \tau \arrow[r, "\eta"] \arrow[rr, bend left, "\otimes"] \arrow[drr, "M\ \text{bi-hom.}"'] & (\sigma \times \tau)^+ \arrow[r, "{[\perp]}"] \arrow[dr, dashed, "\overline{M}"] & \sigma \otimes \tau \arrow[d, dashed, "\overline{\overline{M}}"] \\
& & \rho\text{, abelian group}
\end{tikzcd}$$

Here, $\overline{M}$ is obtained by freeness. The kernel of $\overline{M}$ then contains $\sim$, because M is a bi-homomorphism. This gives us the unique homomorphism $\overline{\overline{M}}$, as indicated. This universal property fully determines $\sigma \otimes \tau$.

Finally, we make a brief digression into dependent type theory (but we keep unchanged our logic of propositions to reason about types and terms). Assume that we have a σ-indexed collection of abelian groups $\tau(x)$, for $x\colon \sigma$. This means that we have $x\colon \sigma \vdash \tau(x)\colon \mathsf{Type}$, with group structure given by

$$x\colon \sigma \vdash 0_x\colon \tau(x), \qquad x\colon \sigma, y_1, y_2\colon \tau(x) \vdash y_1 +_x y_2\colon \tau(x), \qquad x\colon \sigma, y\colon \tau(x) \vdash \perp_x y\colon \tau(x),$$

where we have written the variable x as an index of the group operations, to stress that also this structure is indexed by $x\colon \sigma$.

The dependent product $\Pi x\colon \sigma.\, \tau$ then carries an abelian group structure, by the usual pointwise constructions:

$$\begin{array}{rcl}
& \vdash & 0 \stackrel{\mathrm{def}}{=} \lambda x\colon \sigma.\, 0_x : \Pi x\colon \sigma.\, \tau \\
f, g\colon \Pi x\colon \sigma.\, \tau & \vdash & f + g \stackrel{\mathrm{def}}{=} \lambda x\colon \sigma.\, (fx) +_x (gx) : \Pi x\colon \sigma.\, \tau \\
f\colon \Pi x\colon \sigma.\, \tau & \vdash & \perp f \stackrel{\mathrm{def}}{=} \lambda x\colon \sigma.\, \perp_x (fx) : \Pi x\colon \sigma.\, \tau
\end{array}$$

Also one can form a dependent sum $\bigoplus x\colon \sigma.\, \tau$ of abelian groups (usually called 'direct sum') as a quotient of the free abelian group $(\Sigma x\colon \sigma.\, \tau)^+$ on the dependent sum $\Sigma x\colon \sigma.\, \tau$ of the underlying types. The relation $\sim$ used for this quotient is

$$\begin{array}{rcl}
u\colon (\Sigma x\colon \sigma.\, \tau)^+, v\colon (\Sigma x\colon \sigma.\, \tau)^+ \vdash u \sim v & \stackrel{\mathrm{def}}{=} & \forall R\colon (\Sigma x\colon \sigma.\, \tau)^+ \times (\Sigma x\colon \sigma.\, \tau)^+ \to \mathsf{Prop}. \\
& & \quad \mathrm{Equiv}(R) \wedge \mathrm{Cong}(R) \\
& & \quad \wedge\ \forall x\colon \sigma.\, \forall y, y'\colon \tau(x). \\
& & \qquad \eta(\langle x, y \perp y' \rangle) R (\eta(\langle x, y\rangle) \perp \eta(\langle x, y'\rangle)) \\
& & \quad \supset R(u, v).
\end{array}$$

We write $\bigoplus x\colon \sigma.\, \tau \stackrel{\mathrm{def}}{=} \big((\Sigma x\colon \sigma.\, \tau)^+\big)/\!\sim$ for the resulting quotient, which turns out to be an abelian group again. It is the 'dependent sum of abelian groups': there is an associated pairing (or introduction term),

$$x\colon \sigma, y\colon \tau(x) \vdash \langle\langle x, y\rangle\rangle \stackrel{\mathrm{def}}{=} [\eta(\langle x, y\rangle)] : \bigoplus x\colon \sigma.\, \tau$$

such that for each $x\colon\sigma$ the term

$$\lambda y\colon\tau(x).\,\langle\langle x,y\rangle\rangle \qquad \text{is a homomorphism} \qquad \tau(x) \perp\!\!\!\rightarrow \bigoplus x\colon\sigma.\,\tau.$$

And if ρ is an abelian group together with a term $x\colon\sigma, y\colon\tau \vdash Q(x,y)\colon\rho$ such that for each $x\colon\sigma$, the abstraction term $\lambda y\colon\tau.\,Q(x,y)$ is a homomorphism $\tau(x) \rightarrow \rho$, then there is an associated elimination homomorphism,

$$z\colon\bigoplus x\colon\sigma.\,\tau \vdash \overline{Q}(z) = Q(x,y) \textbf{ with } \langle\langle x,y\rangle\rangle := z : \rho$$

which is unique in satisfying $\overline{Q}(\langle\langle x,y\rangle\rangle) = Q(x,y)$. This follows from the universal property of the quotient, again by a two-step argument. So we get the usual rules for a dependent sum, but this time involving abelian groups, indexed by a type.

(And if one takes a finite type σ as index, say $\sigma = \{1,2,\ldots,n\}$, then the resulting finite direct sum is the same as the finite tensor product $\tau_1 \otimes \cdots \otimes \tau_n$.)

3.1. Remarks. (i) Usually in algebra (see e.g. [6, I,9]) the direct sum $\bigoplus x\colon\sigma.\,\tau$ is constructed as subgroup of the product $\Pi x\colon\sigma.\,\tau$. This crucially depends on the presence of a map $P\colon(\Sigma x\colon\sigma.\,\tau) \rightarrow (\Pi x\colon\sigma.\,\tau)$, given by

$$P(z) = \lambda x\colon\sigma.\left\{\begin{array}{ll} \pi' z & \text{if } x = \pi z \\ 0_x & \text{else.}\end{array}\right.$$

But this map involves an equality test, which is in general not available in type theory.

(ii) One might have also expected a σ-indexed tensor, as a suitable quotient $(\Pi x\colon\sigma.\,\tau) \twoheadrightarrow \bigotimes x\colon\sigma.\,\tau$. But it is not clear how to give an appropriate type theoretic formulation of 'multi-homomorphism' in this case (i.e. a homomorphism in each coordinate $x\colon\sigma$).

We close this example section with some observations on quotients in higher order logic. The first one is again due to Martin Hofmann.

3.2. Remarks. (i) In higher order logic, quotient types are automatically effective: if we have a relation $x\colon\sigma, y\colon\sigma \vdash R(x,y)$: which is provably an equivalence relation, then by transitivity and symmtry, we can form the pick-term

$$\frac{x\colon\sigma, y\colon\sigma \vdash R(x,y)\colon \mathsf{Prop} \qquad x\colon\sigma, y\colon\sigma, z\colon\sigma \mid R(y,z) \vdash R(x,y) =_{\mathsf{Prop}} R(x,z)}{x\colon\sigma, a\colon\sigma/R \vdash \mathsf{pick}\ w\ \mathsf{from}\ a\ \mathsf{in}\ R(x,w)\colon \mathsf{Prop}}$$

Hence by using reflexivity, we get,

$$\begin{array}{rcl} x\colon\sigma, y\colon\sigma \mid [x] = [y] \vdash \top \;=\; R(x,x) & = & \mathsf{pick}\ w\ \mathsf{from}\ [x]\ \mathsf{in}\ R(x,w) \\ & = & \mathsf{pick}\ w\ \mathsf{from}\ [y]\ \mathsf{in}\ R(x,w) \\ & = & R(x,y), \end{array}$$

where $=$ on the right of the turnstile is equality on Prop, which is the same as equivalence $\supset\!\subset$.

(ii) Also, using higher order logic, one can show that for a relation R on σ, the canonical map $[\perp]\colon \sigma \to \sigma/R$ is always surjective (in the logic). Consider therefore the proposition,

$$a\colon \sigma/R \vdash \varphi(a) \stackrel{\text{def}}{=} \exists x\colon \sigma.\, a =_{\sigma/R} [x] : \mathsf{Prop}.$$

One then obviously has $y\colon \sigma \mid \emptyset \vdash \varphi([y]) =_{\mathsf{Prop}} \top$. Thus for $a\colon \sigma/R$ one gets by (η)-expansion,

$$\varphi(a) = \mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ \varphi([y]) = \mathsf{pick}\ y\ \mathsf{from}\ a\ \mathsf{in}\ \top = \top.$$

Thus $\exists x\colon \sigma.\, a =_{\sigma/R} [x]$ holds for $a\colon \sigma/R$.

(iii) The previous result can be used to factor an arbitrary term $x\colon \sigma \vdash M(x)\colon \tau$ as a surjection followed by an injection:

$$\Big(\sigma \xrightarrow{M} \tau \Big) = \Big(\sigma \overset{[\perp]}{\twoheadrightarrow} \sigma/K \overset{\overline{M}}{\rightarrowtail} \tau \Big)$$

In this diagram, K is the kernel relation,

$$x\colon \sigma, y\colon \sigma \vdash K(x,y) \stackrel{\text{def}}{=} (M(x) =_\tau M(y)) : \mathsf{Prop}$$

and $\overline{M}(a) = \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ M(x)$ for $a\colon \sigma/K$. Then obviously $\overline{M}([x]) = M(x)$. Moreover, this term $\overline{M}$ is (internally) injective: one has

$$a\colon \sigma/K, b\colon \sigma/K \mid \overline{M}(a) =_\tau \overline{M}(b) \vdash a =_{\sigma/K} b.$$

This can be seen as follows.

$$\begin{array}{rcl}
\overline{M}(a) =_\tau \overline{M}(b) & = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ M([x]) =_\tau M([y]) \\
& = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ M(x) =_\tau M(y) \\
& = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ K(x, y) \\
& = & \mathsf{pick}\ x, y\ \mathsf{from}\ a, b\ \mathsf{in}\ [x] =_{\sigma/K} [y] \\
& = & a =_{\sigma/K} b.
\end{array}$$

This factorization is familiar from topos theory: it is almost literally as in the proof of [5, Theorem 1.52].

(iv) For an arbitrary relation $x\colon \sigma, y\colon \sigma \vdash R(x,y)\colon \mathsf{Prop}$ one can form in higher order logic the least equivalence relation $\overline{R}$ containing R as

$$x\colon \sigma, y\colon \sigma \vdash \overline{R}(x,y) \stackrel{\text{def}}{=} \forall S\colon \sigma \times \sigma \to \mathsf{Prop}.\, (\mathrm{Equiv}(S) \wedge R \subseteq S) \supset S(x,y) : \mathsf{Prop},$$

where $R \subseteq S$ is an abbreviation for $\forall x\colon \sigma.\, \forall y\colon \sigma.\, R(x,y) \supset S(x,y)$. Then one can prove that R and $\overline{R}$ yield the same quotient type, in the sense that there is an isomorphism of types,

$$\sigma/R \cong \sigma/\overline{R}$$

Thus σ/R is the quotient by the equivalence relation generated by R. This isomorphism is given by the two terms

$$\begin{aligned} a{:}\,\sigma/R \vdash P(a) &\overset{\mathrm{def}}{=} \textsf{pick } x \textsf{ from } a \textsf{ in } [x]_{\overline{R}} : \sigma/\overline{R} \\ b{:}\,\sigma/\overline{R} \vdash Q(b) &\overset{\mathrm{def}}{=} \textsf{pick } y \textsf{ from } b \textsf{ in } [y]_{R} : \sigma/R, \end{aligned}$$

where Q is well-defined because $\overline{R}(x,y)$ implies $[x]_R =_{\sigma/R} [y]_R$, since the latter is an equivalence relation containing R.

4 Categorical foundation

In this section we briefly describe the categorical considerations which underly (and gave rise to) the syntax used earlier. This presentation is not self-contained and presupposes familiarity with the categorical description of logic and type theory in terms of fibred categories. Readers without this background may wish to have a look only at Example 4.3 (iv).

We start from a fibration $\begin{smallmatrix}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{smallmatrix}$, where we think of the base category $\mathbb{B}$ as a model of simple type theory: the objects are types and the morphisms are terms. The fibre category $\mathbb{E}_I$ above an object $I \in \mathbb{B}$ is seen as the category describing the logic in context I. If we think of p as a model of predicate logic, then each fibre category is a poset (or preorder). But the definition of quotients below applies to a more general (non-poset) situation.

We assume that the fibration $\begin{smallmatrix}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{smallmatrix}$ has—besides finite products in its base category and fibred finite products—at least equality. This means that for each pair of objects $I, J \in \mathbb{B}$, the contraction functor $\Delta(I,J)^*$ induced by the parametrized diagonal

$$\Delta(I,J) = id \times \pi' {:}\, I \times J \mathrel{\perp\!\!\!\rightarrow} (I \times J) \times J$$

has a left adjoint $\mathrm{Eq}_{(I,J)}$ (plus a Beck-Chevalley and a Frobenius condition). In particular, we then have that for each ordinary diagonal $\Delta(I) = \langle id, id\rangle {:}\, I \to I \times I$ the functor $\Delta(I)^*$ has a left adjoint Eq_I. We form a new fibration $\begin{smallmatrix}\mathrm{Rel}(\mathbb{E})\\ \downarrow\\ \mathbb{B}\end{smallmatrix}$ by change-of-base (pullback) in

$$\begin{tikzcd} \mathrm{Rel}(\mathbb{E}) \arrow[r] \arrow[d] & \mathbb{E} \arrow[d, "p"] \\ \mathbb{B} \arrow[r, "I \mapsto I \times I"] & \mathbb{B} \end{tikzcd}$$

so that the fibre $\mathrm{Rel}(\mathbb{E})_I$ is the same as the fibre $\mathbb{E}_{I\times I}$ of relations on $I \in \mathbb{B}$. Note however that in the notation $\mathrm{Rel}(\mathbb{E})$ the dependence on p is left implicit. It is not the category of relations in the category $\mathbb{E}$, but in the fibration.

There is then an ‘equality predicate’ functor

$$\mathrm{Eq}\colon \mathbb{B} \perp\!\!\!\longrightarrow \mathrm{Rel}(\mathbb{E}) \qquad \text{by} \qquad I \mapsto \mathrm{Eq}(I) = \mathrm{Eq}_I(1I)$$

where $1I$ is the terminal object in the fibre $\mathbb{E}_I$. A morphism $u\colon I \to J$ in $\mathbb{B}$ is mapped to the composite

$$\mathrm{Eq}(I) = \mathrm{Eq}_I(1I) \perp\!\!\!\longrightarrow (u \times u)^*(\mathrm{Eq}_J(1J)) \perp\!\!\!\longrightarrow \mathrm{Eq}_J(1J) = \mathrm{Eq}(J)$$

where the first part of this map is obtained by transposing the following composite accross the adjunction $\mathrm{Eq}_I \dashv \Delta(I)^*$.

$$1I \cong u^*(1J) \overset{u^*(\eta_J)}{\perp\!\!\!\longrightarrow} u^*\Delta(J)^*\mathrm{Eq}_J(1J) \cong \Delta(I)^*(u \times u)^*(\mathrm{Eq}_J(1J))$$

It may be clear that the functor Eq is a section of the fibration of relations.

For a morphism $u\colon I \to J$ we write

$$\mathrm{Ker}(u) \overset{\mathrm{def}}{=} (u \times u)^*(\mathrm{Eq}(J)) \in \mathrm{Rel}(\mathbb{E})_I$$

for the kernel relation $u(i) = u(i')$. This operation $u \mapsto \mathrm{Ker}(u)$ can be extended to a functor $\mathbb{B}^{\to} \to \mathrm{Rel}(\mathbb{E})$ commuting with the domain functor $\mathrm{dom}\colon \mathbb{B}^{\to} \to \mathbb{B}$.

We can now state our main notion.

4.1. Definition. Let $\left.\begin{array}{c}\mathbb{E}\\ \downarrow{\scriptstyle p}\\ \mathbb{B}\end{array}\right.$ be a fibration as above. We say that p **has quotients** if the equality predicate functor $\mathrm{Eq}\colon \mathbb{B} \to \mathrm{Rel}(\mathbb{E})$ has a left adjoint.

This left adjoint maps a relation $R \in \mathrm{Rel}(\mathbb{E})_I = \mathbb{E}_{I \times I}$ to the quotient object $I/R \in \mathbb{B}$. The unit η_R is a map $R \to \mathrm{Eq}(I/R)$ in $\mathrm{Rel}(\mathbb{E})$. Its underlying map in $\mathbb{B}$ will be written as $c_R\colon I \to I/R$. It is the canonical map associated with the quotient.

Notice that if Eq has a left adjoint, then it must preserve products. Thus we get $\mathrm{Eq}(J \times I) \cong (\pi \times \pi)^*(\mathrm{Eq}(J)) \times (\pi' \times \pi')^*(\mathrm{Eq}(I))$, since the latter is the cartesian product in the category $\mathrm{Rel}(\mathbb{E})$ of relations. This means that equality on products is componentwise equality. Further, we can say that equality on maps is pointwise if Eq preserves exponents. This means informally that

$$\mathrm{Eq}(J \Rightarrow K)(f, g) \cong \forall j, j'\colon J.\, \mathrm{Eq}(J)(j, j') \supset \mathrm{Eq}(K)(f(j), f(j'))$$

see also [2, End of Section 4.4].

There are the following two variations.

4.2. Definition. Let $\left.\begin{array}{c}\mathbb{E}\\ \downarrow{\scriptstyle p}\\ \mathbb{B}\end{array}\right.$ be a fibration with quotients as above.

(i) We say that the quotients satisfy the **Frobenius condition** if for a relation R on I and an object $J \in \mathbb{B}$ we form the relation

$$J^*(R) \overset{\mathrm{def}}{=} (\pi \times \pi)^*(\mathrm{Eq}(J)) \times (\pi' \times \pi')^*(R) \quad \text{on } J \times I$$

then the canonical map

$$(J \times I)/J^*(R) \perp\!\!\!\longrightarrow J \times (I/R)$$

is an isomorphism.

(ii) And if p is a preorder fibration, then we say that **quotients are effective** if for each equivalence relation R on I (in the logic of the fibration p), the unit $\eta_R\colon R \to \mathrm{Eq}(I/R)$ is cartesian.

The canonical map in (i) is obtained by transposing the following composite

$$\begin{tikzcd}
J^*(R) = (\pi \times \pi)^*(\mathrm{Eq}(J)) \times (\pi' \times \pi')^*(R) \arrow[d, "id \times (\pi' \times \pi')^*(\eta)"] \\
(\pi \times \pi)^*(\mathrm{Eq}(J)) \times (\pi' \times \pi')^*(\mathrm{Eq}(I/R)) \cong \mathrm{Eq}(J \times (I/R))
\end{tikzcd}$$

accross the quotient-adjunction. One can show that if the base category $\mathbb{B}$ has exponents $\Rightarrow$ and equality is pointwise, then quotients automatically satisfy Frobenius. And Lemma 2.2 shows that, conversely, Frobenius implies pointwise equality.

In (ii) we restrict ourselves to preorder fibrations, so that we have no dependence on the proofs that R is an equivalence relation. And in this preorder case, all canonical maps $c_R\colon I \to I/R$ are epis in the basis $\mathbb{B}$.

4.3. Examples. (i) For a category $\mathbb{B}$ with finite limits, the subobject fibration $\begin{smallmatrix}\mathrm{Sub}(\mathbb{B})\\ \downarrow\\ \mathbb{B}\end{smallmatrix}$ always has equality given by equalizers. The quotient of a relation $\langle \pi_0, \pi_1 \rangle\colon R \rightarrowtail I \times I$ on I is the coequalizer

$$\begin{tikzcd}
R \arrow[r, shift left, "\pi_0"] \arrow[r, shift right, "\pi_1"'] & I \arrow[r, two heads, "c_R"] & I/R
\end{tikzcd}$$

The above notion of effectivity for quotients means that there is a pullback square

$$\begin{tikzcd}
R \arrow[r] \arrow[d, tail] & I/R \arrow[d, tail, "\Delta(I/R)"] \\
I \times I \arrow[r, "c_R \times c_R"] & (I/R) \times (I/R)
\end{tikzcd}$$

This expresses that R is the kernel of its own coequalizer. But that's equivalent to saying that R is the kernel of some map. And this latter formulation is the usual one in category theory.

(ii) In a similar way one has for a category $\mathbb{B}$ with finite limits, that the codomain fibration $\begin{smallmatrix}\mathbb{B}^{\to}\\ \downarrow\\ \mathbb{B}\end{smallmatrix}$ has equality by diagonals. And it has quotients if and only if the category $\mathbb{B}$ has coequalizers. Indeed, for a parallel pair $f, g\colon R \rightrightarrows I$, the quotient map $I \to I/R$ satisfies precisely the properties to make it the coequalizer of f, g. This is because for this codomain fibration, $\mathrm{Rel}(\mathbb{B}^{\to})$ is the category $\mathbb{B}^{\rightrightarrows}$ of parallel maps in $\mathbb{B}$. And the equality functor $\mathbb{B} \to \mathbb{B}^{\rightrightarrows}$ is the diagonal, mapping $X \in \mathbb{B}$ to the pair of identity maps $X \rightrightarrows X$. We thus see that our definition is more general than the usual definition of coequalizers.

(iii) If X is a poset with bottom $\bot$ and top $\top$ elements, then the family fibration $\begin{smallmatrix}\mathrm{Fam}(X)\\ \downarrow\\ \mathbf{Sets}\end{smallmatrix}$ has equality given for a family $x = (x_{(i,j)})_{(i,j)\in I\times J}$ by

$$\mathrm{Eq}(x)_{(i,j,j')} \;=\; \bigvee\{x_{(i,j)} \mid j = j'\} \;=\; \begin{cases} x_{(i,j)} & \text{if } j = j' \\ \bot & \text{else} \end{cases}$$

Then for a function $u\colon I \to J$, the kernel $\mathrm{Ker}(u)$ as relation on I is given by

$$\mathrm{Ker}(u)_{(i,i')} \;=\; \bigvee\{\top \mid u(i) = u(i')\} \;=\; \begin{cases} \top & \text{if } u(i) = u(i') \\ \bot & \text{else} \end{cases}$$

For a relation $r = (r_{(i,i')})_{i,i'\in I}$ on I in $\mathrm{Fam}(X)$, consider the relation $R = \{(i,i') \mid r_{(i,i')} \neq \bot\} \subseteq I \times I$ and let $\overline{R} \subseteq I \times I$ be the least equivalence relation containing R. Then we get a quotient $I/r \overset{\mathrm{def}}{=} I/\overline{R}$ in **Sets**, with canonical map $c_r = [\bot]\colon I \to I/\overline{R}$. The adjunction boils down to $r \leq \mathrm{Ker}(u) \;\Leftrightarrow\; c_r$ factors through u (i.e. there is a function $f\colon I/\overline{R} \to J$ with $f \circ c_r = u$).

(iv) We can also give a term model of the logic described in Section 2. There is the base category $\mathbb{B}$ with types $\sigma\colon\mathsf{Type}$ as objects and equivalence classes (under conversion) of terms $x\colon\sigma \vdash M(x)\colon\tau$ as morphisms $\sigma \to \tau$. The total category $\mathbb{E}$ as predicates $(x\colon\sigma \vdash \varphi(x)\colon\mathsf{Prop})$ as objects. A morphism $(x\colon\sigma \vdash \varphi(x)\colon\mathsf{Prop}) \to (y\colon\tau \vdash \psi(y)\colon\mathsf{Prop})$ is a map $M\colon\sigma \to \tau$ in $\mathbb{B}$ with $x\colon\sigma \mid \varphi(x) \vdash \psi(M(x))$. There is then an obvious projection functor $\mathbb{E} \to \mathbb{B}$, which is a fibration.

We can form the category $\mathrm{Rel}(\mathbb{E})$. It has relations $(x,x'\colon\sigma \vdash R(x,x')\colon\mathsf{Prop})$ as objects. And a morphism $(x,x'\colon\sigma \vdash R(x,x')\colon\mathsf{Prop}) \to (y,y'\colon\tau \vdash S(y,y')\colon\mathsf{Prop})$ is a morphism $M\colon\sigma \to \tau$ in $\mathbb{B}$ with $x,x'\colon\sigma \mid R(x,x') \vdash S(M(x),M(x'))$. The equality predicate functor $\mathrm{Eq}\colon\mathbb{B} \to \mathrm{Rel}(\mathbb{E})$ is then given by $\tau \mapsto (y,y'\colon\tau \vdash y =_\tau y'\colon\mathsf{Prop})$.

Quotient types as used above constitute a left adjoint to this functor Eq. One maps a relation $(x,x'\colon\sigma \vdash R(x,x')\colon\mathsf{Type})$ to the quotient object σ/R in $\mathbb{B}$. The adjunction involves a bijective correspondence between terms M and N in

$$\frac{(x,x'\colon\sigma \vdash R(x,x')\colon\mathsf{Prop}) \xrightarrow{M} (y,y'\colon\tau \vdash y =_\tau y'\colon\mathsf{Prop})}{\sigma/R \xrightarrow[N]{} \tau}$$

This correspondence is given by

$$M(x) \mapsto \mathsf{pick}\ x\ \mathsf{from}\ a\ \mathsf{in}\ M(x) \qquad \text{and} \qquad N(a) \mapsto N[[x]/a]$$

The (β)- and (η)-conversions precisely say that these operations are each others inverses. And Proposition 2.6 tells that the Frobenius condition automatically holds. This is because of the syntactical formulation with contexts Γ.

There are alternative ways to express that a fibration has quotients. We just mention them and leave the proofs to the interested reader.

4.4. Proposition. *Let* $\begin{array}{c}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{array}$ *be a fibration with equality (as above). The following statements are then equivalent.*

(i) *The fibration p has quotients*

(ii) *The kernel functor* $\mathrm{Ker}\colon \mathbb{B}^{\to} \to \mathrm{Rel}(\mathbb{E})$ *has a left adjoint* $(R \in \mathbb{E}_{I\times I}) \mapsto (c_R\colon I \to I/R)$ *commuting with the domain functor and such that the unit and counit of the adjunction are vertical. This left adjoint then maps opcartesian morphisms to pushout squares.*

(iii) *For each relation R on I, the functor*

$$\begin{array}{ccc} I\backslash\mathbb{B} & \perp\!\!\!\rightarrow & \mathbf{Sets} \\ \Big(I \overset{u}{\perp\!\!\!\rightarrow} J\Big) & \mapsto & \mathrm{Rel}(\mathbb{E})_I\Big(R,\ \mathrm{Ker}(u)\Big) \end{array}$$

is representable—where $I\backslash\mathbb{B}$ is the 'coslice' comma category $(I \downarrow \mathbb{B})$ of objects under I. □

Finally, for a fibration $\begin{array}{c}\mathbb{E}\\ \downarrow p\\ \mathbb{B}\end{array}$ we like to mention the formal similarity in logic between quotients $R \in \mathbb{E}_{I\times I} \mapsto (c_R\colon I \twoheadrightarrow I/R)$ and separation $X \in \mathbb{E}_I \mapsto (\pi_X\colon \{i\colon I \mid X_i\} \rightarrowtail I)$. The former is described by a left adjoint to equality $\mathrm{Eq}\colon \mathbb{B} \to \mathrm{Rel}(\mathbb{E})$, and the latter by a right adjoint to truth $\top\colon \mathbb{B} \to \mathbb{E}$. Also for separation, there is a result like Proposition 4.4.

Acknowledgement

Thanks to Martin Hofmann for sharing his experience with quotient types.

References

[1] R.L. Constable *et al. Implementing Mathematics with the Nuprl Proof Development System.* Prentice Hall, 1986.

[2] C. Hermida. *Fibrations, Logical Predicates and Indeterminates.* PhD thesis, Univ. Edinburgh, 1993. Techn. rep. LFCS-93-277. Also available as Aarhus Univ. DAIMI Techn. rep. PB-462.

[3] M. Hofmann. Elimination of extensionality and quotient types in martin-löf type theory. In H. Barendregt and T. Nipkow, editors, *Proceedings of "Types for Proofs and Programs" at Nijmegen*, number 806 in Lect. Notes Comp. Sci., pages 166–190. Springer, Berlin, 1994.

[4] B. Jacobs and T. Melham. Translating dependent type theory into higher order logic. In M. Bezem and J.F. Groote, editors, *Typed Lambda Calculi and Applications*, number 664 in Lect. Notes Comp. Sci., pages 209–229. Springer, Berlin, 1993.

[5] P.T. Johnstone. *Topos Theory.* Academic Press, London, 1977.

[6] S. Lang. *Algebra.* Addison Wesley, 2^{nd} rev. edition, 1984.

[7] W. Phoa. An introduction to fibrations, topos theory, the effective topos and modest sets. Technical Report LFCS–92–208, Edinburgh Univ., 1992.