Joachim Lambek
Philip Scott

An Exactification of the Monoid of Primitive Recursive Functions

Abstract. We study the monoid of primitive recursive functions and investigate a one-step construction of a kind of exact completion, which resembles that of the familiar category of modest sets, except that the partial equivalence relations which serve as objects are recursively enumerable. As usual, these constructions involve the splitting of symmetric idempotents.

Keywords: primitive recursive function, regular and exact category, pers, idempotent splitting completion, relation calculus.

1. Introduction

One may think that mathematics originated with geometry and computer science with arithmetic. In fact, both these subjects were preceded by the algebra of relations. Though not a formal discipline, this was implicit in the kinship descriptions propagated by the older women of a tribe and could involve some rather sophisticated calculations.

Kinship relations were only analyzed formally by anthropological linguists in the twentieth century, most spectacularly when Lounsbury [Loun65] employed a system of binary relations with clever rewrite rules to make sense of the bizarre kinship terminology of the Trobriand islanders uncovered by Malinowski [Mal32].

Logicians had been looking at relations in the nineteenth century starting with pioneering work of Pierce and Schroeder, while algebraists employed them in the twentieth century to explain the constructions used for proving the butterfly and snake lemmas in homological algebra [Lam96].

Many mathematicians fail to distinguish between binary relations and their graphs. In doing so, they may miss an interesting observation already in the category of sets. If θ is an equivalence relation on a set X, let $[\theta]$ denote its graph, viewed as a subset of $X \times X$, hence equipped with a jointly monic pair of mappings into X. Then the left fork

$$[\theta] \rightrightarrows X \longrightarrow X/\theta$$

Presented by **Wojciech Buszkowski**; *Received* February 12, 2004

is *exact*, in the sense that

$$[\theta] \rightrightarrows X$$

is the kernel of the surjection $X \to X/\theta$ and the latter is the coequalizer of the former.

We were drawn to take another look at binary relations from our study of the free topos $\mathcal{F}$, the Tarski-Lindenbaum category of pure intuitionistic type theory [LS86]. Its objects are closed terms α of type PA, modulo provable equality, where A is any type and PA is the type of all sets of elements of type A. Its arrows $\rho : \alpha \to \beta$, where β is a closed term of type PB, are provably functional relations, also modulo provable equality. In our investigation of intuitionistic principles (via gluing, also known as the Freyd cover of $\mathcal{F}$), we needed the global sections functor $\Gamma = Hom(1, -) : \mathcal{F} \to \mathcal{S}$, where $\mathcal{S}$ is "the" category of sets, there being some doubt about the definite article. While $\mathcal{F}$ may be acceptable as the category of sets by moderate intuitionists ([LS86], pp. 124-128), all toposes in which the terminal object is a generator are possible candidates for such a category for classical mathematicians ([McL92], pp. 211-212).

Global sections $a : 1 \to \alpha$ are essentially closed terms of type A such that $a \in \alpha$ is provable, again modulo provable equality. We were wondering why $\Gamma(\alpha)$ should live in $\mathcal{S}$. After all, the mathematical category of sets does not contain (say) sets of bananas, so why should it contain sets of global sections of another category? One way to answer this question is to borrow an idea of Gödel's. The closed terms of pure intuitionistic type theory can be numbered, never mind how. Now let $\Gamma(\alpha)$ be the set of all Gödel numbers $\#a$ of closed terms a of type A for which $a \in \alpha$ is provable, modulo the equivalence relation: $\#a \equiv \#a'$ iff the equation $a = a'$ is provable. Furthermore, if $\rho : \alpha \to \beta$ is an arrow of $\mathcal{F}$, let $\Gamma(\rho)(\#a) = \#\Gamma(\rho a)$, where $b = \rho a$ means (in the present notation) $b \rho a$, where $a \in \alpha$ and $b \in \beta$.

We have thus observed that the global sections functor $\Gamma : \mathcal{F} \to \mathcal{S}$ lands in a small subcategory of $\mathcal{S}$, whose objects may be viewed as equivalence relations on subsets of $\mathbb{N}$, hence partial equivalence relations on $\mathbb{N}$. In fact they turn out to be recursively enumerable partial equivalence relations and the arrows are induced by recursively enumerable relations (or, equivalently, partial recursive functions, as we shall see). A related small category is called $\mathcal{P}er$, also known as the category of *modest sets* [Ros91, BFSS90], in which *all* partial equivalence relations on $\mathbb{N}$ are admitted as objects, not just the recursively enumerable ones. (This was so because the category in question was intended to be internally complete, which is not our concern here). To distinguish our category from the usual $\mathcal{P}er$, we shall denote it by $\widetilde{\mathcal{N}}$, $\mathcal{N}$ being the monoid of primitive recursive functions.

Here we consider a more general situation. Let $\mathcal{R}$ be a partially ordered category with involution (denoted $\breve{}$), and assume that the hom-sets are $\wedge$-semilattices. We think of $\mathcal{R}$ as a category of *relations*. Consider a non-full subcategory $\mathcal{C}$ of *functions*, i.e. relations $f : A \to B$ such that $ff^{\smallsmile} \leq 1_B$ and $1_A \leq f^{\smallsmile}f$. Assume that every relation $A \xrightarrow{R} B$ has the form $R = fg^{\smallsmile}$, where $f : C \to B$ and $g : C \to A$ are functions from some object $\mathcal{C}$. It follows in particular that a composition $(fg^{\smallsmile})(hk^{\smallsmile})$ should be a relation, which is so if the equation $g^{\smallsmile}h = uv^{\smallsmile}$ holds, for some u and v. In this case the original composite in question becomes $(fu)(kv)^{\smallsmile}$. We are interested in two special cases that have been studied in the literature.

(Case 1). $\mathcal{C} = \mathcal{N}$ is the monoid of primitive recursive functions $\mathbb{N} \to \mathbb{N}$ and $\mathcal{R}$ is the category of recursively enumerable (= r.e.) relations on $\mathbb{N}$, that is, binary relations whose graphs are r.e. subsets of $\mathbb{N} \times \mathbb{N}$. The equation $g^{\smallsmile}h = uv^{\smallsmile}$ then follows from the observation that every recursive set is r.e.

(Case 2). Let $\mathcal{C}$ be a regular category [Barr79] and $\mathcal{R} = \mathit{Rel}(\mathcal{C})$ be the category of relations constructed from spans in $\mathcal{C}$, as usual [Barr79, Bor94]. In particular, $\mathcal{C}$ could be an algebraic category and $\mathcal{R}$ the category of homomorphic relations, that is, binary relations $A \xrightarrow{R} B$ whose graphs are subalgebras of $B \times A$ [Lam57].

Having noticed that the construction of the category $\widetilde{\mathcal{N}}$ in Case 1 is quite similar to the construction of the *exact completion* of $\mathcal{C}$ in Case 2, we aim to bring these two constructions under one hat. One difference between the two cases is that $\widetilde{\mathcal{N}}$ is obtained from $\mathcal{N}$ by adjoining subobjects and quotient objects, while a regular category $\mathcal{C}$ already has all the subobjects that are needed, hence only total (reflexive) equivalence relations are required, not partial ones.

One way of dealing with Case 1 would be to first make $\mathcal{N}$ regular (by embedding it in its regular completion), and then apply the methods of Case 2. This approach may be implicit already in Freyd and Scedrov [FS90]. However we prefer to handle Case 1 by a one-step construction, which resembles that of the category $\mathcal{P}er$ in theoretical computer science and also the idempotent splitting construction (Karoubi envelope) we used for C-mononoids in our book [LS86].

2. Recursively Enumerable Relations and the Category $\widetilde{\mathcal{N}}$

Let us recall some basic definitions of the calculus of relations.

Definition 2.1. A (binary) relation R on $\mathbb{N}$ is said to be *single-valued* if $RR^\smile \subseteq I$, *total* if $I \subseteq R^\smile R$, *surjective* if $I \subseteq RR^\smile$, and *injective* if $R^\smile R \subseteq I$, where I is the identity relation on $\mathbb{N}$.

If $R = fg^\smile$, where f and g are functions $\mathbb{N} \to \mathbb{N}$, then the conditions in the definition above easily translate into: $g^\smile g \subseteq f^\smile f$, $I \subseteq g^\smile g$, $I \subseteq f^\smile f$, $f^\smile f \subseteq g^\smile g$, respectively. Recall, if $R = fg^\smile$, where $f, g \in \mathcal{N}$, we say R is a *recursively enumerable* (= r.e.) relation. A *partial recursive function* may then be defined simply as a recursively enumerable relation $fg^\smile$ which is single-valued; that is, such that $g^\smile g \subseteq f^\smile f$. (This is surely a simpler definition than the usual one involving the minimization scheme.)

Definition 2.2. A *partial equivalence relation* (per) on $\mathbb{N}$ is a symmetric, transitive relation, i.e. a relation A satisfying $A^\smile \subseteq A$ and $AA \subseteq A$.

It follows that a per is a *symmetric idempotent*: $A^\smile = A$ and $AA = A$. For example, for the latter, if $a'Aa$, then $a'Aa \wedge aAa' \wedge a'Aa$, hence $a'AAAa$, and thus $A \subseteq A(AA) \subseteq AA$.

Let R be an r.e. relation on $\mathbb{N}$. We wish to consider r.e. relations R between *pers* A and B. We write (B, R, A) for such a relation, which allows us to keep in mind the source A and target B. The relation (B, R, A) should satisfy

(0) $RA = R = BR$

equivalently, $BRA = R$.

A relation (B, R, A) satisfying (0) is

(1) *Single-valued*	if	$RR^\smile \subseteq B$
(2) *Total*	if	$A \subseteq R^\smile R$
(3) *Surjective*	if	$B \subseteq RR^\smile$
(4) *Injective*	if	$R^\smile R \subseteq A$

The relation (B, R, A) is said to be a *functional relation* or a *function from A to B* if it is single-valued and total. The following facts are an easy calculation:

Proposition 2.3. *Let (B, R, A) and (C, S, B) be functions in the sense above. Then*

(i) *Their composite (C, SR, A) is a function;*
(ii) *If (B, R, A) and (C, S, B) are surjective or injective, then so is their composite;*
(iii) *If (C, SR, A) and (B, R, A) are surjective, then so is (C, S, B).*
(iv) *If (C, SR, A) and (C, S, B) are injective, then so is (B, R, A).*

DEFINITION 2.4. $\widetilde{\mathcal{N}}$ is the category whose objects are r.e. pers, and whose arrows (B, R, A) are r.e. functional relations. $\widetilde{\mathcal{N}}$ is a full subcategory of the category $\mathcal{P}er$, whose objects are arbitrary pers, and whose arrows (B, R, A) are r.e. functional relations.

It is sometimes convenient to forget about condition (0) and to say that a relation R *induces* a function from A to B, denoted $R : A \to B$, if

(1′) $RAR^{\smile} \subseteq B$
(2′) $A \subseteq R^{\smile}BR$

Indeed, (1′) follows from (1) and $RA \subseteq R$, and (2′) follows from (2) and $R \subseteq BR$. The conditions (1′) and (2′) are the induced versions of single-valuedness and totality, respectively.

We can then prove a weaker version of (0):

(0′) $RA \subseteq BR$

since, using (1′) and (2′) and the fact that A and B are idempotents,

$$RA = RAA \subseteq RAR^{\smile}BR \subseteq BBR = BR.$$

Injectivity and surjectivity of $R : A \to B$ can now be written as

(3′) *Surjective* if $B \subseteq BRAR^{\smile}B$
(4′) *Injective* if $AR^{\smile}BRA \subseteq A$

When do two functional relations R and S between A and B induce the same function?

PROPOSITION 2.5. *Let R and S be functions from A to B. The following are equivalent (and assert that R and S induce the same function $A \to B$):*

(a) $RAS^{\smile} \subseteq B$
(b) $A \subseteq R^{\smile}BS$
(c) $BRA = BSA$

In particular, if $R \subseteq S$ or $S \subseteq R$ then R and S induce the same function .

PROOF. Assume (a). Then $A \subseteq AAA \subseteq R^{\smile}BRAS^{\smile}BS \subseteq R^{\smile}BBBS = R^{\smile}BS$, hence (*b*). Now assuming (b), then $BRA \subseteq BRAAA \subseteq BRAR^{\smile}BSA \subseteq BBBSA = BSA$, and similarly for the converse inclusion, hence (c). Finally, assume (c). Then $RAS^{\smile} = RAAAS^{\smile} \subseteq BRAAS^{\smile} = BSAAS^{\smile} \subseteq BSAS^{\smile}B \subseteq BBB = B$, hence (a). (Note that $AS^{\smile} \subseteq SB^{\smile}$ follows from $SA \subseteq BS$, which holds by (0′)). The last remark follows immediately from (c). ∎

If it is not assumed that condition (0) is satisfied, we will write

$$[B, R, A] =_{def} (B, BRA, A)$$

for the function induced by R. We note that the composition $[C, S, B][B, R, A]$ may be written as either $[C, SBR, A]$ or $[C, SR, A]$, since by $(0')$ $CSRA = CSRAA \subseteq CSBRA$, and therefore SBR and SR induce the same function $A \to C$, by the last remark of Proposition 2.5.

Remark 2.6. Proposition 2.5 may be exploited to replace R by the partial recursive function $R^{\#}$, as follows. Writing $R = gf^{\smile}$ for primitive recursive f, g, let

$$R^{\#}a \quad = \quad g(\mu n(f(n) = a)),$$

where $\mu n(\cdots)$ means "the smallest n such that $\cdots$ " . Thus, if we forget condition (0), we may replace r.e. relations by partial recursive functions, as is the custom for describing $\mathcal{P}er$ in the literature.

Since functions induced by (numerical) partial functions need not obey condition (0), from now on we only assume conditions $(1')$ and $(2')$ in the definition of function, unless we state otherwise. In fact, $(2')$ suffices, since if F is such a partial function and if $A \subseteq F^{\smile}BF$ then $FAF^{\smile} \subseteq FF^{\smile}BFF^{\smile} \subseteq IBI = B$.

Thus, if F is a partial recursive function, $[B, F, A] = (B, BFA, A)$ is a function $A \to B$ if and only if $A \subseteq F^{\smile}BF$. In particular, letting $F = I$, the identity function on $\mathbb{N}$, $[B, I, A] = (B, BA, A)$ is a function if and only if $A \subseteq B$. The functions induced by the identity form a subcategory of $\widetilde{\mathcal{N}}$ (cf. Section 4 below).

3. $\mathcal{P}er$ and C-monoids

It is well-known that $\mathcal{P}er$ is cartesian closed, locally cartesian closed, and even has (internal) products [BFSS90, Ros91, LM91, Lam93], but this is not quite the case for $\widetilde{\mathcal{N}}$. The easiest way to see $\mathcal{P}er$ is cartesian closed is to make use of the following partial recursive functions: I, O, P, Q, E and the operations $\langle F, G\rangle$ and H^* defined on given partial recursive functions F, G, H as follows:

$$Ix = x,\ Ox = 0,\ P\langle x, y\rangle = x,\ Q\langle x, y\rangle = y,$$

$$\langle F,\ G\rangle z = \langle Fz, Gz\rangle,\ E\langle x, y\rangle = \{x\}y,\ \{H^*x\}y = H\langle x, y\rangle.$$

Here $\langle -, - \rangle : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is the standard Cantor (primitive recursive) bijection, with projections P and Q, $\{n\}$ is the usual Kleene notation for the nth partial recursive function (i.e. the partial function calculated by the nth program in some standard enumeration), and E and H^* are functions associated with Kleene's Enumeration and S^m_n theorems [Kl52].

One easily establishes the following inclusions, which define what might be called a *partially ordered C-monoid.* That is, following the nomenclature of our book [LS86], we have a partially ordered monoid $\mathcal{M}$, with extra structure $(P, Q, E, ^*, \langle -, - \rangle)$ satisfying:

$$\begin{array}{l} P\langle F, G\rangle \subseteq F \\ Q\langle F, G\rangle \subseteq G \\ H \subseteq \langle PH, QH\rangle \\ H \subseteq E\langle H^* P, Q\rangle \\ K \subseteq (E\langle KP, Q\rangle)^* \end{array}$$

Here inclusion indicates that if the left hand side is defined, so is the right hand side. In the last three inclusions, we could have replaced $\subseteq$ by $=$, but not in the first two. For example, the LHS of $P\langle F, G\rangle z = P\langle Fz, Gz\rangle = Fz$ requires that both Fz and Gz are defined, which is more than necessary for the RHS.

The cartesian closed structure of $\mathcal{P}er$ (with respect to the above-mentioned notion of inclusion) may now be defined as follows:

$$\begin{array}{rcl} 1_A &=& [A, I, A] \\ [C, G, B][B, F, A] &=& [C, GF, A] \\ x \top y &\Leftrightarrow& x = 0 = y \\ x(A \times B)y &\Leftrightarrow& (Px)A(Py) \wedge (Qx)B(Qy) \\ (\text{ i.e. } A \times B &=& P^{\smile}AP \cap Q^{\smile}BQ\ ) \\ uC^B v &\Leftrightarrow& B \subseteq \{u\}^{\smile} C\{v\} \\ !_A &=& [\top, O, A] \\ \pi_{A,B} &=& [A, P, A \times B] \\ \pi'_{A,B} &=& [B, Q, A \times B] \\ \varepsilon_{C,B} &=& [C, E, C^B \times B] \\ \langle\ [A, F, C], [B, G, C]\ \rangle &=& [A \times B, \langle F, G\rangle, C] \\ [B, H, C \times A]^* &=& [B^A, H^*, C] \end{array}$$

All this works for $\widetilde{\mathcal{N}}$ as well, except the exponential structure. Note that arbitrary products in $\mathcal{P}er$ may be defined as intersections, but this does not work in $\widetilde{\mathcal{N}}$, since arbitrary intersections of r.e. pers need not be r.e.

$\widetilde{\mathcal{N}}$ is cartesian with respect to the product structure induced from $\mathcal{P}er$; but unfortunately $\widetilde{\mathcal{N}}$ is not cartesian closed with respect to this induced structure, since the per C^B may fail to be r.e. even if C and B are, as the next example shows. We have not checked if $\widetilde{\mathcal{N}}$ is cartesian closed by another construction.

Example 3.1. In $\widetilde{\mathcal{N}}$, the per C^B, where $B = C = \mathbb{N} \times \mathbb{N}$, is not r.e. Indeed,

$$\begin{aligned} mC^B n &\Leftrightarrow \mathbb{N} \times \mathbb{N} \subseteq \{m\}^{\smile}(\mathbb{N} \times \mathbb{N})\{n\} \\ &\Leftrightarrow \forall i, j \in \mathbb{N}\ \exists k, l \in \mathbb{N}\ (\ \{m\}(i) = k\ \wedge\ \{n\}(j) = l\ ) \end{aligned}$$

In particular, if C^B would be r.e., its diagonalization would be too. Thus the set

$$\{m \in \mathbb{N} \mid \{m\}\ \textit{is a total function}\ \}$$

would be an r.e. set, which is well-known to be false (see e.g. [Cutl80], Theorem 2.9).

4. Regularity and Exactness of $\widetilde{\mathcal{N}}$

Following the discussion at the end of Section 2 and similar notions in $\mathcal{P}er$, in $\widetilde{\mathcal{N}}$ we may consider the subcategory of functions induced by the identity, i.e. functions of the form $[B, I, A]$, where $A \subseteq B$. Such a map is a *canonical surjection* if $BAB = B$ and a *canonical injection* if $ABA = A$.

Proposition 4.1. *Any function in $\widetilde{\mathcal{N}}$ induced by a partial recursive function may be factored as follows*[1]*:*

$$\begin{array}{ccc} A & \xrightarrow{\quad F \quad} & B \\ {\scriptstyle I}\downarrow & & \uparrow{\scriptstyle I} \\ C = AF^{\smile}BFA & \xrightarrow{F} & BFAF^{\smile}B = D \end{array}$$

Thus

$$[B, F, A] = [B, I, D][D, F, C][C, I, A]$$

where

[1] A different factorization for arbitrary maps in $\mathcal{P}er$ is given in [BFSS90], Proposition 2.4.

$[B, I, D]$ is a canonical injection, the *image* of $[B, F, A]$
$[C, I, A]$ is a canonical surjection, the *coimage* of $[B, F, A]$
$[D, F, C]$ is an isomorphism with inverse $[C, (AF^{\smile}B)^{\#}, D]$.

PROOF. Note that by the remark at the end of Section 2, the bottom row of the above square denotes a function, since C and D are partial equivalence relations and

$$C = AF^{\smile}BFA \subseteq F^{\smile}BBFA = F^{\smile}BFAA \subseteq F^{\smile}BFA(F^{\smile}BF) = F^{\smile}DF.$$

since $FA \subseteq BF$ by $(0')$, hence $AF^{\smile} \subseteq F^{\smile}B$.

To see that $(AF^{\smile}B)^{\#}$ or, equivalently, $R = AF^{\smile}B$ induces a function $D \to C$ we note that

$$RDR^{\smile} = AF^{\smile}BFAF^{\smile}BFA = CC = C\ ,$$

$$R^{\smile}CR = BFAF^{\smile}BFAF^{\smile}B = DD = D\ .$$

Moreover, $[C, R, D]$ is the inverse of $[D, F, C]$ since $RF = AF^{\smile}BF \supseteq AA = A$ and $FR = FAF^{\smile}B \subseteq BB = B$, hence the induced functions satisfy

$$[C, R, D][D, F, C] = [C, RF, C] = [C, A, C] = [C, I, C]$$

$$[D, F, C][C, R, D] = [D, FR, D] = [D, B, D] = [D, I, D]$$

Finally, to see that $(AF^{\smile}B)^{\#}$ is a partial recursive function we invoke the fact that the partial equivalence relations A and B are recursively enumerable. This argument works for $\widetilde{\mathcal{N}}$ but not for $\mathcal{P}er$. ■

In what follows, we call surjective and injective functions *surjections* and *injections*, respectively.

COROLLARY 4.2. *In the situation above, $F : A \to B$ is a surjection iff $D = B$. Similarly, F is an injection iff $C = A$. So a surjection factors as a canonical surjection followed by an isomorphism and similarly an injection factors as an isomorphism followed by a canonical injection. Moreover, $F : A \to D$ is a surjection, $F : C \to B$ is an injection, and $F : C \to D$ is both an injection and surjection.*

PROOF. For example, $F : A \to D$ is a surjection, since

$$(DFA)(DFA)^{\smile} = DFAF^{\smile}D = DBFAF^{\smile}BD = DDD = D\ .$$

Since $I : A \to D$ is a surjection, so is $F : C \to D$ by Proposition 2.3 (iii). ■

REMARK 4.3. Proposition 4.1 applies equally to $\mathcal{P}er$, except that the arrow $F : C \to D$ is a an injection and surjection, but not necessarily an iso. As pointed out to us by P. Hofstra and P. Selinger, recursion-theoretic arguments based on the Halting Problem may be used to give examples of arrows which are injections and surjections but are not isos in $\mathcal{P}er$.

DEFINITION 4.4. A category is *regular* ([Barr79, Bor94]) if

(i) it is left exact,

(ii) every kernel pair has a coequalizer,

(iii) regular epis are stable under pullbacks.

A regular category is *exact* if in addition

(iv) every equivalence relation (in the sense of Barr) is a kernel pair.

THEOREM 4.5. $\widetilde{\mathcal{N}}$ *is an exact category.*

PROOF. (1) We already know it has a terminal object and binary cartesian products. It remains to construct equalizers.

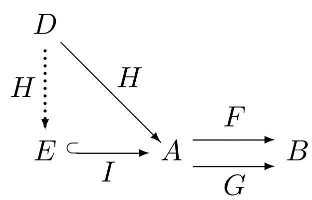
Given two parallel functions $[B, F, A], [B, G, A] : A \to B$, we define their equalizer to be $[A, I, E]$ where $E \subseteq A$ is given by $E = A \cap F^{\smile}BG$ (Recall that the intersection of two r.e. sets is r.e. In our present formalism, this may be shown as follows: $fg^{\smile} \cap hk^{\smile} = (f \times h)(g \times k)^{\smile}$, where $(f \times h)\langle x, y\rangle = \langle fx, hy\rangle$).

First, we must check that E is an equivalence relation on the domain of A. Suppose aEa', that is aAa' and $(Fa)B(Ga')$. Then $a'Aa$ and

$$(Fa')B(Fa)B(Ga')B(Ga)$$

hence $a'Ea$ and so E is symmetric. Transitivity is shown similarly. Reflexivity holds because both F and G are defined on the domain of A.

Now suppose $[A, H, D]$ equalizes $[B, F, A]$ and $[B, G, A]$:



It suffices to show that $[E, H, D]$ is a function. We have

$$D \subseteq (FH)^{\smile}B(GH) = H^{\smile}(F^{\smile}BG)H.$$

Since we also have $D \subseteq H^{\smile}EH$, then in view of the Lemma 4.6 below, we have

$$D \subseteq H^{\smile}(A \cap F^{\smile}BG)H = H^{\smile}EH.$$

It follows that $[E, H, D]$ is a function, since H is single-valued.

LEMMA 4.6. If H is single-valued, then

$$UH \cap VH \subseteq (U \cap V)H \quad \text{and} \quad H^{\smile}U \cap H^{\smile}V \subseteq H^{\smile}(U \cap V)$$

PROOF. For example, to show the former, suppose $x(UH \cap VH)y$, that is $xUHy$ and $xVHy$. Then there exist z and z' such that xUz and zHy and xVz' and $z'Hy$. Since H is single-valued, $z = z'$, hence xUz and xVz, and so $x(U \cap V)z$, and therefore $x(U \cap V)Hy$. ■

(2) Once we have equalizers, we also have pullbacks. To form the pullback of $A \xrightarrow{F} C \xleftarrow{G} B$, consider the equalizer

$$E \overset{I}{\hookrightarrow} A \times B \underset{GQ}{\overset{FP}{\rightrightarrows}} C$$

Then $A \xleftarrow{P} E \xrightarrow{Q} B$ is the required pullback. In particular,

$$E \overset{I}{\hookrightarrow} A \times A \underset{Q}{\overset{P}{\rightrightarrows}} A$$

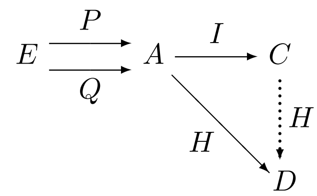
is the kernel pair of $A \xrightarrow{F} C$, where $E = (A \times A) \cap P^{\smile}F^{\smile}CFQ \subseteq A \times A$.

Without loss of generality (by Proposition 4.1, Corollary 4.2, and Proposition 2.3) we may assume $A \subseteq C$, where $C = AF^{\smile}CFA$ is the coimage of F, so that $A \xrightarrow{I} C$ is a canonical surjection. We claim that it is the coequalizer of its kernel pair $E \underset{Q}{\overset{P}{\rightrightarrows}} A$, thus rendering

$$E \underset{Q}{\overset{P}{\rightrightarrows}} A \xrightarrow{I} C$$

an exact left fork.

Suppose $[D, H, A]$ coequalizes $[A, P, E]$ and $[A, Q, E]$:



We claim that $[D, H, C]$ is a function; that is, that $C \subseteq H^{\smile}DH$.

By definition of E (which uses Cantor pairing, by definition of products in $\widetilde{\mathcal{N}}$)

$$\langle a_1, a_2\rangle E\langle a_1', a_2'\rangle \quad \text{iff} \quad (a_1 A a_1' \wedge a_2 A a_2' \wedge a_1 C a_2')$$

It follows that

$$\langle a_1, a_2\rangle E\langle a_1, a_2\rangle \quad \text{iff} \quad (a_1 A a_1 \wedge a_2 A a_2 \wedge a_1 C a_2)$$

That is, if $|A|$ is the domain of A,

$$\langle a_1, a_2\rangle \in |E| \quad \text{iff} \quad (a_1, a_2 \in |A| \wedge a_1 C a_2)$$

This shows that $|E|$ is the graph of C (and E is the equivalence relation on $|E|$ induced by that on $|A| \times |A|$) .

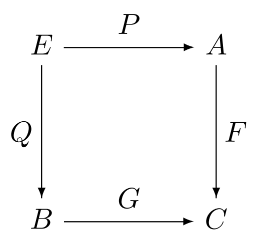
Since $|C| = |A|$, we may turn this around and say

$$a_1 C a_2 \quad \text{iff} \quad (a_1, a_2 \in |A| \wedge \langle a_1, a_2\rangle \in |E|).$$

Now, returning to the main argument, we wish to show that $C \subseteq H^{\smile}DH$. Suppose $c_1 C c_2$, that is $c_1, c_2 \in |A|$ and $\langle c_1, c_2\rangle \in |E|$. Hence $\langle c_1, c_2\rangle E\langle c_1, c_2\rangle$, and so $(Hc_1)D(Hc_2)$. Therefore, $C \subseteq H^{\smile}DH$.

(3) We now return to our main argument to show that the regular epis are stable under pullbacks. Anticipating Proposition 4.8 below (which establishes the equality between surjections and regular epis), we will in fact show that surjections are stable under pullbacks.

Consider the pullback $B \overset{Q}{\longleftarrow} E \overset{P}{\longrightarrow} A$ of $B \overset{G}{\longrightarrow} C \overset{F}{\longleftarrow} A$, where $[C, F, A]$ is a surjection, as in the diagram



Thus $C \subseteq CFAF^{\smallsmile}C$. We claim that $[B, Q, E]$ is also a surjection, that is, $B \subseteq BQEQ^{\smallsmile}B$.

Suppose b_1Bb_2. We wish to show that $b_1BQEQ^{\smallsmile}Bb_2$. Since $[C, G, B]$ is total, we have $B \subseteq BG^{\smallsmile}CGB$, hence there exist b'_1 and b'_2 such that

$$b_1Bb'_1, G(b'_1)CG(b'_2), b'_2Bb_2 \ .$$

Since F is surjective, $C \subseteq CFAF^{\smallsmile}C$. Hence there exist c_1, a_1, a_2, c_2 such that

$$G(b'_1)Cc_1, c_1 = F(a_1), a_1Aa_2, F(a_2) = c_2, c_2CG(b'_2) \ .$$

Now $b_1BQ\langle a_1, b'_1\rangle E\langle a_2, b'_2\rangle$. Recall that $E = (A \times B) \cap P^{\smallsmile}F^{\smallsmile}CGQ$ and note that $\langle a_1, b'_1\rangle(AA \times B)\langle a_2, b'_2\rangle$, since a_1Aa_1 and $b'_1Bb_1Bb_2Bb'_2$. It remans to show $\langle a_1, b'_1\rangle P^{\smallsmile}F^{\smallsmile}CGQ\langle a_2, b'_2\rangle$, that is, $F(a_1)CG(b'_2)$. Now $F(a_1) = c_1$ and $c_1CG(b'_1)$, hence $F(a_1)CG(b'_1)CG(b'_2)$, since $b'_1Bb'_2$ and $[C, G, B]$ is single-valued.

(4) We have now completed the proof that $\widetilde{\mathcal{N}}$ is a regular category (assuming Proposition 4.8) . We claim it is exact. Let

$$E \overset{I}{\hookrightarrow} A \times A$$

be an equivalence relation in $\widetilde{\mathcal{N}}$ in the sense of Barr[2], that is the image of

$$\text{Hom(B,E)} \overset{I}{\hookrightarrow} Hom(B, A \times A) \cong Hom(B, A) \times Hom(B, A)$$

is [the graph of] an equivalence relation on $Hom(B, A)$, for each object B. In particular, take $B = \top$, the terminal object of $\widetilde{\mathcal{N}}$. Then $Hom(\top, A)$ consists of all $[A, F, \top]$ for which $\top \subseteq F^{\smallsmile}AF$, i.e. $(F0)A(F0)$, so $F0 \in |A|$, the domain of A. Thus we may write $F = \hat{a}$, where $\hat{a}0 = a$, for some element $a \in |A|$. Note that $[A, \widehat{a}_1, \top] = [A, \widehat{a}_2, \top]$ if and only if a_1Aa_2. We write $[\hat{a}]$ for arrows $[A, \hat{a}, \top]$ if the meaning is clear.

Now Barr's condition for $B = \top$ asserts that $Hom(\top, E)$ induces an equivalence relation $\equiv$ in the usual sense on the hom set $Hom(\top, A)$. Note that $[\widehat{a}] \equiv [\widehat{a'}]$ if and only if the Cantor pair $\langle a, a'\rangle \in |E|$.

Define the relation C by

$$aCa' \quad \text{if and only if} \quad \langle a, a'\rangle \in |E| \quad \text{if and only if} \quad [\widehat{a}] \equiv [\widehat{a'}] : \top \to A.$$

[2]In $\widetilde{\mathcal{N}}$ every subobject is given by a canonical injection preceded by an iso (see Corollary 4.2). This need not be the case in $\mathcal{P}er$.

Observe that $A \subseteq C$, since $\equiv$ is reflexive:

$$\begin{aligned} aAa' &\Leftrightarrow [\widehat{a}] = [\widehat{a'}] : \top \to A \\ &\Rightarrow [\widehat{a}] \equiv [\widehat{a'}] : \top \to A \\ &\Leftrightarrow aCa'. \end{aligned}$$

It follows that C is an equivalence relation on $|A|$. Indeed, let $a \in |A|$. Then $[\hat{a}] \equiv [\hat{a}]$, hence aCa. If aCa' then $[\widehat{a}] \equiv [\widehat{a'}]$, hence $[\widehat{a'}] \equiv [\widehat{a}]$. and so $a'Ca$. Transitivity of C follows similarly. Moreover, C is recursively enumerable, because $|E|$ is. Thus C is an object of $\widetilde{\mathcal{N}}$.

We claim that

$$E \overset{I}{\hookrightarrow} A \times A \underset{Q}{\overset{P}{\rightrightarrows}} A$$

is the kernel pair of $A \overset{I}{\hookrightarrow} C$. As in (2) above (in the present proof of Theorem 4.5) this means that

$$\langle a_1, a_2 \rangle E \langle a_1', a_2' \rangle \quad \text{iff} \quad a_1 A a_1' \wedge a_2 A a_2' \wedge a_1 C a_2' \ .$$

Indeed the LHS holds iff

$$a_1 A a_1' \wedge a_2 A a_2' \wedge \langle a_1, a_2 \rangle \in |E| \wedge \langle a_1', a_2' \rangle \in |E| \ .$$

We may rewrite this as follows

$$[\widehat{a}_1] = [\widehat{a_1'}] \wedge [\widehat{a}_2] = [\widehat{a_2'}] \wedge [\widehat{a}_1] \equiv [\widehat{a}_2] \wedge [\widehat{a_1'}] \equiv [\widehat{a_2'}]$$

i.e.

$$[\widehat{a}_1] = [\widehat{a_1'}] \wedge [\widehat{a}_2] = [\widehat{a_2'}] \wedge [\widehat{a}_1] \equiv [\widehat{a_2'}] \ ,$$

which is equivalent to the RHS. ■

Proposition 4.7. *In $\widetilde{\mathcal{N}}$, injections are the same as monos.*

Proof. Suppose (B, M, A) is an injection, that is, $M^\smile M = A$. Suppose that (A, R, C) and (A, S, C) are such that $(B, MR, C) = (B, MS, C)$. Then (by (0))

$$R = AR = M^\smile MR = M^\smile MS = AS = S.$$

Hence (B, M, A) is a mono.

Conversely, suppose (B, M, A) is a mono. Put $M^\smile M = fg^\smile$, where f and g are primitive recursive. Then, since $I \subseteq g^\smile g$ and $MM^\smile \subseteq B$,

$$Mf \subseteq Mfg^\smile g \subseteq MM^\smile Mg \subseteq BMg = Mg$$

Therefore $[B, Mf, I] = [B, Mg, I]$, where I is the identity relation on $\mathbb{N}$. It follows that

$$(B, M, A)[A, f, I] = (B, M, A)[A, g, I],$$

hence $[A, f, I] = [A, g, I]$, that is, $AfI = AgI$, so $Af = Ag$. Therefore, $M^{\smile}M = AM^{\smile}MA = Afg^{\smile}A = Agg^{\smile}A \subseteq A$, since $gg^{\smile} \subseteq I$. Thus (B, M, A) is an injection. ■

How do we characterize surjections? On the one hand it is easy to verify that F is a surjection in $\widetilde{\mathcal{N}}$ if and only if the corresponding mapping $|A|/A \to |B|/B$ in $\mathcal{S}$, which sends the equivalence class $[a]_A$ onto the equivalence class $[F(a)]_B$, is a surjection in the usual sense. In the next proposition, we give a more intrinsic characterization.

Proposition 4.8. *Regular epis in $\widetilde{\mathcal{N}}$ are the same as surjections.*

Proof. Recall by Corollary 4.2 that every surjection is a canonical surjection followed by an isomorphism. Moreover, the proof for (2) in Theorem 4.5 showed that every canonical surjection is the coequalizer of its kernel pair, hence a regular epi.

Conversely, every regular epi $F : A \to B$ is the coequalizer of its kernel pair. Now by Proposition 4.1,

$$[B, F, A] = [B, I, D][D, F, C][C, I, A] = [B, F, C][C, I, A]$$

where the injection $[B, I, D]$ and the isomorphism $[D, F, C]$ are both injections and monos (by Proposition 4.7), hence $[B, F, C]$ is a mono. The surjection $[C, I, A]$ also coequalizes the kernel pair of F. Therefore there is a unique arrow (C, R, B) such that $(C, R, B)[B, F, A] = [C, I, A]$.

Now $[B, F, C](C, R, B)[B, F, A] = [B, F, A]$ and since $[B, F, A]$ is an epi, we have $[B, F, C](C, R, B) = [B, I, B]$. Writing $M = BFC$, we infer that $MR = BFCR = B$. Now $[B, F, C] =_{\text{def}} (B, BFC, C) = (B, M, C)$ is an injection, hence $M^{\smile}M = C$, and therefore

$$M^{\smile} = M^{\smile}B = M^{\smile}MR = CR = R$$

Thus $MM^{\smile} = MR = B$, and so $[B, F, C]$ is also a surjection. Therefore, so is $[B, F, A] = [B, F, C][C, I, A]$.

Observe that this argument depends on Proposition 4.1, which applies to $\widetilde{\mathcal{N}}$ and not to $\mathcal{P}er$. ■

Finally, we remark that by the last two propositions, in $\widetilde{\mathcal{N}}$ a map which is injective and surjective is necessarily an iso (since in any category, a morphism which is a monomorphism and a regular epi is automatically an iso).

5. Conclusion

We have shown that the monoid $\mathcal{N}$ of primitive recursive functions can be embedded into a Barr-exact category $\widetilde{\mathcal{N}}$. Our argument also shows that $\mathcal{P}er$ is regular, provided we change Definition 4.4 (iii) to say that surjections are stable under pullbacks. This also seems to be a popular definition of regularity, but it differs from the original definition in the absence of Proposition 4.8. $\mathcal{P}er$ is also regular in the original sense, but that does not follow from our argument. At first sight it seems that we have also proved that $\mathcal{P}er$ is exact. However in Barr's original definition of exactness, an equivalence relation on A was assumed to be an arbitrary subobject of $A \times A$ satisfying certain conditions. Our argument works for *canonical* subobjects of $A \times A$. As we proved, in $\widetilde{\mathcal{N}}$ every subobject is given by a canonical injection preceded by an isomorphism. However this is not the case in $\mathcal{P}er$. In fact, Proposition 4.1 in $\widetilde{\mathcal{N}}$ says $F : C \to D$ is an isomorphism, whereas in $\mathcal{P}er$, F is only an injection and surjection but not an iso.

It seems clear that $\mathcal{N} \to \widetilde{\mathcal{N}}$ is, in some sense, the best approximation of $\mathcal{N}$ by a Barr-exact category. More formally, we expect that $\mathcal{N} \to \widetilde{\mathcal{N}}$ has an appropriate universal property. Exact completions of categories with finite limits have been thoroughly discussed by many authors (e.g. [CV98, Hof03]). Unfortunately, such works do not apply here, since the monoid $\mathcal{N}$ (as a category with one object) does not have equalizers, although it does have products in view of the Cantor isomorphism $\mathbb{N} \times \mathbb{N} \cong \mathbb{N}$. On the other hand, these authors do suggest that $\widetilde{\mathcal{N}}$ may be viewed as an exact completion of its subcategory of regular projectives. Perhaps a comparison might be helpful with the categories studied by Tsalenko et al (see [Cal84]; he has changed the spelling of his name since moving to the U.S.) which admit the construction of relations (see also [Lam93]).

While $\widetilde{\mathcal{N}}$ has the advantage over $\mathcal{P}er$ in having been shown to be exact, $\mathcal{P}er$ has an advantage over $\widetilde{\mathcal{N}}$ in being a CCCP, a cartesian closed category with arbitrary formal products, which can be used for modelling polymorphic lambda calculus.

6. Acknowledgements

We are endebted to Michael Makkai, Robin Cockett, Pieter Hofstra, Pino Rosolini and Peter Selinger for helpful conversations. We wish to thank the referee for pointing out that the category $\widetilde{\mathcal{N}}$ is a pretopos and for suggesting that its topos of sheaves might be of interest. Both authors wish to acknowledge support from NSERC.

References

[BFSS90] Bainbridge, E. S., P. Freyd, A. Scedrov, and P. J. Scott, 'Functorial Polymorphism', *Theoretical Computer Science* 70 (1990), 35–64.

[Barr79] Barr, M., et. al., *Exact categories and categories of sheaves*, Springer Lecture Notes in Mathematics 236, 1971.

[Bor94] Borceux, F., *Handbook of Categorical Algebra 1*, Cambridge, 1994.

[Cal84] Calenko, M. S., et. al., *Ordered Categories with involution*, Dissertaiones Mathematicae 227, 1984.

[CV98] Carboni, A., and E. M. Vitale, 'Regular and Exact Completions', *Journal of Pure and Applied Algebra* 125 (1998), 29–117.

[Cutl80] Cutland, N. J., *Computability: An Introduction to Recursive Function Theory*, Cambridge, 1980.

[FS90] Freyd, P., and A. Scedrov, *Categories, Allegories*, North-Holland, 1990.

[Hof03] Hofstra, P., *Completions in Realizability*, Phd Thesis, Utrecht, 2003.

[Kl52] Kleene, S. C., *Introduction to Metamathematics*, Van Nostrand, New York, 1952.

[Lam57] Lambek, J., 'Goursat's theorem and the Zassenhaus lemma', *Can. J. Math.* 10 (1957), 45–56.

[Lam93] Lambek, J., 'Least fixpoints of endofunctors of cartesian closed categories', *Mathematical Structures in Computer Science* 3 (1993), 229–257.

[Lam96] Lambek, J., 'The butterfly and the serpent', in Agliano et. al., (eds.), *Logic and Algebra*, Marcel Dekker, New York, 1996, pp. 161–179.

[Lam99] Lambek, J., 'Diagram chasing in ordered categores with involution', *J. Pure and Applied Algebra* 143 (1999), 293–307.

[LS86] Lambek, J., and P. J. Scott., *Introduction to Higher Order Categorical Logic*, Cambridge Studies in Advanced Mathematics 7, Cambridge University Press, 1986.

[LM91] Longo, G., and E. Moggi, 'Constructive Natural Deduction and its ω-set interpretation', *Mathematical Structures in Comp. Sci* (1991), 215–254.

[Loun65] Lounsbury, F. G., 'Another view of Trobriand kinship categories', in E. A. Hammel, (ed.), 'Formal Semantics II', *American Anthropologist* 67 (1965), 142–185.

[Mal32] Malinowski, B., *Sexual life of savages*, Routledge and Kegan Paul, London, 1932.

[McL92] McLarty, C., *Elementary Categories, elementary toposes*, Clarendon Press, Oxford, 1992.

[Ros91] Rosolini, G., 'About modest sets', *Internat. J. Found. Comp. Sci.* 1 (1990)

J. Lambek
Department of Mathematics and Statistics,
McGill University,
805 Sherbrooke St. W,
Montreal, P.Q. H3A 2K6, Canada
lambek@math.mcgill.ca

P. Scott
Department of Mathematics and Statistics,
University of Ottawa,
Ottawa, Ontario K1N 6N5, Canada
phil@mathstat.uottawa.ca,
phil@site.uottawa.ca