International Journal of Pure and Applied Mathematics

Volume 12 No. 3 2004, 357-380

CATEGORICAL CODE CONSTRUCTIONS

G.R. Blakley[1] [§], I. Borosh[2], T. Holcomb[3], A. Klappenecker[4]

[1,2]Department of Mathematics
Texas A&M University
College Station, TX 77843-3368, USA
[1]e-mail: blakley@math.tamu.edu
[2]e-mail: borosh@math.tamu.edu

[3]Air Force Research Laboratory
3550 Aberdeen Ave SE
Kirtland AFB, NM 87117, USA

[4]Department of Computer Science
Texas A&M University
College Station, TX 77843-3112, USA
e-mail: klappi@cs.tamu.edu

Abstract: We study categories of codes and precodes. The objects in these categories capture the encoding and decoding process of error control codes, source codes, or cryptographic codes. We show that these categories are complete and cocomplete. This gives a wealth of new code constructions.

AMS Subject Classification: 94A15, 94A60, 18B99
Key Words: categories, codes, precodes, smash, split

1. Introduction

Cryptographers tend to define a cryptosystem as a family of codes, indexed by a set of keys. But what is a code, as far as a cryptographer is concerned? It seems to involve secrecy, and complicated encoding and decoding. So it is not just a subset of a Hamming space, as in information theory.

Received: March 1, 2004

[§]Correspondence author

Some of today's most famous cryptosystems, such as AES, DES, RC5, and RSA, are simple substitution ciphers. In other words, each is a family of pairs (e, d) of encode and decode permutations of a single large alphabet P, which may contain as many as 2^{4096} symbols. These permutations are inverses of one another, that is, $d \circ e$ is the identity function.

We do not use such a narrow definition of a code. We think that there are good reasons to adopt the view that e and d are encoding and decoding relations, rather than bijections. A code consists of a set P of plaintext symbols, a set C of codetext symbols, an encoding relation $e \subseteq P \times C$, and a decode relation $d \subseteq C \times P$ such that the composite relation $d \circ e$ is subdiagonal. An example is given by homophonic substitution ciphers, which may have various alternate encodes for a single plaintext symbol.

Simple substitution ciphers often have small unicity distances for reasonable languages, such as English text written in ASCII characters. For instance, DES, AES, RC5 each have a unicity distance less than about 19 bytes, assuming a key length of 128 bits or less, and RSA even has unicity distance zero. It is well known that homophone-rich and null-rich substitution ciphers have significantly larger unicity distances than simple bijection substitution ciphers, see Appendix G in [9]. In other words, apart from algorithmic details which are a low-level feature of the design process of the encode of the key settings of a cryptosystem, there are high-level, code-theoretic, structural considerations which have an important effect on the security of a design.

These facts are simple examples of a principle which the general theory of codes points up – apart from the nature or complexity of the algorithms employed in encode or decode processes which implement key settings of a cryptosystem, the code-theoretic structure of such key-settings can significantly affect security. Thus, the current emphasis on algorithmic considerations in cryptosystem design must be supplemented by due attention to code-theoretic structure.

The purpose of this paper is to study the construction, the structure, and in particular various methods for the composition of codes and precodes. A precode consists of a plaintext alphabet P, a codetext alphabet C, an encoding relation $e \subseteq P \times C$ and a decoding relation $d \subseteq C \times P$, but does not necessarily satisfy that $d \circ e$ is subdiagonal. Lossy compression methods, such as JPEG, are examples of precodes that are not codes.

At first we viewed a precode as merely a convenient step toward precisely defining a code in accord with centuries of quite inclusive usage of the word. But it turns out that there are more precodes and codes in use than were obvious at first blush. And it turns out that some noncode precodes – such as secret

sharing schemes and lossy compression schemes – are useful precisely because they are not codes.

What forced our attention on precodes as well as codes was the interest generated by the separate but related category-theoretic properties of both precodes and codes. The study of codes and precodes was initiated in the papers [2] and [3], in a purely set-theoretical approach. In contrast, we use a categorical approach to study codes and their homomorphisms here. The new perspective leads to many new constructions and a more systematic treatment of various aspects of the theory.

Another reason to consider the category of precodes is that we do not only get a richer set of examples, but we also obtain a useful way to construct codes from precodes. The reason is that there exists an interesting functor from the category of precodes to the category of codes, namely the smash functor introduced in Section 4 below. This functor induces an equivalence relation on the plaintexts that identifies the elements that are decoded to the same symbol. For instance, in the JPEG example mentioned above all images that essentially look alike and thus yield the same compressed result would be identified under this equivalence relation. The smash functor is thus a most natural construction that produces codes from precodes.

Notations. If A, B, C are sets, and $r \subseteq A \times B$ and $s \subseteq B \times C$ are relations, then $s \circ r$ denotes the composite relation. The product $r \otimes s$ of two relations r and s is given by

$$r \otimes s = \{((r_1, s_1), (r_2, s_2)) \,|\, (r_1, r_2) \in r, (s_1, s_2) \in s\}.$$

2. Basics

A *precode* $\mathcal{A} = (P, C, e, d)$ consists of a set P of plaintext symbols, a set C of codetext symbols, an encoding relation $e \subseteq P \times C$, and a decoding relation $d \subseteq C \times P$. A precode $\mathcal{A}$ is said to be a *code* if and only if the composite $d \circ e$ of the encoding and decoding relation is a subdiagonal relation on P. In other words, a code requires the composite relation

$$d \circ e = \{\, (p_1, p_2) \in P \times P \,|\, \exists c \in C \; (p_1, c) \in e \wedge (c, p_2) \in d \,\}$$

to be a subset of the identity relation $\{(p, p) \,|\, p \in P\}$.

A playful illustration of a precode is given in the next example.

Example 1. Alice and Bob play a simple matching tile domino game. The dealer hands Alice the tiles $e = \{$  ,  ,  ,  $\}$ and Bob the tiles $d = \{$  ,  ,  $\}$. Alice starts by placing one of her tiles on the table. Bob has to match the diamond face value of Alice's tile in the next move. If he is able to do that, then he wins; otherwise he loses.

If the first move of Alice is  , then Bob's move will be  . The precode interpretation of this game is that Alice encodes  into  ; and Bob decodes to . It might seem strange that encoding followed by decoding does not have to be an identity relation. However, a lossy compression scheme such as JPEG does not follow such strict rules either: the decoded image is in general different from the encoded image.

Example 2. Let $\mathbf{F}_q$ be the finite field with q elements. Let $\Lambda = \mathbf{F}_q \times \mathbf{F}_q$ be the set representing nonvertical lines, where $(m, b) \in \Lambda$ represents the line $y = mx+b$. Set $(P, C, e, d) = (\mathbf{F}_q, 2^\Lambda, e, d)$, where (x, S) belongs to the encoding relation e if and only if there exists $y \in \mathbf{F}_q$ such that the point (x, y) lies on each line contained in S; and the decoding relation d is the converse of e. Notice that the cardinality of the encoding and decoding relations $|d| = |e| = q^2 2^q$. This precode is a Blakley 2 out of q threshold scheme. In fact, a subthreshold-size coalition S (i.e., $|S| \leq 1$) decodes to any encoded member x of $\mathbf{F}_q$. This provides Shannon perfect security.

Example 3. Take as a plaintext P the space $C^1([0, 1])$ of continuously differentiable real-valued functions, and as a codetext the space of continuous real-valued functions $C([0, 1])$. If we take differentiation as an encoding relation $e = \{(f(x), f'(x)) \,|\, f(x) \in C^1([0, 1])\}$ and integration as a decoding relation $d = \{(f(x), \int_0^x f(x)dx + k) \,|\, f(x) \in C([0, 1]), k \in \mathbf{R}\}$, then we obtain a precode (P, C, e, d). The opposite (C, P, d, e) is a code.

Example 4. The high security login *à la Purdy* [11] can be understood as a precode $(P, C, e, \emptyset)$, where e is a publicly known one-way function from the set of passwords P to enciphered words C. The decoding relation is by design void. The resulting precode is a code, since $d \circ e = \emptyset$ is a subset of the identity relation on P.

The high security login shows that a code with empty decode relation can be a useful tool. More straightforward examples of precode and codes are provided by error correcting codes or cryptographic codes, such as the following classical polyalphabetic cipher.

Example 5. Let $A = \mathbf{Z}/2^7\mathbf{Z}$ be a 7-bit alphabet codifying ASCII charac-

ters. Denote by $\mathbf{N}$ the natural numbers. A Vigenère cipher over A with a key $(k_0, \ldots, k_{m-1}) \in A^m$ can be described by the precode $(A^{\mathbf{N}}, A^{\mathbf{N}}, e, d)$, where e is the function mapping a sequence $(a_i)_{i\in\mathbf{N}}$ to $(a_i + k_{i \bmod m} \bmod 2^7)_{i\in\mathbf{N}}$, and the decode relation is given by its inverse function $d = e^{-1}$.

The period m of this cipher can be found with the help of a classical method deviced by the Prussian colonel Friedrich Wilhelm Kasiski in 1863. A cryptanalysis may then proceed with the simpler task of deciphering monoalphabetic homomorphic images.

Homomorphisms are generally useful in the design and analysis of codes. We give a formal definition of homomorphisms in the next section.

3. Morphisms

A *homomorphism* from a precode (P, C, e, d) to a precode (P', C', e', d') is given by an ordered pair $\langle h, k\rangle$ of functions $h\colon P \to P'$ and $k\colon C \to C'$ that satisfy $(h \times k)(e) \subseteq e'$ and $(k \times h)(d) \subseteq d'$.

The *category* $\mathfrak{P}$ *of precodes* is defined by taking precodes as *objects* and precode homomorphisms as *morphisms*. The composition of arrows is given by the composition of functions. Similarly, the *category* $\mathfrak{C}$ *of codes* is defined by taking code as objects and precode homomorphisms as morphisms. Clearly, the category $\mathfrak{C}$ is a full subcategory of the category $\mathfrak{P}$ of precodes.

Proposition 6. *Let $f = \langle f_1, f_2\rangle\colon \mathcal{A} \to \mathcal{B}$ be a homomorphism of precodes.*
(a) The morphism f is monic if and only if f_1 and f_2 are injective functions.
(b) The morphism f is epic if and only if f_1 and f_2 are surjective functions.

Proof. (a) Suppose that f_1 and f_2 are injective functions, hence monic morphisms in the category of sets. This immediately implies that f is monic. Conversely, suppose that f is monic. Denote by $\mathcal{S} = (\{p\}, \{c\}, \emptyset, \emptyset)$ a precode with singleton symbol sets. Let x and y be (necessarily constant) morphisms from $\mathcal{S}$ to $\mathcal{A}$. Since $fx = fy$ implies $x = y$, it follows that f_1 and f_2 are injective functions.

(b) Suppose that f_1 and f_2 are surjective functions, hence epimorphisms in the category of sets. This implies that f is an epimorphism. Conversely, suppose that f is an epimorphism. Seeking a contradiction, we assume that not both f_1 and f_2 are surjective. Define the precode $\mathcal{D} = (\mathbf{2}, \mathbf{2}, \mathbf{2} \times \mathbf{2}, \mathbf{2} \times \mathbf{2})$, where $\mathbf{2} = \{0, 1\}$. Let g and h be morphisms from $\mathcal{B}$ to $\mathcal{D}$, namely let g be the morphism that maps plaintext and codetext symbols to 0 and let h be the morphisms that maps all plaintext and codetext symbols in the image of f to

0 and everything else to 1. Therefore $gf = hf$, which implies $h = g$, since f is an epimorphism. Thus we get the desired contradiction, since the morphisms g and h are distinct by construction. □

Remark 7. If $f = \langle f_1, f_2 \rangle$ is an isomorphism in the category of codes or in the category of precodes, then f_1 and f_2 are bijective functions. However, the categories $\mathfrak{C}$ and $\mathfrak{P}$ are not balanced, that is, a monic and epic morphism is not necessarily an isomorphism. To see this, let ι denote the identity function on $\mathbf{2}$. Then $\langle \iota, \iota \rangle$ is a monic and epic morphism from the code $\mathcal{A} = (\mathbf{2}, \mathbf{2}, \emptyset, \emptyset)$ to the code $\mathcal{B} = (\mathbf{2}, \mathbf{2}, id, id)$ with identity encoding and decoding relations. But it is obviously not an isomorphism.

4. Smashing

We establish in this section a fundamental connection between the category of precodes and the category of codes: We derive a smash operation that associates with each precode a code. It turns out that the smash is a functor – a property which will be extremely valuable in the following sections.

Let $\mathcal{A} = (P, C, e, d)$ be a precode. In general, the composition of the encoding and decoding relation $d \circ e$ will fail to be subdiagonal. However, if we denote by E the smallest equivalence relation on P containing $d \circ e$, and by I the identity relation on C, then we obtain a precode $\mathcal{A}_\#$ as a quotient of $\mathcal{A}$ in the following way:

$$\mathcal{A}_\# = (P_\#, C, e_\#, d_\#),$$

where $P_\# = P/E$, $e_\# = e/_{E \otimes I}$, and $d_\# = d/_{I \otimes E}$. We say that $A_\#$ is obtained by *smashing* the plaintext symbols of the precode $\mathcal{A}$, and we refer to E as the *smash equivalence relation*.

Proposition 8. *Let $\mathcal{A}$ be a precode, then $\mathcal{A}_\#$ is a code. If $\mathcal{A}$ is a code, then $\mathcal{A}_\# = \mathcal{A}$. In particular, $(\mathcal{A}_\#)_\# = \mathcal{A}_\#$.*

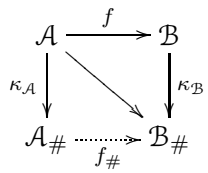
Proof. If $(p_1, p_2) \in d \circ e$, then the plaintext symbols p_1, p_2 are related in the smash equivalence relation E, forcing $d_\# \circ e_\#$ to be subdiagonal. If $\mathcal{A}$ is a code, then the smashing relation of $\mathcal{A}_\#$ is the identity relation, which proves the second assertion. □

Theorem 9. *Let α be a homomorphism from a precode $\mathcal{A}$ to a code $\mathcal{B}$. Denote by κ the natural homomorphism from $\mathcal{A}$ to $\mathcal{A}_\#$. Then there exists a uniquely determined homomorphism β from $\mathcal{A}_\#$ to $\mathcal{B}$ such that $\alpha = \beta \circ \kappa$.*

Proof. Let $\mathcal{A} = (P, C, e, d)$. Suppose that $(p_1, p_2) \in d \circ e$, that is, there exists an encoding of the plaintext symbol p_1 that can be decoded to p_2 in $\mathcal{A}$. The homomorphism $\alpha = \langle \alpha_1, \alpha_2 \rangle$ has to map p_1 to the same plaintext symbol as p_2, since $\mathcal{B}$ is a code. This means that $\alpha_1(p_1) = \alpha_1(p_2)$. Therefore, the equivalence relation on P induced by α_1 contains the smash equivalence relation. Hence, the map β_1 from the plaintext symbol set of $\mathcal{A}_\#$ to the plaintext symbol set of the code $\mathcal{B}$, given by $\beta_1(\overline{p}_1) = \alpha_1(p_1)$, where $\overline{p}_1$ is the equivalence class of p_1 in E, is well-defined. The homomorphism β is given by $\beta = \langle \beta_1, \alpha_2 \rangle$. It is clear from the definitions that this is indeed a homomorphism. This homomorphism is uniquely determined, since κ is an epimorphism. □

Theorem 10. *The smash $(-)_\#$ is a covariant functor from the category $\mathfrak{P}$ of precodes to the category $\mathfrak{C}$ of codes.*

Proof. Suppose that $f : \mathcal{A} \to \mathcal{B}$ is a morphism of precodes. Then we obtain a commuting diagram



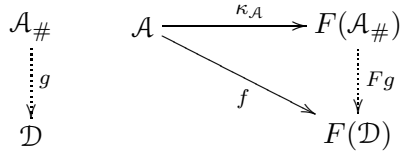
where the vertical arrows are given by the canonical maps from the precodes $\mathcal{A}$ and $\mathcal{B}$ to the codes $\mathcal{A}_\#$ and $\mathcal{B}_\#$, respectively. The diagonal arrow $\kappa_{\mathcal{B}} \circ f$ is a precode homomorphisms from the precode $\mathcal{A}$ to the code $\mathcal{B}_\#$. By Theorem 9, there exists a uniquely determined homomorphism $f_\#$ such that $\kappa_{\mathcal{B}} \circ f = f_\# \circ \kappa_{\mathcal{A}}$. The uniqueness implies that $(g \circ f)_\# = g_\# \circ f_\#$ holds for any composable pair of precode homomorphisms f and g. Therefore $\#$ is a covariant functor from the category $\mathfrak{P}$ of precodes to the category $\mathfrak{C}$ of codes. □

Denote by $F\colon \mathfrak{C} \to \mathfrak{P}$ the inclusion functor from the category of codes to the category of precodes, and by $I_{\mathfrak{P}}$ the identity functor on the category $\mathfrak{P}$ of precodes. Viewing the codes $\mathcal{A}_\#$ and $\mathcal{B}_\#$ as precodes, the diagram in the previous proof shows the following result:

Corollary 11. *Let κ be the transform that associates to each object $\mathcal{A}$ in $\mathfrak{P}$ the canonical homomorphism $\kappa_{\mathcal{A}}\colon \mathcal{A} \to F(\mathcal{A}_\#)$. Then κ is a natural transform from the identity functor $I_{\mathfrak{P}}$ to the functor $F \circ (-)_\#$ given by the composition of the smash functor with the inclusion functor.*

Theorem 12. *The smash functor $(-)_\#\colon \mathfrak{P} \to \mathfrak{C}$ and the inclusion functor $F\colon \mathfrak{C} \to \mathfrak{P}$ constitute an adjoint pair $(-)_\# \dashv F$.*

Proof. Let $\mathcal{A}$ be a precode, and $\mathcal{D}$ be a code. Suppose that there exists a code morphism $g\colon \mathcal{A}_\# \to \mathcal{D}$. According to Theorem 9, the canonical precode morphism $\kappa_{\mathcal{A}}$ from $\mathcal{A}$ to the precode $F(\mathcal{A}_\#)$ is universal in the sense that to each $f\colon \mathcal{A} \to F(\mathcal{D})$ there exists exactly one g as in the following diagram:



In other words, $\theta(g) = Fg \circ \kappa_{\mathcal{A}}$ defines a bijection

$$\theta\colon \mathrm{Mor}_{\mathfrak{C}}(\mathcal{A}_\#, \mathcal{D}) \longrightarrow \mathrm{Mor}_{\mathfrak{P}}(\mathcal{A}, F\mathcal{D}).$$

This bijection θ is natural in $\mathcal{A}$ because κ is natural in $\mathcal{A}$ by Corollary 11, and natural in $\mathcal{D}$ since F is a functor. □

Finding adjoint pairs is always beneficial. For instance, we obtain the following useful fact from general results of category theory:

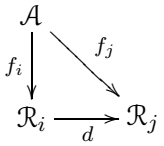
Corollary 13. *The inclusion functor F preserves limits, and the smash functor $(-)_\#$ preserves colimits. The category $\mathfrak{C}$ of codes is a reflective subcategory of the category $\mathfrak{P}$ of precodes.*

We will exploit this fact in the definition of coequalizers of codes in Section 7. This will also allow us to answer the question whether or not it is possible to find a construction dual to the smash.

5. Limits

We focus now on particular constructions of codes and precodes. In this section, we will see that products, pullbacks, and more general limits exist in the categories $\mathfrak{P}$ and $\mathfrak{C}$.

Recall that a *diagram* D in an arbitrary category $\mathfrak{K}$ is a directed graph whose vertices $i \in I$ are labelled by objects $\mathcal{R}_i$ in $\mathfrak{K}$ and whose edges $i \to j$ are labelled by morphisms in $\mathrm{Hom}_{\mathfrak{P}}(\mathcal{R}_i, \mathcal{R}_j)$. The underlying graph is called the *scheme* of the diagram. A family of morphisms $(f_i \colon \mathcal{A} \to \mathcal{R}_i)_{i\in I}$ with common domain $\mathcal{A}$ is said to be a *cone* for D, provided that for each arrow $d : \mathcal{R}_i \to \mathcal{R}_j$ in the diagram D, the triangle



commutes. A *limit* for D is a cone for D with the universal property that any other cone for D uniquely factors through it. In other words, if $(f_i \colon \mathcal{A} \to \mathcal{R}_i)_{i\in I}$ is the limit of a diagram D and $(g_i \colon \mathcal{B} \to \mathcal{R}_i)_{i\in I}$ is a cone for D, then there exists exists exactly one arrow $u \colon \mathcal{B} \to \mathcal{A}$ such that $g_i = f_i \circ u$ for all $i \in I$.

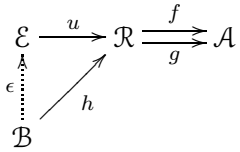
Let $(r_i)_{i\in I}$ be a family of relations indexed by a set I, where $r_i \subseteq P_i \times C_i$. We can define a product of these relations by

$$\prod r_i = \left\{ (p, c) \in \prod_{i\in I} P_i \times \prod_{j\in I} C_j \,|\, \forall i \in I \ (p(i), c(i)) \in r_i \right\}.$$

Theorem 14. *The category $\mathfrak{P}$ of precodes has products. The product of a family of codes is again a code.*

Proof. Let $\mathcal{R}_i = (P_i, C_i, e_i, d_i), i \in I$, be a family of precodes indexed by a set I. The product of this family is obtained by taking cartesian products of the symbol sets, and the product of the encoding and decoding relations. In other words, the product of the family $\mathcal{R}_i$ is given by $(\mathcal{R}, (\pi_i \colon \mathcal{R} \to \mathcal{R}_i)_{i\in I})$, where the precode $\mathcal{R}$ is given by the object $(\prod_{i\in I} P_i, \prod_{i\in I} C_i, \prod_{i\in I} e_i, \prod_{i\in I} d_i)$, and the projection map π_i is the obvious map onto the ith component. It is clear that $\mathcal{R}$ is a code if and only if all $\mathcal{R}_i$ are codes. □

The equalizer $(\mathcal{E}, u)$ of two morphisms $f, g \colon \mathcal{R} \to \mathcal{A}$ is an object $\mathcal{E}$ together with a morphism $u \colon \mathcal{E} \to \mathcal{R}$ such that $fu = gu$, with the additional property that *every* morphism h satisfying $fh = gh$ factors uniquely through u. In other words, the triangle in the following diagram commutes for any such h:



Recall that in the category of sets, the equalizer of two functions $f, g \colon R \to A$ is given by the coincidence set $\{x \in R \mid f(x) = g(x)\}$ with the inclusion mapping.

Theorem 15. *The category $\mathfrak{P}$ of precodes has equalizers. If $(\mathcal{E}, u)$ is the equalizer of two morphisms between codes, then $\mathcal{E}$ is also a code.*

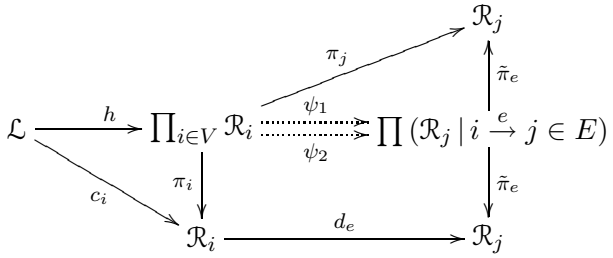
Proof. Let $\mathcal{R} = (P, C, e, d)$ and $\mathcal{A}$ be precodes. Let $f = \langle f_1, f_2 \rangle$ and $g = \langle g_1, g_2 \rangle$ be a pair of morphisms between $\mathcal{R}$ and $\mathcal{A}$. We give an explicit construction of the equalizer.

The equalizer $(\mathcal{E}, u)$ of f and g is given by the precode $\mathcal{E} = (P^*, C^*, e^*, d^*)$, where the plaintext symbols $P^* = \{\, a \in P \mid f_1(a) = g_1(a) \,\}$ and codetext symbols $C^* = \{\, a \in C \mid f_2(a) = g_2(a) \,\}$ are just coincidence sets, and the encoding and decoding relations are obtained from $\mathcal{R}$ by restriction, that is, $e^* = e\,|_{P^*\times C^*}$, $d^* = d\,|_{C^*\times P^*}$, and the morphism $u = \langle \iota_1, \iota_2 \rangle$ is induced by the set inclusion maps $\iota_1 \colon P^* \to P$, $\iota_2 \colon C^* \to C$.

The construction ensures that $u(\mathcal{E})$ is the largest subprecode of $\mathcal{R}$ such that the restrictions of the functions f and g on $u(\mathcal{E})$ coincide, $f|_{u(\mathcal{E})} = g|_{u(\mathcal{E})}$. We can express h by a composition of a morphism $\epsilon \colon \mathcal{B} \to \mathcal{E}$ with u, since $h(\mathcal{B})$ is a subprecode of $u(\mathcal{E})$. The morphism ϵ is uniquely determined, since u is a monomorphism. □

Theorem 16. *The category $\mathfrak{P}$ of precodes and the category $\mathfrak{C}$ of codes are complete.*

Proof. The categories $\mathfrak{P}$ and $\mathfrak{C}$ have products and equalizers and are therefore complete [1, 8]. The main idea of this standard construction goes as follows. Suppose that we are given a diagram D in $\mathfrak{P}$ with sets V of vertices and E of edges. We build two products: the product of all objects in D, and the product indexed by E of all codomains of arrows in D. The universal property of the E-indexed product induces unique maps ψ_1 and ψ_2 as is shown in the following diagram:



The map h is given by the equalizer of ψ_1 and ψ_2, and the maps c_i are given by composition of h with the projection maps π_i, that is, $c_i = \pi_i h$. It is not difficult to see that $(\mathcal{L}, (c_i)_{i\in I})$ is a cone of D. It follows from the universality of the equalizer and of the V-indexed product that this cone is the limit of D. □

6. Examples

In this section, we give some specific examples to illustrate a few essential aspects of the theory developed so far. The first example shows how to view the RSA public key cryptosystem as a code in the sense of Section 2. We show that the RSA scheme is a product of two Pholig-Hellman schemes. On the other hand, under some mild assumptions, it is possible to construct the RSA system as a product of two Pholig-Hellman ciphers. And we give a recent example from coding theory to illustrate the limit concept.

Example 17. (RSA) Denote by p and q two distinct odd primes. A key setting of an RSA public key cryptosystem [12] can be seen as a code over the symbol set $\mathbf{Z}/pq\mathbf{Z}$, where the encoding relation e is given by the function $x \mapsto x^{\varepsilon} \bmod pq$ and the decoding relation d is given by $x \mapsto x^{\delta} \bmod pq$. The exponents are assumed to satisfy the congruence $\varepsilon\delta \equiv 1 \bmod \varphi(pq)$, where φ is Euler's totient function. We denote this code by $\mathcal{RSA} = (\mathbf{Z}/pq\mathbf{Z}, \mathbf{Z}/pq\mathbf{Z}, e, d)$.

Reducing the symbol sets modulo p and q respectively, one obtains two key-settings of Pohlig-Hellman cryptosystems [10], denoted by

$$\mathcal{PH}_1 = (\mathbf{Z}/q\mathbf{Z}, \mathbf{Z}/q\mathbf{Z}, e_1, d_1) \quad \text{and} \quad \mathcal{PH}_2 = (\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z}, e_2, d_2).$$

The encoding and decoding relations are obtained from e and d by reducing modulo p and q respectively. For instance, the relation e_1 is given by the function $x \mapsto x^{\varepsilon} \bmod q$.

The $\mathcal{RSA}$ code is, in the terminology introduced in the previous section, an example of a *product* of the codes $\mathcal{PH}_1$ and $\mathcal{PH}_2$.

Example 18. (RSA, cont'd) Conversely, given two Pohlig-Hellman codes

$$\begin{aligned} \mathcal{PH}_1 &= (\mathbf{Z}/q\mathbf{Z},\, \mathbf{Z}/q\mathbf{Z},\, x \mapsto x^{\varepsilon_1} \bmod q, x \mapsto x^{\delta_1} \bmod q)\,, \\ \mathcal{PH}_2 &= (\mathbf{Z}/p\mathbf{Z},\, \mathbf{Z}/p\mathbf{Z},\, x \mapsto x^{\varepsilon_2} \bmod p, x \mapsto x^{\delta_2} \bmod p)\,, \end{aligned}$$

and assuming that $\gcd(p-1, q-1) | (\varepsilon_1 - \varepsilon_2)$, then it is easy to see that the greatest common divisor of $p-1$ and $q-1$ divides $\delta_1 - \delta_2$. The Chinese Remainder Theorem yields the integers ε, δ satisfying

$$\begin{aligned} \varepsilon &\equiv \varepsilon_1 \bmod q-1, & \delta &\equiv \delta_1 \bmod q-1, \\ \varepsilon &\equiv \varepsilon_2 \bmod p-1, & \delta &\equiv \delta_2 \bmod p-1, \end{aligned}$$

respectively. The $\mathcal{RSA}$ code

$$(\mathbf{Z}/pq\mathbf{Z}, \mathbf{Z}/pq\mathbf{Z}, x \mapsto x^{\varepsilon} \bmod pq, x \mapsto x^{\delta} \bmod pq)$$

is then isomorphic to the product of $\mathcal{PH}_1$ and $\mathcal{PH}_2$.

Example 19. (Codes over p-adic Integers) The famous explanation of the nonlinear Kerdoc and Preparata error control codes as linear codes over $\mathbf{Z}/4\mathbf{Z}$ gave rise to other explorations of Hensel lifting in coding theory. Calderbank and Sloane investigated in [4] a series of Hamming codes over the symbol sets $\mathbf{Z}/2^n\mathbf{Z}$. The familiar binary [7,4] Hamming code has generator polynomial $x^3 + x + 1$. Hensel lifting of this generator polynomial to $\mathbf{Z}/4\mathbf{Z}$ gives a unique monic irreducible polynomial that divides $x^7 - 1$ in $\mathbf{Z}/4\mathbf{Z}[x]$. Proceeding further, one obtains a series of cyclic codes over $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/16\mathbf{Z}$, $\mathbf{Z}/32\mathbf{Z}$, etc. The 2-adic lift of the binary Hamming code is then the error control code over the ring of 2-adic integers with generator matrix

$$\begin{pmatrix} 1 & \lambda & \lambda^* & -1 & 0 & 0 & 0 \\ 0 & 1 & \lambda & \lambda^* & -1 & 0 & 0 \\ 0 & 0 & 1 & \lambda & \lambda^* & -1 & 0 \\ 0 & 0 & 0 & 1 & \lambda & \lambda^* & -1 \end{pmatrix},$$

where λ is the 2-adic integer $(1 - \sqrt{-7})/2$, and $\lambda^* = \lambda - 1$.

The code $(\mathbf{Z}_2^4, \mathbf{Z}_2^7, e, d)$ corresponding to this Hamming code over the 2-adic integers $\mathbf{Z}_2$ is a special case of the *limit* construction of codes described in Section 5.

Example 20. (Diffie-Hellman Key Exchange) A builder, Bill, publishes a (multiplicatively written) group G and a member g of G. We denote by H the cyclic subgroup of G generated by g.

Alice picks a secret exponent $\alpha \in \mathbf{N}$, Bob a secret exponent $\beta \in \mathbf{N}$. Alice sends Bob her public member $a = g^\alpha$ of the group H. Bob sends Alice his public $b = g^\beta$. Alice knows Bob's b and her α, so she is able to decode the codetext pair (b, α) to produce a plaintext $j = b^\alpha = (g^\beta)^\alpha = g^{\beta\alpha} \in H$. Similarly, Bob knows his exponent β and Alice's a, so he can decode the pair (a, β) to produce the same plaintext j, by calculating j as $j = a^\beta = (g^\alpha)^\beta = g^{\alpha\beta} = g^{\beta\alpha}$. Alice and Bob thus share knowledge of j, which they believe others (even Bill) will find hard to calculate. This protocol is the well-known Diffie-Hellman key exchange scheme [5].

The Diffie-Hellman key exchange is a self-companion code (P, C, e, d), that is, the decoding relation d is the converse of the encoding relation. Indeed, take the cyclic group H as plaintext P, the codetext $C = H \setminus \{1\} \times \mathbf{N}$, the decoding relation is $d = \{((h, \tau), h^\tau) : h \in H \setminus \{1\}, \tau \in \mathbf{N}\}$, and the encoding relation is the converse.

It is easy to see that d is a function, hence its converse, e, is a one-to-many relation. And determining an output pair (h, τ) corresponding to an input element j seems a difficult problem. The most obvious way to attack it is to solve a discrete logarithm problem [5].

Who *performed* the encode? Nobody. Bill *produced* the entire encode relation e, but only implicitly, when he chose the group G and its member g. But it is widely believed that, if he chose adroitly, neither he nor anybody else can readily produce a pair $(j, (h, \tau))$ belonging to e, given a randomly chosen element $j \in H$.

7. Colimits

We provide more constructions of codes and precodes in this section. We show that coproducts, coequalizers, pushouts, and more general colimits exist. Unlike in the case of limits, these constructions will now differ in the case of codes and precodes.

Theorem 21. *The category $\mathfrak{P}$ of precodes has coproducts. The coproduct of a family of codes is again a code. In particular, the category $\mathfrak{C}$ of codes has coproducts.*

Proof. The coproduct $(\mathcal{K}, (\iota_i \colon \mathcal{R}_i \to \mathcal{K})_{i\in I})$ of the family $\mathcal{R}_i$ is given by the disjoint union of the symbol sets and the induced disjoint union of the encoding and decoding relations together with the obvious inclusion maps. In other words,

$$\mathcal{K} = \left(\bigcup_{i\in I} P_i \times \{i\}, \bigcup_{i\in I} C_i \times \{i\}, \bigcup_{i\in I} e_i \otimes \Delta_i, \bigcup_{i\in I} d_i \otimes \Delta_i \right),$$

where Δ_i denotes the relation $\Delta_i = \{(i,i)\}$.

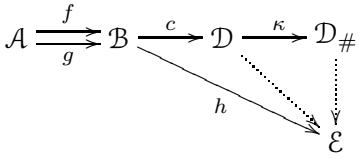
It is clear that $\mathcal{K}$ is a code if and only if all $\mathcal{R}_i$ are codes. □

Theorem 22. *The category $\mathfrak{P}$ has coequalizers.*

Proof. Let $\mathcal{R}$ and $\mathcal{A} = (P, C, e, d)$ be precodes, and let $f = \langle f_1, f_2\rangle$ and $g = \langle g_1, g_2\rangle$ be a pair of morphisms from $\mathcal{R}$ to $\mathcal{A}$. Let E_1 be the smallest equivalence relation on P such that $f_1(a)$ and $g_1(a)$ are equivalent. Similarly, let E_2 be the smallest equivalence relation on P such that $f_2(a)$ and $g_2(a)$ are equivalent. The coequalizer of f and g is given by the precode $(P/E_1, C/E_2, e/E_1 \otimes E_2, d/E_2 \otimes E_1)$ and the morphism $\langle c_1, c_2\rangle$ induced by the canonical quotient maps $c_1 \colon P \to P/E_1$ and $c_2 \colon C \to C/E_2$. □

Theorem 23. *The category $\mathfrak{C}$ of codes has coequalizers.*

Proof. Let $\mathcal{A}$ and $\mathcal{B}$ be codes, and let $f = \langle f_1, f_2\rangle$ and $g = \langle g_1, g_2\rangle$ be a pair of homomorphisms from $\mathcal{A}$ to $\mathcal{B}$. The coequalizer of f and g in the category $\mathfrak{C}$ of codes is the smash of the coequalizer of f and g in the category $\mathfrak{P}$ of precodes. To see this, consider the diagram



Suppose that h is a morphism from $\mathcal{B}$ to a code $\mathcal{E}$ that coequalizes f and g. Denote by $(\mathcal{D}, c)$ the coequalizer of f and g in $\mathfrak{P}$. There exists a unique homomorphism from the precode $\mathcal{D}$ to the code $\mathcal{E}$. Hence, by Theorem 9 there exists a unique homomorphism from the code $\mathcal{D}_\#$ to $\mathcal{E}$. Since the code morphism $\kappa \circ c$ coequalizes f and g, we can conclude that $(\mathcal{D}_\#, \kappa \circ c)$ is the coequalizer of f and g. □

We give an example to illustrate the difference between $\mathfrak{P}$-coequalizers and $\mathfrak{C}$-coequalizers of codes. This shows that colimits of codes are in general not preserved under the inclusion functor $F \colon \mathfrak{C} \to \mathfrak{P}$.

Example 24. Let $\mathcal{A}$ and $\mathcal{B}$ be the codes given by $\mathcal{A} = (\{1,2\},\{1,2\},\emptyset,\emptyset)$ and $\mathcal{B} = (\{1,2\},\{1,2\},id,id)$. Let $f = \langle\iota,\iota\rangle$ and $g = \langle\iota,\sigma\rangle$ be the homomorphisms from $\mathcal{A}$ to $\mathcal{B}$ where ι denotes the identity function and σ the bijection $\sigma = \{1 \mapsto 2, 2 \mapsto 1\}$. The coequalizer of f and g in the category $\mathfrak{P}$ of precodes maps onto the precode $(\{1,2\},\{\mathbf{1}\},\{(1,\mathbf{1}),(2,\mathbf{1})\},\{(\mathbf{1},1),(\mathbf{1},2)\})$. In contrast, the coequalizer of f and g in the category of code maps onto the code $(\{\mathbf{1}\},\{\mathbf{1}\},\{(\mathbf{1},\mathbf{1})\},\{(\mathbf{1},\mathbf{1})\})$.

The combination of the results derived in this section yield the following theorem.

Theorem 25. *The category $\mathfrak{P}$ of precodes and the category $\mathfrak{C}$ of codes are cocomplete.*

Proof. Both categories have coproducts and coequalizers, hence are cocomplete. □

8. Split

In view of Section 4, it is natural to wonder whether or not it is possible to dualize the smash construction. We will refer to this alleged dual as the split. In search of the split construction, we found several interesting results. One of us (T.H.) showed that the split exists if we restrict ourselves to self-companion precodes and codes [7].

Suppose that we are given a homomorphism α from a code $\mathcal{B}$ to a precode $\mathcal{A}$. The question is whether we can associate to the precode $\mathcal{A}$ a code $\mathcal{A}_{\|}$ and a canonical homomorphism $\kappa_{\mathcal{A}}\colon \mathcal{A}_{\|} \to \mathcal{A}$ such that there exists a uniquely determined homomorphism $\beta\colon \mathcal{B} \to \mathcal{A}_{\|}$ satisfying $\alpha = \kappa_{\mathcal{A}} \circ \beta$. We say that $(\mathcal{A}_{\|},\kappa_{\mathcal{A}})$ is the *split* of the precode $\mathcal{A}$.

Theorem 26. *There exists a precode for which no split exists.*

Proof. Seeking a contradiction, we assume that it is possible to find for each precode $\mathcal{A}$ such a code $\mathcal{A}_{\|}$ satisfying the above universality condition. Similar to the arguments in Section 4, we would obtain a covariant functor $\|$. As a consequence of the universality condition, this functor $\|$ must be right adjoint to the inclusion functor F, cf. Theorem 2 (iv) in [8, p. 83]. Thus, in particular, the inclusion functor would be left adjoint. Since left adjoint functors respect colimits, we can conclude from Example 24 that the split does not exist for all precodes. □

9. Factorizations

We investigate now some properties of morphisms in the categories $\mathfrak{P}$ and $\mathfrak{C}$. We will particularly focus on epimorphisms. Several interesting refinements of the concept of an epimorphism have been introduced: extremal, strong and regular epimorphisms. We will characterize these classes of epimorphisms in the categories of precodes and codes. We will obtain most of the results by deriving a factorization structure for precode and code morphisms, which has many other interesting consequences as well.

Recall that an epimorphism in the category of codes is not necessarily surjective on the encoding or decoding relations. This motivates the following definition: An epimorphism $\langle f_1, f_2\rangle\colon (P, C, e, d) \to (P', C', e', d')$ is said to be strong in the sense of Blakley and Borosh or simply *BB-strong* if and only if it is surjective on both the encoding and the decoding relations, that is, if $(f_1 \times f_2)(e) = e'$ and $(f_2 \times f_1)(d) = d'$ holds.

The next proposition relates this set-theoretic concept (which has been introduced in [3]) to a standard notion in category theory. Recall that an epimorphism is said to be *regular* if and only if it is a coequalizer of two arrows.

Proposition 27. *Suppose that f is a morphism in the category $\mathfrak{P}$ of precodes or in the category $\mathfrak{C}$ of codes. Then f is a BB-strong epimorphism if and only if it is a regular epimorphism.*

Proof. Suppose that f is a regular epimorphism. It follows directly from the definitions that f is BB-strong.

Conversely, let $f = \langle f_1, f_2\rangle\colon \mathcal{A} \to \mathcal{B}$ be a BB-strong epimorphism. Construct the pullback of f with itself

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{B}} \mathcal{A} & \xrightarrow{p_2=\langle p_{21}, p_{22}\rangle} & \mathcal{A} \\ {\scriptstyle p_1=\langle p_{11}, p_{12}\rangle}\downarrow & & \downarrow{\scriptstyle f} \\ \mathcal{A} & \xrightarrow[f]{} & \mathcal{B} \end{array}$$

We claim that f is the coequalizer of the projection morphisms p_1 and p_2. It is clear from the construction that f coequalizes p_1 and p_2, that is, $f \circ p_1 = f \circ p_2$. Suppose that $g = \langle g_1, g_2\rangle\colon \mathcal{A} \to \mathcal{D}$ is another morphism coequalizing p_1 and p_2.

Define $k = \langle k_1, k_2\rangle\colon \mathcal{B} \to \mathcal{D}$ as follows. Let $k_1(f_1(p)) = g_1(p)$ for each p in the plaintext of $\mathcal{A}$, and $k_2(f_2(c)) = g_2(c)$ for each c in the codetext of $\mathcal{A}$. Since f is epic, f_1 and f_2 are surjective, hence the maps k_1 and k_2 are determined on all elements of the symbol sets of $\mathcal{B}$. It remains to check that $\langle k_1, k_2\rangle$ is a well-defined homomorphism.

If $\widetilde{p}$ is another element of the plaintext symbol set of $\mathcal{A}$ with $f(\widetilde{p}) = f(p)$, then $(\widetilde{p}, p)$ is in the plaintext of $\mathcal{A} \times_{\mathcal{B}} \mathcal{A}$. Hence $g_1(\widetilde{p}) = (g_1 \circ p_{11})(\widetilde{p}, p) = (g_1 \circ p_{21})(\widetilde{p}, p) = g_1(p)$. Thus the function k_1 is well-defined and $k_1 \circ f_1 = g_1$. Analogously, k_2 is a well-defined function satisfying $k_2 \circ f_2 = g_2$.

For each pair (p', c') in the encoding relation of $\mathcal{B}$ there exists a pair in (p, c) in the encoding relation of $\mathcal{A}$ with $(f_1(p), f_2(c)) = (p', c')$, since f is BB-strong. Hence $(k_1 \times k_2)(p', c') = (k_1 \times k_2)(f_1(p), f_2(c)) = (g_1(p), g_2(c))$. A similar argument shows that each element in the decoding relation of $\mathcal{B}$ is mapped via $k_2 \times k_1$ to an element of the decoding relation of $\mathcal{D}$. Therefore, k is indeed a well-defined homomorphism. This homomorphism is unique since f is epic. Consequently, f is the coequalizer of the projection maps p_1 and p_2, as claimed. □

Proposition 28. *In the category of precodes and in the category of codes, any morphism f can be factored into a regular epimorphism p followed by a monomorphism i, $f = i \circ p$.*

Proof. Factor $f = \langle f_1, f_2 \rangle \colon (P, C, e, d) \to \mathcal{B}$ through its image

$$(f_1(P), f_2(C), (f_1 \times f_2)(e), (f_2 \times f_1)(d)).$$

The morphism obtained from f by restricting the codomain of f to its image is a regular epimorphism according to the previous proposition. □

This proposition has surprisingly many consequences. For instance, it allows us to characterize the extremal epimorphisms. Recall that an epimorphism e is said to be *extremal* if in any factorization $e = m \circ f$, with m a monomorphism, the morphism m must be an isomorphism. It is known that regular epimorphisms are extremal. A direct consequence of the previous proposition is that the converse holds in the category of precodes or codes:

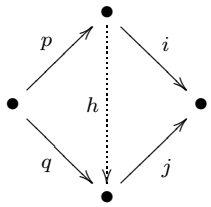
Corollary 29. *In the category $\mathfrak{P}$ of precodes and in the category $\mathfrak{C}$ of codes, an extremal epimorphism is regular.*

It is also known that regular epimorphisms are strong, and strong epimorphism are extremal. Thus, the classes of extremal, strong, and regular epimorphism coincide in the categories $\mathfrak{P}$ and $\mathfrak{C}$.

Another consequence of the previous proposition is that the factorization of a morphism into a regular epimorphism followed by a monomorphism is essentially unique:

Corollary 30. *Let f be a morphism in the category $\mathfrak{P}$ or $\mathfrak{C}$. Suppose that f can be factored as $f = i \circ p$ and as $f = j \circ q$, where p, q are regular epimor-*

phisms, and i, j are monomorphisms. Then there exists a uniquely determined morphism h such that the following diagram commutes



Proof. Any (regular epi, mono)-factorization is unique in the above sense. This is a standard fact of category theory, cf. Proposition 17.18 in [6]. □

We have now established that each morphism can be factorized into a regular epimorphism followed by a monomorphism in an essentially unique way. The class of regular epimorphisms as well as the class of monomorphisms are closed under composition. This demonstrates that the categories $\mathfrak{P}$ and $\mathfrak{C}$ have a (regular epi, mono)-factorization system, cf. [6, §33]:

Corollary 31. *The categories $\mathfrak{P}$ and $\mathfrak{C}$ are (regular epi, mono)-categories.*

Factorization systems always yield a characterization of isomorphisms, namely the intersection of the class of regular epimorphisms with the class of monomorphisms yields precisely the class of isomorphisms:

Corollary 32. *Let f be a morphism in the category $\mathfrak{P}$ or in the category $\mathfrak{C}$. The morphism f is an isomorphism if and only if it is a regular epimorphism as well as a monomorphism.*

10. Regularity

We will show in this section that the categories $\mathfrak{P}$ and $\mathfrak{C}$ are regular. Regular categories allow to formulate the concept of an exact sequence – the pervailing concept of homological algebra – without reference to zero-objects. This level of abstraction is necessary, since zero-objects do not exist in the categories $\mathfrak{P}$ and $\mathfrak{C}$.

The lack of zero-objects, hence kernels, makes it necessary to find a similar but slightly weaker notion. A *kernel pair* is the pullback of an arrow with itself. This concept replaces the familiar notion of a kernel. An exact sequence in a regular category is a diagram

$$P \underset{v}{\overset{u}{\rightrightarrows}} A \xrightarrow{f} B \ ,$$

where (u, v) is the kernel pair of f and f is the coequalizer of (u, v).

A category is said to be *regular* provided that (1) each arrow has a kernel pair, (2) every kernel pair has a coequalizer, and (3) the pullback of regular epimorphisms along any morphism exists and is again regular.

We only need to show condition (3), since the other conditions follow from the completeness and cocompleteness of our categories. Let us introduce some convenient notation. If $\mathcal{A} = (P, C, e, d)$ is a precode, then $\mathbf{P}(\mathcal{A})$ denotes the plaintext symbol set P of $\mathcal{A}$, and $\mathbf{C}(\mathcal{A})$ denotes the codetext symbol set $\mathbf{C}(\mathcal{A})$ of P.

Lemma 33. *The pullback of an epimorphism is again an epimorphism in the category $\mathfrak{P}$ of precodes and in the category $\mathfrak{C}$ of codes.*

Proof. Given a pullback diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{D}} \mathcal{B} & \xrightarrow{p_2=\langle p_{21}, p_{22}\rangle} & \mathcal{B} \\ {\scriptstyle p_1=\langle p_{11}, p_{12}\rangle}\downarrow & & \downarrow{\scriptstyle f=\langle f_1, f_2\rangle} \\ \mathcal{A} & \xrightarrow[g=\langle g_1, g_2\rangle]{} & \mathcal{D} \end{array}$$

with epimorphic f, we need to show that the projection morphism p_1 is epimorphic. The induced commutative squares

$$\begin{array}{ccc} \mathbf{P}(\mathcal{A} \times_{\mathcal{D}} \mathcal{B}) & \xrightarrow{p_{21}} & \mathbf{P}(\mathcal{B}) \\ {\scriptstyle p_{11}}\downarrow & & \downarrow{\scriptstyle f_1} \\ \mathbf{P}(\mathcal{A}) & \xrightarrow[g_1]{} & \mathbf{P}(\mathcal{D}) \end{array} \qquad \begin{array}{ccc} \mathbf{C}(\mathcal{A} \times_{\mathcal{D}} \mathcal{B}) & \xrightarrow{p_{22}} & \mathbf{C}(\mathcal{B}) \\ {\scriptstyle p_{12}}\downarrow & & \downarrow{\scriptstyle f_2} \\ \mathbf{C}(\mathcal{A}) & \xrightarrow[g_2]{} & \mathbf{C}(\mathcal{D}) \end{array}$$

on the plaintext symbol sets and on the codetext symbol sets are pullback squares in the category of sets. Thus p_{11} and p_{12} are epimorphism in sets, hence surjective mappings. Therefore $p_1 = \langle p_{11}, p_{12}\rangle$ is an epimorphism (in $\mathfrak{P}$ or $\mathfrak{C}$). □

Lemma 34. *In $\mathfrak{P}$ and in $\mathfrak{C}$, the pullback of a regular epimorphism is a regular epimorphism.*

Proof. Given a pullback diagram

$$\begin{array}{ccc} \mathcal{A} \times_{\mathcal{D}} \mathcal{B} & \xrightarrow{p_2=\langle p_{21}, p_{22}\rangle} & \mathcal{B} \\ {\scriptstyle p_1=\langle p_{11}, p_{12}\rangle}\downarrow & & \downarrow{\scriptstyle f=\langle f_1, f_2\rangle} \\ \mathcal{A} & \xrightarrow[g=\langle g_1, g_2\rangle]{} & \mathcal{D} \end{array}$$

with regular epimorphic f, we need to show that the projection morphism p_1 is a regular epimorphism. We know that p_1 is an epimorphism by the previous lemma. By Proposition 27, it suffices to show that the encoding and decoding relations of $\mathcal{A} \times_{\mathcal{D}} \mathcal{B}$ are mapped onto the encoding and decoding relations of $\mathcal{A}$, respectively.

Let (p, c) be an arbitrary pair in the encoding relation of $\mathcal{A}$. Since f is surjective on relations, we can find (p', c') in the encoding relation of $\mathcal{B}$ such that $(g_1(p), g_2(c)) = (f_1(p'), f_2(c'))$. Therefore, $((p, p'), (c, c'))$ is in the encoding relation of the pullback $\mathcal{A} \times_{\mathcal{D}} \mathcal{B}$. Hence $(p_{11} \times p_{12})((p, p'), (c, c')) = (p, c)$. Therefore, p_1 maps the encoding relation of $\mathcal{A} \times_{\mathcal{D}} \mathcal{B}$ onto the encoding relation of $\mathcal{A}$. Analogously, one shows that the decoding relation of $\mathcal{A} \times_{\mathcal{D}} \mathcal{B}$ is mapped onto the decoding relation of $\mathcal{A}$. Thus we can conclude that p_1 is BB-strong and hence regular. □

Theorem 35. *The category $\mathfrak{P}$ of precodes and the category $\mathfrak{C}$ of codes are regular.*

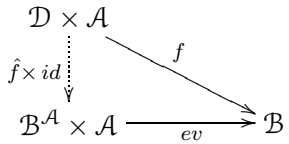
Proof. A category is called regular if it has finite limits, coequalizers, and in which the pullback of a regular epimorphism is a regular epimorphism. The claim follows from Theorem 16, Theorem 25, and Lemma 34. □

11. Cartesian Closedness

We have seen that the categories $\mathfrak{P}$ and $\mathfrak{C}$ share many properties. They are, for instance, both regular, complete, and cocomplete. In this section, we discuss a property which is not shared by both categories.

Recall that a category $\mathfrak{A}$ is called *cartesian closed* provided that it has finite products, and the functors $\_ \times \mathcal{A} \colon \mathfrak{A} \to \mathfrak{A}$ are left adjoint for each object $\mathcal{A}$ in $\mathfrak{A}$. The associated right adjoint is said to be an exponential functor and is denoted by $(\_)^{\mathcal{A}}$.

Thus, a category with finite products is cartesian closed if and only if for each pair $(\mathcal{A}, \mathcal{B})$ of objects there exists an exponential object $\mathcal{B}^{\mathcal{A}}$ and an evaluation morphism $ev \colon \mathcal{B}^{\mathcal{A}} \times \mathcal{A} \to \mathcal{B}$ with the following universal property: for each morphism $f \colon \mathcal{D} \times \mathcal{A} \to \mathcal{B}$ there exists a unique morphism $\hat{f} \colon \mathcal{D} \to \mathcal{B}^{\mathcal{A}}$ such that



commutes. The most familiar example of a cartesian closed category is the category of sets with functions as morphisms:

Example 36. Let Set be the category of sets with functions as morphisms. If A and B are sets, then B^A is given by the set of functions from A to B. Note that ev is given by the usual function evaluation. Suppose that $f\colon D \times A \to B$ is given, then $\hat{f} : D \to B^A$ is determined by the rule $[\hat{f}(d)](a) = f(d, a)$.

We now show that the category of precodes is cartesian closed as well:

Theorem 37. *The category $\mathfrak{P}$ is cartesian closed.*

Proof. Since we already know that finite products exist, we are left to show that an object $\mathcal{B}^{\mathcal{A}}$ and an evaluation map ev with the associated universal properties exists.

1. Suppose that $\mathcal{A} = (P, C, e, d)$ and $\mathcal{B} = (\bar{P}, \bar{C}, \bar{e}, \bar{d})$ are precodes. We define the associated exponential object $\mathcal{B}^{\mathcal{A}} = (\bar{P}^P, \bar{C}^C, E, D)$ with the help of the encoding relation

$$E = \left\{(g_1, g_2) \in \bar{P}^P \times \bar{C}^C \,|\, (p, c) \in e \Rightarrow (g_1(p), g_2(c)) \in \bar{e}\right\},$$

and the decoding relation

$$D = \left\{(h_2, h_1) \in \bar{C}^C \times \bar{P}^P \,|\, (c, p) \in d \Rightarrow (h_2(c), h_1(p)) \in \bar{d}\right\}.$$

The morphism $ev = \langle ev_1, ev_2\rangle$ consists of evaluation maps. Note that this is indeed a homomorphism thanks to the definition of E and D.

2. Let $\mathcal{D} = (P', C', e', d')$ be a precode, and $f = \langle f_1, f_2\rangle\colon \mathcal{D} \times A \to \mathcal{B}$ be a precode homomorphism. We can uniquely define functions $\hat{f}_1\colon P' \to \bar{P}^P$ and $\hat{f}_2\colon C' \to \bar{C}^C$ by their values

$$[\hat{f}_1(p_D)](p_A) = f_1(p_D, p_A) \quad \text{for all} \quad (p_D, p_A) \in \mathbf{P}(\mathcal{D}) \times \mathbf{P}(\mathcal{A}),$$

$$[\hat{f}_2(c_D)](c_A) = f_2(c_D, c_A) \quad \text{for all} \quad (c_D, c_A) \in \mathbf{C}(\mathcal{D}) \times \mathbf{C}(\mathcal{A}).$$

It remains to show that $\hat{f} = \langle \hat{f}_1, \hat{f}_2\rangle$ is a precode homomorphism.

3. Let $(p_D, p_D^*) \in e'$ and $(c_D, c_D^*) \in d'$. Since f is a precode morphism, we obtain for all $(p_A, p_A^*) \in e$ and $(c_A, c_A^*) \in d$ a relation of the the function values

$$(f_1(p_D, p_A), f_1(p_D^*, p_A^*)) \in \bar{e}, \qquad (f_2(c_D, c_A), f_2(c_D^*, c_A^*)) \in \bar{d}.$$

In other words, this shows that

(a) $[\hat{f}_1(p_D)](p_A)$ and $[\hat{f}_1(p_D)](p_A^*)$ are related in $\bar{e}$ for all $(p_A, p_A^*) \in e$,

(b) $[\hat{f}_2(c_D)](c_A)$ and $[\hat{f}_2(c_D)](c_A^*)$ are related in $\bar{d}$ for all $(c_A, c_A^*) \in d$.

It follows from the definition of $\mathcal{B}^{\mathcal{A}}$ that the functions $\hat{f}_1(p_D)$ and $\hat{f}_1(p_D^*)$ are related in E, and that $\hat{f}_2(c_D)$ and $\hat{f}_2(c_D^*)$ are related in D.

Therefore, $\mathfrak{P}$ is cartesian closed. □

The exponential object $\mathcal{B}^{\mathcal{A}}$ is in general not a code, even if both $\mathcal{A}$ and $\mathcal{B}$ are codes. Unfortunately, there is no way to repair this defect, as the following theorem shows.

Theorem 38. *The category $\mathfrak{C}$ of codes is not cartesian closed.*

Proof. If a category is cartesian closed, then this means that each functor $\_\times\mathcal{A}$ is left adjoint. Thus, in particular, this functor must preserve colimits such as coequalizers.

Let $\mathcal{A} = \mathcal{B} = (\{p\}, \{c\}, \emptyset, \emptyset)$ and $\mathcal{D} = (\{1,2\}, \{1,2\}, id, id)$. We define two morphisms $f, g\colon \mathcal{B} \to \mathcal{D}$ with $f = \langle f_1, f_2\rangle$ and $g = \langle g_1, g_2\rangle$ by

$$f_1 = p \mapsto 1, \quad f_2 = c \mapsto 1, \qquad g_1 = p \mapsto 1, \quad g_2 = c \mapsto 2$$

The coequalizer of f and g is given by the code $\mathcal{E} = (\{p\}, \{c\}, \{(p,c)\}, \{(c,p)\})$. Hence, the image under the functor is $\mathcal{E} \times \mathcal{A} \cong \mathcal{A}$.

On the other hand, the coequalizer of $f \times id$ and $g \times id$ from $\mathcal{B} \times \mathcal{A}$ to $\mathcal{D} \times \mathcal{A}$ is given by $\mathcal{K} = (\{1,2\}, \{1\}, \emptyset, \emptyset)$. Therefore, the functor $\_ \times \mathcal{A}$ cannot be left adjoint. □

12. Conclusions

We have investigated the structure of the category of precodes and the category of codes. Limit and colimit constructions yield a wealth of possibilities to build new codes. Error control codes over 2-adic integers are only a first step towards the more general code constructions described in this paper. An interesting aspect of our categorical approach was to explore the relationship between the two categories via functors. We gained deep insights by proving the existence or nonexistence of certain functors. For instance, the smash functor allowed us to transfer all the colimit constructions from the category of precodes to the category of codes. On the other hand, we could show the nonexistence of the split – the dual concept of the smash – by proving the nonexistence of a functor. An interesting direction for future research is the investigation of subcategories. Exploring subcategories of codes with additional algebraic structure will be a natural next step.

Acknowledgements

The research by A. Klappenecker has been supported by NSF grant 0218582, NSF CAREER grant 0347310, and a Texas A&M TITF initiative.

References

[1] M.A. Arbib, E. Manes, *Arrows, Structures, and Functors - The Categorical Imperative*, Academic Press, New York (1975).

[2] G.R. Blakley, I. Borosh, A general theory of codes, I: Basic concepts, In: *Proceedings of the Klagenfurt Conference*, Volume **10** of *Contributions to General Algebra* (Ed-s: D. Dorninger, G. Eigenthaler, H.K. Kaiser, H. Kautschistsch, W. More), Verlag Johannes Heyn, Klagenfurt, Austria (1998), 1-29.

[3] G.R. Blakley, I. Borosh, A general theory of codes, II: Paradigms and homomorphisms, *Information Security, First International Workshop, ISW '97*, Volume **1396** of *LNCS* (Ed-s: E. Okamoto, G. Davida, M. Mambo), Springer Verlag, Berlin (1998), 1-30.

[4] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes, and Cryptography*, **6** (1995), 21-35.

[5] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory*, **22** (1976), 644-654.

[6] H. Herrlich, G.E. Strecker, *Category Theory*, Allyn and Bacon, Boston (1973).

[7] T. Holcomb, *Contributions to a General Theory of Codes*, Ph.D. Dissertation, Texas A&M University, Department of Mathematics (2002).

[8] S. Mac Lane, *Categories for the Working Mathematician*, Springer Verlag, Berlin, 2-nd Edition (1997).

[9] C.H. Meyer, S.M. Matyas, *Cryptography: A New Dimension in Computer Data Security - A Guide for the Design and Implementation of Secure Systems*, John Wiley, New York (1982).

[10] S.C. Pohlig, M.E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Inform. Theory*, **24** (1978), 106-110.

[11] G.P. Purdy, A high-security log-in procedure, *Comm. of the ACM*, **17**, No. 4 (1974), 442-445.

[12] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, **21** (1978), 120-126.