Finite Fields and Their Applications 84 (2022) 102097

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Goppa codes over the p-adic integers and integers modulo p^e

Markel Epelde

Universidad del País Vasco - Euskal Herriko Unibertsitatea, Bizkaia, Spain

ARTICLE INFO

Article history:
Received 11 October 2021
Received in revised form 22 April 2022
Accepted 27 July 2022
Available online 11 August 2022
Communicated by Sergey Rybakov

MSC:
11T71
94B05

Keywords:
Algebraic codes
Goppa codes
McEliece cryptosystem

ABSTRACT

Goppa codes were defined by Valery D. Goppa in 1970. In 1978, Robert J. McEliece used this family of error-correcting codes in his cryptosystem, which has gained popularity in the last decade due to its resistance to attacks from quantum computers. In this paper, we present Goppa codes over the p-adic integers and integers modulo p^e. This allows the creation of chains of Goppa codes over different rings. We show some of their properties, such as parity-check matrices and minimum distance, and suggest their cryptographic application, following McEliece's scheme.

In 1970, Valery D. Goppa defined a new class of error-correcting codes over a finite field $\mathbb{F}_q$, nowadays known as Goppa codes [6]. If we consider q to a prime number p, from an algebraic point of view, Goppa codes are $\mathbb{Z}_p$-subspaces of $\mathbb{Z}_p^n$. As error-correcting codes, there also exists a decoding algorithm for them, i.e., a method to find the closest codeword to a given element in $\mathbb{Z}_p^n$, provided the distance between them is smaller than the error-correcting capability of the Goppa code. In 1978, Robert J. McEliece presented his cryptosystem [9], a method to encrypt a message by encoding an information vector

E-mail address: markel.epelde@ehu.eus.

https://doi.org/10.1016/j.ffa.2022.102097

and adding errors artificially. For his cryptosystem, he suggested the use of binary Goppa codes and, while other approaches of code-based cryptosystems have been successfully attacked, his scheme remains mostly intact. Despite its drawbacks (such as its large key sizes), this scheme has regained popularity due to his quantum resistance and age [12].

In this paper, we define Goppa codes over the p-adic integers and $\mathbb{Z}_{p^e}$, i.e., the ring of integers modulo p^e, based on the original idea from Goppa, and we hint a potential cryptographic application of them. In 2005, Antonio A. de Andrade and Reginaldo Palazzo generalized Goppa codes to finite rings [1], but using a different approach. However, we will rely on the generalization of Goppa's original introduction [6]. This definition was suggested by Markel Epelde et al. in 2020 for $\mathbb{Z}_4$ [5] and, while de Andrade's generalization of the decoding algorithm still works, our definition allows to show some additional properties. Both the definition and its basic consequences can be seen in Section 1. In Section 2, we describe the chains of Goppa codes and the relations between their parity-check matrices. In Section 3, we show how to get isomorphic Goppa codes over different rings by changing one of the parameters of the code. Changing the other parameter leads to some other results in Section 4. Finally, their potential cryptographic application is shown in Section 5.

Let us fix $h \in \mathbb{N} \cup \{0\}$, let $n \in \mathbb{N}$ and let p be a prime number. We will denote by $R_{p^e} = GR(p^e, h)$ the Galois extension of degree h of $\mathbb{Z}_{p^e}$ for any $e \in \mathbb{N}$, and by R_{p^∞} the Galois extension of degree h of the ring of p-adic integers $\mathbb{Z}_{p^\infty}$, i.e.,

$$R_{p^\infty} = \left\{ a_0 + pa_1 + \cdots + p^e a_e + \cdots \mid a_i \in \mathbb{F}_{p^h},\ \forall i \in \mathbb{N} \cup \{0\} \right\}.$$

Observe that this ring is formed by formal infinite sums of elements in an extension of degree h of $\mathbb{Z}_p$.

Let $i, j \in \mathbb{N} \cup \{\infty\}$ such that $i \geq j$. We denote by $\psi_{p^i,p^j} : R_{p^i} \to R_{p^j}$ the natural projection of elements in R_{p^i} to R_{p^j}, and by $\widehat{\psi}_{p^i,p^j}$ the extension of ψ_{p^i,p^j} to n-tuples in $R_{p^i}^n$. Moreover, we define $\Psi_{p^i,p^j} : R_{p^i}[X] \to R_{p^j}[X]$ as the natural generalization of ψ_{p^i,p^j} to polynomials, i.e., satisfying $\Psi_{p^i,p^j}(\sum_{k=0}^n a_k X^k) = \sum_{k=0}^n \psi_{p^i,p^j}(a_k) X^k$ for a $n \in \mathbb{N}$.

1. Definition and basic properties

Let us define Goppa codes over $\mathbb{Z}_{p^e}$, generalizing Goppa's original definition in [6].

Definition 1. Let $e \in \mathbb{N} \cup \{\infty\}$, $L = (\alpha_1, \ldots, \alpha_n) \in R_{p^e}^n$ and $g \in R_{p^e}[X]$ of degree $r < n$ such that $\psi_{p^e,p}(\alpha_i) \neq \psi_{p^e,p}(\alpha_j)$ for $i \neq j$ and $g(\alpha_i)$ is a unit, i.e., $\psi_{p^e,p}(g(\alpha_i)) \neq 0$ for every $i \in \{1, \ldots, n\}$. The *Goppa code of parameters L and g* over $\mathbb{Z}_{p^e}$ is defined as

$$\Gamma_{p^e}(L, g) = \left\{ c \in \mathbb{Z}_{p^e}^n \mid \sum_{i=1}^n \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)} \right\}.$$

Example 1. Let $h = 4$, and let $p = 2$, $e = 3$ and $R_{p^e} = \mathbb{Z}_8[\alpha]$, where α is an element of multiplicative order $p^h - 1 = 15$. Let $g(X) = X^3 + \alpha^4 X^2 + \alpha^5 X$ and, for instance,

$$L = (1, \alpha, \alpha^4, \alpha^3, \alpha^5, \alpha^{11}, \alpha^{14}, \alpha^2, \alpha^8, \alpha^{13}, \alpha^9, \alpha^{12}, \alpha^6).$$

Then $\Gamma_8(L, g)$ is the code generated by

$$G = (2 \quad 1 \quad 2 \quad 5 \quad 5 \quad 2 \quad 0 \quad 3 \quad 2 \quad 5 \quad 3 \quad 3 \quad 6).$$

This code has length 13, 8 elements and minimum distance 7.

Remark 1. Let $\alpha \in R_{p^e}$ and $g \in R_{p^e}[X]$ such that $g(\alpha)$ is a unit. Then,

$$(X - \alpha)^{-1} = -g(\alpha)^{-1} \left(\frac{g(X) - g(\alpha)}{X - \alpha} \right)$$

modulo $g(X)$.

The previous remark allows the proof of the following lemma.

Lemma 1. *Let $e \in \mathbb{N} \cup \{\infty\}$, let $\Gamma_{p^e}(L, g)$ be a Goppa code of length n, and $\mathcal{C} = \{c \in \mathbb{Z}_{p^e}^n \mid cH^\top = \boldsymbol{0}\}$, where*

$$H = \begin{pmatrix} g(\alpha_1)^{-1} & g(\alpha_2)^{-1} & \dots & g(\alpha_n)^{-1} \\ \alpha_1 g(\alpha_1)^{-1} & \alpha_2 g(\alpha_2)^{-1} & \dots & \alpha_n g(\alpha_n)^{-1} \\ \alpha_1^2 g(\alpha_1)^{-1} & \alpha_2^2 g(\alpha_2)^{-1} & \dots & \alpha_n^2 g(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r-1} g(\alpha_1)^{-1} & \alpha_2^{r-1} g(\alpha_2)^{-1} & \dots & \alpha_n^{r-1} g(\alpha_n)^{-1} \end{pmatrix} \tag{1}$$

and $r = \deg g$. Then, $\mathcal{C} \subseteq \Gamma_{p^e}(L, g)$ and, if the leading coefficient of g is a unit or $e = \infty$, the equality holds.

Proof. Let $g(X) = \sum_{i=0}^{r} g_i X^i$ and $c \in \mathbb{Z}_{p^e}^n$. Then, $cH^\top = \mathbf{0}$ implies $cH^\top H_g^\top = \mathbf{0}$, where

$$H_g = \begin{pmatrix} g_r & 0 & 0 & \dots & 0 \\ g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ g_2 & g_3 & \dots & g_r & 0 \\ g_1 & g_2 & \dots & g_{r-1} & g_r \end{pmatrix}.$$

Observe that, when the leading coefficient of g is a unit, the condition is equivalent since H_g is invertible. Since $\mathbb{Z}_{p^\infty}$ is an integral domain, the condition is also equivalent if $e = \infty$. This matrix equality represents the following equations

$$\left.\begin{aligned} g_r(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) &= 0 \\ g_{r-1}(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) + g_r(c_1\alpha_1 g(\alpha_1)^{-1} + \cdots + c_n\alpha_n g(\alpha_n)^{-1}) &= 0 \\ &\vdots \\ g_1(c_1 g(\alpha_1)^{-1} + \cdots + c_n g(\alpha_n)^{-1}) + g_2(c_1\alpha_1 g(\alpha_1)^{-1} + \cdots + c_n\alpha_n g(\alpha_n)^{-1}) & \\ + \cdots + g_r(c_1\alpha_1^{r-1} g(\alpha_1)^{-1} + \cdots + c_n\alpha_n^{r-1} g(\alpha_n)^{-1}) &= 0 \end{aligned}\right\},$$

which can be written compiled into one polynomial equality. Namely,

$$\sum_{k=0}^{r-1}\left(\sum_{j=1}^{r-k} g_{k+j}\sum_{i=1}^{n} c_i\alpha_i^{j-1} g(\alpha_i)^{-1}\right) X^k = 0.$$

Rearranging the terms, it follows that

$$\sum_{i=1}^{n} c_i g(\alpha_i)^{-1}\sum_{k=0}^{r-1} X^k \sum_{j=1}^{r-k} g_{k+j}\alpha_i^{j-1} = 0. \tag{2}$$

Note that

$$\sum_{k=0}^{r-1} X^k \sum_{j=1}^{r-k} g_{k+j}\alpha_i^{j-1} = \sum_{j=1}^{r} g_j \sum_{k=0}^{j-1} \alpha_i^{j-k-1} X^k = \sum_{k=0}^{r} g_k \left(\frac{X^k - \alpha_i^k}{X - \alpha_i}\right) = \frac{g(X) - g(\alpha_i)}{X - \alpha_i}.$$

Since the degree of g is greater than the term on the left-hand side of (2), this equation can be written as

$$\sum_{i=1}^{n} c_i \left(g(\alpha_i)^{-1}\frac{g(X) - g(\alpha_i)}{X - \alpha_i}\right) \equiv 0 \pmod{g(X)}.$$

Therefore, $cH^\top = \mathbf{0}$ implies (and is equivalent to, when the leading coefficient of g is a unit or $e = \infty$)

$$\sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{g(X)}, \qquad \text{i.e., } c \in \Gamma_{p^e}(L, g). \quad \square$$

Remark 2. When $c \in \Gamma_{p^e}(L, g)$ if and only if $cH^\top = \mathbf{0}$, we say that H is a parity-check matrix for the code. However, this is an abuse of the term, since the entries of H do not necessarily belong to $\mathbb{Z}_{p^e}$. In order to write a parity-check matrix in strict sense, we would have to expand each entry as a column formed by its coordinates with respect to a $\mathbb{Z}_{p^e}$-basis of R_{p^e}, and then remove the redundant rows of the matrix.

Example 2. Substituting the entries of the matrix H defined as in (1) for the code in Example 1 with their coordinates with respect to the $\mathbb{Z}_2$-basis $\{1, \alpha, \alpha^2, \alpha^3\}$ results in the parity-check matrix

$$H = \begin{pmatrix} 4 & 3 & 7 & 7 & 4 & 4 & 7 & 0 & 3 & 6 & 3 & 1 & 4 \\ 0 & 7 & 7 & 6 & 1 & 7 & 5 & 4 & 3 & 7 & 3 & 6 & 7 \\ 6 & 6 & 7 & 4 & 7 & 5 & 7 & 7 & 6 & 6 & 2 & 4 & 5 \\ 5 & 2 & 5 & 4 & 7 & 3 & 4 & 6 & 6 & 6 & 0 & 5 & 3 \\ 4 & 6 & 0 & 2 & 0 & 5 & 1 & 3 & 3 & 6 & 1 & 6 & 6 \\ 0 & 3 & 7 & 0 & 7 & 0 & 5 & 6 & 5 & 2 & 5 & 5 & 0 \\ 6 & 3 & 4 & 0 & 3 & 4 & 7 & 2 & 0 & 5 & 7 & 4 & 7 \\ 5 & 0 & 5 & 5 & 4 & 7 & 1 & 1 & 5 & 1 & 1 & 2 & 5 \\ 4 & 0 & 0 & 1 & 4 & 3 & 1 & 1 & 2 & 1 & 3 & 2 & 1 \\ 0 & 6 & 6 & 3 & 0 & 2 & 1 & 3 & 3 & 3 & 2 & 3 & 1 \\ 6 & 3 & 3 & 5 & 6 & 2 & 6 & 5 & 7 & 4 & 2 & 7 & 6 \\ 5 & 3 & 3 & 3 & 5 & 0 & 7 & 3 & 4 & 6 & 0 & 4 & 7 \end{pmatrix}.$$

Recall that a code over a ring R is said to be free if it is isomorphic to R^k for some k. We now prove the following lemma.

Lemma 2. *The Goppa code $\Gamma_{p^\infty}(L, g)$ is a free code, i.e., a free R_{p^∞}-submodule of $R_{p^\infty}^n$.*

Proof. By Lemma 1, $\Gamma_{p^\infty}(L, g)$ is defined as the dual of the code with generator matrix H in (1), and every dual code in $\mathbb{Z}_{p^\infty}$ is free [4]. □

With Lemmata 1 and 2, we can prove the following theorem, which consists of the basic properties of Goppa codes as defined in Definition 1.

Theorem 1. *Let $e \in \mathbb{N} \cup \{\infty\}$ and let $\mathcal{C} = \Gamma_{p^e}(L, g)$ be a Goppa code. Then,*

(i) If $e = \infty$, $\dim_{R_{p^\infty}} \mathcal{C} \geq n - h \deg g$. Otherwise, $|\mathcal{C}| \geq p^{e(n - h \deg g)}$.

(ii) For any $j < e$, $\mathcal{C} \cap p^j \mathbb{Z}_{p^e}^n = p^j \widehat{\psi}_{p^e, p^{e-j}}^{-1}(\Gamma_{p^{e-j}}(\widehat{\psi}_{p^e, p^{e-j}}(L), \Psi_{p^e, p^{e-j}}(g)))$, where $\widehat{\psi}_{p^e, p^{e-j}}^{-1}(A)$ denotes the preimage of a subset $A \subseteq \mathbb{Z}_{p^{e-j}}^n$ through the projection map $\widehat{\psi}_{p^e, p^{e-j}}$. In particular, $\mathcal{C} \cap p^{e-1}\mathbb{Z}_{p^e}^n$ is isomorphic as a $\mathbb{F}_p$-linear space to $\Gamma_p(\widehat{\psi}_{p^e, p}(L), \Psi_{p^e, p}(g))$, and to

$$\Gamma_{p^j}(\widehat{\psi}_{p^e, p^j}(L), \Psi_{p^e, p^j}(g)) \cap p^{j-1}\mathbb{Z}_{p^j}^n.$$

(iii) For any $j \in \mathbb{N} \cup \{\infty\}$ with $j < e$, $\widehat{\psi}_{p^e, p^j}(\mathcal{C})$ is a subcode of $\Gamma_{p^j}(\widehat{\psi}_{p^e, p^j}(L), \Psi_{p^e, p^j}(g)))$. As a consequence, if $e = \infty$ and for a $j \in \mathbb{N}$, $\Gamma_{p^j}(\widehat{\psi}_{p^e, p^j}(L), \Psi_{p^e, p^j}(g)) \subseteq p\mathbb{Z}_{p^j}^n$, then $\mathcal{C} = \{\mathbf{0}\}$ and $n \leq h \deg g$. Moreover, if $e \in \mathbb{N}$ and $\mathcal{C}$ is free, then $\Gamma_{p^j}(\widehat{\psi}_{p^e, p^j}(L), \Psi_{p^e, p^j}(g)) = \widehat{\psi}_{p^e, p^j}(\Gamma_{p^e}(L, g))$.

Proof. Let $r = \deg g$, let H be as defined in (1) and let H' be a parity-check matrix over $\mathbb{Z}_{p^e}$ of the code $\mathcal{C}' = \{c \in \mathbb{Z}_{p^e}^n \mid cH^\top = \mathbf{0}\}$. As a consequence of Remark 2, H' has at most rh rows, $|(\mathcal{C}')^\perp| \leq |\mathbb{Z}_{p^e}|^{rh} = p^{erh}$. Hence, if $e \in \mathbb{N}$, $|\mathcal{C}'| = |\mathbb{Z}_{p^e}^n|/|(\mathcal{C}')^\perp| \geq p^{e(n-rh)}$.

Since, by Lemma 1, $\mathcal{C}' \subseteq \mathcal{C}$, this proves the result. If $e = \infty$, from Lemma 2 it follows that $\Gamma_{p^e}(L, g)$ is a free code and, since from Lemma 1 it follows that $\mathcal{C} = \mathcal{C}'$, a parity-check matrix of $\mathcal{C}$ has at most rh rows and its dimension must be greater than $n - rh$.

For part (ii), $p^j c \in \Gamma_{p^e}(L, g) \cap p^j \mathbb{Z}_{p^e}^n$ if and only if $\sum_{i=1}^n p^j c_i/(X - \alpha_i) \equiv 0 \pmod{g(X)}$ or, equivalently $\sum_{i=1}^n c_i/(X - \alpha_i) \equiv 0 \pmod{g(X)}$ and modulo p^{e-j}. This is exactly the condition for c to be a lift of a codeword in $\Gamma_{p^{e-j}}(\widehat{\psi}_{p^e,p^{e-j}}(L), \Psi_{p^e,p^{e-j}}(g))$. Taking $j = e - 1$ establishes that the set of multiples of p^{e-1} in a Goppa code is isomorphic as a $\mathbb{F}_p$-linear space to its traditional Goppa code projection.

Finally, let us prove (iii). By definition, $c \in \Gamma_{p^e}(L, g)$ if and only if $\sum_{i=1}^n \frac{c_i}{X-\alpha_i} \equiv 0 \pmod{g(X)}$. This congruence is also true modulo p^j, so $\widehat{\psi}_{p^e,p^i}(c)$ belongs to $\Gamma_{p^j}(\widehat{\psi}_{p^e,p^i}, \Psi_{p^e,p^j}(g))$.

In particular, if $e = \infty$, $\widehat{\psi}_{p^\infty,p^j}(\mathcal{C})$ is a free subcode of $\Gamma_{p^j}(\widehat{\psi}_{p^e,p^j}(L), \Psi_{p^e,p^j}(g))$, so if $\mathcal{C} \neq \{\mathbf{0}\}$ then $\Gamma_{p^j}(\widehat{\psi}_{p^e,p^j}(L), \Psi_{p^e,p^j}(g)) \nsubseteq p\mathbb{Z}_{p^j}^n$.

Moreover, if $\Gamma_{p^e}(L, g)$ is free for an $e \in \mathbb{N}$, then $\widehat{\psi}_{p^e,p^j}(\Gamma_{p^e}(L, g))$ is also free and a subcode of $\Gamma_{p^j}(\widehat{\psi}_{p^e,p^j}(L), \Psi_{p^e,p^j}(g))$. Let k be the dimension of $\mathcal{C}$. Since $\widehat{\psi}_{p^e,p^j}(\mathcal{C})$ is free in $\mathbb{Z}_{p^j}$, it has cardinality p^{jk}. On the other hand, by part (ii) and since $\mathcal{C}$ is free,

$$|\widehat{\psi}_{p^e,p^j}(\mathcal{C})| = |\mathcal{C} \cap p^{e-j}\mathbb{Z}_{p^e}^n| = p^{jk}.$$

Since $\widehat{\psi}_{p^e,p^j}(\mathcal{C}) \subseteq \mathcal{C}$ and they have the same cardinality, the equality holds. □

Example 3.

1. Let $\mathcal{C}$ be the code in Example 1. Observe that, as claimed in part (i) of the previous theorem,

$$8 = |\mathcal{C}| \geq p^{e(n - h \deg g)} = 2^{3(13-4\cdot 3)} = 8.$$

Moreover, $\mathcal{C}_4 = \Gamma_4(\widehat{\psi}_{8,4}(L), \Psi_{8,4}(g))$ and $\mathcal{C}_2 = \Gamma_2(\widehat{\psi}_{8,2}(L), \Psi_{8,2}(g))$ are the codes generated by matrices

$$G_4 = (2 \quad 1 \quad 2 \quad 1 \quad 1 \quad 2 \quad 0 \quad 3 \quad 2 \quad 1 \quad 3 \quad 3 \quad 2)$$

and

$$G_2 = (0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0),$$

respectively. On the other hand, $\mathcal{C} \cap 4\mathbb{Z}_8^n$ and $\mathcal{C}_4 \cap 2\mathbb{Z}_4^n$ are generated by

$$G_3 = (0 \quad 4 \quad 0 \quad 4 \quad 4 \quad 0 \quad 0 \quad 4 \quad 0 \quad 4 \quad 4 \quad 4 \quad 0)$$

and

$$G_1 = (0 \quad 2 \quad 0 \quad 2 \quad 2 \quad 0 \quad 0 \quad 2 \quad 0 \quad 2 \quad 2 \quad 2 \quad 0),$$

respectively. As stated in part (ii) of the previous theorem,

$$\mathcal{C} \cap 4\mathbb{Z}_8^{13} \;\cong\; \mathcal{C}_4 \cap 2\mathbb{Z}_4^{13} \;\cong\; \mathcal{C}_2$$

as $\{0,1\}$-linear spaces. Finally, since $\mathcal{C}$ is free, not only are $\widehat{\psi}_{8,4}(\mathcal{C})$ and $\widehat{\psi}_{8,2}(\mathcal{C})$ subcodes of $\mathcal{C}_4$ and $\mathcal{C}_2$, respectively, but the equality also holds here, as established in part (iii) of the theorem.

2. Let g be the same as in Example 1, and let

$$M = (1, \alpha, \alpha^4, \alpha^3, \alpha^5, \alpha^{11}, \alpha^{14}, \alpha^2, \alpha^8, \alpha^{13}, \alpha^9, \alpha^{12}) \in R_8^n.$$

Then, $\mathcal{D} = \Gamma_8(M, g)$ is the code generated by

$$Q = (0 \quad 4 \quad 0 \quad 4 \quad 4 \quad 0 \quad 0 \quad 4 \quad 0 \quad 4 \quad 4 \quad 4).$$

Now, $2 = |\mathcal{D}| \geq 8^{12-4\cdot 3} = 1$, satisfying part (i) of Theorem 1, and, according to part (ii), $\mathcal{D} = \mathcal{D} \cap 4\mathbb{Z}_8^{12} \;\cong\; \mathcal{D}_4 \cap 2\mathbb{Z}_4^{12} \;\cong\; \mathcal{D}_2$, where $\mathcal{D}_4 = \Gamma_4(\widehat{\psi}_{8,4}(M), \Psi_{8,4}(g))$ and $\mathcal{D}_2 = \Gamma_2(\widehat{\psi}_{8,2}(M), \Psi_{8,2}(g))$ is generated by

$$Q_4 = (0 \quad 2 \quad 0 \quad 2 \quad 2 \quad 0 \quad 0 \quad 2 \quad 0 \quad 2 \quad 2 \quad 2)$$

and

$$Q_2 = (0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1).$$

Moving to part (iii), $\widehat{\psi}_{8,4}(\mathcal{D}) = \{\mathbf{0}\}$ is included in $\mathcal{D}_4$ and $\mathcal{D}_2$, and $\widehat{\psi}_{4,2}(\mathcal{D}_4) = \{0\}$ is included in $\mathcal{D}_2$, but the projections and the codes are not identical. Finally, since $\mathcal{D} \subseteq 4\mathbb{Z}_4^{12}$, we know that $\Gamma_{2^\infty}(M', g') = \{\mathbf{0}\}$ for any lift M' and g' of M and g, respectively.

Remark 3. Part 1 of Example 3 shows an instance of a Goppa code over $\mathbb{Z}_8$ being a lift of the corresponding Goppa codes over $\mathbb{Z}_4$ and $\mathbb{Z}_2$, and the code over $\mathbb{Z}_4$ being a lift of the corresponding code over $\mathbb{Z}_2$. However, as we can see in part 2 of the same example, in general, the codes $\Gamma_{p^e}(L, g)$ over $\mathbb{Z}_{p^e}$ are not lifts of its equivalent over $\mathbb{Z}_p$, $\Gamma_p(\widehat{\psi}_{p^e,p}(L), \Psi_{p^e,p}(g))$. For instance, in that example the code over the 2-adic integers is trivial, whereas the codes over $\mathbb{Z}_8$, $\mathbb{Z}_4$ and $\mathbb{Z}_2$ have cardinality 2. In fact, none of them are lifts of the codes below.

Corollary 1. *Let $e \in \mathbb{N} \cup \{\infty\}$ and let $\mathcal{C} = \Gamma_{p^e}(L, g)$ be a Goppa code. The minimum distance of $\mathcal{C}$ satisfies $d(\mathcal{C}) \geq \deg \Psi_{p^e,p}(g) + 1$. Furthermore, if $e = \infty$, $\Gamma_{p^\infty}(L, g)$ satisfies $d \geq \deg g + 1$.*

Proof. Let $e \in \mathbb{N}$. Observe that one can always find a (non-zero) codeword c of minimum weight such that $c \in \mathcal{C} \cap p^{e-1}\mathbb{Z}_e^n$. In fact, if c is a multiple of p^s but not a multiple of p^{s+1}, then $p^{e-s-1}c \in \mathcal{C} \cap p^{e-1}\mathbb{Z}_e^n$ and $w(p^{e-s-1}c) \leq w(c)$. According to part (ii) of Theorem 1,

$$\mathcal{C} \cap p^{e-1}\mathbb{Z}_e^n = p^{e-1}\widehat{\psi}_{p^e,p}^{-1}(\mathcal{C}_p),$$

where $\mathcal{C}_p = \Gamma_p(\widehat{\psi}_{p^e,p}(L), \Psi_{p^e,p}(g)$. Observe that $\mathcal{C}_0$ is a traditional Goppa code, having minimum weight $d(\mathcal{C}_0) \geq \deg \Psi_{p^e,p}g + 1$.

If $e = \infty$, let H be as defined in (1) and let $c \in \Gamma_{p^e}(L, g)$ be a non-zero codeword. Then, by Lemma 1 $cH^\top = \mathbf{0}$ so there exist $w(c)$ linearly dependent columns in H. However, any $r \times r$ submatrix of H reduces to a Vandermonde matrix with a non-zero determinant, so $w(c) \geq r + 1$. Therefore, if $x, y \in \Gamma_{p^e}(L, g)$ are two distinct codewords, $d(x, y) = w(x - y) \geq r + 1$. □

2. Parity-check matrix

In this section, we show the relation between Goppa codes of the same parameters over different rings and their parity-check matrices. First, we present the following lemma, the proof of which can be found in [8].

Lemma 3. *Let $e \in \mathbb{N}$, and let f be a regular polynomial in $\mathbb{Z}_{p^e}[X]$. Then, there exist a polynomial $f^* \in \mathbb{Z}_{p^e}[X]$ and $q \in \mathbb{Z}_{p^e}[X]$ such that $\Psi_{p^e,p}(f) = \Psi_{p^e,p}(f^*)$, $f(X) = q(X)f^*(X)$ and the leading coefficient of f^* is a unit.*

We can also show the following relation between Goppa codes with similar polynomial parameters.

Lemma 4. *Let $e \in \mathbb{N} \cup \{\infty\}$ and let $\Gamma_{p^e}(L, g)$ be a Goppa code. Then, if there exists polynomial $g^*(X)$ such that its leading coefficient is a unit, g is a multiple of g^* and $\Psi_{p^e,p}(g^*) = \Psi_{p^e,p}(g)$, then $\Gamma_{p^e}(L, g) \subseteq \Gamma_{p^e}(L, g^*)$. Moreover, if $e \in \mathbb{N}$, the equality holds.*

Proof. Let $g^*, q \in R_{p^e}[X]$ be such that the leading coefficient of $g^*(X)$ is a unit, $g^*(X)q(X) = g(X)$ and $\Psi_{p^e,p}(g^*) = \Psi_{p^e,p}(g)$. Therefore, for some unit u in $\mathbb{Z}_{p^e}$, $\Psi_{p^e,p}(q) = \psi_{p^e,p}(u) \neq 0$, so $q(X) = u + pm(X)$. This implies that, if $e \in \mathbb{N}$, $q(X)$ is a unit, its inverse being $1 - pu^{-1}m(X) + p^2u^{-2}m(X)^2 + \cdots + (-1)^{e-1}p^{e-1}u^{1-e}m(X)^{e-1}$.

Therefore, $\Gamma_{p^e}(L, g) = \Gamma_{p^e}(L, q \cdot g^*)$ and $c \in \Gamma_{p^e}(L, g)$ iff

$$\sum_{i=1}^{n} \frac{c_i}{X - \alpha_i} \equiv 0 \pmod{q(X)g^*(X)}.$$

Multiplying the term in the left-hand side by $\prod_{i=1}^{n}(X - \alpha_i)$, it follows that $c \in \Gamma_{p^e}(L, q \cdot g^*)$ if and only if $q(X)g^*(X)$ divides

$$\sum_{i=1}^{n} c_i \prod_{\substack{1\le j\le n\\ j\neq i}} (X-\alpha_i).$$

Therefore, if $c \in \Gamma_{p^e}(L,g)$ then $g^*(X)$ divides this term. In fact, if $q(X)g^*(X)$ divides the term then also $g^*(X)$ divides this term. Since $(g^*(X), X-\alpha_i) = 1$ for every $i \in \{1,\dots,n\}$, this is equivalent to $c \in \Gamma_{p^e}(L,g^*)$. Observe that this code is well defined, since for all $i \in \{1,\dots,n\}$, $\psi_{p^e,p}(g^*(\alpha_i)) = \psi_{p^e,p}(g(\alpha_i)) \neq 0$. □

With this information, we can give an explicit expression for a parity-check matrix of every Goppa code.

Theorem 2. *Let $e \in \mathbb{N} \cup \{\infty\}$ and let $\mathcal{C} = \Gamma_{p^e}(L,g)$ be a Goppa code.*

(i) If $e = \infty$, H as in (1) is a parity-check matrix for $\mathcal{C}$.
(ii) If $e \in \mathbb{N}$ and $g^* \in R_{p^e}[X]$ is the polynomial satisfying the conditions in Lemma 4, then

$$H^* = \begin{pmatrix} g^*(\alpha_1)^{-1} & g^*(\alpha_2)^{-1} & \dots & g^*(\alpha_n)^{-1} \\ \alpha_1 g^*(\alpha_1)^{-1} & \alpha_2 g^*(\alpha_2)^{-1} & \dots & \alpha_n g^*(\alpha_n)^{-1} \\ \alpha_1^2 g^*(\alpha_1)^{-1} & \alpha_2^2 g^*(\alpha_2)^{-1} & \dots & \alpha_n^2 g^*(\alpha_n)^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{r^*-1} g^*(\alpha_1)^{-1} & \alpha_2^{r^*-1} g^*(\alpha_2)^{-1} & \dots & \alpha_n^{r^*-1} g^*(\alpha_n)^{-1} \end{pmatrix} \tag{3}$$

is a parity-check matrix for $\mathcal{C}$, where $r^* = \deg g^*$.

Proof. The first part is straightforward from Lemma 1. Let $e \in \mathbb{N}$. By Lemmata 3 and 4, there exists $g^* \in R_{p^e}[X]$ with a unit as leading coefficient such that $\mathcal{C} = \Psi_{p^e,p}(g^*)$ and $\Gamma_{p^e}(L,g) = \Gamma_{p^e}(L,g^*)$. Since the leading coefficient of g^* is a unit, by Lemma 1, H^* is a parity check matrix for $\mathcal{C}$. □

Example 4. Let us consider the parameters in Example 1, and let $f(X) = 2\alpha^{14}X^4 + (1+2\alpha^3)X^3 + 3\alpha^4X^2 + \alpha^5X$. Since the leading coefficient of g is a unit, $\Psi_{8,2}(g) = \Psi_{8,2}(f)$ and $f(X) = (1+2\alpha^{14}X)g(X)$, from Lemma 4 it follows that $\Gamma_8(L,f) = \Gamma_8(L,g)$ and H from Example 2 is a parity-check matrix for $\Gamma_8(L,f)$.

Remark 4. We have presented a parity-check matrix for any Goppa code $\Gamma_{p^e}(L,g)$. This allows the use of the efficient decoding algorithm from [1], based on the parity-check matrix, in our context.

Let us see how the relations between the parity-check matrices for different values of e. In order to prove that, we introduce a topological result.

Definition 2. A non-empty family A of subsets of a set X is said to have the finite intersection property (FIP) if the intersection over any finite subcollection of A is non-empty.

Lemma 5. *A space X is compact if and only if every collection of closed subsets of X satisfying the finite intersection property has non-empty intersection.*

Proof. The proof of this lemma can be found in [10]. □

In the following theorem we consider R_{p^∞} as a topological group under addition. The topology is defined by the open neighbourhoods of $x \in R_{p^\infty}$, $\mathcal{N}(x) = \{x + (p^i)\}_{i\in\mathbb{N}}$. By basic properties of topological groups, R_{p^∞} is compact and these neighbourhoods are also closed sets in R_{p^∞} [3].

Theorem 3. *Let $\{g_{p^i}\}_{i\in\mathbb{N}\cup\{\infty\}}$ be an infinite chain of regular polynomials such that $g_{p^i} \in R_{p^i}[X]$ and $\Psi_{p^i,p^j}(g_{p^i}) = g_{p^j}$ for every $i, j \in \mathbb{N} \cup \{\infty\}$ such that $i \geq j$. Then, there exists $\{g^*_{p^i}(X)\}_{i\in\mathbb{N}\cup\{\infty\}}$ a sequence of polynomials with leading coefficient a unit and $g^*_{p^i} \in R_{p^i}[X]$, such that*

(i) $\Psi_{p^i,p}(g^*_{p^i}) = \Psi_{p^i,p}(g_{p^i})$,
(ii) $g^*_{p^i}(X)$ *divides* $g_{p^i}(X)$,
(iii) $\Psi_{p^i,p^j}(g^*_{p^i}) = g^*_{p^j}$,

for every $i, j \in \mathbb{N} \cup \{\infty\}$ such that $i \geq j$.

Proof. We consider

$$S = \{m \in R_{p^\infty}[X] \mid \deg m \leq r\},$$

where $r = \deg g_{p^\infty}$. Since S is the direct sum of r compact spaces, it is also compact with the sum topology. The sets $m(X) + (p^i) \cap S$ form closed neighbourhoods of $m(X) \in S$, since they are direct sum of closed sets of R_{p^∞}. Let

$$\begin{aligned} S_e = \Big\{ & g^* \in S \mid \psi_{p^\infty,p^e}(g^*) \text{ has leading coefficient a unit,} \\ & \psi_{p^\infty,p}(g^*) = \psi_{p^\infty,p}(g_{p^\infty}),\ \psi_{p^\infty,p^e}(g^*) \mid g_{p^e} \Big\} \\ = \Bigg\{ & g^* \in S \mid \psi_{p^\infty,p^e}(g^*) \text{ has leading coefficient a unit,} \\ & \exists q \in R_{p^\infty}[X] \text{ s. t. } \begin{cases} g^*(X) \equiv g_{p^\infty}(X) \pmod{p} \\ g^*(X)q(X) \equiv g_{p^\infty}(X) \pmod{p^e} \end{cases} \Bigg\} \end{aligned}$$

for all $e \in \mathbb{N}$. Note that the S_e are closed in S, since there are finitely many polynomials in S modulo p^e, and if $g \in S$ then also $g + (p^e) \cap S \subseteq S_e$, so S_e is the union of finitely many closed subsets of S. Moreover, by Lemma 3, the S_e are non-empty, and $S_e \subseteq S_{e-1}$ for $e \geq 2$, so the $A = \{S_e\}_{e\in\mathbb{N}}$ satisfies the FIP. By Lemma 5, the intersection of the subsets of A is non-empty, so there exists $g^*_{p^\infty} \in S$ such that the leading coefficient of $g^*_{p^\infty}$ is a unit and there exists $q_e(X) \in S$ such that $g^*_{p^\infty}(X)q_e(X) = g(X)$ modulo p^e for any $e \in \mathbb{N}$. Now, let us consider

$$Y_e = \{q \in S \mid q(X)g^*_{p^\infty}(X) = g(X) \pmod{p^e}\},$$

for every $e \in \mathbb{N}$. Applying the same lemma, there exists $q \in S$ such that $g^*_{p^\infty}(X)q(X) = g_{p^\infty}(X)$ modulo p^e for any $e \in \mathbb{N}$, so there exists $g^*_{p^\infty} \in R_{p^\infty}[X]$ and $q(X) \in R_{p^\infty}[X]$ such that the leading coefficient of $g^*_{p^\infty}$ is a unit and $g^*_{p^\infty}(X)q(X) = g_{p^\infty}(X)$, so $g^*_{p^\infty}$ divides g_{p^∞}.

Let $\{g^*_{p^i}\}_{i\in\mathbb{N}}$ with $g^*_{p^i} = \Psi_{p^\infty,p^i}(g^*_{p^\infty}) \in R_{p^i}[X]$. Since $g^*_{p^\infty} \in S_i$, $g^*_{p^i}$ divides g_{p^i}. Moreover, since $\Psi_{p^\infty,p^i}(g_{p^\infty}) = g_{p^i}$,

$$\begin{aligned}\Psi_{p^i,p}(g^*_{p^i}) &= \Psi_{p^i,p}(\Psi_{p^\infty,p^i}(g^*_{p^\infty})) = \Psi_{p^\infty,p}(g^*_{p^\infty}) = \Psi_{p^\infty,p}(g_{p^\infty}) = \Psi_{p^i,p}(\Psi_{p^\infty,p^i}(g_{p^\infty}))\\ &= \Psi_{p^i,p}(g_{p^i}).\end{aligned}$$

Finally,

$$\Psi_{p^i,p^j}(g^*_{p^i}) = \Psi_{p^i,p^j}(\Psi_{p^\infty,p^i}(g^*_{p^\infty})) = \Psi_{p^\infty,p^j}(g^*_{p^\infty}) = g^*_{p^j},$$

for any $i, j \in \mathbb{N} \cup \{\infty\}$ such that $i \geq j$. □

Example 5. Let

$$g_{3^\infty}(X) = 3X^2 + \left(1 + \sum_{i=2}^{\infty} 3^i\right) X + \sum_{i=1}^{\infty} 3^i \in R_{3^\infty}[X],$$

and $\{g_{3^i}\}_{i\in\mathbb{N}\cup\{\infty\}}$ such that $g_{3^i} = \Psi_{3^\infty,3^i}(g_{3^\infty}) \in R_{3^i}[X]$. By definition, these sequence forms a chain of lifts of $\Psi_{3^\infty,3}(g_{3^\infty}) = X$, since, for any $i \geq j$,

$$\Psi_{3^i,3^j}(g_{3^i}) = \Psi_{3^i,3^j}(\Psi_{3^\infty,3^i}(g_{3^\infty})) = \Psi_{3^\infty,3^j}(g_{3^\infty}) = g_{3^j}.$$

Let us find a sequence $\{g^*_{3^i}\}_{i\in\mathbb{N}\cup\{\infty\}}$ satisfying the conditions in Theorem 3. Observe that

$$g_{3^\infty}(X) = \left(X + \sum_{i=1}^{\infty} 3^i\right)(3X + 1). \tag{4}$$

Let $g^*_{3^\infty}(X) = X + \sum_{i=1}^{\infty} 3^i \in R_{3^\infty}[X]$, and $g^*_{3^i} = \Psi_{3^\infty,3^i}(g^*_{3^\infty}) \in R_{3^i}[X]$ for $i \in \mathbb{N}$. Since $g^*_{3^\infty}$ is monic, the $g^*_{3^i}$ are also monic. Moroever, for any $i \geq j$,

Table 1
Some examples of the polynomial chains described in Theorem 3.

$\mathbb{Z}_{3^i}$	$g_{3^i}(X)$	$g^*_{3^i}(X)$
$\mathbb{Z}_{3^\infty}$	$3X^2 + \left(1 + \sum_{i=2}^{\infty} 3^i\right) X + \sum_{i=1}^{\infty} 3^i$	$X + \sum_{i=1}^{\infty} 3^i$
$\vdots$	$\vdots$	$\vdots$
$\mathbb{Z}_{27}$	$3X^2 + 10X + 12$	$X + 12$
$\mathbb{Z}_9$	$3X^2 + X + 3$	$X + 3$
$\mathbb{Z}_3$	X	X

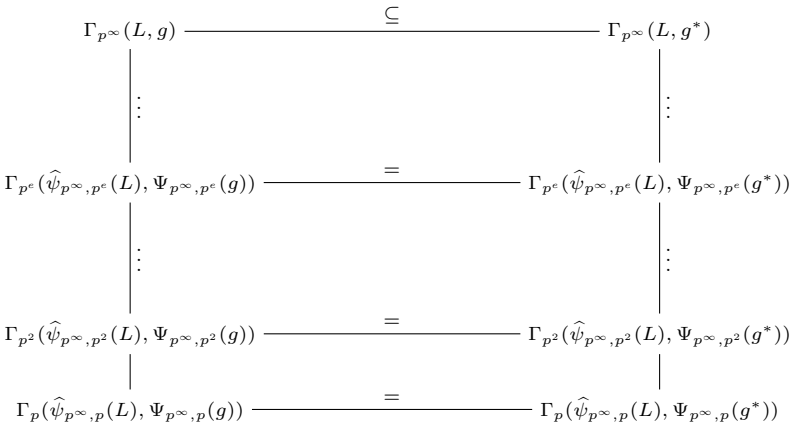

Fig. 1. A map showing the relations between the different Goppa codes presented in this paper. The polynomials of Goppa codes on the right column have a unit as leading coefficient.

$$\Psi_{3^i,3^j}(g^*_{3^i}) = \Psi_{3^i,3^j}(\Psi_{3^\infty,3^i}(g^*_{3^\infty})) = \Psi_{3^\infty,3^j}(g^*_{3^\infty}) = g^*_{3^j}.$$

In particular, for every $i \in \mathbb{N} \cup \{\infty\}$,

$$\Psi_{3^i,3}(g^*_{3^i}(X)) = X = \Psi_{3^i,3}(g_{3^i}(X)).$$

Finally, considering Equation (4) modulo p^i,

$$g_{3^i}(X) = g^*_{3^i}(X)\Psi_{3^\infty,3^i}(3X+1),$$

so $g^*_{3^i}$ divides g_{3^i}. Hence, the sequence of polynomials $\{g^*_{3^i}\}_{i\in\mathbb{N}\cup\{\infty\}}$ satisfies the conditions established in Theorem 3. Table 1 shows some examples of these polynomials.

Remark 5. Lemma 4 creates an infinite chain of codes, as seen in Fig. 1. In general, it is not true that $\Gamma_{p^\infty}(L,g) = \Gamma_{p^\infty}(L,g^*)$. For instance, let $g(X) \in R_{p^\infty}[X]$ such that $\deg g > h \deg g^*$. By the Singleton bound, Corollary 1 and Theorem 1,

$$\dim_{\mathbb{Z}_{p^\infty}} \Gamma_{p^\infty}(L,g) \leq n - d(\Gamma_{p^\infty}(L,g)) + 1$$

$$\begin{aligned} &\leq n - \deg g \\ &< n - h \deg g^* \\ &\leq \dim \Gamma_{p^\infty}(L, g) \end{aligned}$$

This result also lets us set a parity-check matrix for a chain of Goppa codes.

Corollary 2. *Let $\Gamma_{p^\infty}(L, g)$ be a Goppa code, and let $g^* \in R_{p^\infty}[X]$ be the polynomial from Theorem 3. Then, $\Gamma_{p^\infty}(L, g)$ has parity-check matrix (1), and for any $e \in \mathbb{N}$, $\Gamma_{p^e}(\widehat{\psi}_{p^\infty,p^e}(L), \Psi_{p^\infty,p^e}(g))$ has parity-check matrix $\left(\psi_{p^\infty,p^e}(H^*_{ij})\right)$, where H^* is the matrix defined in (3).*

Proof. It is a direct consequence of Theorems 2 and 3. □

3. Direct lifting of Goppa codes

Next, we want to show some special chains of isomorphic Goppa codes for different values of $e \in \mathbb{N}$. We start by the proving some easy computations in R_{p^e}.

Lemma 6. *Let $e, k \in \mathbb{N}$, $a + p^{e-1}b \in R_{p^e}$ a unit and $g \in R_{p^e}[X]$.*

(i) $(a + p^{e-1}b)^k = a^k + p^{e-1}ka^{k-1}b$.
(ii) If a is a unit, $(a + p^{e-1}b)^{-1} = a^{-1}(1 - p^{e-1}a^{-1}b)$.
(iii) $g(a + p^{e-1}b) = g(a) + p^{e-1}bg'(a)$, *where g' denotes the derivative of g.*

Proof. Part (i) can be proved using the binomial formula, and the proof for part (ii) is straightforward. For part (iii), let $g(X) = \sum_{i=1}^{r} g_i X$. By part (i) of this lemma,

$$g(a + p^{e-1}b) = \sum_{i=1}^{r} g_i(a + p^{e-1}b)^i = \sum_{i=0}^{r} g_i a^i + p^{e-1}b \sum_{i=1}^{r} g_i i a^{i-1} = g(a) + p^{e-1}bg'(a). \quad \square$$

Now, we show the intersection of two Goppa codes over $\mathbb{Z}_{p^e}$ generated by the same polynomial modulo p^{e-1}. For the sake of simplicity, from now on we take the components of the parameter L to be units, but these results can be extended to any Goppa codes.

Lemma 7. *Let $e \in \mathbb{N}$, let $\Gamma_{p^e}(L, g)$ be a Goppa code and let $L' = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_{p^h}^n$. Let g^* be a monic polynomial satisfying the conditions from Lemma 3. If $c \in \Gamma_{p^e}(L, g)$, then $c \in \Gamma_{p^e}(L + p^{e-1}L', g)$ if and only if*

$$\sum_{i=1}^{n} c_i g^*(\alpha_i)^{-1} \alpha_i^{j-2} (\alpha_i g^*(\alpha_i)^{-1} g^{*\prime}(\alpha_i) + j - 1)\beta_i = 0 \pmod{p}$$

for all $j \in \{1, \ldots, \deg g^*\}$.

Proof. Let $c \in \Gamma_{p^e}(L, g)$. According to Theorem 2,

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g^*(\alpha_i)^{-1} = 0, \qquad j \in \{1, \dots, r\},$$

where $r = \deg g^*$. Similarly, $c \in \Gamma_{p^e}(L + p^{e-1}L', g)$ if and only if

$$\sum_{i=1}^{n} c_i (\alpha_i + p^{e-1}\beta_i)^{j-1} g^*(\alpha_i + p^{e-1}\beta_i)^{-1} = 0, \qquad j \in \{1, \dots, r\}.$$

By Lemma 6, this is equivalent to

$$\sum_{i=1}^{n} c_i (\alpha_i^{j-1} + p^{e-1}(j-1)\beta_i \alpha_i^{j-2}) g^*(\alpha_i)^{-1} (1 - p^{e-1}\beta_i g^*(\alpha_i)^{-1} g^{*\prime}(\alpha_i)) = 0,$$
$$j \in \{1, \dots, r\}.$$

The equations above can be written as

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g^*(\alpha_i)^{-1} + p^{e-1} \sum_{i=1}^{n} c_i g^*(\alpha_i)^{-1} \alpha_i^{j-2} (\alpha_i g^*(\alpha_i)^{-1} g^{*\prime}(\alpha_i) + j - 1)\beta_i = 0,$$
$$j \in \{1, \dots, r\}.$$

Since $c \in \Gamma_{p^e}(L, g)$, it follows that $c \in \Gamma_{p^e}(L + p^{e-1}L', g)$ if and only if

$$\sum_{i=1}^{n} c_i g^*(\alpha_i)^{-1} \alpha_i^{j-2} (\alpha_i g^*(\alpha_i)^{-1} g^{*\prime}(\alpha_i) + j - 1)\beta_i = 0 \pmod{p}$$

for all $j \in \{1, \dots, r\}$. □

As a consequence, for every Goppa code over $\mathbb{Z}_{p^e}$, there exists an isomorphic Goppa code over $\mathbb{Z}_{p^{e+1}}$.

Theorem 4. *Let $e \in \mathbb{N}$ and let $\Gamma_{p^e}(L, g)$ be a Goppa code. There exists $L' \in \mathbb{F}_{p^{hk}}^n$ such that, for any $f \in R_{p^{e+1}}[X]$ such that $\Psi_{p^{e+1}, p^e}(f) = g$,*

$$\Gamma_{p^{e+1}}(L + p^e L', f) = p\widehat{\psi}_{p^{e+1}, p^e}^{-1}(\Gamma_{p^e}(L, g)).$$

Proof. Let $f \in R_{p^{e+1}}[X]$ be such that $\Psi_{p^{e+1}, p}(f) = g$. We consider the family of lifts of $\Gamma_{p^e}(L, g)$ with polynomial f,

$$C = \{\Gamma_{p^e}(L + p^{e-1}L', f) \mid L' \in \mathbb{F}_{p^{hs}}, s \in \mathbb{N}\}.$$

Since there exists a finite amount of submodules of $\mathbb{Z}_{p^{e+1}}^n$, C is finite. Hence, there exists $h \in \mathbb{N}$ large enough such that $C = \{\Gamma_{p^{e+1}}(L + p^{e-1}L_i, f)\}_{i=1}^{|C|}$ and $L_i = (\beta_1^{(i)}, \dots, \beta_n^{(i)}) \in \mathbb{F}_{p^{hs}}^n$ for $i \in \{1, \dots, |C|\}$. Let us consider a $\mathbb{F}_{p^{hs}}$-basis $\mathcal{B} = \{1, \beta_1, \dots, \beta_n\}$ of $\mathbb{F}_{p^{hs(n+1)}}$. For any $i \in \mathbb{N}$, $\mathcal{B}_i = \{1, \beta_1 - \beta_1^{(i)}, \dots, \beta_n - \beta_n^{(i)}\}$ is also a basis of $\mathbb{F}_{p^{hs(n+1)}}$. We consider $L^* = (\beta_1, \dots, \beta_n)$ and $L_i^* = (\beta_1 - \beta_1^{(i)}, \dots, \beta_n - \beta_n^{(i)})$ for $i \in \{1, \dots, |C|\}$. Let us show that

$$\Gamma_{p^{e+1}}(L + p^e L^*, f) \cap \Gamma_{p^{e+1}}(L + p^e L_i, f) \subseteq p\mathbb{Z}_{p^e}^n.$$

Let $c \in \Gamma_{p^{e+1}}(L+p^eL^*, f) \cap \Gamma_{p^{e+1}}(L+p^eL_i, f)$ be a non-zero codeword, and let $L+p^eL_i = (\alpha_1, \dots, \alpha_n)$. Since $L + p^eL^* = L + p^eL_i + p^eL_i^*$, Lemma 7 implies

$$\sum_{i=1}^{n} c_i f^*(\alpha_i)^{-1} \alpha_i^{j-2} (\alpha_i f^*(\alpha_i)^{-1} f^{*\prime}(\alpha_i) + j - 1)\beta_i = 0 \tag{5}$$

modulo p, for a f^* and for every $j \in \{1, \dots, \deg f^*\}$. Let us assume $\widehat{\psi}_{p^{e+1},p}(c) \neq 0$. Since $c \in \Gamma_{p^{e+1}}(L + p^eL_i, f)$, from Theorem 1 it follows that $\widehat{\psi}_{p^{e+1},p}(c) \in \Gamma_p(\widehat{\psi}_{p^{e+1},p}(L), f)$ and therefore $w(\widehat{\psi}_{p^{e+1},p}(c)) \geq \deg f^* + 1$. If $f^{*\prime}(X) = 0$, Equation (5) for $j = 1$ is a contradiction. In fact, that there are at least $\deg f^* + 1$ non-zero terms modulo p and $\mathcal{B}_i$ is a $\mathbb{F}_{p^{hs}}$-basis of $\mathbb{F}_{p^{hs(n+1)}}$, so any $\mathbb{F}_{p^{hs}}$-linear combination of its elements being zero implies the coefficients being also zero. On the other hand, if $f^{*\prime}(X) \neq 0$, it has at most $\deg f^* - 1$ roots, so at least 2 terms in Equation (5) for $j = 2$ are non-zero. Similarly, $\mathcal{B}_i$ being a basis contradicts the equality. We conclude that $\Gamma_{p^{e+1}}(L+p^eL^*, f) \cap \mathcal{C} \subseteq p\mathbb{Z}_{p^{e+1}}^n$ for any possible Goppa code $\mathcal{C}$, so $\Gamma_{p^{e+1}}(L + p^eL^*, f) \subseteq p\mathbb{Z}_{p^{e+1}}^n$. By Theorem 1,

$$\begin{aligned}
\Gamma_{p^{e+1}}(L + p^eL^*, f) &= \Gamma_{p^{e+1}}(L + p^eL^*, f) \cap p\mathbb{Z}_{p^{e+1}}^n \\
&= p\widehat{\psi}_{p^{e+1},p^e}^{-1}(\Gamma_{p^e}(\widehat{\psi}_{p^{e+1},p^e}(L + p^eL^*), \Psi_{p^{e+1},p^e}(f))) \\
&= p\widehat{\psi}_{p^{e+1},p^e}^{-1}(\Gamma_{p^e}(L, g)). \quad \square
\end{aligned}$$

Example 6. Part 2 of Example 3 shows two instances of Goppa codes over $\mathbb{Z}_{2^e}$ which are exact copies of the codes over $\mathbb{Z}_{2^{e-1}}$ and are obtained by lifting the corresponding L and g.

Corollary 3. *Let $e \in \mathbb{N}$, let $\Gamma_{p^e}(L, g)$ be a Goppa code, and let $g_\infty \in R_{p^\infty}[X]$ such that $\Psi_{p^\infty,p}(g_\infty) = g$. Then, there exists $L_\infty \in R_{p^\infty}$ such that $\widehat{\psi}_{p^\infty,p^e}(L_\infty) = L$, $\Gamma_{p^\infty}(L_\infty, g_\infty) = \{\boldsymbol{0}\}$ and for any $j \geq e$,*

$$\Gamma_{p^j}(\widehat{\psi}_{p^\infty,p^j}(L_\infty), \Psi_{p^\infty,p^j}(g_\infty)) = p^{j-e}\widehat{\psi}_{p^j,p^e}^{-1}(\Gamma_{p^e}(L, g)).$$

Proof. The proof is the result of repeatedly applying Theorem 4 infinitely many times to $\Gamma_e(L, g)$. The resultant lift of L to R_{p^∞} defines a series of Goppa codes over $\mathbb{Z}_{p^j}$ which

are exact copies of the original $\Gamma_{p^e}(L,g)$ and multiples of p^{j-e}. Moreover, by part (iii) of Theorem 1, the code over the p-adic integers must be trivial. □

4. Changes in the polynomial

In the previous section, we have studied the changes in the Goppa codes by modifying L. Now, let us change the Goppa polynomial. First, let us recall the following result for Goppa codes found in [7].

Lemma 8. *Let $g \in R_2[X]$ be a square-free polynomial. Then, $\Gamma_2(L,g) = \Gamma_2(L,g^2)$.*

Now, we can prove the following result for $p = 2$. This theorem is the generalization of its quaternary version, shown in [5].

Theorem 5. *Let $g \in R_{2^e}[X]$ be a square-free polynomial with a unit as its leading coefficient, let $\Gamma_{2^e}(L,g)$ be a Goppa code, and $g_2 \in R_{2^e}[X]$ such that $\deg g_2 \leq \deg g$. Then,*

$$\Gamma_{2^e}(L,g) = \Gamma_{2^e}(L, g + 2^{e-1}g_2).$$

Proof. Let us prove $\Gamma_{2^e}(L,g) \subseteq \Gamma_{2^e}(L, g + 2^{e-1}g_2)$ for any polynomial g_2 satisfying $\deg g_2 \leq \deg g$. Let $c \in \Gamma_{2^e}(L,g)$. According to Theorem 1, $\widehat{\psi}_{2^e,2}(c) \in \Gamma_2(\widehat{\psi}_{2^e,2}(L), \Psi_{2^e,2}(g))$. Since g is square-free, $\Psi_{2^e,2}(g)$ is also square-free, and by Lemma 8, $\widehat{\psi}_{2^e,2}(c) \in \Gamma_2(\widehat{\psi}_{2^e,2}(L), \Psi_{2^e,2}(g)^2)$. By Lemma 1 and since the leading coefficient of g is a unit, this happens when

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} = 0 \pmod 2$$

for all $j \in \{1, \dots 2\deg g\}$. Equivalently,

$$\sum_{i=1}^{n} c_i \alpha_i^{k+j-1} g(\alpha_i)^{-2} = 0 \pmod 2$$

for all $j \in \{1, \dots, \deg g\}$ and $k \in \{0, 1, \dots, \deg g\}$. The equations above can be written as

$$\sum_{k=0}^{r} a_k \sum_{i=1}^{n} c_i \alpha_i^k \alpha_i^{j-1} g(\alpha_i)^{-2} = 0 \pmod 2$$

for all $j \in \{1, \dots, \deg g\}$ and $a_i \in R_{2^e}$ or, equivalently,

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} g_2(\alpha_i) = 0 \pmod 2$$

for all $j \in \{1, \dots, \deg g\}$ and $g_2 \in R_{p^e}[X]$ such that $\deg g_2 \leq \deg g$. Here, we have taken $g_2(X) = \sum_{k=0}^{r} a_k X^k$. Since $c \in \Gamma_{2^e}(L, g)$, by Lemma 1 and since the leading coefficient of g is a unit, $\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} = 0$ for all $j \in \{1, \dots, \deg g\}$, so this is equivalent to

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} + 2^{e-1} \sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-2} g_2(\alpha_i) = 0$$

for all $j \in \{1, \dots, \deg g\}$ and g_2 satisfying the hypothesis. Finally, by Lemma 6, the expression above can be written as

$$\sum_{i=1}^{n} c_i \alpha_i^{j-1} g(\alpha_i)^{-1} (1 - 2^{e-1} g(\alpha_i)^{-1} g_2(\alpha_i)) = 0$$

for all $j \in \{1, \dots, \deg g\}$ and g_2 satisfying the conditions of the theorem. Since the leading coefficient of $g + 2^{e-1} g_2$ is also a unit, this is equivalent to $c \in \Gamma_{2^e}(L, g + 2^{e-1} g_2)$. □

Corollary 4. *Let $e \in \mathbb{N}$, $g \in R_{2^e}[X]$ and let $g^* \in R_{2^e}[X]$ be the polynomial that, by Lemma 3, has the same projection as g and has a unit as its leading coefficient. Let $g_2 \in R_{2^e}[X]$ such that $\deg g_2 \leq \deg g^*$. If $\Psi_{2^e,2}(g)$ is square-free,*

$$\Gamma_{2^e}(L, g) = \Gamma_{2^e}(L, g^* + 2^{e-1} g_2).$$

If q is the polynomial satisfying $q(X) g^*(X) = g(X)$, then

$$\Gamma_{2^e}(L, g) = \Gamma_{2^e}(L, g + 2^{e-1} q g_2).$$

Proof. The proof follows directly from Theorem 5. □

Example 7. Let us consider again Example 1. Observe that $g(X) = X(X^2 + \alpha^4 X + \alpha^5)$, and $X^2 + \alpha^4 X + \alpha^5$ has no roots in R_8, so g is square-free in R_8. By the previous theorem, we can check that $\Gamma_8(L, (1 + 4\alpha^2)X^3 + \alpha^4 X^2 + (\alpha^5 + 4\alpha)X + 4)$ is generated by the same generator matrix G from Example 1.

5. Applications to cryptography

Goppa codes are the core of the original McEliece cryptosystem [9]. This cryptographic scheme, as well as Niederreiter's [11], can be generalized to rings.

Definition 3. Let $e \in \mathbb{N} \cup \{\infty\}$, $n \in \mathbb{N}$ and $\mathcal{C} \subseteq \mathbb{Z}_{p^e}^n$ be a $\mathbb{Z}_{p^e}$-linear code with generator matrix G, error-correcting capacity $t \geq t_0$ and an efficient decoding algorithm $\mathcal{D}$. We define the $\mathbb{Z}_{p^e}$ McEliece cryptosystem as follows. The secret key is formed by G, $\mathcal{D}$, a random permutation matrix P and a random nonsingular matrix S. The pair (G', t_0) forms the public key, where $G' = SGP$. We define the encryption function as $E(m) =$

$mG'+z$, where $z \in \mathbb{Z}_{p^e}^n$ is a randomly generated error satisfying $w(z) \leq \delta$. The decryption process consists of: first, multiplying the ciphertext by P^{-1}, then apply the decoding algorithm $\mathcal{D}$ and finally solving linear equation systems.

The security of the McEliece cryptosystem is based both on the NP-hardness of the decoding problem of random linear codes over $\mathbb{Z}_{p^e}$, and the indistinguishability of the code $\mathcal{C}$, i.e., one should not be able to separate $\mathcal{C}$ from a random $\mathbb{Z}_{p^e}$-linear code.

Regarding the former, Elwyn R. Berlekamp, McEliece and Henk C.A. van Tilborg proved the difficulty of the problem in [2] for the case $p^e = 2$. This proof can be generalized to $\mathbb{Z}_{p^e}$-linear codes [13]. On the other hand, the original McEliece cryptosystem uses binary Goppa codes, and this family of codes still seems to be the most reliable today. When $e \in \mathbb{N}$, one can prove that the distinguishability problem for the binary Goppa codes can be reduced to the distinguishability of p^e-ary Goppa codes. In fact, both distinguishability problems are equivalent.

Theorem 6. *Let $e \in \mathbb{N}$. The distinguishability problems for Goppa codes over $\mathbb{Z}_p$ and $\mathbb{Z}_{p^e}$ are equivalent.*

Proof. Let us assume there exists a distinguisher $\mathcal{D}$ for Goppa codes over $\mathbb{Z}_{p^e}$, i.e., a polynomial time algorithm to distinguish the code. Let $\mathcal{C} = p^{e-1}\widehat{\psi}_{p^e,p}^{-1}(\Gamma_p(L,g))$. According to Corollary 3, $\mathcal{C}$ is a Goppa code over $\mathbb{Z}_{p^e}$ for some L_e and g_e such that $\widehat{\psi}_{p^e,p}(L_e) = L$ and $\Psi_{p^e,p}(g_e) = g$. Applying $\mathcal{D}$ to $\mathcal{C}$ identifies $\mathcal{C}$, hence distinguishing $\Gamma_p(L,g)$.

Now, let us assume there exists a distinguisher $\mathcal{D}$ for p-ary Goppa codes, i.e., a polynomial time algorithm to distinguish a Goppa code over $\mathbb{Z}_p$. Let $\mathcal{C}$ the p-ary code isomorphic to $\Gamma_{p^e}(L,g) \cap p^{e-1}\mathbb{Z}_{p^e}^n$. According to Theorem 1, $\mathcal{C}$ is a Goppa code of parameters $\widehat{\psi}_{p^e,p}(L)$ and $\Psi_{p^e,p}(g)$. Applying $\mathcal{D}$ to $\mathcal{C}$ identifies $\mathcal{C}$, hence also distinguishing $\Gamma_{p^e}(L,g)$. □

This result rises the potential cryptographic interest of Goppa codes. In fact, if $p = 2$, the security of every Goppa code reduces to the security of the original McEliece cryptosystem, which is considered by far one of the safest cryptographic schemes, even resisting attacks by a quantum computer [12].

6. Conclusions and future work

In this paper, we have presented Goppa codes over the p-adic integers and integers modulo a power of p. We have proved their basic properties, and some isomorphisms between Goppa codes over different rings. Finally, while we leave the possible applications of Goppa codes over the p-adics as future work, we have shown a possible cryptographic application of these codes over the integers modulo p^e. This is interesting due to the raising popularity of code-based cryptography as one of the few quantum-resistant families of cryptographic schemes.

Acknowledgments

This work is part of a virtual stay in the University of Scranton. The author wants to thank professor S. Dougherty for his suggestions and comments. The author also thanks the reviewers for their remarks.

References

[1] A.A. de Andrade, R. Palazzo Jr., Goppa and Srivastava codes over finite rings, Comput. Appl. Math. 24 (2) (2005), https://doi.org/10.1590/S0101-82052005000200005.
[2] E. Berlekamp, R. McEliece, H. van Tilborg, On the inherent intractability of certain coding problems (corresp.), IEEE Trans. Inf. Theory 24 (3) (1978), https://doi.org/10.1109/TIT.1978.1055873.
[3] M. Cruz-López, A. Murillo-Salas, A recurrent random walk on the p-adic integers, Braz. J. Probab. Stat. 30 (1) (2016) 145–154, https://doi.org/10.1214/14-BJPS265.
[4] S. Dougherty, Y.H. Park, Codes over the p-adic integers, Des. Codes Cryptogr. 39 (1) (2006) 65–80, https://doi.org/10.1007/s10623-005-2542-x.
[5] M. Epelde, X. Larrucea, I.F. Rúa, On quaternary Goppa codes, Discrete Math. 343 (9) (September 2020), https://doi.org/10.1016/j.disc.2020.111962.
[6] V.D. Goppa, A new class of linear correcting codes, Probl. Pereda. Inf. 6 (3) (1970) 24–30.
[7] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Mathematical Library, vol. 16, North-Holland Publ. Co, Amsterdam, 1981.
[8] B.R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, vol. 28, M. Dekker, New York, ISBN 0824761618, 1974.
[9] R.J. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, Deep Space Network Progress Report 44, 1978.
[10] J. Munkres, Topology, Prentice-Hall of India, New Dehli, ISBN 978-81-203-2046-8, 2004, p. 169.
[11] H. Niederreiter, Knapsack type cryptosystems and algebraic coding theory, Probl. Control Inf. Theory 15 (1986).
[12] Post-quantum cryptography standardization process, https://csrc.nist.gov/Projects/post-quantum-cryptography.
[13] V. Weger, K. Khathuria, A.L. Horlemann, M. Battaglioni, P. Santini, E. Persichetti, On the hardness of the Lee syndrome decoding problem, preprint, https://doi.org/10.48550/arXiv.2002.12785, 2020.