Decoding of (Interleaved) Generalized Goppa Codes

Hedongliang Liu[1,*], Sabine Pircher[1,2,*], Alexander Zeh[2], Antonia Wachter-Zeh[1]
[1]Institute for Communications Engineering, Technical University of Munich (TUM), Munich, Germany
[2]HENSOLDT Cyber GmbH, Research & Development, Ottobrunn, Munich, Germany
{lia.liu, antonia.wachter-zeh}@tum.de, {sabine.pircher, alexander.zeh}@hensoldt-cyber.de

***Abstract*—Generalized Goppa codes are defined by a *code locator* set $\mathcal{L}$ of polynomials and a *Goppa polynomial* $G(x)$. When the degree of all code locator polynomials in $\mathcal{L}$ is one, generalized Goppa codes are classical Goppa codes. In this work, *binary generalized Goppa codes* are investigated. First, a parity-check matrix for these codes with code locators of any degree is derived. A careful selection of the code locators leads to a lower bound on the minimum Hamming distance of generalized Goppa codes which improves upon previously known bounds. A quadratic-time decoding algorithm is presented which can decode errors up to half of the minimum distance. *Interleaved generalized Goppa codes* are introduced and a joint decoding algorithm is presented which can decode errors beyond half the minimum distance with high probability. Finally, some code parameters and how they apply to the *Classic McEliece* post-quantum cryptosystem are shown.**

I. Introduction

Goppa codes [1] are currently receiving renewed attention due to their applicability in the McEliece public-key cryptosystem [2], which has remained unbroken for more than 40 years. *Generalized Goppa codes* (GGCs) are an extension of Goppa codes to a new class of codes which are defined by a set of *code locator polynomials* and a *Goppa polynomial* [3], [4]. A special class of binary GGCs which is perfect in the weighted Hamming metric was introduced in [5] and cyclic GGCs were investigated in [6], [7]. Recent works [8], [9] present a construction of binary GGCs with irreducible code locator polynomials of first and second degree.

The McEliece cryptosystem is believed to be secure against attacks of a capable quantum computer and the Niederreiter's [10] dual version of the McEliece cryptosystem is a finalist in the ongoing post-quantum NIST competition [11] under the name *Classic McEliece* [12]. Wild Goppa codes [13] are shown to have a larger minimum distance than classical Goppa codes and are deployed in *Wild McEliece* [14], which is also part of *Classic McEliece*. In [9], *Classic McEliece* using binary GGCs with code locator polynomials of first and second degree is proposed. Compared to classical Goppa codes, the length of GGCs can be increased by using higher-degree code locators for a fixed field size or, vice versa, for a fixed length, GGCs require a smaller field size. In practice, performing computations over smaller field sizes reduces the complexity of calculations and might therefore lead to more efficient encryption and decryption procedures. GGCs may also be used as locally correctable codes in coded distributed storage systems due to their local error-correction capability on locations of different degrees. In [15] their ability to decode localized errors and to correct more errors than classical Goppa codes (with certain failure probability) was investigated.

In this work, we investigate binary GGCs. Our main contributions are: in Section III, we derive a parity-check matrix for GGCs with code locators of any degree, where an instance for GGCs with degree-2 code locators is presented in [8], [9] without proof; we provide a formal proof for the lower bound on the minimum Hamming distance of GGCs, which was stated in [8], [9] without proof and we show that the lower bound for GGCs with even-degree code locators is improved compared to the general lower bound. In Section IV we provide an explicit decoding algorithm for GGCs and we prove the unique decoding radius for GGCs. To deal with burst errors, we introduce *interleaved generalized Goppa codes* in Section V. We provide an explicit decoding algorithm and derive the new maximum decoding radius for GGCs. Moreover, we list some code parameters of GGCs and discuss their applicability to the McEliece cryptosystem in Section VI.

II. Preliminaries

We denote by $[a, b]$ the set of integers $\{i|a \leq i \leq b\}$ and if $a = 1$, we omit it from our notation and write $[b]$. A finite field of size q is denoted by $\mathbb{F}_q$. Row vectors are denoted by bold lower-case letters (e.g., $\boldsymbol{c}$) and column vectors by $\boldsymbol{c}^\top$. Denote $\mathrm{supp}(\boldsymbol{c}) := \{i|c_i \neq 0\}$. Denote matrices by bold capital letters (e.g., $\boldsymbol{C}$) and its i-th row by $\boldsymbol{c}^{(i)}$. We consider the Hamming metric for weight and distance. Sets are denoted by calligraphic letters (e.g., $\mathcal{L}$) and its size is denoted by $|\mathcal{L}|$.

Let $\mathbb{F}_q[x]$ denote a polynomial ring with coefficients in $\mathbb{F}_q$. For a polynomial $f(x)$, its degree is denoted by $\deg f(x)$ and its formal derivative is denoted by $f'(x)$. The greatest common divisor of two polynomials is denoted by $\gcd(f(x), g(x))$.

Lemma 1 (Roots of Irreducible Polynomials [16, p. 52]). *Let q be a prime power. Any irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ of degree k can be represented as*

$$f(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{k-1}}),$$

where $\beta \in \mathbb{F}_{q^k}$ and $\mathbb{F}_{q^k}$ is called the splitting field *of $f(x)$.*

* The first two authors contributed equally to this work.

The work A. Wachter-Zeh has been supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 801434). The work of H. Liu has been supported by the DFG with a German Israeli Project Cooperation (DIP) under grant no. KR3517/9-1.

Lemma 2 (Number of Irreducible Polynomials [17, p. 225]). *The number $\mathcal{I}_q(t)$ of irreducible polynomials of degree t over $\mathbb{F}_q$ can be calculated by*

$$\mathcal{I}_q(t) = \frac{1}{t}\sum_{k|t} \mu(k)\cdot q^{\frac{t}{k}}$$

where $\mu(t)$ is the Möbius function (cf. [17, p. 224])

$$\mu(t) = \begin{cases} 1 & \text{if } t=1 \\ (-1)^s & \text{if } t \text{ is a product of } s \text{ distinct prime} \\ 0 & \text{otherwise.} \end{cases}$$

III. Binary Generalized Goppa Codes

We introduce a parity-check matrix of generalized Goppa codes (GGCs) with code locators of any degree and provide a proof of the lower bound on the minimum Hamming distance of GGCs which is stated in [8], [9] without proof. We show that with even-degree code locators, the lower bound can be slightly improved.

Definition 1. *Let m,n,r,q be positive integers such that $rm \leqslant n$ and $q=2^m$. Given a polynomial $G(x)\in\mathbb{F}_q[x]$ of degree r and a set of irreducible polynomials*

$$\mathcal{L} = \{f_1(x), f_2(x), \dots, f_n(x)\} \tag{1}$$

with $\gcd(f_i(x), f_j(x)) = 1, \forall i \neq j$, and $\gcd(f_i(x), G(x)) = 1$, $\forall i\in[n]$. Then, the binary generalized Goppa code *is defined by*

$$\Gamma(\mathcal{L}, G) := \left\{ \boldsymbol{c}\in\mathbb{F}_2^n \;\middle|\; \sum_{i=1}^{n} c_i \frac{f_i'(x)}{f_i(x)} = 0 \bmod G(x)\right\}, \tag{2}$$

where $f_i'(x)$ is the formal derivative of $f_i(x)$. We call $G(x)$ the Goppa polynomial *and $\mathcal{L}$ the set of* code locators[1].

In the following theorem, we derive a parity-check matrix for generalized Goppa codes with code locators of arbitrary degree.

Theorem 1 (Parity-Check Matrix). *Given a binary generalized Goppa code $\Gamma(\mathcal{L}, G)$ as in Definition 1, where the code locators in $\mathcal{L}$ are $\mathbb{F}_q$-irreducible polynomials*

$$f_i(x) = \prod_{j=0}^{l_i-1}\left(x-\gamma_i^{q^j}\right),\ \forall i\in[n]$$

of degree l_i, where $\gamma_i^{q^j}\in\mathbb{F}_{q^{l_i}}$ are the roots of $f_i(x)$. Let $r=\deg G(x)$ and $n=|\mathcal{L}|$. A parity-check matrix $\boldsymbol{H}$ of $\Gamma(\mathcal{L},G)$ such that $\boldsymbol{H}\boldsymbol{c}^\top = \boldsymbol{0}$, $\forall \boldsymbol{c}\in\Gamma(\mathcal{L},G)$ is

$$\boldsymbol{H} = [\boldsymbol{h}_1^\top\ \boldsymbol{h}_2^\top\ \cdots\ \boldsymbol{h}_n^\top] \in \mathbb{F}_q^{r\times n} \tag{3}$$

with $\boldsymbol{h}_i = (h_{i,1}\ h_{i,2}\ \cdots\ h_{i,r})$, where

$$h_{i,j} = \sum_{\iota=0}^{l_i-1}\frac{\gamma_i^{(j-1)q^\iota}}{G\left(\gamma_i^{q^\iota}\right)},\ \forall i\in[n],\ j\in[r].$$

Proof: From Definition 1, requiring $\gcd(f_i(x), G(x)) = 1$ implies that the roots of $f_i(x)$ are not roots of $G(x)$, i.e., $G(\gamma_i^{q^j}) \neq 0, \forall j=0,\dots,l_i-1, i\in[n]$. The inverse of a polynomial $f_i(x)$ can be found by the *extended Euclidean (EEA) Algorithm* [17, Sec. 6.4]. Denote the Goppa polynomial by

$$G(x) = G_0 + G_1 x + \cdots + G_r x^r$$

with $G_r \neq 0$. Using the EEA, we obtain

$$\frac{f_i'(x)}{f_i(x)} \bmod G(x) = \left(\prod_{j=0}^{l_i-1} G\left(\gamma_i^{q^j}\right)\right)^{-1}\cdot \sum_{t=0}^{r-1} x^t\left(\sum_{k=t+1}^{r} G_k\left(\sum_{j=0}^{l_i-1}\gamma_i^{(k-1-t)q^j}\prod_{\substack{\xi=0,\\ \xi\neq j}}^{l_i-1} G\left(\gamma_i^{q^\xi}\right)\right)\right) \tag{4}$$

Plugging (4) into (2) and equating the coefficients of $x^t, \forall t\in[0,r-1]$ to zero, it can be verified that $\boldsymbol{c}\in\Gamma(\mathcal{L},G)$ if and only if $\boldsymbol{G}\boldsymbol{H}\cdot\boldsymbol{c}^\top = \boldsymbol{0}$, where

$$\boldsymbol{G} = \begin{bmatrix} G_r & 0 & \dots & 0 \\ G_{r-1} & G_r & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ G_1 & G_2 & \dots & G_r \end{bmatrix}.$$

Therefore, $\widetilde{\boldsymbol{H}} = \boldsymbol{G}\boldsymbol{H}$ is a parity-check matrix of $\Gamma(\mathcal{L},G)$. Since $\boldsymbol{G}$ is invertible, $\widetilde{\boldsymbol{H}}\cdot\boldsymbol{c}^\top = \boldsymbol{0} \iff \boldsymbol{H}\cdot\boldsymbol{c}^\top = \boldsymbol{0}$, which proves the statement. ■

A binary parity-check matrix $\boldsymbol{H}^{\text{bin}}\in\mathbb{F}_2^{rm\times n}$ of $\Gamma(\mathcal{L},G)$ can be obtained by replacing every entry in $\boldsymbol{H}$ from (3) with a length-m column vector representation over $\mathbb{F}_2$ according to some fixed basis of $\mathbb{F}_q$ over $\mathbb{F}_2$.

Theorem 2 (Dimension, Minimum Distance). *Given a binary generalized Goppa code $\Gamma(\mathcal{L},G)$ as in Definition 1, the dimension is*

$$k(\Gamma) = n - \text{rank}(\boldsymbol{H}^{\text{bin}}) \geqslant n - rm, \tag{5}$$

where $\boldsymbol{H}^{\text{bin}}\in\mathbb{F}_2^{rm\times n}$ is the $\mathbb{F}_2$-representation of $\boldsymbol{H}\in\mathbb{F}_{2^m}^{r\times n}$ from Theorem 1. The minimum Hamming distance is

$$d(\Gamma) \geqslant d_{\text{g}} := \frac{r+1}{l},$$

where $l = \max_{f(x)\in\mathcal{L}} \deg f(x)$.

Proof: It can be readily seen that $\boldsymbol{H}\boldsymbol{c}^\top = \boldsymbol{0} \iff \boldsymbol{H}^{\text{bin}}\boldsymbol{c}^\top = \boldsymbol{0}, \forall \boldsymbol{c}\in\Gamma(\mathcal{L},G)$. The dimension follows from the size of the parity-check matrix. To prove the minimum Hamming distance, consider a codeword $\boldsymbol{c}\in\Gamma$. Define

$$F_{\boldsymbol{c}}(x) := \prod_{i\,\in\,\text{supp}(\boldsymbol{c})} f_i(x),$$

where its formal derivative is denoted as

$$F_{\boldsymbol{c}}'(x) := \sum_{i\,\in\,\text{supp}(\boldsymbol{c})} f_i'(x) \prod_{\substack{j\,\in\,\text{supp}(\boldsymbol{c})\\ j\neq i}} f_j(x).$$

Furthermore, let

$$R_{\boldsymbol{c}}(x) := \sum_{i\,\in\,\text{supp}(\boldsymbol{c})} \frac{f_i'(x)}{f_i(x)} = \frac{F_{\boldsymbol{c}}'(x)}{F_{\boldsymbol{c}}(x)}, \tag{6}$$

[1] In the original definition [4], the code locators are defined by $f_i'(x)/f_i(x)$. For ease of notation, we define the code locators by $f_i(x)$ here.

where $f_i'(x)$ is the formal derivative of $f_i(x)$. Since all $f_i(x)$ have distinct roots, $\gcd(F_{\boldsymbol{c}}'(x), F_{\boldsymbol{c}}(x)) = 1$ and since $\gcd(f_i(x), G(x)) = 1,\ \forall i \in [n]$, $\gcd(F_{\boldsymbol{c}}(x), G(x)) = 1$. Then from (6),

$$R_{\boldsymbol{c}}(x) = 0 \mod G(x) \quad \iff \quad G(x)|F_{\boldsymbol{c}}'(x).$$

Note that $F_{\boldsymbol{c}}'(x)$ is the formal derivative of $F_{\boldsymbol{c}}(x)$. Since we are working over a field of characteristic 2, $F_{\boldsymbol{c}}'(x)$ only has even powers and is a perfect square. Let $\bar{G}(x)$ be the lowest-degree perfect square which is divisible by $G(x)$, then

$$G(x)|F_{\boldsymbol{c}}'(x) \quad \iff \quad \bar{G}(x)|F_{\boldsymbol{c}}'(x).$$

Thus,

$$\begin{aligned} \boldsymbol{c} \in \Gamma \quad &\iff \quad R_{\boldsymbol{c}}(x) = 0 \mod G(x) \\ &\iff \quad \bar{G}(x)|F_{\boldsymbol{c}}'(x). \end{aligned} \tag{7}$$

Denote $l_i = \deg f_i(x)$, then $\deg F_{\boldsymbol{c}}(x) = \sum_{i \in \text{supp}(\boldsymbol{c})} l_i$ and

$$\deg F_{\boldsymbol{c}}'(x) \leqslant \deg F_{\boldsymbol{c}}(x) - 1 = \sum_{i \in \text{supp}(\boldsymbol{c})} l_i - 1. \tag{8}$$

Consider a vector $\boldsymbol{v}_m$ whose support $\text{supp}(\boldsymbol{v}_m)$ concentrates on the locators of the highest degree $l = \max_i l_i$, then

$$\deg F_{\boldsymbol{v}_m}'(x) \leqslant \text{wt}(\boldsymbol{v}_m) \cdot l - 1. \tag{9}$$

Note that $\boldsymbol{v}_m$ is not necessarily a codeword. Let $\deg F_{\boldsymbol{v}_m}'(x) \overset{!}{\geqslant} \deg \bar{G}(x)$. We have $\text{wt}(\boldsymbol{v}_m) \geqslant (\deg \bar{G}(x) + 1)/l$. To have (7) fulfilled, we require

$$\deg F_{\boldsymbol{c}}'(x) \geqslant \deg \bar{G}(x) \quad \forall\ \boldsymbol{c} \in \Gamma. \tag{10}$$

Note that for any $\boldsymbol{c}$ with $\text{wt}(\boldsymbol{c}) < \text{wt}(\boldsymbol{v}_m)$, $\deg F_{\boldsymbol{c}}'(x) < \deg F_{\boldsymbol{v}_m}'(x)$, i.e., we cannot find a codeword $\boldsymbol{c}$ with $\text{wt}(\boldsymbol{c}) < \text{wt}(\boldsymbol{v}_m)$ such that $\deg F_{\boldsymbol{c}}'(x) \geqslant \deg F_{\boldsymbol{v}_m}'(x)$. Therefore, to fulfill (10),

$$\begin{aligned} d(\Gamma) &= \min_{\boldsymbol{c} \in \Gamma} \text{wt}(\boldsymbol{c}) \geqslant \text{wt}(\boldsymbol{v}_m) \\ &\geqslant \frac{\deg \bar{G}(x) + 1}{l} \geqslant \frac{\deg G(x) + 1}{l} = d_{\text{g}}. \qquad \blacksquare \end{aligned}$$

Classical Goppa codes with a Goppa polynomial which has only distinct roots are known as *separable* Goppa codes [18, Ch. 12]. In this paper we inherit this name and call the GGCs with a Goppa polynomial which has only distinct roots as *separable generalized Goppa codes*.

Corollary 1. *Given a Goppa polynomial $G(x)$ whose roots are all distinct, the binary* separable *generalized Goppa code $\Gamma(\mathcal{L}, G)$ is the same code as $\Gamma(\mathcal{L}, G^2)$ and the minimum distance is*

$$d(\Gamma) \geqslant d_{\text{sep}} := \frac{2r + 1}{l}. \tag{11}$$

Proof: Since all roots of $G(x)$ are distinct, $\bar{G}(x) = G(x)^2$ in the proof of Theorem 2. The statement follows herein. ■

The following corollary shows that with even-degree code locators, the lower bound on the minimum distance is increased by a difference of $1/l$ compared to (11).

Corollary 2. *Given a code locator set $\mathcal{L}$ of* even-degree *polynomials, the minimum distance of a binary separable generalized Goppa code $\Gamma(\mathcal{L}, G)$ is*

$$d(\Gamma) \geqslant d_{\text{even}} := \frac{2r + 2}{l}.$$

Proof: Since $\deg f_i(x)$ is even for all $f_i(x) \in \mathcal{L}$, $\deg F_{\boldsymbol{c}}(x)$ is even. Then $\deg F_{\boldsymbol{c}}'(x) \leqslant \sum_{i \in \text{supp}(\boldsymbol{c})} l_i - 2$ in (8) and $\deg F_{\boldsymbol{v}_m}'(x) \leq \text{wt}(\boldsymbol{v}_m) \cdot l - 2$ in (9) since we work over a field of characteristic 2. Together with the separable property from Corollary 1, the statement follows from the rest of the proof of Theorem 2. ■

Compared to classical Goppa codes, the code length n of the generalized Goppa codes is not limited by the field size $q = 2^m$, but by the number of irreducible polynomials in $\mathbb{F}_{2^m}[x]$. The result in the following theorem was stated in [8]. As a completion to Theorem 1 and Theorem 2 for the properties of binary generalized Goppa codes, we include it here.

Theorem 3 (Code Length [8])**.** *Let $q = 2^m$ for some integer m. Given a generalized Goppa code $\Gamma(\mathcal{L}, G)$. Denote $l = \max_{f(x) \in \mathcal{L}} \deg f(x)$. The length of $\Gamma(\mathcal{L}, G)$ is limited by*

$$n(\Gamma) \leqslant \sum_{t=1}^{l} \mathcal{I}_q(t), \tag{12}$$

where $\mathcal{I}_q(t)$ is the number of irreducible polynomials of degree t in the polynomial ring $\mathbb{F}_q[x]$ (see Lemma 2).

IV. Decoding of Generalized Goppa Codes

In this section, we present an explicit decoding algorithm for GGCs, where the decoding principle has been mentioned in [8]. This syndrome-based decoding algorithm is also a basis of the joint decoder for interleaved GGCs, which we present in Section V. Moreover, we show that the unique decoding radius for GGCs is $\lfloor \frac{d}{2} \rfloor$, which is different from the usual form $\lfloor \frac{d-1}{2} \rfloor$ for other codes by such decoding algorithm.

Definition 2. *Consider a binary generalized Goppa code $\Gamma(\mathcal{L}, G)$ and an error vector $\boldsymbol{e} \in \mathbb{F}_2^n$ where $n = |\mathcal{L}|$. Let $\mathcal{E} = \text{supp}(\boldsymbol{e})$. Define the* syndrome polynomial

$$s(x) := \sum_{i \in \mathcal{E}} e_i \frac{f_i'(x)}{f_i(x)} \mod G(x), \tag{13}$$

the error locator polynomial (ELP)

$$\Lambda(x) := \prod_{i \in \mathcal{E}} f_i(x), \tag{14}$$

and the error evaluator polynomial (EEP)

$$\Omega(x) := \sum_{i \in \mathcal{E}} e_i f_i'(x) \prod_{j \in \mathcal{E} \setminus \{i\}} f_j(x). \tag{15}$$

Assume transmitting a codeword $\boldsymbol{c} \in \Gamma(\mathcal{L}, G)$ and receiving a vector $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} \in \mathbb{F}_2^n$. The syndrome polynomial can be calculated from the received word $\boldsymbol{r}$ by

$$s(x) = \sum_{i=1}^{n} r_i \frac{f_i'(x)}{f_i(x)} \mod G(x). \tag{16}$$

Denote $s(x) = \sum_{i=1}^{r} s_i x^{r-i}$ where $\boldsymbol{s} = (s_1, \ldots, s_r) = \boldsymbol{r}\widetilde{\boldsymbol{H}}^\top$.

We present a syndrome-based decoder for $\Gamma(\mathcal{L}, G)$ in Algorithm 1. The main step of decoding is to determine $\Lambda(x)$

and $\Omega(x)$ given $s(x)$. In the following lemma we set up a key equation for decoding generalized Goppa codes.

Lemma 3 (Key Equation)**.** *Consider a binary generalized Goppa code* $\Gamma(\mathcal{L}, G)$*. Assume an error* $\mathbf{e}$ *of weight* t *occurs. Then, the following equations hold, which are called the* key equation *for decoding* $\Gamma(\mathcal{L}, G)$*:*

$$\Omega(x) = \Lambda(x)s(x) \mod G(x) \tag{17}$$

$$\gcd(\Lambda(x), \Omega(x)) = 1 \tag{18}$$

$$\deg \Omega(x) < \deg \Lambda(x) \leqslant t \cdot l \tag{19}$$

where $l = \max_{f(x)\in\mathcal{L}} \deg f(x)$*.*

Proof: Denote $\mathcal{E} = \mathrm{supp}(\boldsymbol{e})$ and $t = |\mathcal{E}|$. Eq. (17) follows from (13), (14), and (15) since

$$s(x) = \frac{\sum\limits_{i\in\mathcal{E}} e_i f_i'(x) \prod\limits_{j\in\mathcal{E}\setminus\{i\}} f_j(x)}{\prod\limits_{i\in\mathcal{E}} f_i(x)} = \frac{\Omega(x)}{\Lambda(x)} \mod G(x).$$

Eq. (18) holds since all $f_i(x)$ have distinct roots. From the definitions of ELP in (14), $\deg \Lambda(x) = \sum_{i\in\mathcal{E}} \deg f_i(x) \leqslant t \cdot \max_{i\in\mathcal{E}} \deg f_i(x) \leqslant t \cdot l$. From (15), $\deg \Omega(x) = \deg \Lambda'(x) < \deg \Lambda(x)$. The degree constraints in (19) follow herein. ■

Theorem 4 (Unique Decoding Radius)**.** *Given a binary* separable *generalized Goppa code* $\Gamma(\mathcal{L}, G)$ *with* $d(\Gamma) \geqslant d_{\text{sep}}$*, Algorithm 1 can uniquely decode any error* $\mathbf{e}$ *of weight*

$$t \leqslant t_{\text{sep}} := \left\lfloor \frac{r}{l} \right\rfloor = \left\lfloor \frac{d_{\text{sep}}}{2} \right\rfloor,$$

where $r = \deg G(x)$ *and* $l = \max_{f(x)\in\mathcal{L}} \deg f(x)$*.*

Proof: It follows from [17, Proposition 6.3, 6.4] that Line 2 of Algorithm 1 will find a unique solution of the pair $(\lambda(x), \omega(x))$ such that $\Lambda(x) = c \cdot \lambda(x), \Omega(x) = c \cdot \omega(x)$ for some constant c, if $\deg \omega(x) < \deg \lambda(x) \leqslant \deg(G(x))/2$. At Line 3 of Algorithm 1 we search for the roots of $\lambda(x)$. They are also roots of $\Lambda(x)$ if $\deg \Lambda(x) = \deg \lambda(x) \leqslant \deg(G(x))/2$. Namely, the error locations can be uniquely determined if $\deg \Lambda(x) \leqslant \deg(G(x))/2$.

Since the separable generalized Goppa code $\Gamma(\mathcal{L}, G)$ is the same code as $\Gamma(\mathcal{L}, G^2)$ according to Corollary 1, we can apply Algorithm 1 on $\Gamma(\mathcal{L}, G^2)$ to decode $\Gamma(\mathcal{L}, G)$. Then, the degree constraint for uniquely decoding $\Lambda(x)$ becomes $\deg(G(x)^2)/2$. Thus,

$$\deg \Lambda(x) \leqslant t \cdot l \overset{!}{\leqslant} \frac{\deg(G(x)^2)}{2} = r.$$

It holds that $r/l < r/l + 1/(2l) = d_{\text{sep}}/2$. In particular, $\lfloor r/l \rfloor < \lfloor r/l + 1/(2l) \rfloor$ only if $2l|(2r+1)$, which is impossible for positive integers r and l. Therefore the equality holds. ■

V. Joint Decoding of Interleaved Generalized Goppa Codes

Interleaved codes are known to be able to decode beyond the unique decoding radius [20]–[24], especially in appearance of *burst errors*. Burst errors can be modelled as an error matrix $\boldsymbol{E}$ that only has a few non-zero columns. We denote by $\mathrm{supp}(\boldsymbol{E})$ the indices of the non-zero columns of $\boldsymbol{E}$. We present the explicit decoder and derive the new maximum decoding radius for GGCs, which is different from the general form of that for interleaved Reed-Solomon codes [23] or interleaved classical Goppa codes [24].

Algorithm 1: Syndrome-based Decoding Algorithm

Input: Code $\Gamma(\mathcal{L}, G)$, received word $\boldsymbol{r} \in \mathbb{F}_2^n$

1 Calculate $s(x)$ by (16)

2 $\omega(x), \_, \lambda(x) \leftarrow \mathtt{EEA}(G(x), s(x))$ with the stopping condition that $\deg \omega(x) < \deg \lambda(x) \leqslant \deg G(x)/2$ `// See [17, Sec. 6.4] for EEA`

3 $\mathcal{E} \leftarrow \{i : \lambda(\gamma_i) = 0\}$ * `//` γ_i `is a root of` $f_i(x)$

4 $\boldsymbol{e} \leftarrow \boldsymbol{0}; e_i \leftarrow 1, \forall i \in \mathcal{E}$

Output: $\hat{\boldsymbol{c}} \leftarrow \boldsymbol{r} - \boldsymbol{e}$

*Verifying $\lambda(\gamma_i) = 0$ can be done by applying Chien Search [19] in each splitting field $\mathbb{F}_{q^{l_i}}$ if there is an $f_i(x) \in \mathcal{L}$ of degree l_i and we only need to do this evaluation at one of the roots of $f_i(x)$.

Definition 3 (Interleaved Generalized Goppa Codes)**.** *Let* w *be the interleaving order. Given a generalized Goppa code* $\Gamma(\mathcal{L}, G)$*, a* w-interleaved generalized Goppa code *is denoted by* $w\text{-}\mathcal{I}\Gamma(\mathcal{L}, G)$ *and defined by*

$$w\text{-}\mathcal{I}\Gamma(\mathcal{L}, G) := \left\{ \begin{pmatrix} \boldsymbol{c}^{(1)} \\ \vdots \\ \boldsymbol{c}^{(w)} \end{pmatrix}, \ \forall \boldsymbol{c}^{(i)} \in \Gamma(\mathcal{L}, G), \ i \in [w] \right\}.$$

Consider transmitting a codeword $\boldsymbol{C} \in w\text{-}\mathcal{I}\Gamma(\mathcal{L}, G)$ with $n = |\mathcal{L}|$. An error $\boldsymbol{E} \in \mathbb{F}_2^{w\times n}$ with $\mathcal{E} = \mathrm{supp}(\boldsymbol{E})$ occurs and we receive $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$. We follow the definitions from Definition 2 for the ELP $\Lambda(x)$, the syndromes $s^{(i)}(x)$ and the EEPs $\Omega^{(i)}(x)$ for $\boldsymbol{E}$ with $\mathcal{E} = \mathrm{supp}(\boldsymbol{E})$.

Lemma 4 (Key Equations for Joint Decoding)**.** *The* key equations *for decoding* $w\text{-}\mathcal{I}\Gamma(\mathcal{L}, G)$ *in occurrence of an error* $\boldsymbol{E}$ *with* t *non-zero columns are:*

$$\Omega^{(i)}(x) = \Lambda(x)s^{(i)}(x) \mod G(x)$$

$$\deg \Omega^{(i)}(x) < \deg \Lambda(x) \leqslant t \cdot l$$

for all $i \in [w]$*, where* $l = \max_{f(x)\in\mathcal{L}} \deg f(x)$*.*

Instead of solving the key equations in Lemma 4 for the $\Lambda(x)$ and $\Omega^{(i)}(x)$ which have specific algebraic structures, we solve the following general version of this problem: Given $G(x), s^{(1)}(x), \ldots, s^{(w)}(x) \in \mathbb{F}_q[x]$, find a lowest-degree polynomial $\lambda(x)$ such that there exist polynomials $\omega^{(1)}(x), \ldots, \omega^{(w)}(x) \in \mathbb{F}_q[x]$, not all zero, satisfying

$$\begin{aligned} \omega^{(i)}(x) &= \lambda(x)s^{(i)}(x) \mod G(x) \\ \deg \omega^{(i)}(x) &< \deg \lambda(x) \leqslant t \cdot l \end{aligned} \tag{20}$$

for all $i \in [w]$. This problem can be solved by the *MgLFSR Algorithm* [25], by the *Feng-Tzeng Euclidean algorithm* [26], or by solving a *linear system of equations* (LSE) for the unknown coefficients of $\lambda(x)$ [27, Sec. 4.3.2]. We summarize the decoding procedure in Algorithm 2.

Theorem 5 (Maximum Decoding Radius)**.** *Given a binary interleaved separable generalized Goppa code* $w\text{-}\mathcal{I}\Gamma(\mathcal{L}, G)$

with $d(\Gamma) \geqslant d_{\text{sep}}$, with high probability, Algorithm 2 can decode an error $\boldsymbol{E}$ with t non-zero columns if

$$t \leqslant t_{\max} := \left\lfloor \frac{w}{w+1} \cdot \frac{2r}{l} \right\rfloor \leqslant \left\lfloor \frac{w}{w+1} \cdot d_{\text{sep}} \right\rfloor$$

where $r = \deg G(x)$ and $l = \max_{f(x) \in \mathcal{L}} \deg f(x)$.

Proof: Note that the separable w-$\mathcal{I}\Gamma(\mathcal{L}, G)$ is the same code as w-$\mathcal{I}\Gamma(\mathcal{L}, G^2)$, therefore we can decode w-$\mathcal{I}\Gamma(\mathcal{L}, G)$ by applying Algorithm 2 on w-$\mathcal{I}\Gamma(\mathcal{L}, G^2)$. By setting up the LSE for (20) according to [27, Sec. 4.3.2], we can get

$$\deg(G(x)^2) - \deg \omega^{(i)} - 1 = \deg(G(x)^2) - \deg \lambda(x) \quad (21)$$

equations for $\deg \lambda(x)$ unknowns (i.e., coefficients of $\lambda(x)$) from each congruence. The unknowns are the same for every congruence. In total we have at most $w(\deg(G(x)^2) - \deg \lambda(x))$ equations for $\deg \lambda(x)$ unknowns. To have a unique solution, the number of unknowns should not be more than the number of equations, i.e.,

$$\begin{aligned} \deg \lambda(x) &\leqslant w(\deg(G(x)^2) - \deg \lambda(x)), \\ \deg \lambda(x) &\leqslant \frac{w}{w+1} \deg(G(x)^2). \end{aligned} \quad (22)$$

Suppose $\Lambda(x) = c \cdot \lambda(x)$, $\Omega^{(i)}(x) = c \cdot \omega^{(i)}(x), \forall i \in [w]$. Then, we can get a unique solution for $\Lambda(x), \Omega^{(i)}(x)$ by Algorithm 2 if the solution for $\lambda(x)$ is unique, i.e., if (22) is fulfilled. The second inequality in the statement holds by plugging in d_{sep} from (11). ■

Corollary 3. *Given a binary interleaved separable generalized Goppa code w-$\mathcal{I}\Gamma(\mathcal{L}, G)$ with all code locators of even-degree, with high probability, Algorithm 2 can decode an error $\boldsymbol{E}$ with t non-zero columns if*

$$t \leqslant t_{\max}^{(\text{even})} := \left\lfloor \frac{w}{w+1} \cdot \frac{2r+1}{l} \right\rfloor \leqslant \left\lfloor \frac{w}{w+1} \cdot d_{\text{even}} \right\rfloor,$$

where $r = \deg G(x)$ and $l = \max_{f(x) \in \mathcal{L}} \deg f(x)$.

Proof: For only even-degree code locators, $\deg \Omega^{(i)}(x) \leqslant \deg \Lambda(x) - 2$ since we work in a field of characteristic 2. Therefore, when setting up the LSE, instead of (21), we will have $\deg G(x) - \deg \lambda(x) + 1$ equations from each congruence. The rest of the proof remains the same as for Theorem 5. ■

The maximum decoding radius $t_{\max}^{(\text{even})}$ for interleaved separable GGCs with even-degree code locators can be increased by 1 upon $t_{\max}$ in Theorem 5 if and only if we choose the interleaving order w such that $(w+1) | (2r+1)$ and $l | w$.

Remark 1. *Algorithm 2 may output* `decoding failure` *if the number of errors $t > t_{\text{sep}}$ in Theorem 4. The failure results from the linear dependency of equations in the LSE. An upper bound on the failure probability of decoding interleaved alternant codes has been recently derived in [29], which holds for decoding interleaved GGCs with code locators of degree one.*

VI. Code Parameters

In Table I, we show some examples of code parameters ($k \geqslant$, m, l, r, d_{sep}) of binary separable Goppa codes and binary separable generalized Goppa codes $\Gamma(\mathcal{L}, G(x))$, denoted by GC and GGC-$l$ respectively, for several values of length n.

For GGCs and a fixed code length n, the degree m of the extension field can be reduced according to (12) by increasing the maximum degree l of the code locators in $\mathcal{L}$. By additionally fixing the degree r of the Goppa polynomial, the lower bound on the minimum distance d_{sep} is reduced by the factor of l, according to Corollary 1. Keeping instead d_{sep} fixed, the degree r must be increased to $r = \lceil (l \cdot d_{\text{sep}} - 1)/2 \rceil$. The lower bound on the dimension k is calculated by $n - mr$ and is therefore smaller for a higher degree of r. The specialty of GGCs is that the code length n can be greater than the size of the extension field.

Algorithm 2: Decoding Algorithm for $\mathcal{I}\Gamma(\mathcal{L}, G)$

Input: w-$\mathcal{I}\Gamma(\mathcal{L}, G)$, received word $\boldsymbol{R} \in \mathbb{F}_2^{w \times n}$

Calculate w syndromes $s^{(i)}(x)$, $\forall i \in [w]$ by (16)

Solve (20) for $\lambda(x)$ by solving LSE [27], MgLFSR [25] or Feng-Tzeng EEA [26]

If $\lambda(x)$ is not unique **Return** `decoding failure`

$\mathcal{E} \leftarrow \{i : \lambda(\gamma_i) = 0\}$ * `//` γ_i `is a root of` $f_i(x)$

Calculate $\omega^{(i)}(x) = \lambda(x) s^{(i)}(x) \bmod G(x)$, $\forall i \in [w]$

$\boldsymbol{E} \leftarrow \boldsymbol{0}$; denote by $e_j^{(i)}$ the (i, j)-entry of $\boldsymbol{E}$

foreach $i \in [w], j \in \mathcal{E}$ **do** $e_j^{(i)} = \omega^{(i)}(\gamma_j)/\lambda'(\gamma_j)$ ** `//` γ_j `is a root of` $f_j(x)$

Output: $\widehat{\boldsymbol{C}} = \boldsymbol{R} - \boldsymbol{E}$ or `decoding failure`

*Apply Chien Search [19] for fast implementation. See also in Algorithm 1.

**This follows from *Forney's Algorithm* [28].

Table I
Code parameters for binary separable GGCs.

Code	n	$k \geqslant$	m	l	r	d_{sep}	|pk| *[bytes]*
GC	3488	2720	12	1	64	129	*261 120*
GGC-2	3488	3040	7	2	64	64	*170 240*
GGC-2	3488	2585	7	2	129	129	*291 782*
GC	6960	5413	13	1	119	239	*1 047 319*
GGC-2	6960	6127	7	2	119	119	*637 974*
GGC-3	6960	5170	5	3	358	239	*1 156 788*
GC	8192	6528	13	1	128	257	*1 357 824*
GGC-2	8192	7296	7	2	128	128	*817 152*
GGC-8	8192	6528	2	8	832	208	*1 357 824*

Table I also shows the corresponding public key size of *Classic McEliece* [12], which is the Niederreiter's dual version of the original McEliece cryptosystem and currently a finalist of the NIST competition for post-quantum key encapsulation mechanisms [11]. The cryptosystem is efficient in encoding and decoding, but it has a large public key size, which is a drawback in computation time and storage space. The public key $\mathbf{T}$ is determined by the systematic form of $\boldsymbol{H}_{\text{bin}} = (\mathbf{I}_{n-k} \mid \mathbf{T})$ and has size $|\mathsf{pk}| = (nmr - m^2 r^2)/8$ bytes.

The complexity of all computations including the construction of a parity-check matrix (public key) can be improved by reducing the field size with GGCs. The cost is a larger public key size or a smaller security level, based on the *Information Set Decoding* (ISD) attack by Lee and Brickell [30], whose work factor depends on n, k, d.

References

[1] V. Goppa, "A New Class of Linear Error Correcting Codes," *Problems of Information Transmission*, vol. 6, no. 3, pp. 207–212, 1970.

[2] R. J. McEliece, "A Public-Key Cryptosystem Based On Algebraic Coding Theory," *The Deep Space Network Progress Report*, vol. 44, pp. 114–116, 1978.

[3] N. A. Shekhunova and E. T. Mironchikov, "Cyclic (L,G)-Codes," *Probl. Peredachi Inf.*, vol. 17, pp. 3–9, Sep. 1981.

[4] S. V. Bezzateev and N. A. Shekhunova, "One Generalization of Goppa Codes," in *Proceedings of IEEE International Symposium on Information Theory*, 1997, p. 299.

[5] S. Bezzateev and N. Shekhunova, "Class of Binary Generalized Goppa Codes Perfect in Weighted Hamming Metric," *Designs Codes and Cryptography*, vol. 66, pp. 391–399, 08 2013.

[6] S. Bezzateev, "One Subclass of Cyclic Generalized (L,G) Codes with Separable Goppa Polynomial," in *2014 XIV International Symposium on Problems of Redundancy in Information and Control Systems*, 2014, pp. 30–32.

[7] S. Bezzateev, "Cyclic Generalized Separable (L, G) Codes," in *Coding Theory and Applications*, ser. CIM Series in Mathematical Sciences, R. Pinto, P. Rocha Malonek, and P. Vettori, Eds. Cham: Springer International Publishing, 2015, pp. 53–60.

[8] I. K. Noskov and S. V. Bezzateev, "One Realization of the Generalized (L,G)-Codes," in *2020 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, 2020, pp. 1–5.

[9] I. Noskov and S. Bezzateev, "Effective Implementation of Modern McEliece Cryptosystem on Generalized (L,G)-codes (Russian Only)," *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, vol. 20, pp. 539–544, 08 2020.

[10] H. Niederreiter, "Knapsack-type Cryptosystems and Algebraic Coding Theory," *Problems Control and Inf. Theory*, vol. 15(2), pp. 159–166, Jan. 1986.

[11] NIST CSRC, "Post-Quantum Cryptography," 2020. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography

[12] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, and W. Wang, "Classic McEliece: NIST submission," 2019. [Online]. Available: https://classic.mceliece.org/nist.html

[13] Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, "Further Results on Goppa Codes and Their Applications to Constructing Efficient Binary Codes," *IEEE Transactions on Information Theory*, vol. 22, no. 5, pp. 518–526, September 1976.

[14] D. J. Bernstein, T. Lange, and C. Peters, "Wild McEliece," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, A. Biryukov, G. Gong, and D. R. Stinson, Eds. Berlin, Heidelberg: Springer, 2011, pp. 143–158.

[15] S. V. Bezzateev and N. A. Shekhunova, "Generalized Goppa Codes for Correcting Localized Errors," in *Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)*, 1998, pp. 377–.

[16] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., ser. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996.

[17] R. M. Roth, *Introduction to Coding Theory*. Cambridge University Press, 2006.

[18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Elsevier, 1977, vol. 16.

[19] R. Chien, "Cyclic Decoding Procedures for Bose-Chaudhuri-Hocquenghem Codes," *IEEE Transactions on Information Theory*, vol. 10, no. 4, pp. 357–363, October 1964.

[20] J. J. Metzner and E. J. Kapturowski, "A General Decoding Technique Applicable to Replicated File Disagreement Location and Concatenated Code Decoding," *IEEE Transactions on Information Theory*, vol. 36, no. 4, pp. 911–917, 1990.

[21] D. Bleichenbacher, A. Kiayias, and M. Yung, "Decoding of Interleaved Reed Solomon Codes Over Noisy Data," in *International Colloquium on Automata, Languages, and Programming*. Springer, 2003, pp. 97–108.

[22] J. Justesen, C. Thommesen, and T. Høholdt, "Decoding of Concatenated Codes with Interleaved Outer Codes," in *IEEE International Symposium on Information Theory (ISIT)*, 2004, pp. 328–328.

[23] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Interleaved Reed–Solomon Codes in Concatenated Code Designs," in *IEEE Information Theory Workshop*, 2005, pp. 5–pp.

[24] L. Holzbaur, H. Liu, S. Puchinger, and A. Wachter-Zeh, "On Decoding and Applications of Interleaved Goppa Codes," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 1887–1891.

[25] J. S. Nielsen, "Generalised Multi-Sequence Shift-Register Synthesis Using Module Minimisation," in *IEEE International Symposium on Information Theory (ISIT)*, 2013, pp. 882–886.

[26] A. Zeh and A. Wachter, "Fast Multi-Sequence Shift-Register Synthesis with the Euclidean Algorithm," *Adv. Math. Commun.*, vol. 5, no. 4, pp. 667–680, Nov 2011.

[27] H. Liu, "Decoding of Interleaved Goppa Codes and Their Applications in Code-Based Cryptosystem," Master's thesis, Technische Universität München (TUM), 2019. [Online]. Available: http://mediatum.ub.tum.de/doc/1488548/1488548.pdf

[28] G. Forney, "On decoding BCH codes," *IEEE Transactions on Information Theory*, vol. 11, no. 4, pp. 549–557, 1965.

[29] L. Holzbaur, H. Liu, A. Neri, S. Puchinger, J. Rosenkilde, V. Sidorenko, and A. Wachter-Zeh, "Decoding of Interleaved Alternant Codes," 2020. [Online]. Available: https://arxiv.org/abs/2010.07142

[30] P. J. Lee and E. F. Brickell, "An Observation on the Security of McEliece's Public-Key Cryptosystem," in *Advances in Cryptology — EUROCRYPT '88*. Berlin, Heidelberg: Springer, 1988, pp. 275–280.