Advances in Mathematics of Communications
Volume 15, No. 2, 2021, 219–226
doi:10.3934/amc.2020054

ON THE DIMENSION OF THE SUBFIELD SUBCODES OF 1-POINT HERMITIAN CODES

Sabira El Khalfaoui and Gábor P. Nagy

Bolyai Institute of the University of Szeged
Aradi vértanúk tere 1, H-6720 Szeged, Hungary
and
Department of Algebra of the Budapest University of Technology and Economics
Egry József utca 1, H-1111 Budapest, Hungary

(Communicated by Daniele Bartoli)

Abstract. Subfield subcodes of algebraic-geometric codes are good candidates for the use in post-quantum cryptosystems, provided their true parameters such as dimension and minimum distance can be determined. In this paper we present new values of the true dimension of subfield subcodes of 1–point Hermitian codes, including the case when the subfield is not binary.

1. Introduction

The oldest and best known proposal for post-quantum cryptography schemes are the cryptosystems due to McEliece and Niederreiter. Their security is based on the NP-completeness of the decoding of binary linear codes. Hence, an essential ingredient of their schemes is a binary linear code C which has an efficient decoding algorithm and which cannot be distinguished from the random linear code. McEliece originally proposed the class of extended binary Goppa codes, which are subfield subcodes of the generalized Reed-Solomon codes. Recently, some other classes of codes have been proposed as well, such as LDPC codes and algebraic-geometric codes over larger fields. However, these classes turned out to have serious security flows, see [2, 4, 10, 11, 25]. For the background of code based cryptography we refer to [12, 18, 19], for quantum attacks see [26], and on digital signature schemes based on the Niederreiter scheme see [5].

The Berlekamp-Massey algorithm [7] and its variants provide an efficient decoding for Reed-Solomon codes, which can be used to decode subfield subcodes of generalized Reed-Solomon codes, as well. For the binary linear code C in use, the error correcting bound is determined by these algorithms. Beyond this bound, list-decoding methods are known, cf. [1, 3, 13]. Therefore, it is an important problem to find the true minimum distance and the true dimension of subfield subcodes of generalized Reed-Solomon codes, cf. [6] and the series of papers [22, 23, 24]. The class of algebraic-geometry (AG) codes was introduced by V.D. Goppa. This class is a natural generalization of Reed-Solomon codes. The famous Riemann-Roch Theorem provides theoretical bounds for the dimension and minimum distance of AG codes. The ideas of the Berlekamp-Massey algorithm can be used to design efficient decoding algorithms up to the half of the designed minimum distance of AG codes,

2020 *Mathematics Subject Classification:* Primary: 11T71, 14G50; Secondary: 94B27.
Key words and phrases: AG code, Hermitian code, subfield subcode.

and beyond [9, 15, 17]. Hence, the subfield subcodes of AG codes are also good candidates for the McEliece and Niederreiter cryptosystems. The determination of the true dimension and the true minimum distance of the subfield subcodes of AG codes seems to be a hard problem, the attempts so far focused mainly at 1-point Hermitian codes and their subcodes, with some further restrictions on the parameters [16, 20, 21].

In this paper, we prove new results on the true dimension of the subfield subcodes of 1-point Hermitian codes. Our approach deals also with non-binary subfields. The paper is structured as follows. In section 2, we describe the backgrounds with some important properties of Hermitian curves, their function fields and Riemann-Roch spaces. In section 3, we present AG codes and 1-point Hermitian codes. Section 4 summarizes the definition of the subfield subcodes of AG codes and techniques used to improve the bounds on the dimensions of subfield subcodes of Reed-Solomon codes, these techniques include Delsarte's seminal result on subfield subcodes and trace codes. Section 5 is dedicated to prove our result concerning the true dimension of the subfield subcodes of 1-point Hermitian codes for specific parameters.

2. Hermitian curves, their divisors and Riemann-Roch spaces

Our notation and terminology on algebraic plane curves over finite fields, their function fields, divisors and Riemann-Roch spaces are standard, see for instance [8, 12, 19].

Let $PG(2,\mathbb{F}_{q^2})$ be the projective plane over the finite field of order q^2 equipped with homogeneous coordinates (X,Y,Z). The Hermitian curve in its canonical form is the non-singular plane curve $\mathscr{H}_q$ with equation $Y^qZ + YZ^q = X^{q+1}$. The genus of $\mathscr{H}_q$ equals $g = q(q-1)/2$ and the set $\mathscr{H}_q(\mathbb{F}_{q^2})$ of $\mathbb{F}_{q^2}$-rational points, that is, its points with coordinates over $\mathbb{F}_{q^2}$ has size q^3+1. It is also useful to regard $PG(2,\mathbb{F}_{q^2})$ as the projective closure of the affine plane $AG(2,\mathbb{F}_{q^2})$ with respect to the line $Z=0$ at infinity, so that the $\mathscr{H}_q$ has affine equation $Y^q + Y = X^{q+1}$. In particular, $\mathscr{H}_q$ has just one point at infinity, namely $(0,1,0)$, denoted by P_∞. We remark that Hermitian curves have the maximum number of rational points allowed by the Hasse-Weil bound [8, Theorem 9.18], [12, Theorem 9.10].

The action of the Frobenius automorphism $\mathrm{Frob}_{q^2} : x \mapsto x^{q^2}$ can be extended to the points of $\mathscr{H}_q$ by applying Frob_{q^2} on the coordinates. We denote the extended action by Frob_{q^2} as well. A point P of $\mathscr{H}_q$ is $\mathbb{F}_{q^2}$-rational if and only if $P = \mathrm{Frob}_{q^2}(P)$.

As usual, we also look at the curve $\mathscr{H}_q$ as the curve defined over the algebraic closure $\bar{\mathbb{F}}_{q^2}$. Then, there is a one-to-one correspondence between the points of $\mathscr{H}_q$ and the places of the function field $\bar{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ of $\mathscr{H}_q$.

For a divisor $D = \lambda_1 P_1 + \cdots + \lambda_k P_k$ with $P_1,\ldots,P_k \in \mathscr{H}_q$ and integers $\lambda_1,\ldots,\lambda_k$, its Frobenius image is

$$\mathrm{Frob}_{q^2}(D) = \lambda_1 \mathrm{Frob}_q(P_1) + \cdots + \lambda_k \mathrm{Frob}_q(P_k).$$

A divisor D is $\mathbb{F}_{q^2}$-rational if $D = \mathrm{Frob}_{q^2}(D)$. In particular, if $P_1,\ldots,P_k$ are in $\mathscr{H}_q(\mathbb{F}_{q^2})$ then D is $\mathbb{F}_{q^2}$-rational, but the converse does not hold in general. The degree of D is $\deg(D) = \lambda_1 + \cdots + \lambda_k$, while the support of D is the set of points P_i with $\lambda_i \neq 0$.

For a non-zero function f in the function field $\bar{\mathbb{F}}_{q^2}(\mathscr{H}_q)$ and a point P, $v_P(f)$ stands for the order of f at P. If $v_P(f) > 0$ then P is a zero of f, while if $v_P(f) < 0$,

then P is a pole of f with multiplicity $-v_P(f)$. The principal divisor of a non-zero function f is $(f) = \sum_P v_P(f)P$.

For an $\mathbb{F}_{q^2}$-rational divisor D, the Riemann-Roch space $\mathscr{L}(D)$ is the vector space

$$\mathscr{L}(D) = \{f \in \mathbb{F}_{q^2}(\mathscr{H}_q) \mid (f) \succcurlyeq -D\}.$$

For the dimension $\ell(D)$ of $\mathscr{L}(D)$ the Riemann-Roch Theorem states

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D),$$

where W is a canonical divisor of the Hermitian curve, for example $W = (q-2)(q+1)P_\infty$ is such a canonical divisor. Moreover, if $\deg(D) > 2g - 2$ then the Riemann-Roch Theorem reads $\ell(D) = \deg(D) + 1 - g$. Let s be a positive integer and $D = sP_\infty$ a 1-point divisor of $\mathscr{H}_q$. Then the set

$$\left\{x^i y^j \mid 0 \le i \le q^2 - 1, \quad 0 \le j \le q - 1, \quad v_{P_\infty}(x^i y^j) \le s\right\}$$

of functions forms a basis of the Riemann-Roch space $\mathscr{L}(sP_\infty)$, see [12, Theorem 10.4]. Notice that $v_{P_\infty}(x) = q$, $v_{P_\infty}(y) = q + 1$, and hence the order of $x^i y^j$ at P_∞ is

$$v_{P_\infty}(x^i y^j) = qi + (q+1)j. \tag{1}$$

3. Algebraic geometry codes (briefly AG codes)

Algebraic geometry codes are a type of linear error correcting block codes, arising from algebraic curves defined over a finite field, see [19]. Here we outline the construction when the underlying curve is the Hermitian curve $\mathscr{H}_q$.

Fix a divisor $D = P_1 + ... + P_n$ where all P_i are pairwise distinct $\mathbb{F}_{q^2}$–rational points of $\mathscr{H}_q$. Also, take another $\mathbb{F}_{q^2}$-rational divisor G whose support is disjoint from supp D. The functional AG code $C_L(D, G)$ associated with the divisors D and G is a subspace of the vector space $\mathbb{F}_{q^2}^n$, and defined by

$$C_L(D, G) = \{(f(P_1), ..., f(P_n)) \mid f \in \mathscr{L}(G)\} \subseteq \mathbb{F}_{q^2}^n.$$

In other words, $C_L(D, G)$ is the image of $\mathscr{L}(G)$ under the evaluation map

$$\mathscr{L}(G) \ni f \mapsto (f(P_1), ..., f(P_n)) \in \mathbb{F}_{q^2}^n.$$

Indeed, determining the functions field and the divisors in a pertinent way can make Reed-Solomon codes viewed as particular AG codes, see [19, Section 2.3]. The most fascinating feature of AG codes is that the Riemann-Roch Theorem determines its dimension k and provides a useful bound for its minimum distance d.

Theorem 3.1 ([12, Theorem 10.1])**.** *$C_L(D, G)$ is a linear $[n, k, d]$ code over $\mathbb{F}$ with parameters:*

- $k = \ell(G) - \ell(G - D)$,
- $d \ge n - \deg G$.

Notice that the condition $n > \deg G$ implies the evaluation map $\mathscr{L}(G) \to \mathbb{F}^n$ to be injective. If $n \le \deg G$, then it is possible that $C_L(D, G)$ has dimension less than n and positive true minimum distance. However, this case cannot be described only by the Riemann-Roch Theorem.

By using the differential space $\Omega(G)$ instead of the Riemann-Roch space $\mathscr{L}(G)$, one can define another AG codes, namely the differential AG codes $C_\Omega(D, G)$. It should be noted that the differential code $C_\Omega(D, G)$ is the dual of the functional AG code $C_L(D, G)$.

The main result of this paper deals with 1-point Hermitian codes. Let $n = q^3$ and the divisor $D = P_1 + P_2 + ... + P_n$ be the sum of $\mathbb{F}_{q^2}$–rational affine points of $\mathscr{H}_q$. For a positive integer s, we denote by $\mathcal{H}(q^2, s)$ the 1-point functional AG code $C_L(D, sP_\infty)$. This has length $n = q^3$. If $2g - 2 < s < n$, then the dimension of $\mathcal{H}(q^2, s)$ is $k = s - g + 1$ which is equal to the dimension of the Riemann-Roch space $\mathscr{L}(sP_\infty)$. Under these assumptions, we have equality in Theorem 3.1, hence the minimum distance of $\mathcal{H}(q^2, s)$ is $d = q^3 - s$.

Theorem 3.2 (Dual codes [12, Theorem 10.5]). *For $s > 0$ and $\tilde{s} = q^3+q^2-q-2-s$, the codes $\mathcal{H}(q^2, s)$ and $\mathcal{H}(q^2, \tilde{s})$ are dual to each other. In particular, if q is even and $s = (q^3 + q^2 - q - 2)/2$, then the code $\mathcal{H}(q^2, s)$ is self-dual.*

4. Subfield subcodes of linear codes

Let $\mathbb{F}_r$ be a subfield of a finite field $\mathbb{F}_l$, that is, $l = r^h$ for a positive integer h. Let C be a linear $[n, k, d]$ code over $\mathbb{F}_l$. The subfield subcode $C|\mathbb{F}_r$ consists of all codewords of C whose coordinates are in $\mathbb{F}_r$, that is,

$$C|\mathbb{F}_r = C \cap \mathbb{F}_r^n.$$

This is a linear $[n, k_0, d_0]$ code over $\mathbb{F}_r$ with $d \le d_0 \le n$ and $n - k \le n - k_0 \le h(n - k)$. Therefore for the dimension over $\mathbb{F}_r$

$$k_0 \ge n - h(n - k). \tag{2}$$

A parity check matrix of C over $\mathbb{F}_l$ yields at most $h(n - k)$ linearly independent parity check equations over $\mathbb{F}_r$ for the subfield subcode $C|\mathbb{F}_r$.

In general the true minimum distance of a subfield subcodes is bigger than the minimum distance of the original code. This makes the subfield subcodes very important, especially in the binary case $r = 2$, see [6, Theorem 4].

The trace polynomial $\mathrm{Tr}(X) \in \mathbb{F}_r[x]$ with respect to $\mathbb{F}_l$ is given by

$$\mathrm{Tr}_{\mathbb{F}_l/\mathbb{F}_r}(x) = x + x^r + ... + x^{r^{h-1}}.$$

Clearly, the trace polynomial determines the $\mathbb{F}_r$-linear trace map $\mathbb{F}_l \to \mathbb{F}_r$. For a linear code C over $\mathbb{F}_l$, Delsarte defined the trace code $\mathrm{Tr}(C) = \mathrm{Tr}_{\mathbb{F}_l/\mathbb{F}_r}(C)$ by

$$\mathrm{Tr}(C) = \left\{ \left(\mathrm{Tr}_{\mathbb{F}_l/\mathbb{F}_r}(c_1), ..., \mathrm{Tr}_{\mathbb{F}_l/\mathbb{F}_r}(c_n) \right) \mid (c_1, \ldots, c_n) \in C \right\},$$

and showed that $\mathrm{Tr}(C)$ is a linear $[n, k_1, d_1]$ code over $\mathbb{F}_r$, with $1 \leqslant d_1 \leqslant d$ and $k \leqslant k_1 \leqslant hk$. As for subfield subcodes, the most useful case occurs for $r = 2$.

The following important result by Delsarte relates the class of subfield subcodes to trace codes:

Theorem 4.1 (Delsarte [6]). *Let C be a linear code over an extension field $\mathbb{F}_l$ of $\mathbb{F}_r$. Then $(C|\mathbb{F}_r)^\perp = \mathrm{Tr}(C^\perp)$ holds.*

In [24], Véron pointed out that Delsarte's theorem can be used to compute from (2) the exact dimension

$$k_0 = n - h(n - k) + \dim_{\mathbb{F}_r} \ker(\mathrm{Tr}) \tag{3}$$

of the subfield subcode.

5. Main result

With the above notation, let $l = q^2$ and $h = 2m$. As before, let $\mathbb{F}_r$ be a subfield of $\mathbb{F}_{q^2}$, $q = r^m$, s be a positive integer and D be the sum of affine points of the Hermitian curve $X^{q+1} = Y + Y^q$ over the finite field $\mathbb{F}_{q^2}$. Define $C_{q,r}(s)$ to be the subfield subcode $\mathcal{H}(q^2, s)|\mathbb{F}_r$ of the 1-point Hermitian code $\mathcal{H}(q^2, s)$.

In [16], an algorithm for $\dim C_{q,r}(s)$ is presented. Using this algorithm, the authors explicitly compute the dimension of $C_{4,2}(s)$ for each $s = 0, \ldots, 71$.

From [21, Proposition 3.2],

$$\dim(\mathrm{Tr}(\mathcal{H}(q^2, q))) = 2m + 1,$$

where $q = 2^m$. In our notation, this reads

$$\dim C_{q,r}(q^3 + q^2 - 2q - 2) = q^3 - (2m + 1).$$

In particular, $\dim C_{4,2}(70) = 59$, which is confirmed by [16, Table 2]. In the same table, we find $\dim C_{4,2}(s) = 1$ for $s = 0, \ldots, 31$ and $\dim C_{4,2}(32) = 5$. These values for $\dim C_{4,2}(s)$ are particular cases of the general formula given by the following theorem.

Theorem 5.1. *Let $C_{q,r}(s)$ be a subfield subcode of the Hermitian code $\mathcal{H}(q^2, s)$, where $q = r^m$ is a prime power. Then*

$$\dim C_{q,r}(s) = \begin{cases} 1 & \text{for } 0 \le s < \frac{q^3}{r} \\ 2m + 1 & \text{for } s = \frac{q^3}{r} \end{cases}$$

Proof. Since the constant polynomials are in $\mathscr{L}(sP_\infty)$ for all $s \ge 0$, we have $\dim C_{q,r}(s) \ge 1$. We first show that $\dim C_{q,r}(s) = 1$ for $0 \le s < \frac{q^3}{r}$. Fix an integer $0 < s < \frac{q^3}{r}$ and take an arbitrary element $(c_1, \ldots, c_{q^3}) \in C_{q,r}(s)$. Then there is an element $f \in \mathscr{L}(sP_\infty)$ such that for all $i = 1, \ldots, q^3$, one has $c_i = f(P_i) \in \mathbb{F}_r$. There is an element $\gamma \in \mathbb{F}_r$ such that $c_i = \gamma$ for at least q^3/r indices i. In other words, $f - \gamma \in \mathscr{L}(sP_\infty)$ has at least q^3/r zeros on the Hermitian curve $\mathscr{H}_q$. (This follows from the fact that for a positive divisor G, a non-zero element of $\mathscr{L}(G)$ cannot have more than $\deg G$ zeros.) Therefore, $f - \gamma$ must be the constant zero polynomial, and $c_i = \gamma$ for all i. In particular, $C_{q,r}(s)$ consists of the constant vectors.

Now, we suppose that $s = q^3/r$. Recall that

$$\mathrm{Tr}(X) = X + X^r + \cdots + X^{r^{2m-1}}$$

is the trace polynomial of $\mathbb{F}_{q^2}$ over $\mathbb{F}_r$. We define the polynomial

$$f_{d,\alpha}(X) = d + \mathrm{Tr}(\alpha X)$$

where $d \in \mathbb{F}_r$, $\alpha \in \mathbb{F}_{q^2}$. As a polynomial in one variable, $f_{d,\alpha}$ maps $\mathbb{F}_{q^2}$ to $\mathbb{F}_r$. For a point P with affine coordinates (x, y), we write $f_{d,\alpha}(P) = f_{d,\alpha}(x)$. For the $\mathbb{F}_{q2}$-rational points $P_i(a_i, b_i)$, $i = 1, \ldots, q^3$, we have $f_{d,\alpha}(P_i) \in \mathbb{F}_r$. In other words, the evaluation vector

$$\mathbf{c}_{d,\alpha} = (f_{d,\alpha}(P_1), \ldots, f_{d,\alpha}(P_{q^3})) \in \mathbb{F}_r^n.$$

We claim that $f_{d,\alpha}(x) \in \mathscr{L}\left(\frac{q^3}{r} P_\infty\right)$. In fact, by (1),

$$v_{P_\infty}(x^{r^k}) = qr^k,$$

which is at most $qr^{2m-1} = q^3/r$ for $k \leq 2m-1$. Hence, all monomials of $f_{d,\alpha}(x)$ are in $\mathscr{L}\left(\frac{q^3}{r}P_\infty\right)$, and the claim follows.

From the last two properties of $f_{d,\alpha}$ follows that the evaluation vector $\mathbf{c}_{d,\alpha} \in C_{q,r}(q^3/r)$. Since the map $(d,\alpha) \mapsto \mathbf{c}_{d,\alpha}$ is linear over $\mathbb{F}_r$, and injective, we have $\dim C_{q,r}(q^3/r) \geq 2m+1$.

In the last step we show that the elements $\mathbf{c}_{d,\alpha}$ exhaust the subfield subcode $C_{q,r}(q^3/r)$.

Take an element $g \in \mathscr{L}\left(\frac{q^3}{r}P_\infty\right)$ whose evaluation vector

$$(g(P_1), \ldots, g(P_{q^3})) \in \mathbb{F}_r^n.$$

We can reduce the high y-degree terms by the Hermitian equation $x^{q+1} = y + y^q$. Thus, we can write g in this form:

$$g(x,y) = \sum_{j<q} a_{i,j} x^i y^j.$$

By (1), the order of $x^i y^j$ at P_∞ satisfies $v_{P_\infty}(x^i y^j) \equiv j \pmod q$. Therefore, if $j \leq q-1$ then the order $v_{P_\infty}(x^i y^j)$ determines i and j uniquely. Hence, different terms of $g = \sum_{j \leq q-1} a_{i,j} x^i y^j$ have different orders at P_∞. The order of g at P_∞ is

$$v_{P_\infty}(g) = v_{P_\infty}\left(\sum a_{i,j} x^i y^j\right) = \max_{a_{i,j} \neq 0} \left(v_{P_\infty}(x^i y^j)\right),$$

where the last equality holds since the orders $v_{P_\infty}(x^i y^j)$ are different. If $g \in \mathscr{L}\left(\left(\frac{q^3}{r}-1\right)P_\infty\right)$ then $g = f_{d,0}$ for some $d \in \mathbb{F}_r$ as seen above. Assume now

$$g \in \mathscr{L}\left(\frac{q^3}{r}P_\infty\right) \setminus \mathscr{L}\left(\left(\frac{q^3}{r}-1\right)P_\infty\right).$$

Then, $v_{P_\infty}(g) = q^3/r$ and g has a unique term $\beta x^{\frac{q^2}{r}}$ with order q^3/r at P_∞, $\beta \in \mathbb{F}_{q^2}^*$. Define $\alpha \in \mathbb{F}_{q^2}$ by $\alpha^{r^{2m-1}} = \beta$. Then, $g - f_{0,\alpha} \in \mathscr{L}\left(\frac{q^3}{r}P_\infty\right)$ and arguing as in the first part of the proof, shows that $g - f_{0,\alpha}$ is again a constant $d \in \mathbb{F}_r$. This means $g = f_{d,\alpha}$, and the result follows. □

Similar computation gives that for $\alpha \in \mathbb{F}_{q^2}$,

$$\mathrm{Tr}(\alpha y) \in \mathscr{L}\left(\frac{(q+1)q^2}{r}P_\infty\right).$$

Hence, $\dim C_{q,r}((q+1)q^2/r) \geq 4m+1$. By [16, Table 2], we have equality for $q=4$ and $r=2$. Using our GAP package HERmitian [14], we computed the true dimension of $C_{8,2}(s)$ for all values s from $256 = q^3/r$ to $511 = q^3-1$, see Table 1.

ACKNOWLEDGMENTS

Support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme, within the SETIT Project (2018-1.2.1-NKP-2018-00004). Partially supported by NKFIH-OTKA Grants 119687 and 115288.

s	$\dim C_{8,2}(s)$	$\dim \mathcal{H}(64,s)$		s	$\dim C_{8,2}(s)$	$\dim \mathcal{H}(64,s)$
256	7	229		456	206	429
288	13	261		457	212	430
292	19	265		458	218	431
320	25	293		460	224	433
324	28	297		462	226	435
328	34	301		464	232	437
336	36	309		466	238	439
352	42	325		468	244	441
356	48	329		470	250	443
360	54	333		472	256	445
364	60	337		473	262	446
368	66	341		474	268	447
376	72	349		475	274	448
378	74	351		480	280	453
384	80	357		482	286	455
392	86	365		484	292	457
400	92	373		486	295	459
402	98	375		488	301	461
408	104	381		489	307	462
410	110	383		490	313	463
416	116	389		491	319	464
418	122	391		492	325	465
420	128	393		493	331	466
424	134	397		496	337	469
428	140	401		498	343	471
432	146	405		500	349	473
434	152	407		502	355	475
436	158	409		504	361	477
438	164	411		505	367	478
440	170	413		506	373	479
442	176	415		507	379	480
444	182	417		508	385	481
448	188	421		509	391	482
450	194	423		510	397	483
452	200	425		511	403	484

Table 1: Parameters of $C_{8,2}(s)$ for $s \in \{256, \ldots, 511\}$

REFERENCES

[1] D. Augot, M. Barbier and A. Couvreur, List-decoding of binary Goppa codes up to the binary Johnson bound, *2011 IEEE Information Theory Workshop*, (2011), 229–233.

[2] M. Baldi, LDPC codes in the McEliece cryptosystem: Attacks and countermeasures, *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., IOS, Amsterdam*, **23** (2009), 160–174.

[3] D. J. Bernstein, List decoding for binary Goppa codes, *Coding and Cryptology, Lecture Notes in Comput. Sci., Springer, Heidelberg*, **6639** (2011), 62–80.

[4] D. J. Bernstein, T. Lange and C. Peters, Attacking and defending the McEliece cryptosystem, *Post-quantum cryptography, Lecture Notes in Comput. Sci., Springer, Berlin*, **5299** (2008), 31–46.
[5] N. T. Courtois, M. Finiasz and N. Sendrier, How to achieve a McEliece-based digital signature scheme, *Advances in Cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., Springer, Berlin*, **2248** (2001), 157–174.
[6] P. Delsarte, On subfield subcodes of modified Reed-Solomon codes, *IEEE Trans. Information Theory*, **IT-21** (1975), 575–576.
[7] M. Elia, E. Viterbo and G. Bertinetti, Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm, *Electronics Letters*, **35** (1999), 1720–1721.
[8] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, *Algebraic Curves Over a Finite Field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.
[9] T. Hoholdt and R. Pellikaan, On the decoding of algebraic-geometric codes, *IEEE Transactions on Information Theory*, **41** (1995), 1589–1614.
[10] Y. X. Li, R. H. Deng and X. M. Wang, On the equivalence of McEliece's and Niederreiter's public-key cryptosystems, *IEEE Transactions on Information Theory*, **40** (1994), 271–273.
[11] P. Loidreau and N. Sendrier, Weak keys in the McEliece public-key cryptosystem, *IEEE Trans. Inform. Theory*, **47** (2001), 1207–1211.
[12] A. J. Menezes, I. F. Blake, X. H. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian, *Applications of Finite Fields*, The Kluwer International Series in Engineering and Computer Science, 199. Kluwer Academic Publishers, Boston, MA, 1993.
[13] R. Misoczki and P. S. Barreto, Compact McEliece keys from Goppa codes, *International Workshop on Selected Areas in Cryptography*, (2009), 376–392.
[14] G. P. Nagy and S. El Khalfaoui, HERmitian, Computing with divisors, Riemann-Roch spaces and AG-odes of Hermitian curves, Version 0.1, (2019), GAP package, URL `https://github.com/nagygp/Hermitian`.
[15] R. Pellikaan, On the efficient decoding of algebraic-geometric codes, *Eurocode'92, CISM Courses and Lect., Springer, Vienna*, **339** (1993), 231–253.
[16] F. Piñero and H. Janwa, On the subfield subcodes of Hermitian codes, *Designs, Codes and Cryptography*, **70** (2014), 157–173.
[17] S. Sakata, H. E. Jensen and T. Hoholdt, Generalized Berlekamp-Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound, *IEEE Transactions on Information Theory*, **41** (1995), 1762–1768.
[18] S. A. Stepanov, *Codes on Algebraic Curves*, Kluwer Academic/Plenum Publishers, New York, 1999.
[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.
[20] M. van der Vlugt, The true dimension of certain binary Goppa codes, *IEEE Transactions on Information Theory*, **36** (1990), 397–398.
[21] M. van der Vlugt, On the dimension of trace codes, *IEEE Transactions on Information Theory*, **37** (1991), 196–199.
[22] P. Véron, Goppa codes and trace operator, *IEEE Trans. Inform. Theory*, **44** (1998), 290–294.
[23] P. Véron, True dimension of some binary quadratic trace Goppa codes, *Des. Codes Cryptogr.*, **24** (2001), 81–97.
[24] P. Véron, Proof of conjectures on the true dimension of some binary Goppa codes, *Des. Codes Cryptogr.*, **36** (2005), 317–325.
[25] C. Wieschebrink, Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, *Post-Quantum Cryptography, Lecture Notes in Comput. Sci., Springer, Berlin*, **6061** (2010), 61–72.
[26] S. Y. Yan, *Quantum Attacks on Public-Key Cryptosystems*, Springer, 2013.

Received June 2019; revised September 2019.

E-mail address: `sabira@math.u-szeged.hu`
E-mail address: `nagyg@math.u-szeged.hu`