Finite Fields and Their Applications **6,** 207–217 (2000)
doi:10.1006/ffta.1999.0274, available online at http://www.idealibrary.com on IDEAL®

Decoding Algebraic Geometry Codes by a Key Equation

J. I. Farrán[1]

Universidad de Valladolid, Departamento de Matematica, ETS, Ingenieros Industriales, Paseo del Cance s/n, Valladolid 47011, Spain

Communicated by Oscar Moreno

Received December 12, 1998

A new effective decoding algorithm is presented for arbitrary algebraic-geometric codes on the basis of solving a generalized key equation with the majority coset scheme of Duursma. It is an improvement of Ehrhard's algorithm, since the method corrects up to half of the Goppa distance with complexity order $\mathcal{O}(n^{2.81})$, and with no further assumption on the degree of the divisor G.

Key Words: AG codes; Ehrhard's key equation; majority coset decoding.

1. INTRODUCTION

Decoding algebraic–geometric codes (AG codes in short) in an effective way can be done by solving a key equation, generalizing the ideas of the Berlekamp–Massey algorithm for BCH codes or the Euclidean algorithm for classical Goppa codes (see [1]). In the original version of Porter *et al.* (see [12]), only one-point codes with further assumptions on the curve were decoded, but the main ideas of the method can be extended for arbitrary curves and AG codes with Ehrhard's version of the key equation. Nevertheless, this algorithm does not correct up to the Goppa distance, but the complexity is only $\mathcal{O}(n^3)$ (more details in [4]). Our aim is to include in this method a majority scheme which generalizes the ideas of Feng and Rao for one-point codes (see [6]), together with improving the complexity by using the new methods given in [14] to solve linear equations. Thus, the algorithm that we propose improves both the decoding capacity and the complexity without losing the generality of its application to arbitrary AG codes. It uses

[1]Partially supported by DIGICYT PB94-1111-C02-01.

1071-5797/00 $35.00

the majority coset decoding scheme, which was introduced by Duursma, with the only further assumption that there is an extra rational point in the curve which is not used in the construction of the codes (more details in [2]). This hypothesis is actually a weakening of the assumptions required by Porter's method.

In Section 2 we rewrite Ehrhard's key equation in a way that is closer to the original ideas of Porter *et al.*, in order to show the explicit connection between both works. Afterwards, we summarize in Section 3 the main ideas of Duursma's majority coset scheme, in order to give in Section 4 an algorithm which includes the above majority coset scheme, in order to give in Section 4 an algorithm which includes the above majority scheme in the key equation, so that one can increase the error capacity without the assumption $\deg G \geq 6g - 2\tau - 2$, where τ is the gonality of the curve, which is required in Ehrhard's algorithm given in [5] (see also [3] for further details). In the paper, we fix a non-singular absolutely irreducible projective algebraic curve χ defined over $\mathbb{F}_q$ and rational points $P_1, \ldots, P_n$ of χ.

2. KEY EQUATION AND DECODING

Let G be a rational divisor whose support is disjoint to $D = P_1 + \cdots + P_n$. Assume that $2g - 2 < \deg G < n + g$, and consider the code $C = C_\Omega(D, G)$, which is the image of the linear injective map

$$\mathrm{res}_D\colon \Omega(G - D) \to \mathbb{F}_q^n$$
$$\eta \mapsto \mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta))$$

with dimension $k \geq n - \deg G + g - 1$ and minimum distance $d \geq d^* = \deg G + 2 - 2g$, where g is the genus of the curve. In the sequel, we fix a divisor G^* with $\ell(G^*) = 0$ and $G \geq G^*$. In order to decode C, we will give a result for preparation.

LEMMA 1. *There exists a vector space V of differential forms such that $\Omega(G - D) \subseteq V$ and $\mathrm{res}_D\colon V \to \mathbb{F}_q^n$ is an isomorphism.*

Proof. Since $\Omega(G - D) \subseteq \Omega(G^* - D)$, it suffices to prove that res_D is surjective on $\Omega(G^* - D)$, because it is injective on $\Omega(G - D)$. But the kernel of res_D considered on $\Omega(G^* - D)$ is $\Omega(G^*)$; hence the rank is $i(G^* - D) - i(G^*) = \deg G^* - \deg(G^* - D) = n$, because of the Riemann–Roch formula. ∎

Remark 1. In the remainder of the paper we fix an arbitrary form $\eta \neq 0$ and write $K = (\eta)$. Then for any rational divisor H consider the isomorphism

$$\mathscr{L}(K - H) \to \Omega(H)$$

given by

$$f \mapsto f\eta.$$

This map is compatible with inclusions and restrictions, and so the inclusions $\Omega(G - D) \subseteq V \subseteq \Omega(G^* - D)$ give the corresponding $\mathscr{L}(K + D - G) \subseteq U \subseteq \mathscr{L}(K + D - G^*)$, where the map $f \mapsto \mathrm{res}_D\,(f\eta)$ is an isomorphism from U onto $\mathbb{F}_q^n$. Denote the inverse of this last map by $\mathbf{y} \mapsto h_\mathbf{y}$; i.e., $h_\mathbf{y}$ is the unique element in U such that $\mathrm{res}_D\,(h_\mathbf{y}\eta) = \mathbf{y}$.

Because of the bijection $C \xrightarrow{\sim} \mathscr{L}(K + D - G)$ given by $\mathbf{y} \leftrightarrow h_\mathbf{y}$, the *decoding problem* can be obviously described as follows:

($*$) *Given* $\mathbf{y} \in \mathbb{F}_q^n$, *find a function* $h_\mathbf{c} \in \mathscr{L}(K + D - G)$ *such that* $h_\mathbf{e}\eta$ *has a minimal number of poles in* sup (D), *where* $h_\mathbf{e} = h_\mathbf{y} - h_\mathbf{c}$.

This problem will be solved by the following definition and results.

DEFINITION 1. *Given an arbitrary divisor* F, *a solution of the key equation for the received word* $\mathbf{y}$ (*related to* F) *is a triple* $(f, q, r) \in (\mathscr{L}(F) \setminus \{0\}) \times \mathscr{L}(K + F + D - G) \times \mathscr{L}(K + F - G^*)$ *such that* $f\,h_\mathbf{y} = q + r$.

Notice that this definition means that $h_\mathbf{y} = q/f + r/f$ and $h_c = q/f \in \mathscr{L}(K + D - G)$. Thus, what we need to solve the decoding problem is to give conditions such that $h_\mathbf{e} = r/f$ has few poles in sup (D). This is done by the following theorem.

THEOREM 1 (Decoding Theorem). *Let* $\mathbf{y} = \mathbf{c} + \mathbf{e}$, *where* $\mathbf{c} \in C$. *Then*:

1. *If* $\mathscr{L}(F - D_\mathbf{e}) \neq 0$, *then there exists a solution of the key equation.*
2. *If* $\deg F + \mathrm{wt}(\mathbf{e}) < d^*$, *then any solution* (f, q, r) *of the key equation satisfies*

$$\mathrm{res}_D\left(\frac{q\eta}{f}\right) = \mathbf{c} \qquad \text{and} \qquad \mathrm{res}_D\left(\frac{r\eta}{f}\right) = \mathbf{e}.$$

Proof.

1. Take a nonzero function $f \in \mathscr{L}(F - D_\mathbf{e}) \subseteq \mathscr{L}(F)$. Then $(f h_\mathbf{c}) \geq G - D - F - K$, $(f h_\mathbf{e}) \geq -F + D_\mathbf{e} + G^* - D_\mathbf{e} - K = G^* - F - K$, and $f h_\mathbf{y} = f h_\mathbf{c} + f h_\mathbf{e}$; hence the triple $(f, f h_\mathbf{c}, f h_\mathbf{e})$ is a solution of the key equation.

2. Denote by $D_\mathbf{e}$ the divisor of poles of $h_\mathbf{e}\eta$ in the support of D. Let (f, q, r) be a solution of the key equation and set $\varphi \doteq r - f h_\mathbf{e} = f h_\mathbf{c} - q$. One can estimate the divisors

$$K + (r - f h_\mathbf{e}) \geq \min\{G^* - F,\, G^* - F - D_\mathbf{e}\} = G^* - F - D_\mathbf{e}$$

and

$$K + (fh_{\mathbf{c}} - q) \geq G - F - D,$$

which means that $\varphi \in \mathscr{L}(K + F + D_{\mathbf{e}} - G^*) \cap \mathscr{L}(K + F + D - G) = \mathscr{L}(K + F + D_{\mathbf{e}} - G) = 0$, since by assumption $\deg(K + F + D_{\mathbf{e}} - G) = 2g - 2 + \deg(F) + \mathrm{wt}(\mathbf{e}) - \deg(G) < 0$. Hence $\varphi = r - fh_{\mathbf{e}} = fh_{\mathbf{c}} - q = 0$, that yields the theorem. ■

Assume from now on that $\mathscr{L}(F - D_{\mathbf{e}}) \neq 0$ and $\deg F + \mathrm{wt}(\mathbf{e}) < d^*$ (notice that both assumptions are satisfied if $\mathrm{wt}(\mathbf{e}) \leq v$ and $\deg(F) = v + g$, where $v \doteq \lfloor (d^* - g - 1)/2 \rfloor$, that is, when there are few errors and F is small). Thus, for a fixed $\mathbf{y} \in \mathbb{F}_q^n$ define the linear map

$$\begin{array}{cccc} \varepsilon_{\mathbf{y}}\colon & \mathscr{L}(F) & \to & \mathscr{L}(K + F + D - G^*) \\ & f & \mapsto & fh_{\mathbf{y}}. \end{array}$$

Since $\deg(G - F) > \deg G - d^* = 2g - 2$, one has $\mathscr{L}(K + F + D - G) \cap \mathscr{L}(K + F - G^*) = \mathscr{L}(K + F - G) = 0$, and hence there exists a vector space W such that

$$\mathscr{L}(K + F + D - G^*) = \mathscr{L}(K + F + D - G) \oplus \mathscr{L}(K + F - G^*) \oplus W.$$

Denoting by π_W and π^* the natural projections onto W and $\mathscr{L}(K + F - G^*)$, respectively, notice that the key equation means that $\varepsilon_{\mathbf{y}}(f)$ has a null projection onto W. Therefore, if there exists a codeword $\mathbf{c}$ satisfying $\mathrm{wt}(\mathbf{y} - \mathbf{c}) \leq t$, where $0 < t \leq \lfloor (d^* - g - 1)/2 \rfloor$, is fixed, one can compute the error vector with the following algorithm, where a suitable basis for every above function space is assumed to be previously calculated. Such bases can be computed by means of the Brill–Noether algorithm (see [9]).

ALGORITHM 1. ($\mathscr{K}_G(F)$).

1. *Compute a matrix for the linear map* $\varepsilon_{\mathbf{y}}$.
2. *Find a non-zero function* $f \in \ker(\pi_W \circ \varepsilon_{\mathbf{y}})$.
3. *Compute* $r = \pi^*(\varepsilon_{\mathbf{y}}(f))$.
4. *Compute* $\mathbf{e} = \mathrm{res}_D(r\eta/f)$, *checking that* $\mathbf{y} - \mathbf{e} \in C$ *and* $\mathrm{wt}(\mathbf{e}) \leq \lfloor (d^* - 1)/2 \rfloor$.

Notice that most of the calculations in this algorithm are concentrated in the first two steps, and thus its complexity is that of solving linear equations (see [4]). Also notice that the algorithm may fail in the second or fourth steps if the number of committed errors is greater than the bound $\lfloor (d^* - g - 1)/2 \rfloor$, and hence it cannot correct in general up to the half of the Goppa distance. In order to do it, we can use a majority voting scheme, what will be explained in the next sections.

Remark 2. We show now how the above results generalize those of Porter *et al.*, and why they are stronger. Following the notations from [12], the original algorithm works with the codes $C = C_\Omega(D, E - \mu P)$, where E is the divisor of zeros of a function $h \in K_\infty(P)$ without zeros in $\sup(D)$, $K_\infty(P)$ being the ring of those functions having poles only at P, P being a rational point distinct from $\sup(D)$, and where μ is a positive integer. In this case, we can obviously take $G^* = -\mu P$. For the sake of simplicity, assume that there exists a differential form η such that $(\eta) = (2g-2)P$.

First, from the isomorphism given by Lemma 1 we obtain a basis $\varepsilon_1, \dots, \varepsilon_n$ of V such that $\mathrm{res}_D(\varepsilon_1), \dots, \mathrm{res}_D(\varepsilon_n)$ is the canonical basis of $\mathbb{F}_q^n$. Then, Porter defines a "syndrome function" by

$$S_{\mathbf{y}} \cdot \eta = \sum_{j=1}^{n} y_j \left(1 - \frac{h}{h(P_j)}\right) \varepsilon_j.$$

Notice that $S_{\mathbf{y}} \in K_\infty(P)$, $S_{\mathbf{y}} \equiv h_{\mathbf{y}} \pmod h$, and $-v_P(S_{\mathbf{y}}) \leq m + 2g - 1$, where $m \doteq -v_P(h)$. On the other hand, Porter's result to decode C can be rewritten as follows (see [4] for further details):

> If there is an integer t such that $t + \mathrm{wt}(\mathbf{e}) < d^*$ and functions f, q, $r \in K_\infty(P)$ satisfying $-v_P(r) \leq t + 2g - 2 + \mu$, $-v_P(f) \leq t$, and the polynomial key equation
>
> $$f S_{\mathbf{y}} = gh + r$$
>
> then $h_{\mathbf{e}} = r/f$.

Such triples (f, g, r) are called valid solutions in [12]. Thus, by taking $K = (\eta) = (2g-2)P$ and $F = tP$, one has $f \in \mathscr{L}(F)$ and $r \in \mathscr{L}(K + F - G^*)$, and hence this a particular case of our method.[2] Moreover, one obtains $\mathbf{e} = \mathrm{res}_D(r\eta/f)$ where f has few zeros for F small (because of $(f) + F \geq 0$) and thus, for a suitable choice of t and $\mathrm{wt}(\mathbf{e})$, $r\eta/f$ has a minimal number of poles in $\sup(D)$, according to the formulation $(*)$ of the decoding problem. This is actually the underlying idea of Porter, which was carried out by a row reduction process in a certain resultant matrix, but of course it can be done by simple techniques of linear algebra, as we have explained above.

Thus, the results of our paper are stronger than the original results, since they work with an arbitrary divisor G and we do not require any special differential form η or rational function h, what is actually a very strong restriction. Moreover, one obtains a quite similar formula to compute the error just from $h_{\mathbf{y}}$, without the need of the syndrome $S_{\mathbf{y}}$.

[2]In particular, the condition of being minimal for a valid solution can be dismissed from the results of Porter.

3. MAJORITY COSET DECODING

This section is abstracted from [2]. Assume that these exists a rational point $P_\infty \notin \sup(D)$, and let H_1 be a rational divisor whose support is disjoint to $\sup(D)$. Set $H_0 = H_1 - P_\infty$ and $H_2 = H_1 + P_\infty$. For $i = 0, 1, 2$, let $C_i = C_\Omega(D, H_i)$ and $d_i^* = \deg(H_i) + 2 - 2g$. One obviously has $C_0 \supseteq C_1 \supseteq C_2$.

For an error vector $\mathbf{e}$ such that $\mathrm{wt}(\mathbf{e}) \leq (d_1^* - 1)/2$ we want to solve the following problem:

Given $\mathbf{y}_1$ with $\mathbf{y}_1 - \mathbf{e} \in C_1$, find $\mathbf{y}_2$ such that $\mathbf{y}_2 - \mathbf{e} \in C_2$.

This problem is called the *coset decoding procedure related to the extension* $C_1 \supseteq C_2$, where we obviously can assume that $C_1 \neq C_2$.

Thus, for a given $\mathbf{y} \in \mathbb{F}_q^n$ and for any rational function h without poles in $\sup(D)$, one defines the syndrome $S_\mathbf{y}(h)$ by the expression

$$S_\mathbf{y}(h) \doteq \sum_{j=1}^{n} y_j h(P_j) \in \mathbb{F}_q$$

which is linear with respect to both $\mathbf{y}$ and h.

It is very easy to prove that the syndrome is a *coset invariant*, i.e., $S_\mathbf{y}(h) = S_\mathbf{e}(h)$ for all $h \in \mathscr{L}(H_i)$ if and only if $\mathbf{y} - \mathbf{e} \in C_i$, for $i = 0, 1, 2$. Hence, $\mathbf{y} \in C_i$ if and only if $S_\mathbf{y}(h) = 0$ for all $h \in \mathscr{L}(H_i)$.

On the other hand, for an arbitrary divisor F defined over $\mathbb{F}_q$ and $i = 0, 1, 2$, one defines the kernels $K_i(F)$ associated to the error vector $\mathbf{e}$ by

$$K_i(F) \doteq \{ f \in \mathscr{L}(F) \mid S_\mathbf{e}(f \cdot g) = 0, \ \forall g \in \mathscr{L}(H_i - F) \}.$$

All the vector spaces $K_1(F + P_\infty)/K_0(F)$, $K_0(F)/K_1(F)$, $\mathscr{L}(H_1 - F)/\mathscr{L}(H_1 - F - P_\infty)$, $K_1(F + P_\infty)/K_2(F + P_\infty)$ and $K_2(F + P_\infty)/K_1(F)$ have dimension at most one. Thus, we are interested in the conditions

(A1) $K_1(F + P_\infty) \neq K_0(F)$
(A2) $K_0(F) = K_1(F)$
(A3) $\mathscr{L}(H_1 - F) \neq \mathscr{L}(H_1 - F - P_\infty)$.

(B1) $K_1(F + P_\infty) = K_2(F + P_\infty)$
(B2) $K_2(F + P_\infty) \neq K_1(F)$

Define the conditions (A) $\Leftrightarrow$ (A1) $\wedge$ (A2) $\wedge$ (A3) and (B) $\Leftrightarrow$ (B1) $\wedge$ (B2). Since one has (A1) $\wedge$ (B1) $\Leftrightarrow$ (A2) $\wedge$ (B2), the conditions (A) and (B) together are equivalent to (A1), (A3), and (B1).

It follows from [2, Sections II and III] that if (A) and (B) are satisfied, then the *coset decoding procedure* can be implemented by the following algorithm, where D and P_∞ are fixed.

ALGORITHM 2 ($\mathscr{C}_{H_1}(F)$).
Input $:= \mathbf{y}_1$.
If $C_1 = C_2$ *then* $\mathbf{y}_2 = \mathbf{y}_1$ *else*:
- *Find* $\mathbf{c}_0 \in C_1 \backslash C_2$.
- *Find* $f \in K_1(F + P_\infty) \backslash K_0(F)$.
- *Find* $g \in \mathscr{L}(H_1 - F) \backslash \mathscr{L}(H_1 - F - P_\infty)$.
- *Compute* $\lambda = S_{\mathbf{y}_1}(fg)/S_{\mathbf{c}_0}(fg)$.
- *Set* $\mathbf{y}_2 = \mathbf{y}_1 - \lambda \mathbf{c}_0$.

Output $:= \mathbf{y}_2$.

Unfortunately we are not able in practice to check the condition (B), since $K_2(F + P_\infty)$ is not known from the received word $\mathbf{y}$. This problem can be solved by means of *majority voting*, on the basis of the following result due to Duursma (see [2] for further details).

THEOREM 2 (Main Theorem). *Let* $C_0 \supseteq C_1 \supseteq C_2$ *be the extension of codes given by* $C_i \doteq C_\Omega(D, H_i)$, *where* H_1 *has disjoint support with* D, $H_0 \doteq H_1 - P_\infty$ *and* $H_2 \doteq H_1 + P_\infty$. *Assume that the genus is* $g \geq 1$, *and take numbers* $t, r \geq 0$ *such that* $2t + r + 1 \leq d_1^* \doteq \deg H_1 + 2 - 2g$. *Take an arbitrary divisor* F_0 *of degree* t, *and define* $F_i \doteq F_0 + iP_\infty$ *for* $i = 1, \ldots, 2g - 1$. *For an error vector* $\mathbf{e}$ *with weight* $\mathrm{wt}(\mathbf{e}) \leq t$, *define*

$$I \doteq \{r, r+1, \ldots, 2g-2\}$$

$$T \doteq \{i \in I \mid (\mathrm{A}) \wedge (\mathrm{B}) \text{ hold for } F = F_i\}$$

$$F \doteq \{i \in I \mid (\mathrm{A}) \wedge \neg(\mathrm{B}) \text{ hold for } F = F_i\}.$$

Then at least one of the following conditions holds:

(i) $$\mathscr{L}(H_1 - F_{2g-1} - D_{\mathbf{e}} - rP_\infty) \neq 0$$

(ii) $$\mathscr{L}(F_r - D_{\mathbf{e}}) \neq 0$$

(iii) $$\sharp T > \sharp F.$$

In the last section we will see how to apply this majority scheme in order to improve the correction capacity of the decoding algorithm by solving the Ehrhard's key equation up to the half of the Goppa distance. The procedure so obtained is thus the best possible one by solving a key equation, looking at the generality and the capacity of the algorithm.

4. DECODING BY A KEY EQUATION WITH MAJORITY VOTING

Let $C = C_\Omega(D, G)$ be a *strongly algebraic-geometric code*, i.e., such that $2g - 2 < \deg(G) < n$. For our purpose, we can assume that $g > 0$, since otherwise the key equation corrects C up to the half of the Goppa distance and we do not need any majority voting.

Consider successive divisors $G_r = G + rP_\infty$, for $r = 0, 1, \dots, g$. Notice that for any such divisor G_r one has $2g - 2 < \deg(G_r) < n + g$, and thus all these divisors are in the situation of the first paragraph in Section 2. On the other hand, take $t \doteq \lfloor (d^* - 1)/2 \rfloor$, where $d^* \doteq \deg(G) + 2 - 2g$, and assume $t > 0$. Take then a divisor F_0 with degree t and set $F_i \doteq F_0 + iP_\infty$ for $i = 1, \dots, 2g - 1$.

Thus we can consider the following algorithm, which brings together the methods of Ehrhard and Duursma. In the algorithm, the main idea is that the conditions (i) and (ii) given by Theorem 2 allows us to get the error vector by means of a key equation for some suitable G and F, and otherwise the condition (iii) provides us with a majority test to solve the coset decoding problem and decrease the size of the code. We assume that bases for the involved function and differential spaces are previously calculated together with the spaces U, V, W as in Section 2, for all of the possible cases when Algorithm 1 is applied.

ALGORITHM 3 ($\mathscr{D}_G(F_0)$).
Input:= $\mathbf{y} \in \mathbb{F}_q^n$.
Set $\mathbf{y}_1 = \mathbf{y}$.
From $r = 0$ *to* $r = g$ *do*:

- *Set* $H_1 = G + rP_\infty$
- *If* $\mathscr{K}_G(G - F_{2g-1})$ *gets the error vector from* $\mathbf{y}_1$, *then return* $\mathbf{e}$ and *STOP*.
- *Otherwise, if* $\mathscr{K}_{H_1}(F_r)$ *gets the error vector from* $\mathbf{y}_1$, *then return* $\mathbf{e}$ *and STOP*.
- *Otherwise, compute* $I_A \doteq \{i = r, \; r + 1, \dots, 2g - 2 | (\mathrm{A})$ holds for $F = F_i\}$, *apply the coset decoding procedure* $\mathscr{C}_{H_1}(F_i)$ *for* $i \in I_A$ *with input* $\mathbf{y}_1$ *and get a vector* $\mathbf{y}_2$ *whose coset with respect to* $C_2 \doteq C_\Omega(D, H_1 + P_\infty)$ *occurs most of the time*.

Set $\mathbf{y}_1 = \mathbf{y}_2$ *and NEXT* r.

Notice that Algorithm 1 is always applied to one of the divisors G_r. Thus, if we take a divisor G^* such that $\ell(G^*) = 0$ and $G^* \leq G \leq G_r$, we can use the same divisor G^* for all the involved key equations.

Finally, since every functional code can be expressed as a differential code and vice versa, we can prove the following new result, which incorporates the Duursma version of the majority voting scheme into the Ehrhard's version of the key equation.

THEOREM 3. *Let χ be a nonsingular absolutely irreducible projective algebraic curve defined over the finite field $\mathbb{F}_q$ with at least $n+1$ rational points. Let $C = C_\Omega(D, G)$ be an algebraic-geometric code with length n such that $2g-2 < \deg(G) < n$. Let F_0 be any divisor with degree $t \doteq \lfloor (d^* - 1)/2 \rfloor$, where $d^* \doteq \deg(G) + 2 - 2g$ is the Goppa distance of C. Then the algorithm $\mathscr{D}_G(F_0)$ decodes C up to t errors with complexity $\mathcal{O}(n^{2.81})$.*

Proof. First of all, the condition $2t + r + 1 \le d_1^* = \deg(H_1) + 2 - 2g$ is satisfied by every divisor $H_1 = G_r$ from $r = 0$ to $r = g$, and for $t \doteq \lfloor (d^* - 1)/2 \rfloor$; thus we can apply Theorem 2 in every step of the algorithm, provided $\mathrm{wt}(\mathbf{e}) \le t$.

For a fixed $H_1 = G_r$, if the condition (i) $\mathscr{L}(H_1 - F_{2g-1} - D_\mathbf{e} - rP_\infty) = \mathscr{L}(G - F_{2g-1} - D_\mathbf{e}) \neq 0$ holds together with $\mathrm{wt}(\mathbf{e}) \le t$, then the key equation $\mathscr{K}_G(F)$ obtains the error vector for $F = G - F_{2g-1}$, since $\deg F + \mathrm{wt}(\mathbf{e}) < d^*$ and $\mathscr{L}(F - D_\mathbf{e}) \neq 0$, and Theorem 1 can be applied.

In the same way, if the condition (ii) $\mathscr{L}(F_r - D_\mathbf{e}) \neq 0$ holds together with $\mathrm{wt}(\mathbf{e}) \le t$, then the key equation $\mathscr{K}_{G_r}(F_r)$ obtains the error vector, since $\deg F_r + \mathrm{wt}(\mathbf{e}) < \deg(G_r) + 2 - 2g$ and $\mathscr{L}(F_r - D_\mathbf{e}) \neq 0$, and Theorem 1 can also be applied.

Otherwise, the condition (iii) implies that the algorithm $\mathscr{C}_{G_r}(F_i)$ is correct for most of the *candidates* $i \in I_A$, and we can carry on with the next step. Finally, for $r = g$ the condition $\mathscr{L}(F_r - D_\mathbf{e}) \neq 0$ is always true and the algorithm stops at most in $g + 1$ steps, if not too many errors occur,

Notice that the complexity of this algorithm is still equivalent to that of solving a linear system of size n, since most of the computations come from either applications of the algorithm $\mathscr{K}_G(F)$ or finding a function in $K_1(F + P_\infty) \setminus K_0(F)$ (more details in [2]). Thus, the complexity is actually $\mathcal{O}(n^{2.81})$,[3] since solving linear equations can be done faster than Gaussian elimination (see for instance [14]). ■

Remark 3. Notice that the complexity $\mathcal{O}(n^{2.81})$ is even better than the complexity of Sakatas' algorithm $\mathcal{O}(n^{3-2/(r+1)})$ if the curve χ is embedded in an affine r-space with $r > 10$ (what happens in the constructions of asymptotically good codes given in [8]). Thus, general decoding methods which are based on solving linear equations are not as far from fast decoding as they are supposed to be (see [11] for a survey on decoding).

EXAMPLE 1. *Consider the Klein quartic $\mathbf{X}^3\mathbf{Y} + \mathbf{Y}^3\mathbf{Z} + \mathbf{Z}^3\mathbf{X} = 0$ over $\mathbb{F}_8$. This curve has genus $g = 3$ and 24 rational points, namely, $Q_0 = (1:0:0)$, $Q_1 = (0:1:0)$, and $Q_2 = (0:0:1)$ on the coordinate lines, and all the others are in the affine plane, namely, $P_1, \ldots, P_{21}$ (see [10] for details). Set $H_1 = G = 4(Q_0 + Q_1 + Q_2)$, $D = P_1 + \cdots + P_{21}$ and define the code $C_1 = C =$*

[3] Nowadays there are even some improvements of this complexity.

$C_\Omega(D, G)$, with parameters $[21, 11, \geq 8]$. Consider the vector $\mathbf{y}_1 = (1, 0, 1, \alpha, 0, \dots, 0))$ as a received word, where $\alpha \in \mathbb{F}_8$ satisfies $\alpha^3 + \alpha + 1 = 0$, and take the divisor $F_0 = 3P_\infty$, where $P_\infty = Q_2$. Notice that the correction capacity of our algorithm is $t = 3$, whereas the key equation only corrects two errors.

Thus, in the step $r = 0$ one easily checks that the conditions (i) *and* (ii) *from Theorem 2 are not satisfied, and hence the key equation cannot correct this error. Then, one computes the set $I_A = \{3\}$ and applies $\mathscr{C}_G(F)$ to the only candidate $F = F_3$:*

- *Take $\mathbf{c} = (\alpha, \alpha^5, \alpha^3, 0, \alpha^4, \alpha^2, \alpha^6, 1, 0, 1, 1, 0, \dots, 0) \in C_1)\backslash C_2$.*
- *Take $f = \alpha^3 + \mathbf{Z}^3/\mathbf{X}^2\mathbf{Y} \in K_1(F_3 + P_\infty)\backslash K_0(F_3)$.*
- *Take $g = \mathbf{X}/\mathbf{Y} \in \mathscr{L}(G - F_3)\backslash\mathscr{L}(G - F_3 - P_\infty)$.*
- *Compute $\lambda = S_{\mathbf{y}_1}(fg)/S_{\mathbf{c}}(fg) = \alpha^3$.*
- *Return $\mathbf{y}_2 = \mathbf{y}_1 - \lambda\mathbf{c} = (\alpha^5, \alpha, \alpha^2, \alpha, 1, \alpha^5, \alpha^2, \alpha^3, 0, \alpha^3, \alpha^3, 0, \dots, 0)$.*

In this case we have no voting since there is only one candidate, and the above solution is the new $\mathbf{y}_1$ for the next step of the algorithm, which works in a smaller code, we go on until the key equation gets the error vector.

EXAMPLE 2. *Consider now the Hermite curve $\mathbf{Y}^4\mathbf{Z} + \mathbf{Y}\mathbf{Z}^4 + \mathbf{X}^5 = 0$ over $\mathbb{F}_{16}$. It has 64 affine rational points and only one point P_∞ at infinity. Let $D = P_1 + \cdots + P_{64}$, $G_1 = 32P_\infty$ and define the code $C = C_\Omega(D, G_1)$, which is of type $[64, 46, \geq 13]$. Consider then $\mathbf{y}_1 = (\alpha^{12}, \alpha^4, \alpha^7, \alpha^8, \alpha^9, \alpha^9, 0, \dots, 0))$ as a received word, where $\alpha \in \mathbb{F}_{16}$ satisfies $\alpha^4 + \alpha + 1 = 0$, and take the divisor $F_0 = 6P_\infty$.*

Now for $r = 0$ again (i) *and* (ii) *do not hold, and one computes $I_A \sim \{1, 2, 3, 5, 7, 8, 9\}$. In this case, voting actually occurs and the procedure is equivalent to the algorithm of Feng and Rao* (*see* [6]).

REFERENCES

1. E. R. Berlekamp, "Algebraic Coding Theory," McGraw–Hill, New York, 1968.
2. I. M. Duursma, Majority coset decoding, *IEEE Trans. Inform. Theory* **39** (1993), 1067–1071.
3. I. M. Duursma, "Decoding Codes from Curves and Cyclic Codes," Ph.D. thesis, Univ. Eindhoven, 1993.
4. D. Ehrhard, "Über das Dekodieren Algebraisch–Geometrischer Codes," Ph.D. thesis, Universität Düsseldorf, 1991.
5. D. Ehrhard, Achieving the designed error capacity in decoding algebraic-geometric codes. *IEEE Trans. Inform. Theory* **39** (1993), 743–751.
6. G. L. Feng and T. R. N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance, *IEEE Trans. Inform. Theory* **39** (1993), 37–45.
7. W. Fulton, "Algebraic Curves," Benjamin, Elmsford, NY, 1969.
8. A. García and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vlăduţ bound, *Invent. Math.* **121** (1995), 211–222.

9. G. Haché and D. Le Brigand, Effective construction of algebraic geometry codes, *IEEE Trans. Inform. Theory* **41** (1995), 1615–1628.

10. J. P. Hansen, Codes on the Klein quartic, ideals and decoding, *IEEE Trans. Inform. Theory* **33** (1987), 923–925.

11. T. Høholdt and R. Pellikaan, On the decoding of algebraic–geometric codes, *IEEE Trans. Inform. Theory* **41** (1995), 1589–1614.

12. S. C. Porter, B.-Z. Shen, and R. Pellikaan, On decoding geometric Goppa codes using an extra place, *IEEE Trans. Inform. Theory* **38** (1992), 1663–1676.

13. H. Stichtenoth, "Algebraic Function Fields and Codes," Universitext, Springer–Verlag, Berlin/New York, 1993.

14. V. Strassen, Algebra and complexity, *in* "1st European Congress of Math.," Vol. II, Part 2, Progress in Math., Vol. 120, pp. 429–446, Birkhäuser, Basel, 1994.