The Key Equation for One-Point Codes and Efficient Error Evaluation*†

Michael E. O'Sullivan
Department of Mathematical and Computer Sciences
San Diego State University
San Diego, CA 92182-7720 USA
m.osullivan@math.sdsu.edu

December 13, 2000

Abstract

Index Terms: Algebraic geometry codes, key equation, error evaluator.

In this article, the key equation and the use of error evaluator polynomials are generalized from the case of BCH codes to one-point codes. We interpret the syndrome of the error vector e as a differential ω_e which has simple poles on the support of e and, in general, at the one-point Q used to define the codes. The decoding problem is to find a function f and differential ϕ having poles only at Q such that $f\omega_e = \phi$. Then if f has a simple pole at an error position P, the error value is $e_P = \phi(P)/df(P)$. We amend an iterative algorithm that computes a Gröbner basis for I_e, the ideal of functions vanishing on the support of e, so that it also computes the corresponding error evaluators. That is we produce $f\omega_e$ for each f in the Gröbner basis.

---

*

†This research was supported by the National Science Foundation through Grants SBIR-#9403420 and CCR-98-05080

1 Introduction

The decoding problem for Reed-Solomon codes was reformulated by Berlekamp and others as a problem of finding a pair of polynomials of minimal degree—the error locator and error evaluator—which solve a "key equation." In this article, we derive a generalization to one-point codes of this key equation. We also show that the algorithm presented in [14], which efficiently computes error locator polynomials, can be modified slightly to compute error evaluator polynomials as well.

For Reed-Solomon codes the key equation is usually presented as follows [13, §12.9]. Let $a_1, \ldots, a_t$ be the field elements where errors occured and let $e_1, \ldots, e_t$ be the error values. We define the syndrome polynomial to be $S = \sum_{i=1}^{m-1} s_i x^i$ where m is the number of check symbols and where $s_i = \sum_{k=1}^{t} e_k a_k^i$. The key equation is $\sigma S = \omega \mod x^m$. The decoding problem is, given S to find σ and ω of minimal degree solving this equation. One can show that $\sigma = \prod_{k=1}^{t}(1 - a_k x)$. Since the zeros of σ are the reciprocals of the error locations, σ is called the error locator polynomial. The error value at P_k is given by $e_k = -a_k \omega(a_k^{-1})/\sigma'(a_k^{-1})$, so ω is called the error evaluator polynomial.

From the more general perspective of algebraic geometry codes, it is more natural to define an error locator as vanishing at the locations of the errors, rather than at the reciprocals. The problem in generalizing the key equation is then, what algebraic object should the syndrome be? For Reed-Solomon codes one can simply take $S = \sum_{k=1}^{t} e_k/(x - a_k) = (1/x)\sum_{k=0}^{\infty} s_i x^{-i}$. This approach was extended by Chabanne and Norton [1] to define a key equation for n-dimensional cyclic codes. We will show that it generalizes in a very natural way to one-point codes.

Let C be a smooth curve defined over a perfect field k. Let Q be a rational point on C and let R be the ring of functions with poles only at Q. Let us assume for simplicity that $(2g-2)Q$ is canonical. For an error vector e, we let S_e be the syndrome map associated to a vector $e = (e_1, \ldots, e_n)$; $S_e(f) = \sum_{k=1}^{n} e_k f(P_k)$. We show there exists a function h_e such that any $f \in R$ is an error locator if and only if fh_e is also in R, that is, it has no poles away from Q. Furthermore, if f has a simple zero at an error position P then fh_e and the derivative f' can be used to evaluate the error at P. For general curves—$(2g-2)$ not canonical—we use a differential ω_e to represent the syndrome.

Several approaches to defining a key equation and error evaluators have appeared previously [1, 2, 3, 5, 8, 10, 11, 12, 17, 20, 21]. Porter, Shen and Pellikaan [17] work with general codes on curves, but later papers [20, 21] consider the particular case of one-point codes. For one-point codes, they follow the traditional approach to the key equation for BCH codes by defining the syndrome of a received vector as an element of the ring R. To decode $C_\Omega(D, mQ)$, an auxiliary function $h \in R$ is introduced and one uses a decoding algorithm for the isometric code $C_\Omega(D, E - \mu P)$ where the divisor $(h) = E - (m + \mu)Q$.

Ehrhard [2] also defines a key equation for arbitrary codes on curves and his definition also requires choosing a number of auxiliary divisors and differentials. Ehrhard's decoding algorithm [3] starts with an arbitrary divisor F of degree $2g + \tau$ where τ is the number of errors to be corrected and g is the genus of the curve. The idea is to apply extra conditions on this space so that at the end of g iterations the only functions left must vanish at the error positions. In the case of one-point codes, one could start with the space $L((t+2g)Q)$ of functions with poles only at Q and of order at most $2t+g$. The algorithm successively chooses points $P_{k_1}, \ldots, P_{k_r}$ and computes the spaces $H_l = L((2t+g)Q - P_{i_1} - \cdots - P_{i_l})$. The P_{i_j} are chosen to reduce the dimension of a certain linear space by 2. At the end of the algorithm we have a set of locators. Furthermore, if we interpret the syndrome as a differential, the product of the syndrome and a locator can be used to calculate the error values.

Another approach to error evaluation is to compute for each error position P some function σ_P which does not vanish at P but does vanish at the other error positions. The error values are then $S_e(\sigma_P)/\sigma_P(P)$ where $S_e(\sigma_P)$ is the syndrome of the function σ_P. Leonard [11] offers a number of ways to construct the σ_P and in [12] gives an efficient algorithm for computing them from the error locator ideal. For plane curves, Kötter, Jensen and Hansen [5] also seek functions σ_P vanishing at all error positions except $P = (a, b)$. In the case of a Hermitian curve, defined by $H(x, y)$, they show how to compute a simple expression for σ_P that involves the product of the error locator function with $H(x-a, y)/(y-b)$. In [10], the σ_P are used to show that an error evaluator function can be computed directly from the error locator and the syndrome array.

Elements of each of these approaches will be found in this article. Since we restrict to the case of one-point codes we can assign to each error vector a uniquely defined differential (modulo a certain space of differentials). This eliminates the need to introduce auxiliary divisors and other complex aspects involved in the implementation of the Porter/Shen and Ehrhard algorithms. In the case of Hermitian curves we obtain the same error evaluator as Kötter et al. An important difference in the description here is that we express all of the mathematics in terms of the function field of the curve rather than a polynomial ring. This simplifies the expression of the key equation and the error evaluator. It also shows that error evaluator polynomials may be computed along with error locator polynomials in the usual iterative algorithm. In fact, the efficient implementation in [9] may be slightly changed to compute error evaluators.

Section 2 summarizes notation and basic results about one-point codes. Section 3 shows that the syndrome map S_e may be thought of as a differential ω_e which acts on R by taking residues at the one-point Q, $S_e(f) = -\operatorname{res}_Q(f\omega_e)$. Section 4 treats several examples, in particular the Hermitian curve and the Klein quartic. Section 5 defines the key equation while Section 7 shows how to define approximate solutions to the key equation and connects the approach here with Sakata's algorithm. Section 6 shows the existence of functions $\{z_u \in K\}$ and differentials $\{\zeta_v \in \Omega\}$ which are dual relative to res_Q. Then we show that there is a *unique* ω_e which can be expressed as a series in the ζ_v with coefficients $S_e(z_v)$ where v ranges over the set of nongaps at the one-point Q. In addition, for any $f \in R$, the product $f\omega_e$, when expressed as a series in the ζ_v, has coefficients which are syndromes of either multiples of f, or approximations of multiples of f (Proposition 6.8). This rather technical result is just what is needed to make an efficient Sakata-type algorithm which will compute error evaluators as well as locators. Section 8 presents this algorithm.

2 Preliminaries

This section summarizes notation that will be used throughout this article. Let K be a function field of transcendence degree one over a perfect field k. We assume that k is algebraically closed in K. Let C be the smooth curve over k defined by K and let g be its genus. Let Q be a rational point of C, and let R be the ring of functions on $C \setminus Q$. Take $P_1, P_2, \ldots, P_n$ to be distinct rational points on C, each different from Q, and let $D = P_1 + P_2 + \cdots + P_n$. We define the evaluation map ev as follows.

$$\begin{aligned} ev : R &\to k^n \\ f &\to (f(P_1), f(P_2), \ldots, f(P_n)) \end{aligned}$$

Let $L(mQ)$ be the space of functions on C having poles only at Q and of order at most m there. Each $L(mQ)$ contains $L((m-1)Q)$, and is either equal to it, when we say m is a gap, or of dimension one larger, when m is a nongap. The union of the $L(mQ)$ is the ring R,

$$R = \bigcup_{m=0}^{\infty} L(mQ)$$

Let Λ be the set of nongaps. We consider the family of codes $C_L(D, mQ) = ev(L(mQ))$, for $m \in \Lambda$, used as parity check codes. The dual codes, $C_\Omega(D, mQ)$, are used for encoding.

Let e be a vector in k^n indexed by the P_k. The weight of e, $\operatorname{wt} e$, is the number of nonzero coordinates of e. The syndrome map associated to e is

$$S_e : R \to k \tag{1}$$

$$f \to \sum_{k=1}^{n} e_k f(P_k) \tag{2}$$

For each point P of C, rational or not, there is a valuation map $\nu_P : K \setminus \{0\} \longrightarrow \mathbb{Z}$. For the point Q we will also use the pole order function, $o(f) = -\nu_Q(f)$ for $f \in R$. When there is no danger of ambiguity we will use ν_k for the valuation of K centered at P_k and res_k for the residue of a differential at P_k.

3 The Syndrome Differential

In this section we will prove the main results that allow us to define the key equation and error-evaluator differentials (or polynomials). The main result, Theorem 3.3, says that given a vector e, there exists a differential ω_e such that

$$S_e(f) = -\operatorname{res}_Q f\omega_e \tag{3}$$

Furthermore, ω_e is unique modulo differentials that have poles only at Q. If $(2g-2)Q$ is a canonical divisor, then we can write everything in terms of functions. Let ω_0 have divisor $(2g-2)Q$. Then there is an h_e such that

$$S_e(f) = -\operatorname{res}_Q f h_e \omega_0 \tag{4}$$

and h_e is unique modulo R. The final result of the section is that ω_e (or h_e) can be used for error evaluation.

We start this section with a review of differentials, see [22]. The module of differentials Ω of K over k is a one dimensional vector space over K. There is a map $d : K \to \Omega$ linear over k and satisfying the product rule $d(fg) = f dg + g df$. For each differential ω, there is a divisor (ω)

which is nonzero at a finite number of points and has degree $2g-2$. Let $\Omega(D) = \{\omega : (\omega) \geq D\}$. The Riemann-Roch theorem says that $\dim L(D) - \dim \Omega(D) = \deg D - g + 1$. For any rational point Q there is a k-linear map $\operatorname{res}_Q : K \to k$. When k is algebraically closed the sum of the residues of a differential at all points of the curve is zero, $\sum_{Q \in C} \operatorname{res}_Q \omega = 0$. When k is not algebraically closed and ω has poles only at rational points the sum of the residues at the rational points is zero.

Proposition 3.1. *Let C be a smooth curve over a perfect field k and let Q and P be distinct rational points on C. Then there exists a differential ω_P such that $\nu_P(\omega_P) = \nu_Q(\omega_P) = -1$, $\operatorname{res}_P(\omega_P) = -\operatorname{res}_Q(\omega_P) = 1$ and ω_P has no other poles.*

PROOF: From the Riemann-Roch theorem we have $\dim \Omega(0) = g$, $\dim \Omega(-P) = \dim \Omega(-Q) = g$ and $\dim \Omega(-P-Q) = g+1$. Thus there is a differential which has poles at both P and Q and nowhere else. Since the sum of the residues is zero, the residue at P and Q must have opposite signs. Multiplying by an element of k, we can adjust so that the residue is 1 at P and -1 at Q. □

Lemma 3.2. *Let $f \in R$ and let ω_P be as in the proposition. Then $\operatorname{res}_Q f\omega_P = -f(P)$.*

PROOF: Write $f = a_0 + a_1 t + a_2 t^2 + \ldots$ where t is a uniformizing parameter at P and $a_i \in k$. Since ω_P has a pole of order one at P and residue 1, $\omega_P = (1 + b_1 t + b_2 t^2 + \cdots)dt/t$ with $b_i \in k$. Thus $f\omega_P = (a_0 + (a_1 + a_0 b_1)t + \cdots)dt/t$ and $\operatorname{res}_P f\omega_P = f(P)$. Since $f\omega_P$ has poles only at P and Q, the sum of residues theorem says that $\operatorname{res}_Q f\omega_P = -f(P)$. □

Theorem 3.3. *Let C be a smooth curve over a perfect field k with function field K and module of differentials Ω. Let Q, $P_1, \ldots P_n$ be distinct rational points of C and let S_e be the syndrome map defined by $e \in k^n$. Then there exists an $\omega_e \in \Omega$ such that for all $f \in R$,*

$$S_e(f) = -\operatorname{res}_Q f\omega_e \tag{5}$$

If ω'_e is any other differential satisfying the same property then $\omega_e - \omega'_e$ has poles only at Q.

PROOF: Let ω_k be such that $\nu_k(\omega_k) = \nu_Q(\omega_k) = -1$, $\operatorname{res}_k \omega_k = -\operatorname{res}_Q \omega_k = 1$ and ω_k has no other poles, as in Proposition 3.1. Let $\omega_e = \sum_{k=1}^n e_k \omega_k$. Then

$$\begin{aligned}\operatorname{res}_Q f\omega_e &= \sum_{k=1}^n e_k \operatorname{res}_Q f\omega_k \\ &= -\sum_{k=1}^n e_k f(P_k) \\ &= -S_e(f)\end{aligned}$$

Suppose now that ω'_e also satisfies the proposition. Then $\operatorname{res}_Q f(\omega_e - \omega'_e) = 0$ for all $f \in R$. The following lemma shows that $\omega_e - \omega'_e$ has poles only at Q. □

Lemma 3.4. *Let η be any nonzero differential having a pole at some point P distinct from Q. Then there exists an $f \in R$ such that $\operatorname{res}_Q f\eta \neq 0$.*

PROOF: Let $P, Q_1, Q_2, \ldots, Q_t$ be the poles of η distinct from Q. By the strong approximation theorem [22, I.6.4] there exists an $f \in K$ such that

$$\begin{aligned}&\nu_{Q_i}(f) = -\nu_{Q_i}(\eta) \text{ for } 1 \leq i \leq t\\&\nu_P(f) = -\nu_P(\eta) - 1 \text{ and,}\\&\nu_T(f) \geq 0 \text{ for all } T \neq Q \text{ and } T \neq P, Q_1, \ldots, Q_t\end{aligned}$$

Since f has no poles except at Q, $f \in R$. Furthermore, $\nu_T(f\eta) \geq 0$ for all $T \neq P, Q$, and $\nu_P(f\eta) = -1$. Thus $\mathrm{res}_P\, f\eta \neq 0$. Since the only other pole of $f\eta$ is at Q, the residue theorem gives $\mathrm{res}_P\, f\eta + \mathrm{res}_Q\, f\eta = 0$. Thus $\mathrm{res}_Q\, f\eta \neq 0$. □

Corollary 3.5. *Suppose that $(2g-2)Q$ is a canonical divisor, and let ω_0 have divisor $(2g-2)Q$. Then there exists an $h_e \in K$ such that*

$$S_e(f) = -\mathrm{res}_Q\, f h_e \omega_0$$

If $h'_e \in K$ also satisfies this property then $h_e - h'_e \in R$.

PROOF: Let ω_e satisfy (5) in the theorem. Clearly $h_e = \omega_e/\omega_0$ satisfies the statement of the corollary. Furthermore if h'_e satisfies (3.5), then $h'_e\omega_0$ satisfies (5) and $\omega_e - h'_e\omega_0$ has poles only at Q. Dividing by ω_0, $h_e - h'_e$ has poles only at Q, so it is in R. □

The final result of this section is that a function $f \in R$ vanishing at a point of D_e and its product with ω_e (or h_e) can be used for error evaluation.

Proposition 3.6. *Let C be a smooth curve over a perfect field k. Let Q and $P_1, \ldots, P_n$ be distinct rational points on C, let $e_1, \ldots, e_n \in k$ and let ω_e satisfy Theorem 3.3. Suppose that f has a zero of multiplicity one at P_k. Then*

$$\frac{f\omega_e}{df}(P_k) = e_k$$

PROOF: Suppose first that $\omega_e = \sum e_j\omega_j$ where ω_j has simple poles at P_j and Q and no other poles and $\mathrm{res}_{P_j}\, \omega_j = 1$. Let t be a uniformizing parameter at P_k. Since ω_k is the only term in ω_e which has a pole at P_k, ω_e has a simple pole at P_k with residue e_k. Thus $\omega_e = (e_k + b_1 t + b_2 t^2 + \cdots)dt/t$ for some $b_i \in k$. Since f has a simple zero at P_k, $f = a_1 t + a_2 t^2 + \cdots$ and $df = (a_1 + 2a_2 t + \cdots)dt$ with $a_1 \neq 0$. Then

$$\begin{aligned}\frac{f\omega_e}{df} &= \frac{(a_1 t + a^2 t^2 + \cdots)(e_k + b_1 t + b_2 t^2 + \cdots)dt/t}{(a_1 + 2a^2 t + \cdots)dt}\\&= \frac{(a_1 + a^2 t + \cdots)(e_k + b_1 t + b_2 t^2 + \cdots)}{(a_1 + 2a_2 t + \cdots)}\end{aligned}$$

Evaluating at P_k, (where $t(P_k) = 0$) gives the result.

Now let ω'_e be any other differential satisfying Theorem 3.3. Then $\nu_k(\omega'_e - \omega_e) \geq 0$ while $\nu_k(f) = 1$, so $(f(\omega'_e - \omega_e)/df)(P_k) = 0$. Therefore $(f\omega'_e/df)(P_k) = (f\omega_e/df)(P_k) = e_k$. □

Corollary 3.7. *Suppose that $(2g-2)Q$ is a canonical divisor, and let ω_0 have divisor $(2g-2)Q$. If h_e satisfies Corollary 3.5, and f has a zero of multiplicity one at P_k, then*

$$e_k = \frac{f h_e(P_k)}{f'(P_k)}$$

where f' is such that $df = f'\omega_0$.

4 Examples

If P is a rational point on a curve we let S_P be the syndrome map corresponding to an error vector which has a single error at the position P and error value 1. So S_P takes $f \in R$ to $f(P)$.

Example 4.1. Let Q be a point on the projective line $\mathbb{P}^1$ and let $k[x]$ be the ring of functions on $\mathbb{P}^1 \setminus Q$. Let P be the rational point with coordinate $a \in k$, so $x - a$ is a uniformizing parameter at P. Since $dx/(x-a)$ has poles only at P and Q and residue 1 at P, it may be taken to be ω_P. Thus $S_P(f) = \operatorname{res}_P(f(dx)/(x-a)) = -\operatorname{res}_Q(f(dx)/(x-a)) = f(a)$ for $f \in k[x]$. Since $-2Q$ is a canonical divisor and $(dx) = -2Q$, we define h_P by $\omega_P = h_P dx$. Thus

$$
\begin{aligned}
h_P &= \frac{1}{x-a} \\
&= \frac{1}{x}\frac{1}{(1-\frac{x}{a})}
\end{aligned}
$$

Expanding as a power series in $1/x$,

$$h_P = \frac{1}{x}(1 + \frac{a}{x} + \frac{a^2}{x^2} + \frac{a^3}{x^3} + \cdots)$$

If h_e is the function associated to a vector e which is non-zero at the points $P_1, \ldots, P_t$ with coordinates $a_1, \ldots, a_t$ then

$$h_e = \sum_{k=1}^{t} \frac{e_k}{x - a_k} \tag{6}$$

Rewriting using the power series expansion,

$$
\begin{aligned}
h_e &= \frac{1}{x}\sum_{k=1}^{t} e_k \sum_{i=0}^{\infty} \frac{a_k^i}{x^i} \\
&= \frac{1}{x}\sum_{i=0}^{\infty} \frac{1}{x^i} \sum_{k=1}^{t} e_k a_k^i \\
&= \frac{1}{x}\sum_{i=0}^{\infty} \frac{s_i}{x^i}
\end{aligned} \tag{7}
$$

where $s_i = S_e(x^i) = \sum_{k=1}^{t} e_k a_k^i$ are the usual syndrome values.

Example 4.2. Let C be a smooth plane curve over a perfect field k such that L_∞ meets C in a unique point Q which is the intersection of L_∞ with the y-axis. Let $f(x,y)$ be the equation of C in the affine plane and let f_x and f_y be the derivatives of f with respect to x and y. Since $f_x dx + f_y dy = 0$, we may set $\omega_0 = dx/f_y = -dy/f_x$. Since C is smooth, f_x and f_y have no common zeros with C. Thus for any point $P \neq Q$ defined over the algebraic closure of k, either $f_x(P) \neq 0$ or $f_y(P) \neq 0$. Consequently, $\nu_P(\omega_0) \geq 0$. On the other hand, since at least one of $x - x(P)$ or $y - y(P)$ is a uniformizing parameter at P, $\nu_P(\omega_0) \leq 0$. Thus ω_0 is supported only at Q, $(\omega_0) = (2g-2)Q$.

Let P be a rational point of C with coordinates (a, b). Then we have $S_P : k[x,y]/f \to k$ such that $S_P(g) = g(P)$. This time we cannot use $dx/(x-a)$ for ω_P because it has other poles besides P. I claim

$$h_P = \frac{f(a,y)}{(y-b)(x-a)}$$

has a simple pole at P, a pole of order $2g-1$ at Q and no other poles, so ω_P is some constant multiple of $h_P\omega_0$.

For any point $P' = (a, b')$ on the intersection of C with the line $x = a$, $y - b'$ is a root of $f(a,y)$ of multiplicity $\nu_{P'}(x-a)$. If $P' \neq P$, then $\nu_{P'}(y-b) = 0$, and therefore $\nu_{P'}(h_P) \geq 0$. At P,

$$\begin{aligned}
\nu_P(h_P) &= \nu_P(f(a,y)) - \nu_P(y-b) - \nu_P(x-a) \\
&= (\nu_P(y-b))(\nu_P(x-a)) - \nu_P(y-b) - \nu_P(x-a) \\
&= (\nu_P(y-b) - 1)(\nu_P(x-a) - 1) - 1
\end{aligned}$$

Since C is smooth, one of $x-a$ or $y-b$ has valuation 1. So $\nu_P(h_P) = -1$. Thus h_P has a simple pole at P, and no other poles except perhaps at Q. We now analyze the behavior at Q. Let f have degree d. Since C meets L_∞ only at Q, the degree d part of f is x^d and L_∞ meets C with multiplicity d at Q. Thus $\nu_Q(y-b) = -d$ and since $x-a$ passes through Q, $\nu_Q(x-a) = -d+1$. We assumed C is smooth at Q, so f has a nonzero term in y^{d-1}. Thus $\deg f(a,y) = d-1$ and $\nu_Q(f(a,y)) = -d(d-1)$. Finally, $\nu_Q(h_P) = -(d-1)d+d+(d-1) = -(d^2-3d+1) = -(2g-1)$, so h_P has a pole of order $2g-1$ at Q.

This analysis also works in the case when C is singular only at Q, provided the desingularization $\tilde{C}$ has a unique rational point $\tilde{Q}$ above Q. Suppose that $\nu_{\tilde{Q}}(x) = -k$ and $\nu_{\tilde{Q}}(y) = -d$ with $k < d$. Then f has non-zero terms in x^d and y^k and other terms with lower pole order. Thus $\deg f = d$, $\deg f(a,y) = k$ and $g(\tilde{C}) = (d-1)(k-1)/2$. Now, $\nu_{\tilde{Q}}(h_P) = -kd + d + k = -(2g_{\tilde{C}} - 1)$.

Example 4.3. Let C be the Hermitian curve in the plane over $\mathbb{F}_{q^2}$ defined by $f(x,y) = x^{q+1} - y^q - y = 0$ and let Q be the point at infinity. This is a special case of the previous example, and we have $f_y = 1$ so $\omega_0 = dx$. Let P have coordinates (a, b). Applying the previous example, we have

$$\begin{aligned}
h_P &= \frac{a^q - y - y^q}{(x-a)(y-b)} \\
&= \frac{x^5 - a^5}{(x-a)(y-b)}
\end{aligned}$$

Expanding as a power series in $1/x$ and $1/y$,

$$\begin{aligned} h_P &= \frac{x^q}{y}(1+\frac{a}{x}+\frac{a^2}{x^2}+\cdots+\frac{a^q}{x^q})(1+\frac{b}{y}+\frac{b^2}{y^2}+\frac{b^3}{y^3}+\cdots) \\ &= \frac{x^q}{y}\sum_{i=0}^{q}\sum_{j=0}^{\infty}\frac{a^i b^j}{x^i y^j} \end{aligned}$$

If S_e is the syndrome map associated to a vector e which is non-zero at the points $P_1,\dots,P_t$ with coordinates (a_k, b_k), then

$$\begin{aligned} h_e &= \frac{x^q}{y}\sum_{k=1}^{t} e_k \sum_{i=0}^{q}\sum_{j=0}^{\infty}\frac{a_k^i b_k^j}{x^i y^j} && (8) \\ &= \frac{x^q}{y}\sum_{i=0}^{q}\sum_{j=0}^{\infty}\frac{1}{x^i y^j}\sum_{k=1}^{t} e_k a_k^i b_k^j \\ &= \frac{x^q}{y}\sum_{i=0}^{q}\sum_{j=0}^{\infty}\frac{s_{ij}}{x^i y^j} && (9) \end{aligned}$$

where the s_{ij} are the usual syndrome values for $x^i y^j$ with $0 \le i \le q$ and $0 \le j$; $s_{ij} = S_e(x^i y^j) = \sum_{k=1}^{t} e_k a_k^i b_k^j$.

Example 4.4. Let C be the Klein quartic defined by $X^3Y + Y^3Z + Z^3X$ in the projective plane over a perfect field k. We assume $\operatorname{char} k \neq 7$ since the curve is not smooth in that case. There are two points on the line $Z = 0$, $Q = [0 : 1 : 0]$ and $P = [1 : 0 : 0]$. Let $O = [0 : 0 : 1]$. Then the lines determined by X, Y and Z cut out the following divisors, $(X) = 3O + Q$, $(Y) = 3P + O$ and $(Z) = 3Q + P$. Consider now the affine plane with $x = X/Z$, and $y = Y/Z$ and where $f = x^3y + y^3 + x$ is the polynomial defining the curve. One can check that $(x) = 3O - 2Q - P$, $(y) = 2P + O - 3Q$, $(xy) = 4O + P - 5Q$ and $x^2y = 7O - 7Q$. Let R be the ring of functions with poles only at Q. Then R is generated by y, xy and x^2y and the nongap sequence Λ is generated by $3, 5, 7$.

Differentiating the equation for the curve, $f = 0$, we get $-(3x^2y + 1)dx = (3y^2 + x^3)dy$. Set $\omega_0 = -dx/(3y^2 + x^3) = dy/(3x^2y + 1)$. As in Example 4.2, ω_0 is supported on the points on $Z = 0$, that is P and Q. In fact, $(\omega_0) = 3Q + P$.

One can verify that $\omega_P = x^2\omega_0$ has simple poles at P and Q and no other poles and that its residue at P is 1. Let T be a rational point of C with coordinates (a, b). The function $g = f(x, b)/(x - a)(y - b)$ has a simple pole at T, and a pole of order 4 at Q, but it also has a pole of order 2 at P. Thus $g\omega_0$ has simple poles at T, Q and also P. If we adjust by adding

$x^2\omega_0$, the pole at P vanishes. Thus we set

$$\begin{aligned}\omega_T &= \frac{f(x,b)}{(x-a)(y-b)}\omega_0 + x^2\omega_P \\ &= \frac{bx^2+abx+a^b+1}{y-b}\omega_0 + \frac{yx^2-bx^2}{y-b}\omega_0 \\ &= \frac{\omega_0}{y}\left(\frac{1}{1-y/b}\right)\left(yx^2+1+abx+a^2b\right)\end{aligned}$$

We now rewrite this as a sum of three infinite sums.

$$\omega_T = \omega_0(yx^2+1)\sum_{j=0}^{\infty}\frac{b^j}{y^{j+1}} + x\omega_0\sum_{j=0}^{\infty}\frac{ab^{j+1}}{y^{j+1}} + \omega_0\sum_{j=0}^{\infty}\frac{a^2b^{j+1}}{y^{j+1}} \tag{10}$$

The numerators in the infinite sums are just the functions y^j, xy^{j+1} and x^2y^{j+1} evaluated at the point T. We can express ω_P in this form as well. All of these functions vanish at P except $y^0(P)=1$ and $x^2y(P)=-1$ Then (10) becomes

$$\begin{aligned}\omega_P &= \omega_0(x^2+\frac{1}{y}) + \omega_0\frac{-1}{y} \\ &= x^2\omega_0\end{aligned}$$

For an arbitrary error vector e we have

$$\omega_e = \omega_0(yx^2+1)\sum_{j=0}^{\infty}\frac{S_e(y^j)}{y^{j+1}} + x\omega_0\sum_{j=0}^{\infty}\frac{S_e(xy^{j+1})}{y^{j+1}} + \omega_0\sum_{j=0}^{\infty}\frac{S_e(x^2y^{j+1})}{y^{j+1}} \tag{11}$$

This expression is the analogue of (7) for Reed-Solomon codes and is the application of the formula 25 in Section 6 to the Klein quartic.

5 The Key Equation

In this section we generalize the notion of the key equation for BCH codes to one-point codes.

We define

$$\Omega(-\infty Q) = \{\omega \in \Omega : \nu_P(\omega) \geq 0 \text{ for all } P \in C \setminus Q\}$$

Notice that $\Omega(-\infty Q) = \cup_{m=1}^{\infty}\Omega(-mQ)$ is the analogue for differentials of the ring R. For the error vector $e \in k^n$, we define the error divisor D_e to be the sum of all points P_k such that $e_k \neq 0$ and the error locator ideal I_e to be the ideal of locator functions, those elements in R vanishing on D_e. We will continue to use S_e for the syndrome map, ω_e for the associated differential, and h_e for the associated function in the case when $(2g-2)Q$ is canonical. By Theorem 3.3 and its corollary, ω_e is uniquely defined modulo $\Omega(-\infty Q)$ and h_e is uniquely defined modulo R.

Theorem 5.1. *Let $I_e \subset R$ be the ideal of functions vanishing on all P_k such that $e_k \neq 0$ and let $f \in R$. The following are equivalent:*

1. $f \in I_e$,
2. $f\omega_e \in \Omega(-\infty Q)$,
3. $fh_e \in R$, *in the case when* $(2g-2)Q$ *is canonical.*

PROOF: Recall that $\omega_e = \sum_{k=1}^{n} e_k \omega_k$ and that each ω_k has poles at only P_k and Q and those of order one. If f vanishes at all P_k such that $e_k \neq 0$ then $f\omega_e$ has no poles except perhaps at Q, so $f\omega_e \in \Omega(-\infty Q)$. Conversely, if f does not vanish at some P_k such that $e_k \neq 0$ then $f\omega_k$ has a pole at P_k. Since the other $f\omega_j$ have nonnegative valuation at P_k, $f\omega_e$ will have a pole at P_k Thus $f \in I_e$ if and only if $f\omega_e \in \Omega(-\infty Q)$.

The equivalence of the last two items is immediate since $\omega_e = h_e\omega_0$ where $(\omega_0) = (2g-2)Q$.
□

Definition 5.2. We will say that $f \in R$ and $\phi \in \Omega(-\infty Q)$ *satisfy the key equation* if $f\omega_e = \phi$. We say that $f \in R$ and $\phi \in \Omega(-\infty Q)$ *satisfy the mth approximation to the key equation* (or the mth key equation for short) if $\nu_Q(f\omega_e - \phi) \geq m$.

Similarly, if $(2g-2)Q$ is a canonical divisor, we say that $f, \phi \in R$ *satisfy the key equation* if $fh_e = \phi$. They *satisfy the mth approximation to the key equation* if $\nu_Q(fh_e - \phi) \geq m - 2g + 2$.

If $f \in R$ and $\phi \in \Omega(-\infty Q)$ satisfy the mth key equation, and $(\omega_0) = (2g-2)Q$, then f and $\phi/\omega_0 \in R$ also satisfy the mth key equation since $\nu_Q(f\omega_e/\omega_0 - \phi/\omega_0) \geq m - 2g + 2$.

6 A Useful Expansion

In this section we show the existence of bases for R and for $\Omega(-\infty Q)$ that have useful computational properties and that allow us to work with a uniquely defined ω_e.

Let $\Lambda^c = \mathbb{Z} \setminus \Lambda$. The proof of the following lemma is elementary and therefore omitted.

Lemma 6.1. *Let γ be the smallest positive integer in Λ. For $i = 0, \ldots, \gamma - 1$, let λ_i be the smallest integer in Λ such that $\lambda_i \cong i \mod \gamma$. Then for each $i = 0, \ldots, \gamma - 1$, the largest integer in Λ^c congruent to i mod γ is $\lambda_i - \gamma$.*

The next lemma shows that the set of valuations of elements of $\Omega(-\infty Q)$ is related to the nongap sequence Λ.

Lemma 6.2. *An integer m is a gap at Q if and only if there exists a differential ω such that $\nu_Q(\omega) = m - 1$ and $\omega \in \Omega(-\infty Q)$. Thus $\Lambda^c = \{\nu_Q(\omega) - 1 : \omega \in \Omega(-\infty Q)\}$.*

PROOF: Let $i(mQ) = \dim \Omega(mQ)$. From the Riemann-Roch theorem,

$$l((m-1)Q) = m - g + i((m-1)Q)$$
$$l(mQ) = m + 1 - g + i(mQ)$$

so taking the difference,

$$l((m-1)Q) - l(mQ) = i((m-1)Q) - i(mQ) - 1$$

If there is a differential ω with pole order $m-1$ at Q, then $i((m-1)Q) = i(mQ)+1$, so m is a gap. Conversely, if no such differential exists, then $i((m-1)Q) = i(mQ)$ so $l(mQ) = l((m-1)Q)+1$ and m is a nongap. □

We come now to the main result.

Theorem 6.3. *Let C be a smooth curve over a perfect field k, let K and Ω be the field of functions and the space of differentials of C. Let Q be a rational point of C and let t be a uniformizing parameter at Q. There exist sets $\{z_u \in K : u \in \mathbb{Z}\}$ and $\{\zeta_v \in \Omega : u \in \mathbb{Z}\}$ such that*

$$\begin{aligned} \nu_Q(z_u) &= -u, & (12)\\ \nu_Q(\zeta_v) &= v-1, & (13)\\ \nu_Q(z_u - t^{-u}) &> -u, & (14)\\ \nu_Q(\zeta_v - t^{v-1}dt) &> v-1, & (15) \end{aligned}$$

and for $u \in \Lambda$ and $v \in \Lambda^c$,

$$\begin{aligned} z_u &\in R, & (16)\\ \zeta_v &\in \Omega(-\infty Q), & (17) \end{aligned}$$

and such that for any $u, v \in \mathbb{Z}$,

$$\operatorname{res}_Q z_u\zeta_v = \begin{cases} 1 & \textit{if } v = u \\ 0 & \textit{otherwise} \end{cases} \qquad (18)$$

Furthermore any $f \in K$ and $\omega \in \Omega$ may be uniquely expressed as series in the z_u and ζ_v.

$$\begin{aligned} f &= \sum_{u \le -\nu_Q(f)} a_u z_u, & (19)\\ \omega &= \sum_{v \ge \nu_Q(\omega)+1} t_v \zeta_v & (20)\\ & & (21) \end{aligned}$$

with $a_u, t_v \in k$.

Proof: Suppose that we have z_i satisfying (12). The series expansion (19) for f is obtained in a similar manner to the power series for f with respect to a uniformizing parameter at Q. Let $s = -\nu_Q(f)$ and let a_s be such that $\nu_Q(f - a_s z_s) > s$. Then define inductively a_u for $u < s$ by $\nu_Q(f - \sum_{i=u+1}^{s} a_i z_i - a_u z_u) > -u$. The series is a well defined element of the completion of K with respect to ν_Q and it is clearly uniquely defined and equal to f. A similar argument shows that any ω may be expressed as in (20) given $\{\zeta_v\}$ satisfying (13).

Let γ and λ_i be as in Lemma 6.1. Let $z_\gamma \in R$ have pole order γ. By multiplying by a constant we may also assume that $\nu_Q(z_\gamma - t^{-\gamma}) > -\gamma$. I claim that for each $i = 0, \ldots, \gamma-1$ there are $z_{\lambda_i} \in R$ and $\zeta_{\lambda_i - \gamma} \in \Omega(-\infty Q)$ satisfying (12) (13), (14) and (15) such that

$$\operatorname{res}_Q z_{\lambda_i}\zeta_{\lambda_j-\gamma} z^{-r} = \begin{cases} 1 & \text{if } i = j \text{ and } r = 1 \\ 0 & \text{otherwise} \end{cases} \qquad (22)$$

Suppose this is true. For any other $u \in \mathbb{Z}$ write $u = \lambda_i + k\gamma$ and define

$$z_u = z_{\lambda_i} z_\gamma^k$$

Then $\nu_Q(z_u) = -\lambda_i - k\gamma = -u$ and one easily verifies that (14) holds. Furthermore, if $u \in \Lambda$ then $k \geq 0$ so $z_u \in R$. For any $v \in \mathbb{Z}$, write $v = \lambda_j + l\gamma$ and define

$$\zeta_v = \zeta_{\lambda_j - \gamma} z_\gamma^{-l-1}$$

Then $\nu_Q(\zeta_v) = \lambda_j - \gamma - 1 + (l+1)\gamma = v - 1$ and (15) holds. Furthermore if $v \in \Lambda^c$ then $l < 0$ so $-l-1 \geq 0$ and therefore $\zeta_v \in \Omega(-\infty Q)$. Thus, assuming (22), we have constructed z_u and ζ_v for all $u, v \in \mathbb{Z}$ satisfying (12) (13), (14), (15), (16) (17) and (19), (20).

Now we have

$$\begin{aligned} \operatorname{res}_Q z_u \zeta_v &= \operatorname{res}_Q z_{\lambda_i} \zeta_{\lambda_j - \gamma} z_\gamma^{k-l} \\ &= \begin{cases} 1 & \text{if } i = j \text{ and } k = l \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

But if $i = j$ and $k = l$ then $v = u$, so this establishes (18). This completes the proof of the theorem, contingent on establishing (22).

For each $j = 0, \ldots, \gamma - 1$, there exist $\zeta_{\lambda_j - \gamma} \in \Omega(-\infty Q)$ with valuation $\lambda_j - \gamma - 1$ by Lemma 6.2, and they can be chosen to satisfy (15). Let $y_{\lambda_i} \in R$ of pole order λ_i be arbitrary. If $r \leq 0$ then $y_{\lambda_i} \zeta_{\lambda_j - \gamma} z_\gamma^{-r} \in \Omega(-\infty Q)$. This must have residue 0 at Q since it has at most one pole and the sum of the residues is 0. On the other hand, if

$$r > 1 + (\lambda_i - \lambda_j)/\gamma \tag{23}$$

then

$$\begin{aligned} \nu_Q(y_{\lambda_i} \zeta_{\lambda_j - \gamma} z_\gamma^{-r}) &= -\lambda_i + \lambda_j - \gamma - 1 + r\gamma \\ &> -1 \end{aligned}$$

and again the residue at Q is 0. Thus for each i, j there are only a finite number of conditions represented by (22). In particular, if $\lambda_i < \lambda_j$ then $r > 0$ implies (23) so for all r, $\operatorname{res}_Q y_{\lambda_i} \zeta_{\lambda_j - \gamma} z_\gamma^{-r} = 0$.

Let $0 = \kappa_0 < \kappa_1 < \cdots < \kappa_{\gamma-1}$ be a rearrangement of the λ_i in increasing order. We now construct inductively z_{κ_i} satisfying (22). The preceding paragraph shows that $z_0 = 1$ already satisfies (22) for all $\zeta_{\kappa_j - \gamma}$ and r. For $i = 1, \ldots, \gamma - 1$, we do the following. For $j = 0, \ldots, i-1$, let $M_j = 1 + \lfloor (\kappa_i - \kappa_j)/\gamma \rfloor$. For $r = 1, \ldots, M_j$, let

$$\alpha_{jr} = \operatorname{res}_Q y_{\kappa_i} \zeta_{\kappa_j - \gamma} z_\gamma^{-r}$$

Then set

$$x_i = \sum_{j=0}^{i-1} \sum_{r=1}^{M_j} \alpha_{jr} z_{\kappa_j} z_\gamma^{r-1}$$

By the induction hypothesis, for $j < i$, z_{κ_j} satisfies (22). Thus for j, r in the ranges above,

$$\operatorname{res}_Q x_i \zeta_{\kappa_j - \gamma} z_\gamma^{-r} = \alpha_{jr}$$

and for either j or r outside of that range the residue is 0. Finally, $\alpha = \operatorname{res}_Q y_{\kappa_i} \zeta_{\kappa_i - \gamma} z_\gamma^{-1}$ must be nonzero since $y_{\kappa_i} \zeta_{\kappa_i - \gamma} z_\gamma^{-1}$ has a pole of order 1 at Q. Therefore, we define $z_{\kappa_i} = \alpha^{-1}(y_{\kappa_i} - x_i)$, and this satisfies (22). □

Recall that for a vector e, ω_e in Theorem 3.3 was only uniquely defined modulo $\Omega(-\infty Q)$. With respect to the ζ_v, of the previous theorem we may now define a unique differential ω_e.

Proposition 6.4. *Let $\omega_P = -\sum_{u \in \Lambda} z_u(P)\zeta_u$. Then ω_P has poles only at P and Q and these are of order one. Furthermore* $\operatorname{res}_P \omega_P = -\operatorname{res}_Q \omega_P = 1$.

Proof: Let $g \in R$ and write $g = \sum_{v \in \Lambda} g_v z_v$. Then

$$\begin{aligned}
\operatorname{res}_Q g\omega_P &= -\operatorname{res}_Q \Big(\sum_{v \in \Lambda} g_v z_v\Big)\Big(\sum_{u \in \Lambda} z_u(P)\zeta_u\Big) \\
&= -\sum_{v \in \Lambda} \sum_{u \in \Lambda} g_v z_u(P) \operatorname{res}_Q (z_v \zeta_u) \\
&= -\sum_{v \in \Lambda} g_v z_v(P) \\
&= -g(P)
\end{aligned}$$

In particular $\operatorname{res}_Q(\omega_P) = -1$.

Now suppose that ω'_P is any differential having poles only at P and Q, that these are simple poles and that $\operatorname{res}_P \omega'_P = -\operatorname{res}_Q \omega'_P = 1$. Then $\operatorname{res}_Q g\omega'_P = -g(P)$ by Lemma 3.2. Thus for any $g \in R$, $\operatorname{res}_Q g(\omega_P - \omega'_P) = 0$. By Lemma 3.4, $\omega_P - \omega'_P$ has no poles away from Q. We conclude that ω_P, like ω'_P must have a simple pole at P and since $\nu_Q(\zeta_0) = -1$ it also has a simple pole at Q. □

Henceforth, we define for $k = 1, \ldots, n$

$$\omega_k = -\sum_{u \in \Lambda} z_u(P_k)\zeta_u \tag{24}$$

and for an error vector e,

$$\begin{aligned}
\omega_e &= \sum_k e_k \omega_k \\
&= \sum_{u \in \Lambda} s_u \zeta_u
\end{aligned} \tag{25}$$

where

$$\begin{aligned}
s_u &= -\sum_k e_k z_u(P_k) && (26)\\
&= -S_e(z_u) && (27)\\
&= \operatorname{res}_Q(z_v \omega_e) && (28)
\end{aligned}$$

In the particular case where the z_u and ζ_u are chosen as in the proof of the theorem we may write

$$\begin{aligned}\omega_e &= \sum_{i=0}^{\gamma-1}\sum_{j=0}^{\infty} S_e(z_{\lambda_i} z_\gamma^j)\zeta_{\lambda_i-\gamma} z_\gamma^{-j-1} \\ &= \sum_{i=0}^{\gamma-1}\zeta_{\lambda_i-\gamma}\sum_{j=0}^{\infty}\frac{S_e(z_{\lambda_i}z_\gamma^j)}{z_\gamma^{j+1}}\end{aligned} \tag{29}$$

There are many choices of bases $\{z_u\}$ and $\{\zeta_v\}$ satisfying the theorem. For example consider $\mathbb{P}^1$ and let $R = k[x]$. Then one may take, for any $a \in k$, $z_u = (x-a)^u$ and $\zeta_u = (x-a)^{-u-1}dx$.

Example 6.5. Consider the Klein quartic of Example 4.4. The smallest positive nongap is $\gamma = 3$ and since Λ is generated by $3, 5, 7$, we have $\lambda_0 = 0$, $\lambda_1 = 7$ and $\lambda_2 = 5$. Let $z_3 = y$, and $z_0 = 1$, $z_5 = xy$, $z_7 = x^2y$ and—for $\lambda_i - \gamma$—let $\zeta_4 = -\omega_0$, $\zeta_2 = -x\omega_0$ and $\zeta_{-3} = -(x^2y+1)\omega_0$. Let us first check that $\operatorname{res}_Q z_{\lambda_i}\zeta_{\lambda_i-3}z_3^{-1} = 1$ for $i = 0,1,2$. For $i = 1,2$ this simplifies to $\operatorname{res}_Q -x^2\omega_0$ which has residue -1 at P and 1 at Q. For $i = 0$,

$$\begin{aligned}z_0\zeta_{-3}z_3^{-1} &= -(x^2y+1)\omega_0/y \\ &= -\frac{x^2y+1}{3x^2y+1}\frac{dy}{y}\end{aligned}$$

Since y is a uniformizing parameter at O the residue at O is -1. One can check that this differential has poles only at O and Q, so the residue at Q is 1.

It remains to verify (22) for $i \neq j$. From (23) we need only check that

$$z_{\lambda_i}\zeta_{\lambda_j-3}z_3^{-r} = 0$$

for $i \neq j$ and $1 \leq r \leq (\lambda_i - \lambda_j)/\gamma$. That is, for z_5, ζ_{-3}, and $r = 1,2$, for z_7, ζ_{-3} and $r = 1,2,3$, and for z_7, ζ_2 and $r = 1$.

We find that $z_5\zeta_{-3}z_3^{-1} = y^3\omega_0$, and $z_5\zeta_{-3}z_3^{-2} = y\omega_0$ both of which are in $\Omega(-\infty Q)$ and therefore have residue 0 at Q. Similarly $z_7\zeta_{-3}z_3^{-3} = x\omega_0 \in \Omega(-\infty Q)$. Therefore $z_7\zeta_{-3}z_3^{-3}$, $z_7\zeta_{-3}z_3^{-2}$, and $z_7\zeta_{-3}z_3^{-1}$ have residue 0 at Q. Finally, $z_7\zeta_2 z_3^{-1} = x^3\omega_0 = (y^2 + x/y)\omega_0$. Since $y^2\omega_0 \in \Omega(-\infty Q)$ and $\nu_Q((x/y)\omega_0) \geq 0$, both have residue 0 at Q. Consequently, $z_7\zeta_2z_3^{-1}$ does also.

The formula for h_e in Example 4.4 is now seen to be in the form of (29).

Example 6.6. Consider again the Hermitian curve of Example 4.3. For any $u \in \mathbb{Z}$ write $u = iq + j(q+1)$ with $0 \leq i \leq q$. Let $z_u = x^iy^j$ and let $\zeta_u = -x^{q-i}y^{-1-j}dx$. It is shown in [16] that z_u and ζ_u satisfy the theorem. The expansion of h_e in Example 4.3 is now seen to be in the form (25).

This is not the type of functions constructed in the theorem. The minimal positive nongap is q and the construction allowed division by $z_q = x$ not $z_{q+1} = y$. An alternative would be as follows. For $0 \leq i < q$, we have $\lambda_i = i(q+1)$. Set $z_{\lambda_i} = y^i$. For $j \neq 0$, set $\zeta_{\lambda_j - q} = -y^{q-1-j}dx$ and for $j = 0$ set $\zeta_{-q} = -(y^{q-1}+1)dx$. I claim that these satisfy (22).

For $i = j = 0$, $\lambda_0 = 0$ and

$$\begin{aligned} z_0 \zeta_{-q} z_q^{-1} &= -((y^{q-1} + 1)/x)dx \\ &= -(x^q/y)dx \end{aligned}$$

This has poles at the origin and Q with residue -1 at the origin. So the residue is 1 at Q. For $i = j \neq 0$, $z_{\lambda_i} \zeta_{\lambda_i - q} z_q^{-1} = -(y^{q-1}/x)dx$ which differs from $-(x^q/y)dx$ by $-(y/x)dx$. The latter has positive valuation at Q. Thus $\operatorname{res}_Q z_{\lambda_i} \zeta_{\lambda_i - q} z_q^{-1} = 1$.

By (23) we must check that $\operatorname{res}_Q z_{\lambda_i} \zeta_{\lambda_j - q} z_q^{-r} = 0$ for $i > j$ and $r = 1, \ldots, i - j + 1$. For $j \neq 0$,

$$\begin{aligned} z_{\lambda_i} \zeta_{\lambda_j - q} z_q^{-r} &= -y^{q-1+i-j} x^{-r} dx \\ &= -\frac{x^{q+1} - y}{y^q} y^{q-1+i-j} x^{-r} dx \\ &= -x^{q+1-r} y^{i-j-1} dx + y^{i-j} x^{-r} dx \end{aligned}$$

Since $i > j$ and $r \leq q$, the first term is in $\Omega(-\infty Q)$ and has residue 0. The second term has valuation

$$\begin{aligned} -(i-j)(q+1) + rq + q^2 - q - 2 &\geq -(q-2)(q+1) + rq + q^2 - q - 2 \\ &= rq \end{aligned}$$

and therefore has positive valuation and residue 0 at Q. Finally for $j = 0$ and $i > j$,

$$\begin{aligned} z_{\lambda_i} \zeta_{-q} z_q^{-r} &= -y^i (y^{q-1} + 1) x^{-r} dx \\ &= -y^{i-1} x^{q+1-r} dx \end{aligned}$$

which is in $\Omega(-\infty Q)$.

Dividing out by dx we can write h_e in the form of (29).

$$h_e = \left(\sum_{j=0}^{q-1} (y^{q-1-j} + \delta(j)) \right) \sum_{i=0}^{\infty} \frac{S_e(x^i y^j)}{x^{i+1}}$$

where $\delta(j) = 1$ for $j = 1$ and $\delta(j) = 0$ otherwise.

Definition 6.7. Let $f \in K$ and write $f = \sum_{u \in \mathbb{Z}} a_u z_u$. We call $\sum_{u \in \Lambda} a_u z_u$ the *R-part of f*. We say that f has leading coefficient $a_{o(f)}$.

The term R-part is somewhat of a misnomer since it depends on the choice of $\{z_u\}$ not just on R, but this should not cause any confusion.

Proposition 6.8. *Let ω_e be as in* (25)*. For $f \in R$, let $t_v \in k$ be such that*

$$f\omega_e = \sum_{v \in \mathbb{Z}} t_v \zeta_v \tag{30}$$

Then $t_v = -S_e(\tilde{f})$ where $\tilde{f}$ is the R-part of $f z_v$.

PROOF: Write $fz_v = \sum_{u\in\mathbb{Z}} b_u z_u$. Then $\tilde{f} = \sum_{u\in\Lambda} b_u z_u$ and $fz_v = \tilde{f} + \sum_{u\in\Lambda^c} b_u z_u$. From (18), $t_v = \mathrm{res}_Q\, z_v(f\omega_e)$. But,

$$\mathrm{res}_Q(fz_v)\omega_e = \mathrm{res}_Q\, \tilde{f}\omega_e + \mathrm{res}_Q \sum_{u\in\Lambda^c} b_u z_u \omega_e$$

Since the non-zero terms in ω_e are indexed by nongaps, the second term is zero. Thus,

$$\begin{aligned} t_v &= \mathrm{res}_Q\, \tilde{f}\omega_e \\ &= -S_e(\tilde{f}) \end{aligned}$$

□

We will often write the series expansion in (19) and (20) as sums over $\mathbb{Z}$ or even without limits (implicitly summing over $\mathbb{Z}$) with the understanding that for either $u > -\nu_Q(f)$ (in the case of $f \in K$) or $u \leq \nu_Q(\omega)$ (in the case of $\omega \in \Omega$) the coefficients are zero.

7 Approximate Solutions of the Key Equation

We now review terminology and basic results used in defining the decoding algorithm. The algorithm is based on Sakata's algorithm [18]. The adaptation to curves appears in [7]. The discussion here is based on the approach in [14], see also [6].

For $f \in R \setminus I_e$, let

$$\begin{aligned} \mathrm{span}\, f &= \min\{c : S_e(fg) \neq 0 \text{ for some } g \in L_c\} \\ \mathrm{fail}\, f &= o(f) + \mathrm{span}\, f \end{aligned}$$

For $f \in I_e$ we take $\mathrm{span}\, f$ and $\mathrm{fail}\, f$ to be infinity.

Proposition 7.1. *Let $f \in R$. Then $\mathrm{span}\, f > r$ if and only if there exists a $\phi \in \Omega(-\infty Q)$ such that f, ϕ satisfy the rth key equation.*

PROOF: Suppose first that f, ϕ satisfy the rth key equation. Then $\nu_Q(f\omega_e - \phi) \geq r$, so for any $g \in L(rQ)$, $\nu_Q(fg\omega_e - g\phi) \geq 0$ and therefore $\mathrm{res}_Q(fg\omega_e - g\phi) = 0$. Since $g\phi \in \Omega(-\infty Q)$, $\mathrm{res}_Q\, g\phi = 0$. Thus we have $S_e(fg) = \mathrm{res}_Q\, fg\omega_e = 0$ and $\mathrm{span}\, f > r$.

Conversely, suppose that $\mathrm{span}\, f > r$. Let $\{z_u\}$ and $\{\zeta_u\}$ satisfy Theorem 6.3 and write $f\omega_e = \sum t_v \zeta_v$. For each $u \in \Lambda$ and $u \leq r$, $t_u = \mathrm{res}_Q(z_u f\omega_e) = -S_e(z_u f) = 0$. Let $\phi = \sum_{v\leq r} t_v \zeta_v$. Then $\phi \in \Omega(-\infty Q)$ because the only nonzero terms occur when $v \in \Lambda^c$. Now $\nu_Q(f\omega_e - \phi) \geq r$, so f, ϕ satisfy the rth key equation. □

Although we proved the proposition using particular functions and differentials satisfying Theorem 6.3, the result is independent of that choice.

With respect to the error vector e we define

$$\begin{aligned} \Sigma &= \{s \in \Lambda : \exists f \in I_e \text{ with } o(f) = -s\} \\ \Delta &= \{c \in \Lambda : \exists g \in R \setminus I_e \text{ with } \mathrm{span}\, g = c\} \end{aligned}$$

Since I_e is an ideal of R, Σ is closed under addition by elements of Λ. Furthermore, Δ is closed under subtraction by elements of Λ, provided that the difference is a nongap. An important result is that Σ and Δ partition Λ.

For any subset A of Λ we define

$$\min A = \{a \in A : \forall \lambda \in \Lambda \setminus \{0\}, a - \lambda \notin A\}$$
$$\max A = \{a \in A : \forall \lambda \in \Lambda \setminus \{0\}, a + \lambda \notin A\}$$

Then we set

$$\sigma = \min \Sigma$$
$$\delta = \min \Delta$$

A set of polynomials $\{f_s \in I_e : s \in \sigma, \text{ and } o(f_s) = s\}$ generates the ideal I_e. It will be called a Gröbner basis for I_e. Let $s_{\max}$ be the largest integer in σ and let $c_{\max}$ be the largest integer in δ.

Remark 7.2. If $f \in R$ satisfies $\operatorname{fail} f > o(f) + c_{\max}$ then $\operatorname{span} f > c_{\max}$ and this clearly implies that f must be in I_e, that is, f is a locator.

We now show that if f is a locator and f, ϕ satisfy the $(2g-1)$th approximation to the key equation then f, ϕ satisfy the key equation. Since f is a locator, $f\omega_e$ has no poles away from Q. We also have $\nu_Q(f\omega_e - \phi) \geq 2g - 1$, and therefore $\deg(f\omega_e - \phi) \geq 2g-1$. Any non-zero differential has degree exactly $2g-2$, so this implies that $f\omega_e - \phi = 0$. Thus f, ϕ satisfy the key equation.

The idea of Sakata's algorithm is to compute successive approximations of Σ and Δ and along with them functions f with increasing $\operatorname{fail} f$. For each $m \in \mathbb{Z}$ let

$$\Sigma_m = \{s \in \Lambda : \exists f \in R \text{ with } \nu_Q(f) = -s \text{ and } \operatorname{fail} f > m\}$$
$$\Delta_m = \{c \in \Lambda : \exists g \in R \text{ with } \operatorname{span} g = c \text{ and } \operatorname{fail} g \leq m\}$$

Note that $\Sigma_m = \Lambda$ for $m < 0$ and $\Sigma_m = \Sigma_{m-1}$ if m is a gap. As is the case with Σ and Δ, Σ_m and Δ_m partition Λ.

Proposition 7.3. $\Sigma_m = \Sigma$ *for* $m > 2c_{\max}$

Proof: Let $c \in \Delta$ and let $g \in R \setminus I_e$ have order c and span d. Then $c \in \Delta_{c+d}$. Since each of c and d is less than $c_{\max}$, $c \in \Delta_{2c_{\max}}$. The choice of $c \in \Delta$ was arbitrary, so $\Delta_{2c_{\max}} = \Delta$ and $\Sigma_{2c_{\max}} = \Sigma$. □

Definition 7.4. Let $f \in R$ and let $f\omega_e = \sum t_v \zeta_v$. For any $p < \operatorname{span} f$ we will call

$$\sum_{v \leq p} t_v \zeta_v$$

the *pth approximation to* $f\omega_e$. We call t_c where $c = \operatorname{span} f$ the *discrepancy* of $f\omega_e$.

Let $\phi = \sum_{v \in \Lambda^c} b_v \zeta_v$. The *pth truncation* of ϕ is

$$\overline{\phi} = \sum_{\substack{v \in \Lambda^c \\ v \leq p}} b_v \zeta_v \tag{31}$$

The following proposition is used in the updating procedure of KEY EQUATION.

Proposition 7.5. *Let $f \in R$ and let $c = \operatorname{span} f$. Let ϕ be the $(c-1)$th approximation of $f\omega_e$ and let α be the discrepancy of $f\omega_e$. For $v \in \Lambda$, let $\overline{\phi z_v}$ be the $(c-v-1)$th truncation of ϕz_v. If $c-v$ is a gap, then* $\operatorname{span} f z_v > c - v$ *and the $(c-v)$th approximation of $f z_v \omega_e$ is $\overline{\phi z_v} + \alpha\zeta_{p-v}$. If $c-v$ is a nongap then* $\operatorname{span} f z_v = c - v$ *and the $(c-v-1)$th approximation of $f z_v \omega_e$ is $\overline{\phi z_v}$ while the discrepancy is α.*

PROOF: Since $\zeta_c = t^{c-1}dt$ modulo terms with higher valuation, we have $\nu_Q(f\omega_e - \phi - \alpha t^{c-1}dt) \geq c$. Multiplying by z_v,

$$\nu_Q(f z_v \omega_e - \phi z_v - \alpha t^{c-v-1}dt) \geq c - v$$

Since $\phi \in \Omega(-\infty Q)$ and v is a nongap, $\phi z_v \in \Omega(-\infty Q)$ so we can write $\phi z_v = \sum_{u \in \Lambda^c} b_u \zeta_u$. Although the terms in the expansion of ϕ all have valuation at most $c-1$, some of the b_u may be nonzero for $u \geq c - v$ since it is not necessarily true that $z_v \zeta_u = \zeta_{u-v}$. Let

$$\overline{\phi z_v} = \sum_{\substack{u \in \Lambda^c \\ u \leq c-v}} b_u \zeta_u$$

Then

$$\nu_Q(f z_v \omega_e - \overline{\phi z_v} - \alpha t^{c-v-1}dt) \geq c - v$$

If $c-v$ is a nongap then ζ_{c-v} does not appear in the expansion of $\overline{\phi z_v}$, so $\operatorname{span} f z_v = c - v$, $\overline{\phi z_v}$ is the $(c-v-1)$th approximation of $f\omega_e$ and α is the discrepancy. If $c-v$ is a gap, then $\operatorname{span} f z_v > c - v$ and the $(c-v)$th approximation of $f z_v \omega_e$ is $\overline{\phi z_v} + \alpha\zeta_{c-v}$. □

8 The Decoding Algorithm

In this section, I present the algorithm KEY EQUATION which amends the decoding algorithm of [14] to compute error evaluators along with the iterative computation of error locators.

Let the check code be defined by $m^\star Q$. KEY EQUATION has iterations from $m = 0$ to $m = M$, with M generally larger than $m^\star$. Majority voting is used to compute the unknown syndromes. Since majority voting is amply treated elsewhere [4, 6, 9, 14, 19] the details are omitted. The choice of the last iteration M depends on several factors and will be discussed at the end of this section.

Upon completion of the mth iteration, the algorithm stores sets of nongaps σ_m and δ_m. For each $s \in \sigma_m$ it stores $F_m(s) \in R$ and $\phi_m(s) \in \Omega(-\infty Q)$, considered valid at the current iteration. For each $c \in \delta_m$, it stores $G_m(c) \in R$ and $\psi_m(c) \in \Omega(-\infty Q)$, which failed at a previous iteration. Upon completion of the algorithm, $\sigma_M = \min \Sigma$, $F_M(\sigma)$ is a Gröbner basis for I_e, and $F_M(s)$, $\phi_m(s)$ solve the key equation. At any given error location, P_k, there is at least one s such that $F_M(s)$ has multiplicity one at P_k, so e_k can be found from the formula in Proposition 3.6.

Each iteration has 4 steps. Step 1 tests the polynomials from the previous iteration, $F_{m-1}(s)$ for $s \in \sigma_{m-1}$, at the mth syndrome. If $m - s$ is a nongap and $F_{m-1}(s), \phi_m(s)$ is no longer valid, $m - s$ is stored temporarily in δ'. Majority voting for the mth syndrome also occurs if $m > m^\star$. Step 2 computes the new set δ_m which contains the maximal elements of $\delta_{m-1} \cup \delta'$. Then, σ_m is computed from δ_m. Step 3 assigns the new $G_m(c)$ and $\psi_m(c)$ based on whether c is due to a new failure ($c \in \delta'$) or c remains from the previous iteration. Finally step 4 computes the new valid data $F_m(t), \phi_m(t)$ for $t \in \sigma_m$.

The Algorithm: KEY EQUATION

Assumptions .

- C is a smooth curve over a perfect field k, Q is a rational point of C, and R is the ring of functions of $C \setminus Q$,
- Λ is the set of nongaps at Q, $\Lambda^c = \mathbb{Z} \setminus \Lambda$.
- $\{z_u\}_{u \in \mathbb{Z}}$ and $\{\zeta_v\}_{v \in \mathbb{Z}}$ as in Theorem 6.3.
- The expansions of the products $z_w z_v$ and $z_w \zeta_v$ with respect to the respective bases $\{z_u\}$ and $\{\zeta_u\}$ are computable.
- $m^\star \in \Lambda$ defines the check code: $s_u = S_e(z_u)$ are known for $u \in \Lambda$ and $u \le m^\star$.
- $M \in \Lambda$ defines the last iteration of the algorithm.
- $P_1, P_2, \ldots, P_n$ are distinct rational points of $C \setminus Q$.
- $e \in k^n$. D_e is the divisor of points P_k such that $e_k \ne 0$, and I_e is the ideal of functions in R vanishing on D_e.

Data Structures Compute for each m:

$$\begin{array}{lll} \sigma_m \subset \Lambda & F_m : \sigma_m \longrightarrow R & \phi_m : \sigma_m \longrightarrow \Omega(-\infty Q) \\ \delta_m \subset \Lambda & G_m : \delta_m \longrightarrow R & \psi_m : \delta_m \longrightarrow \Omega(-\infty Q) \end{array}$$

Temporary Structures Used within an iteration.

$$\alpha : \sigma_m \longrightarrow k \qquad \delta' \subset \Lambda$$

Initialization For $m = -1$

$$\begin{array}{lll} \sigma_{-1} = \{0\} & F_{-1}(0) = 1 & \phi_{-1}(0) = 0 \\ \delta_{-1} = \emptyset & & \end{array}$$

Algorithm For $m = 0$ to M,

1. For each $s \in \sigma_{m-1}$:
   Compute $\tilde{f} = R$-part of $F_{m-1}(s) z_{m-s}$.
   If $m \le m^\star$ or $m \in \Lambda^c$,
      $\alpha(s) = S_e(\tilde{f})$.
   If $m > m^\star$ and $m \in \Lambda$:
      Compute $S_e(\tilde{f} - z_m)$.
      Compute $s_m = S_e(z_m)$ by majority voting.
      $\alpha(s) = S_e(\tilde{f} - z_m) + s_m$.

2. Compute σ_m and δ_m:

$$\begin{aligned}
\delta' &= \{m - s : s \in \sigma_{m-1}, m - s \in \Lambda \text{ and } \alpha(s) \neq 0\} \\
\delta_m &= \max(\delta_{m-1} \cup \delta') \\
\sigma_m &= \min\{s \in \Lambda : \forall c \in \delta_m, c - s \notin \Lambda\}
\end{aligned}$$

3. For each $c \in \delta_m$, set

$$G_m(c) = \begin{cases} G_{m-1}(c) & \text{if } c \in \delta_{m-1} \\ \alpha(m-c)^{-1} F_{m-1}(m-c) & \text{otherwise} \end{cases}$$

$$\psi_m(c) = \begin{cases} \psi_{m-1}(c) & \text{if } c \in \delta_{m-1} \\ \alpha(m-c)^{-1} \phi_{m-1}(m-c) & \text{otherwise} \end{cases}$$

4. For each $t \in \sigma_m$:
   Find $s \in \sigma_{m-1}$ and $a \in \Lambda$ such that $s + a = t$.
   Let $f = F_{m-1}(s) z_a$ and let ϕ be the $(m-t)$th truncation of $\phi_{m-1}(s) z_a$.
   If $m - t$ is a gap, set

$$\begin{aligned}
F_m(t) &= f \\
\phi_m(t) &= \phi + \alpha(s)\, \zeta_{m-t}
\end{aligned}$$

   If $m - t$ is a nongap and $\alpha(s) = 0$ then also $t = s$ and $a = 0$; set

$$\begin{aligned}
F_m(t) &= f \\
\phi_m(t) &= \phi
\end{aligned}$$

   If $m - t$ is a nongap and $\alpha(s) \neq 0$, find $c \in \delta_{m-1}$ and $b \in \Lambda$ such that $c - b = m - t$. Let $g = G_{m-1}(c) z_b$ and let ψ be the $(m-s)$th truncation of $\psi_{m-1}(c) z_b$. Set

$$\begin{aligned}
F_m(t) &= f - \alpha(s) g \\
\phi_m(t) &= \phi - \alpha(s) \psi
\end{aligned}$$

Theorem 8.1. *The algorithm above computes a Gröbner basis for the ideal I_e and the products of the basis elements with ω_e. If we let $s_{\max}$ be the largest integer in σ, and $c_{\max}$ the largest integer in δ and let $M = \max\{2c_{\max}, s_{\max} + c_{\max}, s_{\max} + 2g - 1\}$, then the computation is complete after M iterations. Moreover, for each m:*

1. *$\sigma_m = \min \Sigma_m$, and $\delta_m = \max(\Delta_m)$*

2. *For each $s \in \sigma_m$, $o(F_m(s)) = s$ and f has leading coefficient 1; $\operatorname{fail} F_m(s) > m$ and $\phi_m(s)$ is the $(m-s)$th approximation to $F_m(s)\omega_e$.*

3. *For each $c \in \delta_m$, $\operatorname{span} G_m(c) = c$, and $\operatorname{fail} G_m(c) \leq m$; $\psi_m(c)$ is the $(c-1)$th approximation of $G_m(c)\omega_e$ with discrepancy 1.*

PROOF: Suppose that the statements 1), 2), 3) about the data of the mth iteration are true. If $m \geq 2c_{\max}$ then by Proposition 7.3, $\Sigma_m = \Sigma$ so $\sigma_m = \sigma$. If m is also at least $s_{\max} + c_{\max}$ then each of the functions $F_m(s)$ for $s \in \sigma_m$ has fail larger than $s + c_{\max}$ by 2) of the theorem, so by Remark 7.2 each $F_m(s)$ is in a locator. Finally, if m is also larger than $s_{\max} + 2g - 1$ then each pair $F_m(s), \phi_m(s)$ solves the key equation as discussed in Remark 7.2. Thus the algorithm produces a Gröbner basis for I_e and the corresponding products with ω_e after $M = \max\{2c_{\max}, s_{\max} + c_{\max}, s_{\max} + 2g - 1\}$ iterations.

We now prove the statements about the data after the mth iteration by induction. the case $m = -1$ is trivial. We assume the statements true for $m - 1$. We will show first that item 1) is easily deduced from items 2) and 3). The existence of $F_m(s)$ for each $s \in \sigma_m$ with fail larger than m shows that $\sigma_m \subset \Sigma_m$. Similarly 3) implies that $\delta_m \subset \Delta_m$. It is clear that the sets $A = \{s \in \Lambda : \forall c \in \delta_m, c - s \notin \Lambda\}$ and $B = \{s \in \Lambda : \exists c \in \delta_m, c - s \in \Lambda\}$ partition Λ. In the algorithm, σ_m is defined to be $\min A$. Therefore item (2) implies $A \subset \Sigma_m$. Similarly $\delta_m = \max B$ so $B \subset \Delta_m$. Since A and B partition Λ we must have $A = \Sigma_m$, $B = \Delta_m$. This gives 1).

We now prove 3). In step 3 of the algorithm we either assign $G_m(c) = G_{m-1}(c)$ and the induction hypothesis says that 3) holds, or $c \in \delta'$ and $c = m - s$ for some $s \in \sigma_{m-1}$. In this case $m - s$ is a nongap and $\alpha(s)$ as computed in step 1 is nonzero. Consequently, $\operatorname{span} F_{m-1}(s) = m - s$ and $\alpha(s)^{-1}\phi_{m-1}(s)$ is the best approximation to $F_{m-1}(s)\omega_e$. Therefore, the assignment of $G_m(m - s)$ and $\psi_{m-1}(c)$ satisfies 3).

We now prove 2). By Proposition 6.8, $\alpha(s)$ as computed in step 1 of the algorithm is the coefficient of ζ_{m-s} in the expansion of $F_{m-1}(s)\omega_e$. In step 4, if $m - t$ is a gap then Proposition 7.5 shows that $\phi_m(s)$ is the $(m-s)$th approximation of $F_m(s)$ and $\operatorname{fail} F_m(s) > m$. If $m - t$ is a nongap and $\alpha(s) = 0$, then in fact $\operatorname{span} F_m(t) > m - s$ so $s \in \sigma_m$ and t must be equal to s. No updating is necessary. If $m - t$ is a nongap and $\alpha(s) \neq 0$ then there exist $c \in \delta_{m-1}$ and $b \in \Lambda$ such that $m - t = c - b$. This was proved in [14]. Proposition 7.5 shows that ϕ and ψ are the $(m - s - 1)$th approximations of f and g respectively and both f and g have span $m - s$. The linear combination is such that the discrepancies cancel. So again, $\phi_m(s)$ is the $(m - s)$th approximation of $F_m(s)$ and $\operatorname{fail} F_m(s) > m$. □

The following result is readily established from Remark 7.2.

Corollary 8.2. *The algorithm computes the error locator of lowest pole order after $M = s_{\min} + \max\{c_{\max}, 2g - 1\}$ iterations where $s_{\min}$ is the smallest integer in σ.*

Let d be the minimum distance of the code $C_\Omega(D, m^\star Q)$ and let $\tau = \lfloor (d-1)/2 \rfloor$. For any vector e of weight at most τ we must have $c_{\max} \leq \tau + 2g - 1$, $s_{\min} \leq \tau + g$ and $s_{\max} \leq \tau + 2g$. (In [14], Prop. 6.2 should say $\sigma \subset \mathbb{Z}_\tau^{\tau+2g}$.) These upper bounds for $c_{\max}$ and $s_{\max}$ may be plugged into the formula of either the Theorem or the Corollary to choose the value of the last iteration M depending on whether one wants to compute the entire set of locators and evaluators or just the minimal degree pair.

There is an alternative method for computing M that is more appropriate given the capabilities of the algorithm. Suppose that $m^\star$ is such that majority voting produces a correct answer for all $m > m^\star$. Then the algorithm can proceed indefinitely and will eventually produce the error locators and evaluators.

Let $C \in \Delta$. We now show how to choose M, the last iteration, and $m^\star$, which determines the code used, so that all error vectors having $c_{\max} \leq C$ can be corrected. From the arithmetic of Λ one can readily compute an upper bound on $s_{\max}$ and $s_{\min}$. Thus the value of M can be found from the Theorem (or Corollary). It remains to choose $m^\star$ so that majority voting is guaranteed to be correct for all $m > m^\star$. This also depends just on the arithmetic of Λ and is readily computed. This topic is pursued in greater depth in [15], but we give a brief example here.

Example 8.3. Consider again the Hermitian code over $\mathbb{F}_{q^2}$. Let $\tau < q$. The smallest code having minimum distance $2\tau + 1$ has $m^\star = (2\tau - 1)(q + 1)$. Let $C = (\tau - 1)(q + 1)$. One can show that majority voting beyond $m^\star$ will be successful provided that $c_{\max} \leq C$. Thus an error vector such that Δ consists of all nongaps less than or equal to C can be corrected. The number of nongaps less than or equal to C is $\binom{\tau+1}{2}$, so it is possible to correct $\binom{\tau+1}{2}$ errors. Experiments show that the vast majority of error vectors of that weight do consist of all nongaps less than or equal to C, so the code $C_\Omega(D, m^\star Q)$ performs very much like a $\binom{\tau+1}{2}$ error correcting code although its minimum distance is $2\tau + 1$. Since τ was chosen very small, $C, s_{\max} < 2g - 1$. so the value of M in the Theorem is $s_{\max} + 2g - 1$ and in the Corollary, $s_{\min} + 2g - 1$.

Acknowledgement

I would like to thank Ralf Kötter for many helpful conversations and clever insights.

References

[1] H. Chabanne, G. Norton, The n-dimensional key equation and a decoding application, IEEE Trans. Inform. Theory, 40 no. 1 (1994), 200-203.

[2] D. Ehrhard, Decoding algebraic-geometric codes by solving a key equation, in: Proc. AGCT-3, Luminy 1991, Lect. Notes in Mathematics, vol. 1518, Springer, Berlin (1992) pp. 18-25.

[3] D. Ehrhard, Achieving the designed error capacity in decoding algebraic-geometric codes, IEEE Trans. Inform. Theory 39 no. 3 (1993), 743-751.

[4] G.L. Feng, T.R.N. Rao, Decoding algebraic-geometric codes up to the designed minimum distance," IEEE Trans. Inform. Theory 39 no. 1 (1993), 37-45.

[5] J. P. Hansen, H. E. Jensen, R Kötter, Determination of error values for algebraic geometry codes and the Forney formula, IEEE Trans. Inform. Theory 44 no. 5 (1998), 1881-1886.

[6] T. Høholdt, R. Pellikaan, J.H. van Lint: Algebraic geometry codes, in: W.C.Huffmann, V. Pless (Eds.) Handbook of Coding Theory, Elsevier, 1998, pp. 871-962.

[7] J. Justesen, K. Larsen, H. E. Jensen and T. Høholdt, Fast decoding of codes from algebraic plane curves, IEEE Trans. Inform. Theory 38 no. 1 (1992), 111-119.

[8] R. Kötter , A formula for the determination of error values for Hermitian codes, in: Proc. IEEE 1997 International Symposium on Information Theory, p. 382.

[9] R. Kötter, A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes, IEEE Trans. Inform. Theory 44 no. 4 (1998), 1353-1368.

[10] R. Kötter, On the determination of error values for codes from a class of maximal curves, in: Proc. 35th Allerton Conf. on Communication, Control and Computing, Univ. Illinois, 1997, pp. 44-53.

[11] D. Leonard, A generalized Forney formula for algebraic-geometric codes, IEEE Trans. Inform. Theory 42 no. 4 (1996), 1263-1268.

[12] D. Leonard, Efficient Forney functions for decoding AG codes, IEEE Trans. Inform. Theory 45 no. 1 (1999), 260-265.

[13] F, J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, New York, 1988.

[14] M. E. O'Sullivan, Decoding of codes defined by a single point on a curve, IEEE Trans. Inform. Theory 41 no. 6 (1995) 1709-1719.

[15] M. E. O'Sullivan, Decoding of Hermitian codes beyond the minimum distance bound, manuscript.

[16] M. E. O'Sullivan, Decoding of Hermitian codes: the key equation and efficient error evaluation, IEEE Trans. Inform. Theory 46 no. 2 (2000) 512-523..

[17] S. C. Porter, B.-Z. Shen, R. Pellikaan, Decoding geometric Goppa codes using an extra place, IEEE Trans. Inform. Theory 38 no. 6, (1992), 1663-1676.

[18] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, Informat. Comput. 84 (Feb. 1990), 207-239.

[19] S. Sakata, H.E. Jensen, T. Høholdt, Generalized Berlekamp-Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound, IEEE Trans. Inform. Theory 41no. 6 (1995), 1762-1768.

[20] B.-Z. Shen, On encoding and decoding of the codes from Hermitian curves, in: Cryptography and Coding III, IMA Conf. Proc., Ser. 45, Oxford Univ. Press, Oxford, UK, 1993, pp. 337-356.

[21] B.-Z. Shen, K. K. Tzeng, Decoding geometric Goppa codes up to the designed minimum distance by solving a key equation in a ring, IEEE Trans. Inform. Theory 41 no. 6 (1995), 1694-1702.

[22] H. Stichtenoth, Algebraic Function Fields and Codes, Springer Verlag Universitext, Berlin, 1993.