On Koetter's Algorithm and the Computation of Error Values

Michael E. O'Sullivan
Mathematics Department
San Diego State University
San Diego, CA 92182
mosulliv@math.sdsu.edu

June 28, 2002

Key Words: Algebraic geometry codes, key equation, error evaluation.

Abstract

In this article, we show that Koetter's algorithm for decoding one-point codes can compute error evaluator polynomials as well. We also show that the error evaluators do not need to be computed. The updating functions used in Koetter's algorithm can be used to compute error values instead.

1 Introduction

An important step in the development of an efficient decoding algorithm for algebraic geometry codes was Sakata's generalization of the Berlekamp-Massey algorithm to polynomial rings [16]. There are subtle differences in the manner in which Sakata's algorithm has been applied, and I would like to begin by looking at these differences.

Consider the case of one-point codes. We choose a rational point Q on a smooth and absolutely irreducible curve $\mathcal{C}$ over a finite field k. We let R be the ring of functions on $\mathcal{C}$ with poles only at Q. The major step in decoding is to compute an error locator function, $f \in R$ which vanishes at all the positions where the error vector is nonzero. More precisely, the algorithms usually find a generating set for the ideal I of functions vanishing at the error locations. Since R is a quotient ring of a polynomial ring, Sakata's algorithm can be used to determine I by finding a generating set for the pre-image of I in the polynomial ring. This is the approach used in the articles [6, 17].

A somewhat different approach is to generalize Sakata's algorithm to the ring R itself. In fact, Sakata's work can be adapted in a straightforward manner to any ordered domain, of which our ring R and polynomial rings are both examples. This approach is used in [5, 12, 14].

A third approach is used by Ralf Koetter [8]. Let γ be the smallest positive pole order of functions in R and let $x \in R$ have pole order γ. Koetter's algorithm treats the ring R as a free module over the polynomial ring $k[x]$. The error locator ideal I is also a free module over $k[x]$ and Koetter's algorithm finds a basis for I.

The advantage of Koetter's approach is that the decoder is more regular in structure. The updating of the polynomials involves multiplication by x only, and is therefore simple to implement using linear shift registers. The second approach above has the advantage that the key equation for Reed-Solomon codes can be generalized in a natural way to one-point codes, and Sakata's algorithm can be amended to compute the error evaluator polynomials. The aim of this article is to show that Koetter's algorithm may also be used to compute error evaluator polynomials. We show in addition that the error evaluator polynomials are unnecessary. One can use the update polynomials and the derivatives of the locators to compute error values.

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. Let $\mathcal{C}$ be the smooth curve over k defined by K and let g be the genus. We assume that k is algebraically closed in K, which is equivalent to $\mathcal{C}$ being absolutely irreducible. Let Q be a rational point of $\mathcal{C}$ and let ν_Q be the associated valuation of K. Let $L(mQ)$ be the space of functions on $\mathcal{C}$ having poles only at Q and of order at most m there. By the Riemann-Roch theorem, 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*. Let Λ be the set of nongaps and let Λ^c be its complement in $\mathbb{Z}$. The union of the $L(mQ)$ is a ring,

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

For functions in $f \in R$, we define $o(f) = -\nu_Q(f)$ to be the pole order of f at Q. Formally, we set $o(0) = -\infty$.

We have parallel constructions for differentials. Let Ω be the space of differentials of K over k. Let $\Omega(mQ)$ be the space of differentials which have valuation *at least* m at Q and which have nonnegative valuation elsewhere.

Let

$$\Omega(-\infty Q) = \bigcup_{m=0}^{\infty} \Omega(-mQ)$$

It is evident that $\Omega(-\infty Q)$ is a module over R. It is isomorphic to R when $(2g-2)Q$ is a canonical divisor.

Take $P_1, P_2, \ldots, P_n$ to be distinct rational points on $\mathcal{C}$, each different from Q, and let $D = P_1 + P_2 + \cdots + P_n$.

We define the evaluation map ev as follows.

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

We consider the family of codes $C_L(D, mQ) = ev(L(mQ))$, for $m \in \Lambda$, used as decoding codes. The dual codes, $C_\Omega(D, mQ)$, are used for encoding, which will not be discussed.

Let $\mathbf{e}$ be a vector in k^n indexed by the P_k. We will use $\mathrm{wt}\,\mathbf{e}$ for the number of nonzero coordinates of $\mathbf{e}$. The syndrome map associated to $\mathbf{e}$ is

$$S_{\mathbf{e}} : R \longrightarrow k \tag{1}$$

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

3 A Useful Basis and Its Dual

Let γ be the smallest positive integer in Λ and let x have pole order γ. We will show in this section that R is a free module of rank γ over $k[x]$. We will show that there are bases for R and for $\Omega(-\infty Q)$ over $k[x]$ that are dual with respect to the operation of taking the residue at the point Q. In later sections we will formulate Koetter's algorithm using these bases.

For $i = 0, \ldots, \gamma - 1$, let λ_i be the smallest integer in Λ such that $\lambda_i \equiv i \mod \gamma$. It is clear that 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. The following theorem and proposition establish the existence of the bases for R and $\Omega(-\infty Q)$ and several useful properties. The lemma and theorem—in slightly different form—are proved in [13, §6].

Lemma 3.1. *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 $\Lambda^c = \{\nu_Q(\omega)+1 : \omega \in \Omega(-\infty Q)\}$.*

Theorem 3.2. *Let $\mathcal{C}$ be a smooth absolutely irreducible curve over a perfect field k, let K and Ω be the field of functions and the space of differentials of $\mathcal{C}$. Let Q be a rational point of $\mathcal{C}$ and let t be a uniformizing parameter at Q. Let Λ be the set of nongaps at Q. Let γ be the smallest positive nongap and let $x \in R$ have pole order γ. For each $i = 0, \ldots, \gamma - 1$ let λ_i be the smallest nongap congruent to i mod γ. There exist sets $\{z_{\lambda_i} \in R : i = 0, \ldots, \gamma - 1\}$ and $\{\zeta_{\lambda_i - \gamma} \in \Omega(-\infty Q) : i = 0, \ldots, \gamma - 1\}$ such that*

$$\nu_Q(z_{\lambda_i}) = -\lambda_i \tag{3}$$

$$\nu_Q(\zeta_{\lambda_i-\gamma}) = \lambda_i - \gamma - 1, \tag{4}$$

$$\nu_Q(z_{\lambda_i} - t^{-\lambda_i}) > -\lambda_i, \tag{5}$$

$$\nu_Q(\zeta_{\lambda_i-\gamma} - t^{\lambda_i-\gamma-1}dt) > \lambda_i - \gamma - 1, \tag{6}$$

and such that

$$\operatorname{res}_Q z_{\lambda_i}\zeta_{\lambda_j-\gamma}x^{-r} = \begin{cases} 1 & \textit{if } i=j \textit{ and } r=1 \\ 0 & \textit{otherwise} \end{cases} \tag{7}$$

Proposition 3.3. *With the notation of the theorem, $\{z_{\lambda_i}\}_{i=0}^{\gamma-1}$ is a basis for K over $k(x)$ and also a basis for R over $k[x]$ (so R is a free module). Similarly $\{\zeta_{\lambda_i-\gamma}\}_{i=0}^{\gamma-1}$ is a basis for Ω over $k(x)$ and also a basis for $\Omega(-\infty Q)$ over $k[x]$.*

Proof: Since x has a pole of order γ at Q and no other poles, the dimension $[K : k(x)] = \gamma$. We will show that the z_{λ_i} are linearly independent over $k(x)$, so they form a basis for K over $k(x)$. For any $r(x) \in k(x)$, and any $i = 0, \ldots, \gamma-1$, $o(r(x)z_{\lambda_i}) \equiv i \mod \gamma$. Therefore in a sum, $\sum_i r_i(x)z_{\lambda_i}$, each term has a different pole order and so the pole order of the sum is the maximum of the pole orders of the terms. Then the sum can be zero only if each term is zero.

For any $u \in \mathbb{Z}$, let i be the least nonnegative residue of u mod γ and let r be the unique integer such that $u = \lambda_i + kr$. Let $z_u = z_{\lambda_i}x^r$, so $\nu_Q(z_u) = -u$. Then $u \in \Lambda$ if and only if $r \geq 0$ and this is true if and only if $z_u \in R$. For any $f \in R$, let $o(f) = u$ and choose i and $r \geq 0$ as above. There is a unique $\beta \in k$ such that $o(f - \beta z_u) < u$, and of course $f - \beta z_u \in R$. Continuing in this manner we can write f in the form $\sum_{i=0}^{\gamma-1} a_i(x)z_{\lambda_i}$ with the $a_i(x)$ polynomials. The expression is unique since the z_{λ_i} are independent in K, so the z_{λ_i} form a basis for R over $k[x]$.

Similar arguments establish the statements for differentials. ☐

Corollary 3.4. *Given $\{z_{\lambda_i}\}_{i=0}^{\gamma-1}$ the equations* (7) *uniquely determine the $\zeta_{\lambda_i-\gamma}$.*

PROOF: Let $\omega \in \Omega$ and write $\omega = \sum_{j=0}^{\gamma-1} a_j(x)\zeta_{\lambda_j-\gamma}$. The $a_j(x)$ are rational functions in x, but we will use their power series expansions, $a_j(x) = \sum_{k\in\mathbb{Z}} \alpha_{jk}x^k$. Here $\alpha_{jk} = 0$ for all k below some bound which depends on a_j. Now

$$\begin{aligned}\mathrm{res}_Q(z_{\lambda_i}\omega x^{-r}) &= \mathrm{res}_Q\, z_{\lambda_i}\sum_{j=0}^{\lambda-1}\zeta_{\lambda_j-\gamma}\sum_k \alpha_{jk}x^{k-r}\\ &= \alpha_{i,r-1}\end{aligned}$$

using (7). Therefore $a_i(x) = \sum_{r\in\mathbb{Z}} x^{r-1}\,\mathrm{res}_Q(z_{\lambda_i}\omega x^{-r})$ and the series expansion for ω can be recovered by using (7) for all values of $i \in \{0,\ldots,\gamma-1\}$ and $r \in \mathbb{Z}$. In particular, for each i the only differential satisfying (7) for all i, r is $\zeta_{\lambda_i-\gamma}$.

$\square$

Let Tr be the trace map from K to $k(x)$. Recall that the dual basis to $\{z_{\lambda_i}\}_{i=0}^{\gamma-1}$ is the unique set of elements of K, $z^\star_{\lambda_0},\ldots,z^\star_{\lambda_{\gamma-1}}$ such that $\mathrm{Tr}(z_{\lambda_i}z^\star_{\lambda_j}) = \delta_{ij}$ (1 if $i = j$ and 0 otherwise). The next proposition shows the relationship between the dual basis and the $\zeta_{\lambda_i-\gamma}$ of the theorem. We will need to use a result that is not explicitly stated in many references on function fields, but does appear as Proposition 8 in Ch. X of [10]: Let K be a separable finite extension of $k(x)$ and let $Q_1,\ldots Q_r$ be the distinct points over a point P of $k(x)$. Let y be an element of K. Then

$$\sum_{i=1}^{r}\mathrm{res}_{Q_i}(ydx) = \mathrm{res}_P(\mathrm{Tr}(y)dx)$$

The theorem assumes k is algebraically closed. It is also true if k is not algebraically closed provided P, Q_i are rational points since the residues are defined for rational points and unchanged when one passes to the algebraic closure.

Proposition 3.5. *With the notation of the theorem, let* $\{z^\star_{\lambda_i}\}_{i=0}^{\gamma-1}$ *be the dual basis to* $\{z_{\lambda_i}\}_{i=0}^{\gamma-1}$ *with respect to the trace map from* K *to* $k(x)$*. Then*

$$\zeta_{\lambda_i-\gamma} = -z^\star_{\lambda_i}dx \tag{8}$$

Proof: By the previous corollary it is enough to show that for all i

$$\operatorname{res}_Q z_{\lambda_i}z^\star_{\lambda_j}x^{-r}dx = \begin{cases} -1 & \text{if } i=j \text{ and } r=1 \\ 0 & \text{otherwise} \end{cases}$$

since this uniquely determines $-\zeta_{\lambda_j}$. We apply the theorem quoted above. There is a unique point Q above the point ∞ which is the pole of x on the projective line, so

$$\begin{aligned} \operatorname{res}_Q z_{\lambda_i}z^\star_{\lambda_j}x^{-r}dx &= \operatorname{res}_\infty \operatorname{Tr}(z_{\lambda_i}z^\star_{\lambda_j}x^{-r})dx \\ &= \operatorname{res}_\infty \delta_{ij}x^{-r}dx \\ &= \begin{cases} -1 & \text{if } i=j \text{ and } r=1 \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

□

Finally we have another result that is not readily available in the literature, but which is not difficult to derive from a standard result (cited in the proof). It will be used to give a new formula for computing error values.

Theorem 3.6. *Let* M/L *be a finite separable field extension and let* Tr *be the trace map from* M *to* L*. Let* $z_1,\dots,z_n$ *be a basis for* M *over* L *and let* $z_1^\star,\dots,z_n^\star$ *be the dual basis. Then*

$$\sum_{i=1}^{n} z_iz_i^\star = 1 \tag{9}$$

PROOF: We will show that $\sum_{i=1}^{n} z_i z_i^\star = 1$ is independent of the basis chosen and then use a particular basis to get the result.

Suppose $\{z_i\}$ and $\{y_j\}$ are both bases for M over L and let $\{z_i^\star\}$ and $\{y_j^\star\}$ be the respective dual basis. Let $b_{ij} \in L$ be such that $y_i = \sum_{j=1}^{n} b_{ij} z_j$ and let B be the $n \times n$ matrix $[b_{ij}]$. Similarly, let $c_{uv} \in L$ be such that $y_u^\star = \sum_{v=1}^{n} c_{uv} z_v^\star$ and let C be the $n \times n$ matrix $[c_{uv}]$. Then

$$\begin{aligned}
\delta_{iu} &= \mathrm{Tr}(y_i y_u^\star) \\
&= \mathrm{Tr}\left(\sum_j b_{ij} z_j \sum_v c_{uv} z_v^\star\right) \\
&= \sum_j \sum_v b_{ij} c_{uv}\, \mathrm{Tr}(z_j z_v^\star) \\
&= \sum_j \sum_v b_{ij} c_{uv} \delta_{jv} \\
&= \sum_j \sum_v b_{ij} c_{uj}
\end{aligned}$$

Thus $BC^T = I$ or $C^T = B^{-1}$. Now,

$$\begin{aligned}
\sum_i y_i y_i^\star &= \sum_i \sum_j b_{ij} z_j \sum_v c_{iv} z_v^\star \\
&= \sum_j \sum_v z_j z_v^\star \sum_i b_{ij} c_{iv}
\end{aligned}$$

The coefficient of $z_j z_v^\star$ is $(B^T C)_{jv} = \delta_{jv}$ so $\sum_i y_i y_i^\star = \sum_j z_j z_j^\star$.

Since M is finite and separable over L there is some $y \in M$ such that $M = L(y)$. Let $\phi(T)$ be the minimal polynomial of y and let $\phi'(T)$ be it's formal derivative. Let

$$\begin{aligned}\psi(T) &= \frac{\phi(T)}{T-y} \\ &= c_{n-1}T^{n-1} + c_{n-2}T^{n-2} + \cdots + c_1 T + c_0\end{aligned}$$

where $c_i \in M$ and $c_{n-1} = 1$. The proof of [19, III.5.10] (or [11, VI.5.5]) shows that the dual basis to $1, y, y^2, \ldots, y^{n-1}$ is $c_0/\phi'(y), \ldots, c_{n-1}/\phi'(y)$. For this basis, the sum in (9) is

$$\sum_{i=1}^{\gamma-1} y^i \frac{c_i}{\phi'(y)} = \frac{1}{\phi'(y)}\psi(y) \tag{10}$$

In some algebraic closure of M, let $y_1, y_2, \ldots, y_{n-1}$ be the roots of ϕ that are distinct from y and let $y_n = y$. Then $\psi(y) = \prod_{i=1}^{n-1}(y - y_i)$. Since $\phi'(T) = \sum_{i=1}^{n}\prod_{j\neq i} T - y_i$, $\phi'(y) = \prod_{i=1}^{n-1}(y - y_i)$. So the sum in (10) is 1. □

Combining the last theorem and the previous proposition we immediately have the following.

Corollary 3.7.

$$\sum_{i=1}^{n} z_{\lambda_i}\zeta_{\lambda_i - \gamma} = -dx \tag{11}$$

Two standard examples of one-point codes are given below. One is the Hermitian code, for which $(2g-2)Q$ is canonical. We also consider the Klein quartic, which must be embedded in 3-space to have the one-point be the sole point at infinity and for which $(2g-2)Q$ is not canonical. Justification for the values of the ζ_u are in [13].

Example 3.8. Let $\mathcal{C}$ be the Hermitian curve in the plane over $\mathbb{F}_{q^2}$ defined by $x^{q+1} = y^q + y$ and let Q be the point at infinity. The sequence of nongaps,

Λ is generated by q and $q+1$, so $\gamma = q$ and $\lambda_j = j(q+1)$. At Q, the function x has a pole of order q and y has a pole of order $q+1$. Therefore we take $z_{\lambda_j} = y^j$. For $j \neq 0$, set $\zeta_{\lambda_j - q} = -y^{q-1-j}dx$ and for $j = 0$ set $\zeta_{-q} = -(y^{q-1}+1)dx$. This choice satisfies (7).

Example 3.9. Let $\mathcal{C}$ be the Klein quartic defined by $X^3Y + Y^3Z + Z^3X$ in the projective plane over a finite 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 $P = [1:0:0]$. We will take Q as the one-point defining our codes. The function $y = Y/Z$ has a pole of order 3 at Q, $u = XY/Z^2$ has a pole of order 5, and $v = X^2Y/Z^3$ has a pole of order 7. The nongap sequence Λ is generated by $\gamma = 3$, $\lambda_1 = 7$ and $\lambda_2 = 5$. The ring R is a free module of rank 3 over $k[y]$ generated by $z_0 = 1$, $z_5 = u$, and $z_7 = v$. Let

$$\begin{aligned} \zeta_{-3} &= -\frac{v+1}{3v+1}dy \\ \zeta_2 &= -\frac{u}{y(3v+1)}dy \\ \zeta_4 &= -\frac{1}{3v+1}dy \end{aligned}$$

This choice satisfies (7).

4 The Syndrome Differential

We now define a unique differential which represents the syndrome map $S_{\mathbf{e}}$. The results in this section are proved in [13], although we have changed the sign in the definition of ω_e (15).

For any $u \in \mathbb{Z}$, there are unique i, r such that $u = \lambda_i + r\gamma$. Let

$$z_u = z_{\lambda_i} x^r \tag{12}$$

$$\zeta_u = \zeta_{\lambda_i - \gamma} x^{-r-1} \tag{13}$$

Then $\nu_Q(z_u) = -u$ and $z_u \in R$ if and only if $u \in \Lambda$. Similarly, $\nu_Q(\zeta_u) = -u - 1$ and $\zeta_u \in \Omega(-\infty Q)$ if and only if $v \in \Lambda^c$. Furthermore, from (7),

$$\mathrm{res}_Q\, z_u \zeta_v = \delta_{uv} \tag{14}$$

Definition 4.1. For $v \in \Lambda$, let $s_v = S_{\mathbf{e}}(z_v)$. We define the *syndrome differential* to be

$$\omega_{\mathbf{e}} = \sum_{u \in \Lambda} s_u \zeta_u \tag{15}$$

Since $\nu_Q(\zeta_0) = -1$, $\nu_Q(\omega_{\mathbf{e}}) \geq -1$. If $\mathbf{e}$ has support at a single point then $\nu_Q(\omega_{\mathbf{e}}) = -1$. For example, suppose that $\mathbf{e}$ is the kth basis vector and let ω_k be the associated syndrome differential. Then

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

Using the definition of z_u and ζ_v above,

$$\begin{aligned}
&= \sum_{i=0}^{\gamma-1} z_{\lambda_i}(P_k) \zeta_{\lambda_i - \gamma} \sum_{r=0}^{\infty} (x(P_k))^r x^{-r-1} \\
&= \frac{1}{x} \left(\sum_{r=0}^{\infty} \frac{(x(P_k))^r}{x^r} \right) \left(\sum_{i=0}^{\gamma-1} z_{\lambda_i}(P_k) \zeta_{\lambda_i - \gamma} \right) \\
&= \frac{1}{x} \left(\frac{1}{1 - \frac{x(P_k)}{x}} \right) \left(\sum_{i=0}^{\gamma-1} z_{\lambda_i}(P_k) \zeta_{\lambda_i - \gamma} \right) \\
&= \frac{1}{x - x(P_k)} \sum_{i=0}^{\gamma-1} z_{\lambda_i}(P_k) \zeta_{\lambda_i - \gamma}
\end{aligned}$$

For an arbitrary error vector $\mathbf{e}$,

$$\begin{aligned}\omega_{\mathbf{e}} &= \sum_{u\in\Lambda} S_{\mathbf{e}}(z_u)\zeta_u \\ &= \sum_{u\in\Lambda}\sum_{k} e_k z_u(P_k)\zeta_u \\ &= \sum_{k}\left(\frac{e_k}{x-x(P_k)}\sum_{i=0}^{\gamma-1} z_{\lambda_i}(P_k)\zeta_{\lambda_i-\gamma}\right)\end{aligned}$$

In this form it is evident that $\omega_{\mathbf{e}}$, which we defined as a series, really is a differential.

From Theorem 3.2 we have that $s_v = S_{\mathbf{e}}(z_v) = \operatorname{res}_Q(z_v\omega_{\mathbf{e}})$. Both $S_{\mathbf{e}}$ and res_Q are linear operators so we get the following result.

Proposition 4.2. *For any $f \in R$, $S_{\mathbf{e}}(f) = \operatorname{res}_Q f\omega_{\mathbf{e}}$.*

It is an immediate corollary that for any $f \in R$, $S_{\mathbf{e}}(f)$ is the coefficient of ζ_0 in the ζ series expansion for $f\omega_{\mathbf{e}}$. The following proposition gives a much stronger result concerning all the coefficients of $f\omega_{\mathbf{e}}$.

Definition 4.3. 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*.

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

Proposition 4.4. *Let $\omega_{\mathbf{e}}$ be as in* (15)*. For $f \in R$, let*

$$f\omega_{\mathbf{e}} = \sum_{v\in\mathbb{Z}} t_v\zeta_v \tag{16}$$

Then $t_v = S_{\mathbf{e}}(\tilde{f})$ where $\tilde{f}$ is the R-part of fz_v.

5 The Key Equation

Generalizations of the key equation from the case of BCH codes to codes on curves have been presented by Ehrhard [1, 2], and by Porter, Shen and Pellikaan [15, 18]. In this section we describe the key equation for one-point codes in a form suitable for Koetter's algorithm.

Definition 5.1. We will say that $f \in R$ and $\phi \in \Omega(-\infty Q)$ *satisfy the key equation (for* $\mathbf{e}$*)* if $f\omega_{\mathbf{e}} = \phi$.

The utility of a solution to the key equation is that ϕ can be used for error evaluation. For this reason ϕ is called the error evaluator (associated to f).

Proposition 5.2. *Let P_k be an error position and let t_k be a uniformizing parameter at P_k. If f is an error locator and $\phi = f\omega_{\mathbf{e}}$, then*

$$e_k \frac{df}{dt_k}(P_k) = -\frac{\phi}{dt_k}(P_k) \tag{17}$$

In particular, if f has a simple zero at P_k then $df/dt_k(P_k) \neq 0$ and this formula can be solved for e_k.

Proof: [13, 3.6] □

Definition 5.3. For $f \in R$ we define $\operatorname{span} f$ to be the smallest nongap c such that $S_{\mathbf{e}}(z_c f) \neq 0$ (or $\operatorname{span} f = \infty$ if no such c exists). We say that $f \in R$ and $\phi \in \Omega(-\infty Q)$ satisfy the *nth key equation* if ϕ is a linear combination of the ζ_v with $v \in \Lambda^c$ and $v \leq n$, and

$$\nu_Q(f\omega_{\mathbf{e}} - \phi) \geq n$$

Provided $f \neq 0$, we will also say that ϕ is the *nth approximation of* $f\omega_{\mathbf{e}}$. The *discrepancy of* f, ϕ *at* $n+1$ is the unique $\alpha \in k$ such that

$$\nu_Q(f\omega_{\mathbf{e}} - \phi - \alpha t^n dt) > n \tag{18}$$

Using (6), we may also write (18) as $\nu_Q(f\omega_{\mathbf{e}} - \phi - \alpha\zeta_{n+1}) > n$. Consequently, if $n+1$ is a gap then $\phi + \alpha\zeta_{n+1}$ is the $(n+1)$th approximation of $f\omega_{\mathbf{e}}$. The definition allows for $f = 0$. For example, if $v \in \Lambda^c$ then $0, \zeta_v$ satisfy the $(v-1)$th key equation and the discrepancy at v is -1 by (6).

If f, ϕ satisfy the nth key equation then $n < \operatorname{span} f$. For if u is a nongap and $u \leq n$ then $S_{\mathbf{e}}(fz_u) = \operatorname{res}_Q fz_u\omega_{\mathbf{e}} = \operatorname{res}_Q \phi z_u$. The second equality follows from the nth key equation because $v_Q(fz_u\omega_{\mathbf{e}} - \phi z_u) \geq n - u \geq 0$ so $\operatorname{res}_Q(fz_u\omega_{\mathbf{e}} - \phi z_u) = 0$. Since ϕ only has terms ζ_v with $v \in \Lambda^c$, $\operatorname{res}_Q \phi z_u = 0$ by (7). Thus $S_{\mathbf{e}}(fz_u) = 0$ for all nongaps $u \leq n$, and consequently, $n < \operatorname{span} f$.

For $f \neq 0$, write $f\omega_{\mathbf{e}} = \sum t_v\zeta_v$. If $n < \operatorname{span} f$, then the nth approximation of $f\omega_{\mathbf{e}}$ is just $\sum_{v \leq n} t_v\zeta_v$ and the discrepancy at $n+1$ is t_{n+1}. In particular, if $\operatorname{span} f = c$ is finite then $\phi = \sum_{v<c} t_v\zeta_v$ is the $(c-1)$th approximation of $f\omega_{\mathbf{e}}$ and t_c is the discrepancy at c.

Lemma 5.4. *If f, ϕ satisfy the $n-1$th key equation with discrepancy α at n, then for $k \geq 0$, $fx^k, \phi x^k$ satisfy the $(n - \gamma k - 1)$th key equation with discrepancy α at $n - \gamma k$. If $f \neq 0$, $\alpha \neq 0$ and $n - \gamma k$ is a nongap then $\operatorname{span} fx^k = n - \gamma k$. If $f \neq 0$ and $n - k\gamma$ is a gap, then fx^k and $\phi x^k + \alpha\zeta_{n-k\gamma}$ satisfy the $(n - k\gamma)$th key equation.*

PROOF: It is clear that $\nu_Q(fx^k\omega_{\mathbf{e}} - \phi x^k) \geq n - \gamma k - 1$. From (13), for any v, $x^k\zeta_v = \zeta_{v-k\gamma}$. Therefore ϕx^k when written as a linear combination of the ζ_v involves only terms with $v \leq n - \gamma k - 1$. Thus $fx^k, \phi x^k$ satisfy the

$(n-\gamma k-1)$th key equation. Furthermore, since $\nu_Q(f\omega_{\mathbf{e}}-\phi-\alpha t^{n-1}dt)\geq n$, we have

$$\nu_Q(fx^k\omega_{\mathbf{e}}-\phi x^k-\alpha t^{n-k\gamma-1}dt)\geq n-k\gamma \tag{19}$$

so the discrepancy of fx^k at $n-k\gamma$ is α.

Now suppose that $f\neq 0$. If $\alpha\neq 0$ and $n-k\gamma$ is a nongap then span $fx^k=n-k\gamma$ because $z_{n-k\gamma}\in R$ and $S_{\mathbf{e}}(fx^k z_{n-k\gamma})=\alpha$. If $n-k\gamma$ is a gap then we may substitute $\zeta_{n-k\gamma}$ for $t^{n-k\gamma-1}dt$ in (19) and get that $\phi x^k+\alpha\zeta_{n-k\gamma}$ is the $n-k\gamma$ approximation of fx^k. □

Lemma 5.5. *Suppose f, ϕ and g, ψ both satisfy the $(n-1)$th key equation with α and β the respective discrepancies at n. Then $f-(\alpha/\beta)g$ and $\phi-(\alpha/\beta)\psi$ satisfy the nth key equation. If n is a nongap then* span $f=$ span $g=n$ *and* span $f-(\alpha/\beta)g>n$.

Proof: We have $\nu_Q(f\omega_{\mathbf{e}}-\phi-\alpha t^n dt)>n$ and $\nu_Q(g\omega_{\mathbf{e}}-\psi-\beta t^n dt)>n$. Thus

$$\nu_Q(f-\alpha/\beta g-(\phi-(\alpha/\beta)\psi))>n$$

□

6 Solution of the Key Equation using Koetter's Algorithm

We now present the version of Koetter's algorithm that computes error evaluators. The algorithm performs best when used in conjunction with majority voting for unknown syndromes—due to Feng and Rao. Since majority voting is amply treated elsewhere [3, 8, 12, 17] the details are omitted. Using majority voting enables the decoder to correct errors having weight less than $d_{FR}/2$ where d_{FR} is the Feng-Rao bound on the minimum distance of the code. In fact, for some codes (e.g. high rate Hermitian codes) many error vectors with much larger weight can be decoded. We will not discuss the Feng-Rao bound or the performance of the decoder in this article. We will assume that our check code is such that the error vector $\mathbf{e}$ can be decoded using the algorithm.

Let the check code be defined by $m^\star Q$. The algorithm has iterations from $m = 0$ to $m = M$, with M generally larger than $m^\star$. The value of M at which to terminate the algorithm is dealt with at the end of the section. We continue with all the notation of the previous sections. We will use $[m - i]$ to indicate the least nonnegative residue of $m - i$ modulo γ.

The Algorithm:

Data Structures Compute for each m and for each $i = 0, \ldots, \gamma - 1$:

$$B_i^{(m)} = \begin{bmatrix} f_i^{(m)} & \phi_i^{(m)} \\ g_i^{(m)} & \psi_i^{(m)} \end{bmatrix}$$

where $f_i^{(m)}, g_i^{(m)} \in R$ and $\phi_i^{(m)}, \psi_i^{(m)} \in \Omega(-\infty Q)$.

Initialization For $m = -1$,

$$B_i^{(-1)} = \begin{bmatrix} z_{\lambda_i} & 0 \\ 0 & -\zeta_{\lambda_i - \gamma} \end{bmatrix}$$

Algorithm For $m = 0$ to M,

1. For each $i = 0, \ldots, \gamma - 1$, let $s_i = o(f_i^{(m-1)})$,
   Compute $\tilde{f}_i = R$-part of $f_i^{(m-1)} z_{m-s_i}$
   Compute $\alpha_i = S_{\mathbf{e}}(\tilde{f}_i)$ (Use majority voting if $m > m^\star$).

2. For each $i = 0, \ldots, \gamma - 1$, let $j = [m - i]$,

   Set

$$r_i = 1 + (m - s_i - s_j)/\gamma \tag{20}$$

   If $r_i \leq 0$ or $\alpha_i = 0$, set

$$A_i = \begin{bmatrix} 1 & -\alpha_i x^{-r_i} \\ 0 & 1 \end{bmatrix} \tag{21}$$

   If $r_i > 0$, set

$$A_i = \begin{bmatrix} x^{r_i} & -\alpha_i \\ \alpha_i^{-1} & 0 \end{bmatrix} \tag{22}$$

   Then

$$\begin{bmatrix} f_i^{(m)} & \phi_i^{(m)} \\ g_j^{(m)} & \psi_j^{(m)} \end{bmatrix} = A_i \begin{bmatrix} f_i^{(m-1)} & \phi_i^{(m-1)} \\ g_j^{(m-1)} & \psi_j^{(m-1)} \end{bmatrix}$$

We remark that the incorporation of the error evaluator computation into Koetter's algorithm leads to subtle changes in the updating process. In Koetter's original approach, if $m - s_i$ is a gap then there is no updating, $f_i^{(m)} = f_i^{(m-1)}$. In this algorithm there is updating even when $m - s_i$ is a gap. This means that the final error locator functions output by the two algorithms may not be the same. Consequently, the error evaluation formula that we establish in the next section will not work, in general, for Koetter's original algorithm.

We now prove that the algorithm computes error locators and evaluators. We will say that $f \in R$ with $o(f) = s$ has *leading coefficient* β if $o(f - \beta z_s) < s$. Recall that if f, ϕ satisfy the nth key equation, then $\operatorname{span} f \geq n + 1$ with equality if $n + 1$ is a nongap and the discrepancy at $n + 1$ is nonzero.

Theorem 6.1. *Upon completion of the mth iteration of the algorithm:*

1. *$o(f_i^{(m)}) \equiv i \mod \gamma$, and $f_i^{(m)}$ has leading coefficient 1;*

2. *$f_i^{(m)}$ and $\phi_i^{(m)}$ satisfy the $m - o(f_i^{(m)})$ key equation;*

3. *$o(g_i^{(m)}) \leq m - o(f_i^{(m)}) + \gamma$;*

4. *$g_i^{(m)}$ and $\psi_i^{(m)}$ satisfy the $o(f_i^{(m)}) - \gamma - 1$ key equation with discrepancy 1 at $o(f_i^{(m)}) - \gamma$; and*

5. *$o(f_i^{(m)}) = \lambda_i$ if and only if $g_i^{(m)} = 0$, in which case $\psi_i^{(m)} = -\zeta_{\lambda_i - \gamma}$.*

Proof: When $m = -1$ we have $f_i^{(-1)} = z_{\lambda_i}$ which has pole order $\lambda_i \equiv i \mod \gamma$. Since $\nu_Q(z_{\lambda_i}\omega_{\mathbf{e}}) \geq -1 - \lambda_i$, $f_i^{(-1)}$ and 0 satisfy the $(-1 - \lambda_i)$th key equation. From Definition 5.3 and (6), 0 and $-\zeta_{\lambda_i - \gamma}$ satisfy the $\lambda_i - \gamma - 1$ key equation with discrepancy 1. Since $o(0) = -\infty$, item 3) is also satisfied.

Proceeding by induction, we assume that the statement of the theorem is true for $m - 1$ and prove it for m. It is sufficient to verify the result for an arbitrary pair i, j such that $i + j \equiv m \mod \gamma$. Let $s_i = o(f_i^{(m-1)})$, and let $s_j = o(f_j^{(m-1)})$. It is clear that $r_i = r_j$, so we drop the subscript. We remark also that by Proposition 4.4, α_i is the discrepancy of $f_i^{(m-1)}, \phi_i^{(m-1)}$ at $m - s_i$.

Let us first show that

$$o(f_i^{(m)}) = \begin{cases} s_i + r\gamma & \text{if } r > 0 \\ s_i & \text{if } r \leq 0 \end{cases} \tag{23}$$

By the induction hypothesis and the definition of r in (20),

$$\begin{aligned} o(g_j^{(m-1)}) &< m - s_j + \gamma \\ &= s_i + r\gamma \end{aligned}$$

Consequently, if $r > 0$ then $o(g_i^{(m-1)}) < o(f_i^{(m-1)}x^r)$ and if $r \leq 0$, then $o(g_i^{(m-1)}x^{-r}) < o(f_i^{(m-1)})$. Since $f_i^{(m)}$ is a linear combination of one of these two pairs its order is the same as $f_i^{(m-1)}x^r$, in the first case, or $f_i^{(m-1)}$ in the second as claimed in (23). Furthermore, it is clear that the leading coefficient of $f_i^{(m)}$ is 1 either way. We have therefore shown that item 1) holds.

Consider the case where $r \leq 0$. Then $g_i^{(m)} = g_i^{(m-1)}$ and $\psi_i^{(m)} = \psi_i^{(m-1)}$. By (23), $o(f_i^m) = s_i$, so items 3), 4), and 5) of the theorem are immediate from the induction hypothesis. We have $f_i^{(m-1)}$ and $\phi_i^{(m-1)}$ satisfy the $m - 1 - s_i = s_j + r\gamma - \gamma - 1$ key equation with discrepancy α_i at $s_j + r\gamma - \gamma$. By the induction hypothesis and Lemma 5.4, $g_j^{(m-1)}x^{-r}$ and $\psi_j^{(m-1)}x^{-r}$ satisfy the $s_j + r\gamma - \gamma - 1$ key equation as well, with discrepancy 1 at $s_j + r\gamma - \gamma$. Thus Lemma 5.5 shows that $f_i^{(m)}$ and $\phi_i^{(m)}$ satisfy the $m - s_i$ key equation, as required in item 2). The same argument also holds for j, so we have established the induction step for $r \leq 0$.

Assume now that $r > 0$. We show first that $\alpha_i = \alpha_j = S_{\mathbf{e}}(f_i^{(m-1)}f_j^{(m-1)}x^{r-1})$. We know that $f_j^{(m-1)}x^{r-1} \in R$, that $o(f_j^{(m-1)}x^{r-1}) = s_j + (r-1)\gamma = m - s_i$ and that $f_j^{(m-1)}x^{r-1}$ has leading coefficient 1. Since $\operatorname{span} f_i^{(m-1)} \geq m - s_i$, $S_{\mathbf{e}}(f_i^{(m-1)}(f_j^{(m-1)}x^{r-1} - z_{m-s_i})) = 0$. Thus $\alpha_i = S_{\mathbf{e}}(f_i^{(m-1)}z_{m-s_i}) = S_{\mathbf{e}}(f_i^{(m-1)}f_j^{(m-1)}x^{r-1})$. The same argument may be made for α_j, so $\alpha_i = \alpha_j$.

If $\alpha_i = 0$ then also $\alpha_j = 0$ and $f_i^{(m-1)}$, $\phi_i^{(m-1)}$ satisfy the $m - s_i$ key equation while $f_j^{(m-1)}$, $\phi_j^{(m-1)}$ satisfy the $m - s_j$ key equation. Thus all of the data in $B_i^{(m-1)}$ and $B_j^{(m-1)}$ is retained for the next iteration.

If $\alpha_i = \alpha_j \neq 0$ then by Lemma 5.4, $f_i^{(m-1)}x^r$ and $\phi_i^{(m-1)}x^r$ satisfy the $m - 1 - s_i - r\gamma = s_j - \gamma - 1$ key equation with discrepancy α_i at $s_j - \gamma$. By the induction hypothesis $g_j^{(m-1)}$ and $\psi_j^{(m-1)}$ satisfy the same key equation with discrepancy 1. Thus Lemma 5.5 shows that the $f_i^{(m)}$ and $\phi_i^{(m)}$ satisfy the $m - s_i - r\gamma = m - o(f_i^{(m)})$ key equation. The analogous results hold for $f_j^{(m)}$ and $\phi_j^{(m)}$, so item 2) holds.

Finally, we verify the claims for $g_i^{(m)}$ and $\psi_i^{(m)}$ (the j case is identical). We remark first that because $r > 0$, $o(f_i^{(m)}) > \lambda_i$. We have $g_i^{(m)} = \alpha_j^{-1} f_j^{(m-1)}$ is nonzero with pole order $s_j = m - o(f_i^{(m)}) + \gamma$ in agreement with items 3) and 5). Additionally, $g_i^{(m)}$ and $\psi_i^{(m)} = \alpha^{-1}\phi_j^{(m-1)}$ satisfy the $m - s_j - 1 = s_i + r\gamma - \gamma - 1 = o(f_i^{(m)}) - \gamma - 1$ key equation with discrepancy 1 as in item 4).

This completes the proof. □

The algorithm for majority voting for the syndrome s_m is actually very simple from this set up. Each f_i gets r_i votes for the value of s_m. The value of the vote by $f_i^{(m-1)}$ is $S_{\mathbf{e}}(\tilde{f}_i - z_m)$ where $\tilde{f}_i$ is defined as in the algorithm.

Finally, we determine the value of M at which the algorithm can be terminated. For each $i = 0, \ldots, \gamma-1$, let $t_i = \min\{o(f) : f \in I_{\mathbf{e}}$ and $o(f) \equiv i \mod \gamma\}$. Let $t_{\max} = \max\{t_i\}$. For each i, let $c_i = t_i - \gamma$. Let $c_{\max} = \max\{t_i - \gamma : t_i \neq \lambda_i\}$.

Proposition 6.2. *Let $M = t_{\max} + \max\{c_{\max}, 2g-1\}$. At the end of the Mth iteration, the computation of the error locators and error evaluators is complete, that is:*

1. *The $f_i^{(M)}$ are a basis for $I_{\mathbf{e}}$ as a module over $k[x]$.*

2. *For each i, $f_i^{(M)}, \phi_i^{(M)}$ satisfy the key equation.*

PROOF: Let $\Delta = \{\operatorname{span} g : g \in R \setminus I_{\mathbf{e}}\}$. We will use the well known fact that $\Delta = \Lambda \setminus \{o(f) : f \in I_{\mathbf{e}}\}$. Note that $c_{\max}$ is the largest integer in Δ. Let $s_i = o(f_i^{(M)})$. We have $\operatorname{span} f_i^{(M)} > M - s_i \geq s_{\max} + c_{\max} - s_i \geq c_{\max}$.

Since the span of any element of $R \setminus I_e$ is at most $c_{\max}$, we have $f_i^{(M)} \in I_e$. Furthermore, since $\operatorname{span} g_i^{(M)} = s_i - \gamma$ we know $s_i - \gamma \in \Delta$. Thus $s_i = t_i$.

Let $h \in I_e$, and let i be the least positive residue of $o(h)$ modulo γ. By the definition of t_i, $o(h) \geq t_i$. Let $r = (o(h) - t_i)/\gamma$. There is some $\beta \in k$ such that $o(h - \beta x^r f_i^{(M)}) < o(h)$, and of course $h - \beta x^r f_i^{(M)} \in I_e$. Continuing in this manner we can write h as a linear combination of the $f_i^{(M)}$ with coefficients polynomials in x. This establishes item 1).

Since $f_i^{(M)}, \phi_i^{(M)}$ satisfy the $(M-s_i)$th key equation, $\nu_Q(f_i^{(M)}\omega_{\mathbf{e}} - \phi_i^{(M)}) \geq M - s_i \geq s_{\max} + 2g - 1 - s_i \geq 2g - 1$. Since $f_i^{(M)}\omega_{\mathbf{e}} - \phi_i^{(M)}$ has no poles away from Q, $\deg(f_i^{(M)} - \phi_i^{(M)}) \geq 2g - 1$. Any nonzero differential has degree $2g - 2$, so it must be the case that $f_i^{(M)}\omega_{\mathbf{e}} - \phi_i^{(M)} = 0$. Consequently $f_i^{(M)}$, $\phi_i^{(M)}$ satisfy the key equation. This establishes item 2). $\square$

7 Evaluation of Errors Using Update Polynomials

In [9], Koetter remarked on a formula for evaluation of errors for Reed-Solomon codes that is easily derived from the Berlekamp-Massey algorithm but seems to be ignored in textbooks. If f is the locator polynomial and g is the update polynomial remaining after the last iteration of the Berlekamp-Massey algorithm, then for any error position, P_k,

$$e_k = \frac{1}{f'(P_k)g(P_k)}$$

We now generalize this formula.

We assume that $m^\star$ defining the check code is large enough that majority voting will always produce the correct syndrome for our given error vector $\mathbf{e}$. Let M be as in Proposition 6.2, so that the computation of locators and evaluators is complete. Let

$$f_i = f_i^{(M)} \quad \phi_i = \phi_i^{(M)}$$
$$g_i = g_i^{(M)} \quad \psi_i = \psi_i^{(M)}$$

Then the f_i are a basis for $I_{\mathbf{e}}$ and f_i, ϕ_i satisfy the key equation. The pairs g_i, ψ_i are special as well, we will show that

$$\sum_{i=0}^{\gamma-1} (f_i \psi_i - g_i \phi_i) = dx \tag{24}$$

Let us postpone the proof of this result, since it is very technical, and instead use it to prove the following theorem concerning evaluation of errors. For any $f \in R$ let $f' = df/dx$. We will need to assume that $x - x(P_k)$ is a uniformizing parameter at each P_k. This ensures that $\nu_{P_k}(dx) = 0$ and therefore that f' has no poles among the P_k.

Theorem 7.1. *Assume that for each $k = 1, \ldots, n$, $x - x(P_k)$ is a uniformizing parameter at P_k. Let P_k be an error position,. Then*

$$e_k = \left(\sum_{i=0}^{\gamma-1} f_i'(P_k) g_i(P_k) \right)^{-1} \tag{25}$$

PROOF: Dividing (24) by dx we get

$$\sum_{i=0}^{\gamma-1} \left(f_i \frac{\psi_i}{dx} - g_i \frac{\phi_i}{dx} \right) = 1$$

Since $x - x(P_k)$ is a uniformizing parameter at P_k, $\nu_{P_k}(dx) = 0$. Both ψ_i and ϕ_i have no poles away from Q, so we can evaluate this equation at P_k. Furthermore, we can apply Proposition 5.2 with $t_k = x - x(P_k)$ so that $e_k f_i'(P_k) = -(\phi_i/dx)(P_k)$. Since each f_i is a locator, $f_i(P_k) = 0$. Thus

$$\sum_{i=0}^{\gamma-1} g_i(P_k) e_k f_i'(P_k) = 1$$

Factoring out e_k, the formula (25) follows. $\square$

Now let us establish (24).

Theorem 7.2. *For all m,*

$$\sum_{i=0}^{\gamma-1} \det B_i^{(m)} = -\sum_{i=0}^{\gamma-1} z_{\lambda_i}\zeta_{\lambda_i-\gamma} = dx \tag{26}$$

PROOF: We proceed by induction. The case $m = -1$ is immediate from Corollary 3.7. Assume that the statement of the theorem is true for $m-1$; we will prove it for m. It is sufficient to show that $\det B_i^{(m)} = \det B_i^{(m-1)}$ if $2i \equiv m \mod \gamma$ and $\det B_i^{(m)} + \det B_j^{(m)} = \det B_i^{(m-1)} + \det B_j^{(m-1)}$ if $i+j \equiv m \mod \gamma$ and $i \neq j$.

In the mth iteration of the algorithm we use a matrix A_i satisfying either (21) or (22) to compute $B_i^{(m)}$. If $2i \equiv m \mod \gamma$, then $B_i^{(m)} = A_i B_i^{(m-1)}$. Since $\det A_i = 1$, we have $\det B_i^{(m)} = \det B_i^{(m-1)}$.

Assume now that $i+j \equiv m \mod \gamma$ and that $i \neq j$. In the proof of Theorem 6.1 we showed that $\alpha_i = \alpha_j$ if $r > 0$. In fact, Proposition 7.3 below shows that $\alpha_i = \alpha_j$ even when $r \leq 0$. Thus we have $A_i = A_j$ and we may suppress the subscript on α. For the sake of legibility we will also suppress the superscripts on components of $B_i^{(m-1)}$ and $B_j^{(m-1)}$.

$$B_i^{(m)} = \begin{cases} \begin{bmatrix} f_i - \alpha g_j x^{-r} & \phi_i - \alpha\psi_j x^{-r} \\ g_i & \psi_i \end{bmatrix} & \text{if } r \leq 0 \\ \begin{bmatrix} f_i x^r - \alpha g_j & \phi_i x^r - \alpha\psi_j \\ \alpha^{-1} f_j & \alpha^{-1}\phi_j \end{bmatrix} & \text{if } r > 0 \end{cases}$$

Therefore,

$$\det B_i^{(m)} = \begin{cases} f_i\psi_i - g_i\phi_i - \alpha x^{-r}(g_j\psi_i - g_i\psi_j) & \text{if } r \leq 0 \\ f_j\psi_j - g_j\phi_j - \alpha^{-1}x^r(f_i\phi_j - f_j\phi_i) & \text{if } r > 0 \end{cases}$$

When we take the sum of $\det B_i^{(m)}$ and $\det B_j^{(m)}$ the final terms cancel. Thus $\det B_i^{(m)} + \det B_j^{(m)} = \det B_i^{(m-1)} + \det B_j^{(m-1)}$ as was to be proved. $\square$

Finally, the following proposition gives the key element used in the proof of Theorem 7.2.

Proposition 7.3. *In the mth iteration of the algorithm, $\alpha_i = \alpha_{[m-i]}$ where $[m-i]$ is the least positive residue of $m-i$ modulo γ.*

Furthermore, for any m,

$$\operatorname{res}_Q \det \begin{bmatrix} f_i^{(m)} & \phi_i^{(m)} \\ g_j^{(m)} & \psi_j^{(m)} \end{bmatrix} x^a = \begin{cases} 1 & \textit{if } i = j \textit{ and } a = -1 \\ 0 & \textit{otherwise} \end{cases} \tag{27}$$

$$\operatorname{res}_Q \det \begin{bmatrix} f_i^{(m)} & \phi_i^{(m)} \\ f_j^{(m)} & \phi_j^{(m)} \end{bmatrix} x^a = 0 \tag{28}$$

$$\operatorname{res}_Q \det \begin{bmatrix} g_i^{(m)} & \psi_i^{(m)} \\ g_j^{(m)} & \psi_j^{(m)} \end{bmatrix} x^a = 0 \tag{29}$$

PROOF: The proof has two parts. First we show that if (27), (28), (29) hold for $m-1$ then in the mth iteration of the algorithm, $\alpha_i = \alpha_{[m-i]}$. Second, we prove by induction that (27), (28), (29) hold for all m. Thus we can conclude that for any mth iteration of the algorithm, $\alpha_i = \alpha_{[m-i]}$.

Assume that (27), (28), (29) hold for $m-1$. Let $j = [m-i]$ and let α_i, α_j, s_i and s_j be as in Step 1 of the algorithm. We will suppress the superscripts on $f_i^{(m-1)}$ and the other data from the $(m-1)$th iteration. By Proposition 4.4 and Theorem 6.1

$$\nu_Q(f_i h_{\mathbf{e}} - \phi_i - \alpha_i \zeta_{m-s_i}) \geq m - s_i \tag{30}$$

From (20) it can be seen that $f_j x^{r-1}$ has pole order $m - s_i$. Its leading coefficient is 1 so multiplying (30) by $f_j x^{r-1}$ we get

$$\nu_Q(f_i f_j x^{r-1} h_{\mathbf{e}} - f_j \phi_i x^{r-1} - \alpha_i f_j x^{r-1} \zeta_{m-s_i}) \geq 0$$

By (7), $\mathrm{res}_Q\, f_j x^{r-1}\zeta_{m-s_i} = 1$, so

$$\mathrm{res}_Q(f_i f_j x^{r-1} h_{\mathbf{e}} - f_j \phi_i x^{r-1}) = \alpha_i \tag{31}$$

By (28), $\mathrm{res}_Q\, f_i\phi_j = \mathrm{res}_Q\, f_j\phi_i$, so we may substitute in (31) to obtain

$$\mathrm{res}_Q(f_i f_j x^{r-1} h_{\mathbf{e}} - f_i \phi_j x^{r-1}) = \alpha_i \tag{32}$$

On the other hand, the term on the left is also equal to α_j by the analogous argument—with i, j interchanged—used to derive (31). Thus $\alpha_i = \alpha_j$ as was to be proved.

Now we prove (27), (28), (29) by induction. For $m = -1$, (28) and (29) are immediate since the determinants are 0, and (27) holds by (7). Assume now that (27), (28), (29) hold for $m-1$, we will establish the formulas for m.

Consider the $2\gamma \times 2$ matrix

$$\mathbf{B}^{(m)} = \begin{bmatrix} B_0^{(m)} \\ B_1^{(m)} \\ \cdots \\ \cdots \\ \cdots \\ B_{\gamma-1}^{(m)} \end{bmatrix}$$

We will index a row of $\mathbf{B}^{(m)}$ by (i, f) for $[f_i^{(m)}, \phi_i^{(m)}]$ or (i, g) for $[g_i^{(m)}, \psi_i^{(m)}]$. From the algorithm, it is evident that $\mathbf{B}^{(m)}$ is a linear function of $\mathbf{B}^{(m-1)}$. Let $\mathbf{B}^{(m)} = \mathbf{T}\mathbf{B}^{(m-1)}$. Equations (27), (28), (29) concern determinants of 2×2 submatrices of $\mathbf{B}^{(m)}$. Let I be a pair of row indices for $\mathbf{B}^{(m)}$. Then by the Cauchy-Binet theorem

$$\det \mathbf{B}_I^{(m)} = \sum \det \mathbf{T}_I^J \det \mathbf{B}_J^{(m-1)} \tag{33}$$

where J ranges over distinct pairs of indices for rows of $\mathbf{B}^{(m-1)}$. By the induction hypothesis, $\text{res}_Q \det \mathbf{B}_J^{(m-1)} x^a = 0$ for all a unless $J = \{(j,f),(j,g)\}$ for some fixed j. Thus the only terms in (33) which affect (27), (28), (29) are of the form $J = \{(j,f),(j,g)\}$.

From the algorithm it is clear that only $f_j^{(m)}$ and $g_{[m-j]}^{(m)}$ depend on $f_j^{(m-1)}$. Therefore the (j,f) column of $\mathbf{T}$ can only be nonzero in rows (j,f) and $([m-j],g)$. Similarly, $g_j^{(m-1)}$ only affects $g_j^{(m)}$ and $f_{[m-j]}^{(m)}$, so the (j,g) column of $\mathbf{T}$ can be nonzero only in rows (j,g) and $([m-j],f)$. Consequently, if $J = \{(j,f),(j,g)\}$ then $\mathbf{T}_I^J$ has a row which is zero—and therefore determinant 0—unless

$$I \subset \{(j,f),(j,g),([m-j],f),([m-j],g)\} \tag{34}$$

If I does not satisfy (34) for some value of j, then $\det \mathbf{T}_I^J = 0$ for all $J = \{(j,f),(j,g)\}$ and thus $\text{res}_Q \det \mathbf{B}_I^{(m)} x^a = 0$ for all a.

We have now reduced the problem to verifying (27), (28), (29) for I satisfying (34). Furthermore, for such I

$$\text{res}_Q \det \mathbf{B}_I^{(m)} x^a = \text{res}_Q \det \mathbf{T}_I^J \det \mathbf{B}_J^{(m-1)} x^a + \text{res}_Q \det \mathbf{T}_I^{\overline{J}} \det \mathbf{B}_{\overline{J}}^{(m-1)} x^a$$

where $J = \{(j,f),(j,g)\}$ and $\overline{J} = \{([m-j],f),([m-j],g)\}$. From the algorithm, the update of $B_j^{(m)}$ and $B_{[m-j]}^{(m)}$ may be written as one of the following matrix equations

$$\begin{bmatrix} f_j & \phi_j \\ g_j & \psi_j \\ f_{[m-j]} & \phi_{[m-j]} \\ g_{[m-j]} & \psi_{[m-j]} \end{bmatrix}^{(m)} = \begin{bmatrix} 1 & 0 & 0 & -\alpha_j x^{-r} \\ 0 & 1 & 0 & 0 \\ 0 & -\alpha_j x^{-r} & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} f_j & \phi_j \\ g_j & \psi_j \\ f_{[m-j]} & \phi_{[m-j]} \\ g_{[m-j]} & \psi_{[m-j]} \end{bmatrix}^{(m-1)} \tag{35}$$

$$\begin{bmatrix} f_j & \phi_j \\ g_j & \psi_j \\ f_{[m-j]} & \phi_{[m-j]} \\ g_{[m-j]} & \psi_{[m-j]} \end{bmatrix}^{(m)} = \begin{bmatrix} x^r & 0 & 0 & -\alpha_j \\ 0 & 0 & \alpha_j^{-1} & 0 \\ 0 & -\alpha_j & x^r & 0 \\ \alpha_j^{-1} & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} f_j & \phi_j \\ g_j & \psi_j \\ f_{[m-j]} & \phi_{[m-j]} \\ g_{[m-j]} & \psi_{[m-j]} \end{bmatrix}^{(m-1)} \tag{36}$$

We have used the result proved earlier—since (27), (28) and (29) hold for $(m-1)$, the discrepancies at iteration m are equal, $\alpha_j = \alpha_{[m-j]}$. There are now $\binom{4}{2}$ choices for I to check for each of the two matrices. When $I = J$ or $I = \overline{J}$ either $\det \mathbf{T}_I^J = 1$ and $\det \mathbf{T}_I^{\overline{J}} = 0$ or vice-versa. Thus the induction hypothesis shows that $\mathrm{res}_Q \det \mathbf{B}_I^{(m)} x^a = 1$ if and only if $a = -1$ as in (27). For $I = \{(j,f),([m-j],g)\}$ or $I = \{(j,g),([m-j],g)\}$, we have $\det \mathbf{T}_I^J = \det \mathbf{T}_I^{\overline{J}} = 0$ for either choice of $\mathbf{T}$. Thus $\mathrm{res}_Q \det \mathbf{B}_I^{(m)} x^a = 0$. This finishes the proof of (27) and establishes (29). Finally, for $I = \{(j,f),([m-j],f)\}$, and for the matrix (35), $\det \mathbf{T}_I^J = -\det \mathbf{T}_I^{\overline{J}} = -\alpha_j x^{-r}$. Thus

$$\mathrm{res}_Q \det \mathbf{B}_I^{(m)} x^a = -\alpha_j \left(\mathrm{res}_Q \det \mathbf{B}_J^{(m-1)} x^{a-r} - \mathrm{res}_Q \mathbf{B}_{\overline{J}}^{(m-1)} x^{a-r} \right)$$

The induction hypothesis shows that the two residues on the right are equal so $\mathrm{res}_Q \det \mathbf{B}_I^{(m-1)} x^a = 0$ for all a. The same argument works for equation (36). Thus (28) is established. □

Acknowledgments

The author is grateful for the opportunity to collaborate with Dick Blahut and Ralf Koetter of the Coordinated Sciences Laboratory of the University of Illinois at Urbana-Champaign which was made possible by NSF grant CCR-9805080.

References

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

[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] G. L. Feng and T. R. N. Rao, Decoding algebraic-geometry codes up to the designed minimum distance, *IEEE Trans. Inform. Theory*, Vol. 39, No. 1, (1993) 37-45.

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

[5] T. Høholdt, R. Pellikaan, J.H. van Lint, Algebraic geometry codes, *Handbook of Coding Theory* (W.C.Huffmann, V. Pless eds.) Elsevier, 1998, pp. 871-961.

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

[7] R. Koetter , A formula for the determination of error values for Hermitian codes, in Proc. IEEE 1997 International Symposium on Information Theory, Ulm , Germany p. 382.

[8] R. Koetter, A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes, IEEE Trans. Inform. Theory, Vol. 44, No. 4 (1998), pp. 1353-1368.

[9] R. Koetter, 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.

[10] S. Lang, Introduction to Algebraic Geometry, Interscience Tracts in Pure and Applied Mathematics No. 5, Interscience Publishers, N. Y., (1958).

[11] S. Lang, *Algebra*, third ed. Addison-Wesley Pub. Co., Reading, Mass., (1993).

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

[13] M. E. O'Sullivan, The key equation for one-point codes, *J. Pure Appl. Algebra*, Vol. 169 No. 2-3 (2002) pp. 295-320.

[14] M. E. O'Sullivan, New Codes for the Berlekamp-Massey-Sakata algorithm, *Finite Fields Applic.* Vol. 7, (2001) pp. 293-317.

[15] 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.

[16] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, *Information and Computation*, Vol. 84, (1990) pp. 207-239.

[17] 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* Vol. 41, No. 6 (1992), pp. 1762-1768.

[18] 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.

[19] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Verlag Universitext, Berlin, (1993).