The Key Equation for Hermitian codes

Michael E. O'Sullivan

San Diego State University

July 11, 2008, S^3CM, Soria, Spain

The Hermitian curve and points

- $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$.
- $n = q^3$ points over $\mathbb{F}_{q^2}$.
- Let $P_k = (\alpha_k, \beta_k)$, and $D = P_1 + \cdots + P_n$.
- Let $P_\infty = [0 : 1 : 0]$ be the point on L_∞.

The ring of functions

- $R = \mathbb{F}_{q^2}[x, y]/\langle y^q + y - x^{q+1}\rangle$.
- x has a pole of order q at P_∞.
- y has a pole of order $q+1$ at P_∞.
- The pole order of $x^i y^j$ is $\rho(x^i y^j) = iq + j(q+1)$.
- Treat R as an $\mathbb{F}_{q^2}[x]$-module with basis $1, \ldots, y^{q-1}$.
- R has an $\mathbb{F}_{q^2}$-basis $\{x^i y^j\}_{\substack{0 \leq i \\ 0 \leq j < q}}$.
- $\Lambda = \{iq + j(q+1) : 0 \leq i, 0 \leq j < q\}$ is the set of nongaps.
- $\Lambda^c = \mathbb{Z} \setminus \Lambda$.

The codes

- Recall the definition of evaluation codes

$$
\begin{aligned}
R &\xrightarrow{ev} \mathbb{F}_{q^2}^n \\
f &\mapsto (f(P_1), \ldots, f(P_n)) \\
L(mP_\infty) &\mapsto C_L(D, \bar{m}P_\infty)
\end{aligned}
$$

- Codewords from $C_\Omega(D, \bar{m}P_\infty) = C_L(D, \bar{m}P_\infty)^\perp$ are sent.
- Suppose $\bar{m} = iq + j(q+1)$. The check matrix is

$$
H = \begin{bmatrix} ev(1) \\ ev(x) \\ ev(y) \\ ev(x^2) \\ \ldots \\ ev(x^i y^j) \end{bmatrix}
$$

Decoding Problem

- Send $c \in C_\Omega(D, \bar{m}P_\infty)$.
- Receive $v \in \mathbb{F}_{q^2}^n$.
- Error is $e = v - c$.
- The *error locator ideal* is $I^e = \{f : f(P_k) = 0 : \text{ when } e_k \neq 0\}$.
- The *syndrome* is

$$S = \sum_{i=1}^{n} e_k \frac{x^{q+1} - \alpha_k^{q+1}}{(x - \alpha_k)(y - \beta_k)}$$

- I'll argue that this is the right definition!

Note!

$$\begin{aligned}\frac{x^{q+1} - \alpha^{q+1}}{x - \alpha} &= \alpha^q \frac{\left(\frac{x}{\alpha}\right)^{q+1} - 1}{\frac{x}{\alpha} - 1} \\ &= \alpha^q \left(\left(\frac{x}{\alpha}\right)^q + \left(\frac{x}{\alpha}\right)^{q-1} + \cdots + \frac{x}{\alpha} + 1 \right) \\ &= x^q + \alpha x^{q-1} + \cdots + \alpha^{q-1} x + \alpha^q\end{aligned}$$

and

$$\begin{aligned}\frac{y^q + y - \beta^q - \beta}{y - \beta} &= 1 + \frac{y^q - \beta^q}{y - \beta} \\ &= 1 + y^{q-1} + \beta y^{q-2} + \cdots + \beta^{q-2} y + \beta^{q-1}\end{aligned}$$

Product of a locator with the syndrome

Lemma

If $f \in I^e$ then $fS \in \mathbb{F}_{q^2}[x,y]$.

Proof.

Enough to show for any position k,

$$(\star) \qquad f\frac{x^{q+1}-\alpha_k^{q+1}}{(x-\alpha_k)(y-\beta_k)} \in R$$

Since $f \in I^e$, there exist g and h in $\mathbb{F}_{q^2}[x,y]$ such that $f = g(x-\alpha_k)+h(y-\beta_k)$ Hence, $(\star)$ is

$$g\left(\frac{y^q+y-\beta_k^q-\beta_k}{y-\beta_k}\right)+h\left(\frac{x^{q+1}-\alpha_k^{q+1}}{x-\alpha_k}\right)$$

which belongs to $\mathbb{F}_{q^2}[x,y]$. □

Error evaluation

Lemma

Let $f \in I^e$ and $\varphi = fS$.
If P_k is an error position then $e_k f'(P_k) = fS(P_k)$.
So if $f'(P_k) \neq 0$ we can solve for e_k.

- φ is the error evaluator associated to f.
- f' means df/dx.
- We use $d(x^iy^j) = ix^{i-1}y^j + x^ijy^{j-1}(dy/dx)$,
- From the equation of the curve

$$(qy^{q-1}+1)dy = (q+1)x^q dx$$
$$dy/dx = x^q$$

Proof

- $\varphi = fS = \sum_{j=1}^{n} e_j \frac{x^{q+1} - \alpha_j^{q+1}}{(x-\alpha_j)(y-\beta_j)} f.$
- Suppose e_k is not zero. The fraction in the sum may be evaluated for $j \neq k$, and f vanishes at P_k.
- So the only term that contributes is the kth.
- Using $f = g(x-\alpha_k) + h(y-\beta_k)$ as before,

$$\varphi(P_k) = e_k\Big(g(P_k) + h(P_k)\alpha_k^q\Big)$$
$$f'(P_k) = g(P_k) + h(P_k)\alpha_k^q$$

Expansion of the syndrome

Lemma

Let $S_{a,b} = ev(x^a y^b) \cdot e = \sum_k e_k \alpha_k^a \beta_k^b$. *Then*

$$S = \frac{1}{x} \sum_{b=0}^{q-1} \sum_{a=0}^{\infty} s_{a,b} x^{-a}(y^{q-1-b} + \delta_b)$$

where δ_b *is 1 when* $b = 0$ *and 0 otherwise.*

Proof.

A computation. □

Let $z_j^* = y^{q-1-j} + \delta_j$.
This gives a dual basis for $\{y^b : b = 0, \ldots, q-1\}$ relative to the trace map: $K(R) \to \mathbb{F}(x)$.

Characterization of I^e

Using the set Δ^e from the order domains lecture we have a corollary to the earlier result that $f^e S \in R$.

Proposition

If the expansion of fS in the $*$-basis has zero coefficients for all $x^{-a-1} z_b^*$ such that $aq + b(q+1) \in \Delta^e$ then $f \in I^e$.

Proof.

Suppose $e_k \neq 0$; show $f(P_k) = 0$.
Trick: Look at gfS where g has support in Δ^e and g vanishes at all error locations $P_j \neq P_k$. □

Data for the algorithm

- **Data:** For each i from 0 to $q - 1$ we have a matrix

$$B_i = \begin{pmatrix} f_i & \varphi_i \\ g_i & \psi_i \end{pmatrix}$$

- Each entry is an element of $R = \mathbb{F}_{q^2}[x, y]$ where $y^q = x^{q+1} - y$.
- **Initialize:** For $i = 0$ to $q - 1$, set

$$B_i^{(0)} = \begin{pmatrix} f_i^{(0)} & \varphi_i^{(0)} \\ g_i^{(0)} & \psi_i^{(0)} \end{pmatrix} = \begin{pmatrix} y^i & 0 \\ 0 & -z_i^* \end{pmatrix}$$

- Recall $z_i^* = y^{q-1-i} + \delta_0$.

Algorithm

- For $m = 0$ to M, and for each pair i, j such that $m \equiv i + j \mod q$,
- **Compute shifts:**

$$d_i = \rho(f_i^{(m)}) \qquad d_j = \rho(f_j^{(m)})$$

$$r_i = \frac{m - d_i - j(q+1)}{q} \qquad r_j = \frac{m - d_j - i(q+1)}{q}$$

$$p = \frac{d_i + d_j - m}{q} - 1$$

- **Compute discrepancies**

$$\tilde{f}_i = y^j f_i \qquad \tilde{f}_j = y^i f_j$$

$$\mu_i = \sum_{c=0}^{q-1} \sum_a (\tilde{f}_i)_{a,c} s_{a+r_i,c} \qquad \mu_j = \sum_{c=0}^{q-1} \sum_a (\tilde{f}_j)_{a,c} s_{a+r_j,c}$$

Algorithm: Update

- The update for j is analogous to the one for i given below.
- **Compute the update matrix**

$$U_i^{(m)} = \begin{cases} \begin{pmatrix} 1 & -\mu_i x^p \\ 0 & 1 \end{pmatrix} & \text{if } \mu_i = 0 \text{ or } p \geq 0 \\ \begin{pmatrix} x^{-p} & -\mu_i \\ 1/\mu_i & 0 \end{pmatrix} & \text{otherwise.} \end{cases}$$

- **Update**

$$\begin{pmatrix} f_i^{(m+1)} & \varphi_i^{(m+1)} \\ g_j^{(m+1)} & \psi_j^{(m+1)} \end{pmatrix} = U_i^{(m)} \begin{pmatrix} f_i^{(m)} & \varphi_i^{(m)} \\ g_j^{(m)} & \psi_j^{(m)} \end{pmatrix}$$

- **Output:** $f_i^{(M+1)}, \varphi_i^{(M+1)}$ for $0 \leq i < q$.

Theorem

For $m \geq 0$,

1. $f_i^{(m)}$ is monic and $\rho(f_i^{(m)}) \equiv i \mod q$.
2. $f_i^{(m)}, \varphi_i^{(m)}$ satisfy the $m - \rho(f_i^{(m)})$ approximation of the key equation.
3. $g_i^{(m)}, \psi_i^{(m)}$ satisfy the $\rho(f_i^{(m)}) - q$ approximation of the key equation and $g_i^{(m)} S - \psi_i^{(m)}$ is monic of order $q^2 - 1 - \rho(f_i^{(m)})$.
4. $\rho(g_i^{(m)}) < m - \rho(f_i^{(m)}) + q$.

The Key Equation

- We say that $f, \varphi \in \mathbb{F}_{q^2}[x, y]$ solve the key equation for syndrome S when $fS = \varphi$.
- We say that f and φ in $\mathbb{F}_{q^2}[x, y]$, with f nonzero, solve the Kth approximation of the key equation for syndrome S when the following two conditions hold.
  1. $\rho(fS - \varphi) \leq q^2 - q - 1 - K$,
  2. φ, written in the z^*-basis, is a sum of terms whose order is at least $q^2 - q - K$.
- We will also say that 0 and $x^{-a-1} z_b^*$, for $a < 0$, solve the $aq + b(q + 1)$ key equation.

Stopping criteria

As in the order domains lecture, let $\Sigma = \{\rho(f) : f \in I^e\}$ and $\sigma = \min_{\preccurlyeq} \Sigma$.
Let $\Delta = \Lambda \setminus \Sigma$ and $\delta = \max_{\preccurlyeq} \Delta$.

Proposition

Let $\sigma_{\max} = \max\{\sigma_i : 0 \le i \le q-1\}$ *and let* $\delta_{\max} = \max\{c \in \Delta^e\}$. *(max and min in the usual sense in* $\mathbb{N}$*.)*

For $m > \sigma_{\max} + \delta_{\max}$*, each of the polynomials* $f_i^{(m)}$ *belongs to* I^e*.*

Let $M = \sigma_{\max} + \max\{\delta_{\max}, q^2 - q - 1\}$*. Each of the pairs* $f_i^{(M+1)}, \varphi_i^{(M+1)}$ *satisfies the key equation.*

Generalization of Horiguchi's formula

We don't need the error evaluator polynomials!

Proposition

Let $B_i^{(M)} = \begin{pmatrix} f_i^{(m)} & \varphi_i^{(m)} \\ g_i^{(m)} & \psi_i^{(m)} \end{pmatrix}$*. Then for all m,*

$$\sum_{i=0}^{q-1} \det B_i^{(m)} = -\sum_{i=0}^{q-1} y^i z_i^* = -1 \tag{1}$$

Proof This took some work.

Theorem

If P_k *is an error position.*

$$e_k = \left(\sum_{i=0}^{q-1} f_i'(P_k) g_i(P_k) \right)^{-1} \tag{2}$$

One-point codes

- $\mathcal{X}$, a projective (smooth absolutely irreducible) curve over $\mathbb{F}$.
- Q, an $\mathbb{F}$-point on $\mathcal{X}$.
- $K(\mathcal{X})$ the function field of $\mathcal{X}$.
- Let R be the ring of functions with poles only at Q.

$$R = \{f \in K(\mathcal{X}) : v_P(f) \geq 0 \text{ for } P \neq Q\}$$

- We have the evaluation map

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

- Let $L(mQ)$ be the elements of R with pole order at most m at Q.

$$\begin{aligned} E(D, m) &= ev(L(mQ)) \\ C(D, m) &= E(D, m)^{\perp} \end{aligned}$$

Dual bases

- Let κ be the smallest positive element of Λ.
- For $j = 0, \ldots, \kappa - 1$ let $\lambda_j \in \Lambda$ be the smallest element congruent to j modulo κ.
- Let x have pole order κ
  and let z_j have pole order λ_j.
- z_j is a basis for R as $\mathbb{F}_q[x]$ module (and for K over $\mathbb{F}[x]$).
- The dual basis to $\{z_b\}_{b=0}^{\kappa-1}$ is the unique set of elements of K, $z_0^*, \ldots, z_{\kappa-1}^*$ such that $\mathrm{Tr}(z_b z_j^*)$ is 1 if $b = j$ and 0 otherwise.

Dual basis and differentials

Proposition

For each $b \in \{0, \ldots, \kappa - 1\}$, $z_b^* dx$ is an element of $\Omega(-\infty Q)$, $-z_b^* dx$ is monic, relative to t_Q, and $\nu_Q(z_b^* dx) = \lambda_b - \kappa - 1$. Additionally,

$$\mathrm{res}_Q(z_j z_b^* x^a dx) = \begin{cases} -1 & \text{when } a = -1 \text{ and } j = b \\ 0 & \text{otherwise} \end{cases}$$

The syndrome

Definition

For a point P, let

$$h_P = \frac{1}{x - x(P)} \sum_{b=0}^{\kappa-1} z_b(P) z_b^*.$$

We define the *syndrome* of e to be

$$S = \sum_{k=1}^{n} e_k h_{P_k}.$$

Lemma

Let $s_{a,b} = \sum_{k=1}^{n} e_k (x(P_k))^a (z_b(P_k))$. Then

$$S = \frac{1}{x} \sum_{b=0}^{\kappa-1} \sum_{a=0}^{\infty} s_{a,b} x^{-a} z_b^*$$

Conclusions

- The decoding algorithm given earlier applies to one point codes with some minor change of notation.
- The algorithm computes successively better approximations to the key equation.
- In the update of polynomials the only computations are multiplication by x and field elements: amenable to hardware.
- The only multiplication by y is in the computation of $\widetilde{f}$ to get discrepancies.
- The algorithm requires iterations for each $m \in \mathbb{N}_0$; not just $m \in \Lambda$.
- Caution: Majority voting may be necessary to compute all the syndromes $s_{a,b}$ needed.

References

These notes are based on the presentation of the key equation in

- Bras-Amorós, O'Sullivan, "The Key Equation for One-point Codes" in *Advances in Algebraic Geometry Codes*, Martinez-Moro, Munuera, Ruano eds., Series on Coding and Cryptology, World Scientific, 2008.

There are many references to the development of the subject in that chapter. In particular, we mention

- Ralf Kötter. A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes. *IEEE Trans. Inform. Theory*, 44(4):1353–1368, 1998.