THE KEY EQUATION FOR ONE-POINT CODES

Michael E. O’Sullivan
National University of Ireland, Cork

- Reed-Solomon Codes Revisited
- One-Point Codes
- The Key Equation
- Extension of Kötter’s Algorithm
- Computation of Error Values

Joint work with Ralf Kötter.
Supported by an NSF grant “Construction of a Practical Decoder for AG Codes.”
Work in the polynomial ring $\mathbb{F}[x]$.
Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be elements of $\mathbb{F}$.
Use the check matrix

\[
M = \begin{bmatrix}
1 & 1 & 1 & \ldots & 1 \\
\alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \\
\alpha_1^2 & \alpha_2^2 & \alpha_3^2 & \ldots & \alpha_n^2 \\
\alpha_1^3 & \alpha_2^3 & \alpha_3^3 & \ldots & \alpha_n^3 \\
\vdots & \vdots & \vdots & \ldots & \vdots
\end{bmatrix}
\]

So $M_{ik} = (\alpha_i)^k$. 

The Syndrome

Let $e \in \mathbb{F}^n$ be an error vector.

The *syndrome map* due to $e$ is

$$S_e : \mathbb{F}[x] \longrightarrow \mathbb{F}$$

$$f \mapsto \sum e_k f(\alpha_k)$$

Let

$$s_u = S_e(x^u) = \sum e_k (\alpha_k)^u$$

Then if $f = \sum a_u x^u$,

$$S_e(f) = \sum a_u s_u$$

Mention duality.
The Key Equation

The syndrome differential is

$$\omega_e = (s_0 + \frac{s_1}{x} + \frac{s_2}{x^2} + \frac{s_3}{x^3} + \ldots) \frac{1}{x} dx$$

**Proposition:** $S_e(f) = \text{res}_Q(f \omega_e)$

We say that $f \in \mathbb{F}[x]$ and $\varphi \in \mathbb{F}[x]dx$ satisfy the key equation if

$$f \omega_e = \varphi$$

**Proposition:**

$f$ satisfies the key equation $\iff$

$$f(\alpha_k) = 0 \text{ at all error positions } (k : e_k \neq 0).$$
The Berlekamp-Massey Algorithm

Data Structure

\[ B^{(m)} = \begin{bmatrix} f & \varphi \\ g & \psi \end{bmatrix}^{(m)} \]

Initialization

\[ B^{(-1)} = \begin{bmatrix} 1 & 0 \\ 0 & -dx \end{bmatrix} \]

Algorithm For \( m = 0 \) to “large enough”,

1. Compute the discrepancy,
   
   Let \( s = \deg f \), let
   
   \[ \alpha = S_e(fx^{m-s}) \]

2. Let \( r = m - 2s + 1 \), then
   
   \[ B^{(m)} = AB^{(m-1)} \]

   where

   \[ A = \begin{cases} 
   \begin{bmatrix} 1 & -\alpha x^{-r} \\ 0 & 1 \end{bmatrix} & \text{if } r \leq 0 \text{ or } \alpha = 0 \\
   \begin{bmatrix} x^r & -\alpha \\ \alpha^{-1} & 0 \end{bmatrix} & \text{if } r > 0 
   \end{cases} \]
For each $P_k$ such that $f(P_k) = 0$,

$$e_k = \frac{\varphi}{df}(P_k)$$

$$= \frac{\varphi}{df/dx}(P_k)$$
One-Point Codes

Notation:

$X$, an algebraic curve over $\mathbb{F}$.

$Q$, a $\mathbb{F}$-point on $X$.

$R$, the ring of functions with poles only at $Q$

$\Lambda$, the pole orders of elements of $R$.

Examples

1) $X$ is the projective line over $\mathbb{F}$.

$Q$ is the point “at infinity.”

$R = \mathbb{F}[x]$

$\Lambda = \mathbb{N}_0$. The pole order of a function is its degree.
2) \( X \) is the Hermitian curve defined by \( y^4 + y = x^5 \) in the plane over \( \mathbb{F}_{16} \).
\[
R = \mathbb{F}_{16}[x, y]/(y^4 + y + x^5)
\]
Since we are doing computations in this ring, we will always replace \( y^4 \) with \( x^5 + y \).

3) \( X \) is the Klein quartic defined by \( x^3y + y^3 + x \) in the projective plane over \( \mathbb{F} \).
\[
R \subset \mathbb{F}[x, y]/(x^3y + y^3 + x)
\]
\( R \) is generated by \( y, xy, \) and \( x^2y \)
In this ring we always replace \( x^3y \) with \( -y^3 - x \).
CONSTRUCTION OF THE CODES

Let \( P_1, P_2, \ldots, P_n \) be \( \mathbb{F} \)-points on the curve \( X \).

Let \( f_0 = 1, f_1, f_2, \ldots \) be elements of \( R \).

Define the code via the check matrix

\[
M = \begin{bmatrix} f_i(P_k) \end{bmatrix}
\]

EXAMPLES REVISITED

Recall that \( \Lambda \) is the set of pole orders of functions in \( R \).

1) For the projective line we take

\[
\begin{align*}
\{f_i\} & \quad 1 \ x \ x^2 \ x^3 \ \ldots \\
\Lambda & \quad 0 \ 1 \ 2 \ 3 \ \ldots 
\end{align*}
\]

2) For the Hermitian curve,

\[
\begin{align*}
\{f_i\} & \quad 1 \ x \ y \ x^2 \ xy \ y^2 \ x^3 \ \ldots \ xy^3 \ x^5 \ \ldots \\
\Lambda & \quad 0 \ 4 \ 5 \ 8 \ 9 \ 10 \ 12 \ \ldots \ 19 \ 20 \ \ldots 
\end{align*}
\]

3) For the Klein quartic

\[
\begin{align*}
\{f_i\} & \quad 1 \ xy \ y^2 \ x^2y \ xy^2 \ y^3 \ \ldots \\
\Lambda & \quad 0 \ 3 \ 5 \ 6 \ 7 \ 8 \ 9 \ \ldots 
\end{align*}
\]
**Fundamental Result**

**Theorem:** There exist functions \( \{z_u \in K\} \) and differentials \( \{\zeta_v \in \Omega\} \) such that

\[
\nu_Q(z_u) = -u, \quad (1)
\]
\[
\nu_Q(\zeta_v) = v - 1, \quad (2)
\]

and for \( u \in \Lambda \) and \( v - 1 \in \Lambda^c \),

\[
z_u \in R, \quad (3)
\]
\[
\zeta_v \in \Omega(-\infty Q), \quad (4)
\]

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

\[
\text{res}_Q z_u \zeta_v = \begin{cases} 
-1 & \text{if } v = u \\
0 & \text{otherwise}
\end{cases} \quad (5)
\]

Furthermore any \( f \in K \) and \( \omega \in \Omega \) may be uniquely expressed as series in the \( z_u \) and \( \zeta_v \).

\[
f = \sum_{u \geq \nu_Q(f)} a_u z_{-u}, \quad (6)
\]
\[
\omega = \sum_{v \geq \nu_Q(\omega) + 1} t_v \zeta_v \quad (7)
\]
Let $e \in \mathbb{F}^n$ be an error vector.

The *syndrome map* due to $e$ is

$$S_e : R \longrightarrow \mathbb{F}$$

$$f \longmapsto \sum e_k f(P_k)$$

For $u$ a nongap, define

$$s_u = S_e(z_u)$$

$$= \sum e_k z_u(P_k)$$

Then if $f = \sum a_u z_u$,

$$S_e(f) = \sum a_u s_u$$
The **key equation**

The *syndrome differential* is

\[ \omega_e = \sum_{u \in \Lambda} s_u \zeta_u \]

**Proposition:** \( S_e(f) = \text{res}_Q(f \omega_e) \)

We say that \( f \in R \) and \( \varphi \)—a differential with poles only at \( Q \)—**satisfy the key equation** if

\[ f \omega_e = \varphi \]

**Proposition:**

\[ f \text{ satisfies the key equation} \iff f(P_k) = 0 \text{ at all error positions } (k : e_k \neq 0). \]
Kötter’s Algorithm: Preparation

Let $p$ be the smallest positive nongap

$$p = \begin{cases} 
1 & \text{for the line (RS codes)} \\
4 & \text{for the Hermitian curve over } \mathbb{F}_{16} \\
3 & \text{for the Klein quartic}
\end{cases}$$

For $i = 0$ to $p - 1$, let $\lambda_i$ be the smallest nongap congruent to $i$ modulo $p$.

We may take $\{z_u\}$ and $\{\zeta_u\}$ such that

$$z_u = z_{\lambda_i} z_p^k \quad (9)$$
$$\zeta_u = \zeta_{\lambda_i - p} z_p^{-k-1} \quad (10)$$

where $u = \lambda_i + kp$. 
**Extension of Kötter’s Algorithm**

**Data Structure** For $i = 0, \ldots, p - 1$,

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

**Initialization**

$$B_i^{(-1)} = \begin{bmatrix} z_i & 0 \\ 0 & -\zeta_i \end{bmatrix}$$
**Algorithm** For $m = 0$ to “large enough”,

1. Compute the discrepancies,
   Let $s_i = \deg f_i$, let
   
   $$\alpha_i = S_e(f_i z_{m-s_i})$$

2. For each $i = 0, \ldots, p - 1$, let $j$ be the least positive residue of $m - i$ modulo $p$
   Set $r_i = 1 + (m - s_i - s_j)/p$
   If $r_i \leq 0$ or $\alpha_i = 0$, set
   
   $$A_i = \begin{bmatrix} 1 & -\alpha_i z_p^{-r_i} \\ 0 & 1 \end{bmatrix} \quad (11)$$

   If $r_i > 0$, set

   $$A_i = \begin{bmatrix} z_p^{r_i} & -\alpha_i \\ \alpha_i^{-1} & 0 \end{bmatrix} \quad (12)$$

Then

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

15
These have got to be true!

**Conjecture:** The sum of the determinants of the $B_i$ is independent of $m$.

$$
\sum_{i=0}^{p-1} \det B_i^{(m)} = - \sum_{i=0}^{p-1} z_{\lambda_i} \zeta_{\lambda_i - p}
$$

**Conjecture:** This determinant is related to the function $z_p$ in a canonical way.

$$
\sum_{i=0}^{p-1} z_{\lambda_i} \zeta_{\lambda_i - p} = d z_p
$$
ERROR EVALUATION

If \( f \) has a zero of order 1 at an error position \( P_k \) then

\[
e_k = \frac{\varphi}{df}(P_k)
\]

Practical problem: Computing all of the \( \varphi_i \) and \( \psi_i \) takes

A LOT more memory. But, there is hope, ...

Kötter noticed that for Reed-Solomon codes, the error value can also be found as follows,

\[
\frac{1}{e_k} = g(P_k) \frac{df}{dx}(P_k)
\]

so you don’t need the evaluator \( \varphi \).

This should work for AG codes too.

Conjecture:

\[
\frac{1}{e_k} = \sum_{i=0}^{p-1} g_i(P_k) \frac{df}{dz_p}(P_k)
\]