An Introduction to AG Codes with a Gröbner Basis Perspective

Douglas A. Leonard
Department of Mathematics and Statistics
Auburn University
Auburn, AL 36849

Linear Codes

In this session we will restrict ourselves to *linear, block codes* C over $\mathbf{F}_q$ (the finite field of q elements). This means that *information* is written as *messages* of the form

$$\underline{m} \in (\mathbf{F}_q)^k.$$

These have *redundancy* added to them by *encoding* them as *codewords* of the form

$$\underline{c} \in (\mathbf{F}_q)^n,$$

normally by

$$\underline{c} := \underline{m}G,$$

for G a $k \times n$ *generator matrix*.

This codeword is *transmitted* over a *noisy channel*, where an *error* is added to give a *received word* $\underline{r} = \underline{c} + \underline{e}$.

A *decoder* normally computes *syndromes*

$$\underline{s} := \underline{r}H = \underline{m}GH + \underline{e}H = \underline{e}H$$

independent of the codeword sent, with H an $n \times (n-k)$ *parity-check matrix* (which is also the transpose of a generator matrix for the orthogonal complement of the subspace C, also called the dual code $C^{\perp}$). The syndromes are used to predict the *most-likely error* $\underline{e'}$ with

$$\underline{e'}H = \underline{s}$$

to undo what the channel did, before producing the most-likely message $\underline{m'}$ with or without producing the most-likely codeword $\underline{c'}$ first.

The basic parameters of *wordlength*, n, *dimension*, k, and *minimum distance*, d, are loosely dependent, given that they satisfy the *Singleton bound*

$$d + k \leq n + 1.$$

Since any error of size t can definitely be decoded if $2t < d$, this translates into a tradeoff between the *information rate* k/n and the error rate t/n.

Reed-Solomon Codes

There are well-known *Reed-Solomon codes* that satisfy the Singleton bound. These have a *generator polynomial*

$$g(x) := \prod_{j=l+1}^{l+d-1} (x - \gamma^j) | (x^{q-1} - 1), \; c(x) := m(x)g(x)$$

and *parity-check polynomial*

$$h(x) := \frac{(x^{q-1} - 1)}{g(x)}, \; s(x) := r(x)h(x) \; (mod \; x^{q-1} - 1).$$

The matrices G and H are implicit rather than explicit here, but would have entries of the form $x^i(\gamma^j)$ for $\gamma^j \in \mathbf{F}_q$ and appropriate values of i.

The *Berlekamp-Massey algorithm* is an efficient method of row-reducing the Hankel ($\equiv$ back-shifted) matrix $S = H\Delta(\underline{r})H^T$ to produce an *error-locator polynomial* $\sigma(x)$ and *error-evaluator polynomial* $\tau(x)$ minimal with respect to $\sigma(x)s(x) \equiv \tau(x)$. The *error positions* are the roots γ^j of $\sigma(x)$. There are several methods for producing the *error magnitudes* e_j. The one most interesting from an ideal perspective is to use $\sigma(x)/(x - \gamma^j)$ and the *Forney formula*.

The only seeming drawback to Reed-Solomon codes is that $n \leq q - 1$ (or q for extended codes), with q the size of the field in which the computations are done.

A Berlekamp-Massey algorithm

The syndrome vector

$$s := \begin{pmatrix} 0 & \gamma^1 & \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 \end{pmatrix}$$

relative to the underlying functions

$$s := \begin{pmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 \end{pmatrix}$$

is a shiftable shorthand for the syndrome matrix

$$S = H\Delta(\underline{r})H^T =$$

$$\begin{array}{cccccc}
0 & \gamma^1 & \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 \\
\gamma^1 & \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 & \\
\gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 & & \\
\gamma^2 & \gamma^{13} & \gamma^1 & & & \\
\gamma^{13} & \gamma^1 & & & & \\
\gamma^1 & & & & &
\end{array}$$

γ^0				0	γ^1		
0	γ^0			γ^0			
γ^4	γ^0	γ^0		0	0	γ^{12}	
γ^4	γ^{14}	γ^7	γ^0	0	0	0	0

0							0	γ^1	γ^1	γ^2	γ^{13}	γ^1			γ^0	0	–
1						0	γ^1	γ^1	γ^2	γ^{13}	γ^1			γ^0		2	–
2				0	γ^1		γ^1	γ^2	γ^{13}	γ^1			γ^0			1	1
3			0	γ^1		0	γ^5	γ^{14}	γ^{12}			γ^0	γ^0			3	1
4		0	γ^1	0		0	γ^{12}	γ^4			γ^0	γ^0	γ^4			4	2
5	0	γ^1	γ^8	0		0	γ^{12}			γ^0	γ^9	γ^3				5	4
6	0 γ^1	γ^{10}	0	0		0			γ^0	γ^7	γ^{14}	γ^4				6	5

0				–	1		
–	0			0			
4	0	0		–	–	12	
4	14	7	0	–	–	–	–

0							–	1	1	2	13	1			0	0	–
1						–	1	1	2	13	1			0		2	–
2					–	1	1	2	13	1			0			1	1
3				–	1	–	5	14	12			0	0			3	1
4			–	1	–	–	12	4			0	0	4			4	2
5		–	1	8	–	–	12			0	9	3				5	4
6	–	1	10	–	–	–			0	7	14	4				6	5

$$\sigma(x) = x^3 + \gamma^7 x^2 + \gamma^{14} x + \gamma^4 = (x+\gamma^0)(x+\gamma^1)(x+\gamma^3),$$

$$\tau(x) = 0x^2 + \gamma^1 x + \gamma^{10}.$$

Forney functions and the Forney formula

It is easy to prove that

$$e_i = \frac{\sum_{j=0}^{t-1} \sigma_j^{(i)} s_j}{\sum_{j=0}^{t-1} \sigma_j^{(i)} \gamma^{l+1+j}}.$$

with

$$\sigma(x) = (x - \gamma_j)\sigma^{(i)}(x) = \sum_{j=0}^{t-1} \sigma_j^{(i)} x^j.$$

$$\left.\begin{array}{ccc|c} \gamma^0 & \gamma^9 & \gamma^4 & \gamma^0 \\ \gamma^0 & \gamma^{14} & \gamma^3 & \gamma^1 \\ \gamma^0 & \gamma^4 & \gamma^1 & \gamma^3 \end{array}\right.$$

$$e_0 = \frac{\gamma^0\gamma^2 + \gamma^9\gamma^1 + \gamma^4\gamma^1}{\gamma^0\gamma^0 + \gamma^9\gamma^0 + \gamma^4\gamma^0} = \gamma^5$$

$$e_1 = \frac{\gamma^0\gamma^2 + \gamma^{14}\gamma^1 + \gamma^3\gamma^1}{\gamma^0\gamma^2 + \gamma^{14}\gamma^1 + \gamma^3\gamma^0} = \gamma^7$$

$$e_3 = \frac{\gamma^0\gamma^2 + \gamma^4\gamma^1 + \gamma^1\gamma^1}{\gamma^0\gamma^6 + \gamma^4\gamma^3 + \gamma^1\gamma^0} = \gamma^{12}$$

Curves

To find longer length codes similar to these, first think of the function x^i as a *rational homogeneous function* $(X/Z)^i$ and the point of evaluation, γ^j as a point $P_j := (\gamma^j : 1)$ on the *projective line*, with $(X/Z)^i$ having its only poles (of order i) at the point $P_\infty := (1 : 0)$ where $Z = 0$.

Then replace the projective line by a *projective curve* $\mathbf{X}$ in higher dimensions, with the number of points near the *Weil bound*

$$n \leq 1 + q + 2g\sqrt{q},$$

g being the *genus* (the penalty in the equation $d + k = n + 1 - g$), with reasonable dimension k and minimum distance d.

An example of such is the *Hermitian code*, defined by

$$Y^4Z + YZ^4 = X^5$$

having $1 + 16 + 2 \cdot 6\sqrt{16} = 65 > 1 + 16$ projective points rational over $\mathbf{F}_{16}$, and genus $g = 6$.

Since X/Z has pole order 4 and Y/Z pole order 5, there are functions of the form $(X/Z)^i(Y/Z)^j$ of every pole order other than $1, 2, 3, 6, 7, 11$.

Feng-Rao example

(also in Leonard)

The syndrome "vector"

$$s := \left(\begin{array}{cccccccccc}
\gamma^1 & \gamma^{14} & \gamma^{11} & \gamma^4 & \gamma^0 & \gamma^1 & \gamma^5 & \gamma^{12} & \gamma^2 & \gamma^6 \\
\gamma^2 & \gamma^4 & \gamma^{11} & \gamma^6 & \gamma^{12} & \gamma^7 & \gamma^1 & \gamma^{14} & & \\
\gamma^9 & \gamma^{10} & \gamma^8 & \gamma^5 & \gamma^1 & \gamma^7 & 0 & & & \\
\gamma^5 & \gamma^2 & \gamma^{10} & \gamma^4 & \gamma^9 & \gamma^0 & & & & \\
\hline
\gamma^5 & \gamma^8 & \gamma^0 & \gamma^3 & \gamma^4 & & & & & \\
\gamma^0 & & & & & & & & &
\end{array}\right)$$

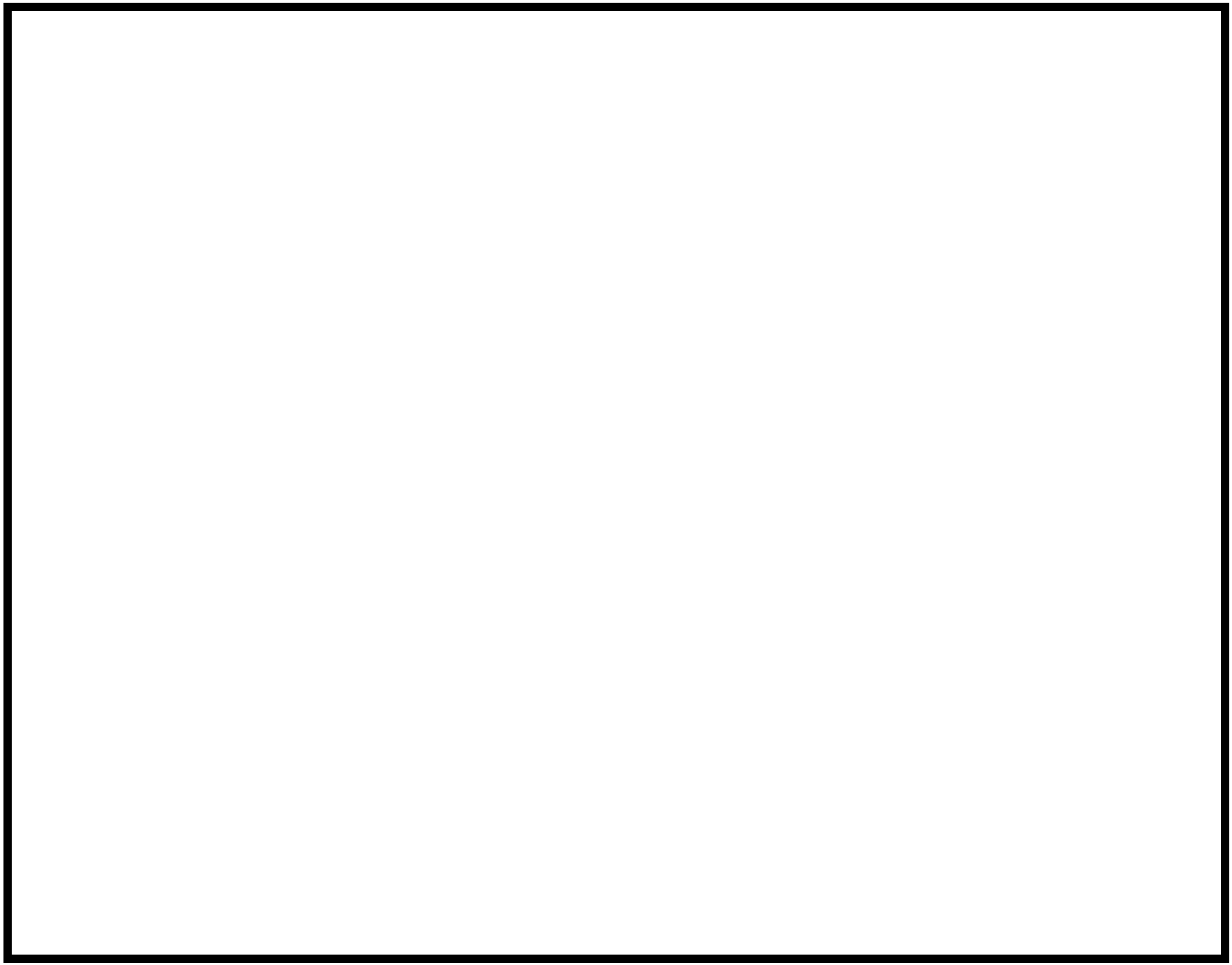
relative to the underlying functions

$$s := \left(\begin{array}{ccccccccccc} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & x^9 \\ y & yx & yx^2 & yx^3 & yx^4 & yx^5 & yx^6 & yx^7 & & \\ y^2 & y^2x & y^2x^2 & y^2x^3 & y^2x^4 & y^2x^5 & y^2x^6 & & & \\ y^3 & y^3x & y^3x^2 & y^3x^3 & y^3x^4 & y^3x^5 & & & & \\ \hline y^4 & y^4x & y^4x^2 & y^4x^3 & y^4x^4 & & & & & \\ y^5 & & & & & & & & & \end{array}\right)$$

is a shiftable shorthand for the syndrome matrix $S = H\Delta(\underline{e})H^T$.

$$
\begin{array}{cccccccccccccccccccc}
\gamma^{1} & . & . & . & \gamma^{14} & \gamma^{2} & . & . & \gamma^{11} & \gamma^{4} & \gamma^{9} & . & \gamma^{4} & \gamma^{11} & \gamma^{10} & \gamma^{5} & \gamma^{0} & \gamma^{6} & \gamma^{8} & \gamma^{2} & \gamma \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & \\
\gamma^{14} & . & . & . & \gamma^{11} & \gamma^{4} & . & . & \gamma^{4} & \gamma^{11} & \gamma^{10} & . & \gamma^{0} & \gamma^{6} & \gamma^{8} & \gamma^{2} & \gamma^{1} & \gamma^{12} & \gamma^{5} & \gamma^{10} & \gamma^{5} \\
\gamma^{2} & . & . & . & \gamma^{4} & \gamma^{9} & . & . & \gamma^{11} & \gamma^{10} & \gamma^{5} & . & \gamma^{6} & \gamma^{8} & \gamma^{2} & \gamma^{5} & \gamma^{12} & \gamma^{5} & \gamma^{10} & \gamma^{8} & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & \\
\gamma^{11} & . & . & . & \gamma^{4} & \gamma^{11} & . & . & \gamma^{0} & \gamma^{6} & \gamma^{8} & . & \gamma^{1} & \gamma^{12} & \gamma^{5} & \gamma^{10} & \gamma^{5} & & & & \\
\gamma^{4} & . & . & . & \gamma^{11} & \gamma^{10} & . & . & \gamma^{6} & \gamma^{8} & \gamma^{2} & . & \gamma^{12} & \gamma^{5} & \gamma^{10} & \gamma^{8} & & & & & \\
\gamma^{9} & . & . & . & \gamma^{10} & \gamma^{5} & . & . & \gamma^{8} & \gamma^{2} & \gamma^{5} & . & \gamma^{5} & \gamma^{10} & \gamma^{8} & & & & & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & & & & \\
\gamma^{4} & . & . & . & \gamma^{4} & \gamma^{11} & . & . & \gamma^{1} & \gamma^{12} & \gamma^{5} & . & \gamma^{5} & & & & & & & & \\
\gamma^{11} & . & . & . & \gamma^{11} & \gamma^{10} & . & . & \gamma^{12} & \gamma^{5} & \gamma^{10} & . & & & & & & & & & \\
\gamma^{10} & . & . & . & \gamma^{10} & \gamma^{5} & . & . & \gamma^{5} & \gamma^{10} & \gamma^{8} & & & & & & & & & & \\
\gamma^{5} & . & . & . & \gamma^{5} & \gamma^{0} & . & . & \gamma^{10} & \gamma^{8} & & & & & & & & & & & \\
\gamma^{4} & . & . & . & \gamma^{1} & \gamma^{12} & . & . & \gamma^{5} & & & & & & & & & & & & \\
\gamma^{11} & . & . & . & \gamma^{12} & \gamma^{5} & . & . & & & & & & & & & & & & & \\
\gamma^{10} & . & . & . & \gamma^{5} & \gamma^{10} & . & & & & & & & & & & & & & & \\
\gamma^{5} & . & . & . & \gamma^{10} & \gamma^{8} & & & & & & & & & & & & & & & \\
\gamma^{1} & . & . & . & \gamma^{5} & & & & & & & & & & & & & & & & \\
\gamma^{12} & . & . & . & & & & & & & & & & & & & & & & & \\
\gamma^{5} & . & . & & & & & & & & & & & & & & & & & & \\
\gamma^{10} & . & & & & & & & & & & & & & & & & & & & \\
\gamma^{5} & & & & & & & & & & & & & & & & & & & &
\end{array}
$$

1	·	·	·	14	2	·	·	11	4	9	·	4	11	10	5	0	6	8	2	1	12	5	10	5
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·		
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·			
14	·	·	·	11	4	·	·	4	11	10	·	0	6	8	2	1	12	5	10	5				
2	·	·	·	4	9	·	·	11	10	5	·	6	8	2	5	12	5	10	8					
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·						
·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·							
11	·	·	·	4	11	·	·	0	6	8	·	1	12	5	10	5								
4	·	·	·	11	10	·	·	6	8	2	·	12	5	10	8									
9	·	·	·	10	5	·	·	8	2	5	·	5	10	8										
·	·	·	·	·	·	·	·	·	·	·	·	·	·											
4	·	·	·	4	11	·	·	1	12	5	·	5												
11	·	·	·	11	10	·	·	12	5	10	·													
10	·	·	·	10	5	·	·	5	10	8														
5	·	·	·	5	0	·	·	10	8															
4	·	·	·	1	12	·	·	5																
11	·	·	·	12	5	·	·																	
10	·	·	·	5	10	·																		
5	·	·	·	10	8																			
1	·	·	·	5																				
12	·	·	·																					
5	·	·																						
10	·																							
5																								



γ^0					γ^1							
γ^{13}	γ^0				0	γ^0						
γ^7	γ^1				0	0						
γ^0					γ^5							
γ^3	γ^{14}	γ^0			0	0	0	0	γ^{12}			
0					0	0	0					
					0	0						
					0							
γ^7	γ^{14}	γ^1			0	0	0	0	0	0	0	
γ^0	γ^0				0	0	0	0	0	0		
					0	0	0	0	0			
					0	0	0	0				
γ^7	γ^{14}	0			0	0	0	0	0	0	0	
γ^0	γ^1				0	0	0	0	0	0		
γ^0					0	0	0	0	0			
					0	0	0					
0	γ^3	γ^{14}	γ^0		0	0	0	γ^{12}				
0	0				0	0						
0					0							
0	0	γ^3	γ^{14}	γ^0	0	0	γ^{12}					
0	0	0			0							
0	0											
0												
0	γ^{12}	0	0	γ^0	γ^0	0	0	0	0	0		
γ^{11}	0	0	0			0	0	0				
0	0	0				0	0					
0	0					0						

So a minmal, reduced Gröbner basis for the error-locator ideal I is

$$yx + x^2 + y + x,\ y^2 + x^2 + \gamma^4 y + \gamma^4 x,\ x^5 + x^4 + \gamma^{11} y + \gamma^{12} x$$

relative to a weighted grevlex order with $wt(y) = 5$ and $wt(x) = 4$.

A factored lex basis is

$$x(x+1)(x^4 + x^3 + 1),\ (x+1)(y+x),\ y^2 + \gamma^4 y + x^2 + \gamma^4 x.$$

So the variety (of error positions) is

$$(0,0),\ (\gamma,1),\ (\gamma^7,\gamma^7),\ (\gamma^{14},\gamma^{14}),\ (\gamma^{13},\gamma^{13}),\ (\gamma^{11},\gamma^{11}).$$

As a *warning*, there are two types of AG codes– the type above which uses syndrome decoding is based on the assumption that the *parity-check* matrix H has entries of the form $f_i(P_j)$ for the appropriate choice of (rational, homogeneous) functions and (projective, rational) points; the other type being dual to these is based on the assumption that the *generator* matrix G has entries of the form $f_i(P_j)$, a so-called *functional encoding* used when talking about *list-decoding*.

For Reed-Solomon codes and some other AG codes *both* the codes and their duals have such entries, but that is not true for most AG codes.

Interpolation

Given a codeword $\underline{c} = (c_0, \ldots, c_{n-1})$ with $\underline{c}_i = m(x_i)$ for $0 \leq i < n$, it may be possible to recover $m(x) := \sum_{j=0}^{k-1} m_j x^j$ from a received word $\underline{r} = (r_0, \ldots, r_{n-1})$ by interpolation. First define an ordering by the matrix $M := \begin{pmatrix} k-1 & 1 \\ 1 & 0 \end{pmatrix}$, so that $(\gamma, \delta) \succ (\alpha, \beta)$ iff $(k-1)\gamma + \delta > (k-1)\alpha + \beta$ or $(k-1)\gamma + \delta = (k-1)\alpha + \beta$ and $\delta > \beta$. Then start with $f_{0,1}^{(0)}(r, x) := x - x_0$, $f_{1,0}^{(0)}(r, x) := r - r_0$, interpolating the zero-th pair (r_0, x_0). Recursively

1. compute $f_{\alpha,\beta}^{(i)}(r_{i+1}, x_{i+1})$;
2. find (α, β) *smallest* with $f_{\alpha,\beta}^{(i)}(r_{i+1}, x_{i+1})$;

3. for $(\gamma, \delta) \neq (\alpha, \beta)$ define

$$f^{(i+1)}_{\gamma,\delta}(r, x) := f^{(i)}_{\gamma,\delta}(r, x) - \frac{f^{(i)}_{\gamma,\delta}(r_{i+1}, x_{i+1})}{f^{(i)}_{\alpha,\beta}(r_{i+1}, x_{i+1})} f^{(i)}_{\alpha,\beta}(r, x)$$

4. if necessary, let

$$f^{(i+1)}_{\alpha,\beta+1}(r, x) := (x - x_{i+1}) f^{(i)}_{\alpha,\beta}(r, x))$$

$$f^{(i)}_{\alpha+1,\beta}(r, x)) := (r - r_{i+1}) f^{(i)}_{\alpha,\beta}(r, x)$$

Then find factors of the form $r - m(x)$ of $f^{(n-1)}_{\alpha,\beta}(r, x)$.

The following is the input for a Reed-Slomon example over $\mathbf{F}_{16}$.

$$\underline{r} = (\gamma^{14}, 0, \gamma^6, \gamma^{11}, 0, \gamma, \gamma^3, \gamma^6, \gamma^{10}, \gamma^6, \gamma^{10}, \gamma^2, \gamma^{11}, 1, \gamma^3, \gamma^2)$$

relative to

$$\underline{x} = (1, \gamma^1, \gamma^2, \gamma^3, \gamma^4, \gamma^5, \gamma^6, \gamma^7, \gamma^8, \gamma^9, \gamma^{10}, \gamma^{11}, \gamma^{12}, \gamma^{13}, \gamma^{14}, 0).$$

Two of the Gröbner basis elements produced by interpolation factor as:

$$(r + \gamma^7 x^3 + \gamma^6 x^2 + \gamma^7 x + \gamma^2)(r + \gamma^{14} x^3 + \gamma^7 x^2 + \gamma^4 x + \gamma^3)$$

and

$$x(x + \gamma^3)(x + \gamma^4)(x + \gamma^5)(r + \gamma^{14} x^3 + \gamma^7 x^2 + \gamma^4 x + \gamma^3).$$

And $m(x) = \gamma^{14} x^3 + \gamma^7 x^2 + \gamma^4 x + \gamma^3$ interpolates all the pairs except possibly the four with $x \in \{\gamma^3, \gamma^4, \gamma^5, 0\}$.

Modular curve example

Let

$$p_I(T) := \sum_{k=0}^{m} a_k T^k \in_q [T]$$

be monic and irreducible. Define inductively, $P_k \in_q [x, y]$ by $P_0(x, y) := 1$ and

$$P_{k+1}(x, y) := xP_k(x, y)^{q^2} + yP_k(x, y)^q \quad \text{for } k \geq 0.$$

Then let

$$F(x, y) = F_I(x, y) := \sum_{k=0}^{m} a_k P_k(x, y).$$

The equation $F_I(x, y) = 0$ is an analogue of the modular equation.

As a small example, let $q := 2$ and $p_I(T) := 1 + T + T^3$. Then

$$P_1(x, y) = x + y, \quad P_2(x, y) = x^5 + x^2y + xy^4 + y^3,$$

$$P_3(x, y) = x^{21} + x^{10}y + x^9y^4 + x^5y^{16} + x^4y^3 + x^2y^9 + xy^{12} + y^7,$$

$$F(x, y) = x^{21}+x^{10}y+x^9y^4+x^5y^{16}+x^4y^3+x^2y^9+x(y^{12}+1)+(y^7+y+1).$$

Start by using $x_1 := x$ and $x_2 := y + x$ to get

$$x_1^5(x_2^{16}+x_2^8)+x_1^3(x_2^8+x_2^4)+x_1^2(x_2^9+x_2^5)+x_1(x_2^{12}+x_2^6)+(x_2^7+x_2+1),$$

$$(x_1) = (-8) \cdot P_1 + (-4) \cdot P_2 + (-4) \cdot P_3 + 5 \cdot P_4 + 4 \cdot P_5 + \sum_{j=1}^{7} 1 \cdot Q_j,$$

$$(x_2) = 0 \cdot P_1 + 2 \cdot P_2 + 3 \cdot P_3 + (-1) \cdot P_4 + (-4) \cdot P_5 + \sum_{j=1}^{7} 0 \cdot Q_j.$$

Use $y_2 := x_1 x_2$ to get

$$x_1^{11} + x_1^{10}(y_2^4 + y_2) + x_1^8(y_2^8 + y_2^5) + x_1^6(y_2^8 + y_2^6) + x_1^4(y_2^9 + y_2^7) + (y_2^{16} + y_2^{12}),$$

$$(y_2) = (-8) \cdot P_1 + (-2) \cdot P_2 + (-1) \cdot P_3 + 4 \cdot P_4 + 0 \cdot P_5 + \sum_{j=1}^{7} 1 \cdot Q_j.$$

Use $y_1 := x_1/y_2$, to get

$$y_1^{11} + y_1^{10}(y_2^3 + 1) + y_1^8(y_2^5 + y_2^2) + y_1^6(y_2^3 + y_2) + y_1^4(y_2^2 + 1) + (y_2^5 + y_2),$$

$$(y_1) = 0 \cdot P_1 + (-2) \cdot P_2 + (-3) \cdot P_3 + 1 \cdot P_4 + 4 \cdot P_5 + \sum_{j=1}^{7} 0 \cdot Q_j.$$

Use $z_2 := y_2(y_1 + 1)^2$ to get

$$z_2^5 + z_2^3 y_1^6 + z_2^2(y_1^6 + y_1^4) + z_2(y_1^6 + 1) + y_1^4(y_1 + 1)^2(y_1^7 + y_1 + 1),$$

$$(z_2) = 2 \cdot P_1 + (-6) \cdot P_2 + (-7) \cdot P_3 + 4 \cdot P_4 + 0 \cdot P_5 + \sum_{j=1}^{7} 1 \cdot Q_j.$$

Use

$$h_{21} := y_1^7 + z_2^2 y_1 + z_2 y_1^2 + z_2 + y_1^2,$$

$$h_{25} := z_2 y_1^6 + z_2^3 + z_2^2 y_1 + z_2 y_1 + y_1^5 + y_1^3 + y_1^2 + 1,$$

to get

$$h_{25}^{21} + h_{25}^{20}h_{21} + h_{25}^{18}(h_{21}^{3} + h_{21} + 1) + h_{25}^{17}(h_{21}^{3} + 1)$$

$$+h_{25}^{16}(h_{21}^{4} + h_{21}) + h_{25}^{15}(h_{21}^{7} + h_{21}^{6} + h_{21}^{3} + h_{21} + 1) + h_{25}^{14}h_{21}^{7}$$

$$+h_{25}^{13}(h_{21}^{8} + h_{21}^{7} + h_{21}^{6} + h_{21}^{4} + h_{21}^{3} + 1) + h_{25}^{12}(h_{21}^{9} + h_{21}^{8} + h_{21}^{4} + 1)$$

$$+h_{25}^{11}(h_{21}^{11} + h_{21}^{9} + h_{21}^{8} + h_{21}^{5} + h_{21}^{4} + h_{21}^{3} + h_{21}^{2})$$

$$+h_{25}^{10}(h_{21}^{12} + h_{21}^{9} + h_{21}^{8} + h_{21}^{7} + h_{21}^{5} + h_{21}^{3} + h_{21} + 1)$$

$$+h_{25}^{9}(h_{21}^{14} + h_{21}^{13} + h_{21}^{10} + h_{21}^{9} + h_{21}^{8} + h_{21}^{7} + h_{21}^{6} + h_{21}^{3} + h_{21}^{2} + 1)$$

$$+h_{25}^{8}(h_{21}^{13} + h_{21}^{9} + h_{21}^{8} + h_{21}^{6} + h_{21}^{4} + h_{21}^{3} + h_{21})$$

$$+h_{25}^{7}(h_{21}^{16} + h_{21}^{15} + h_{21}^{13} + h_{21}^{12} + h_{21}^{11} + h_{21}^{7} + h_{21}^{3} + h_{21})$$

$$+h_{25}^{6}(h_{21}^{17} + h_{21}^{16} + h_{21}^{13} + h_{21}^{9} + h_{21}^{8} + h_{21})$$

$$+h_{25}^{5}(h_{21}^{17} + h_{25}^{16} + h_{25}^{12} + h_{21}^{7} + h_{21}^{5} + h_{21}^{2} + h_{21} + 1)$$

$$+h_{25}^{4}(h_{21}^{19} + h_{21}^{16} + h_{21}^{15} + h_{21}^{12} + h_{21}^{6} + h_{21}^{5} + h_{21}^{3} + 1)$$

$$+h_{25}^{3}(h_{21}^{18} + h_{21}^{15} + h_{21}^{12} + h_{21}^{10} + h_{21}^{9} + h_{21}^{7} + h_{21}^{4} + h_{21})$$

$$+h_{25}^{2}(h_{21}^{22} + h_{21}^{21} + h_{21}^{20} + h_{21}^{18} + h_{21}^{13} + h_{21}^{12} + h_{21}^{9} + h_{21}^{8} + h_{21}^{7} + h_{21}^{5} + h_{21}^{4} + h_{21}^{3})$$

$$+h_{25}(h_{21}^{23} + h_{21}^{22} + h_{21}^{20} + h_{21}^{17} + h_{21}^{15} + h_{21}^{14} + h_{21}^{12} + h_{21}^{9})$$

$$+(h_{21}^{25} + h_{21}^{23} + h_{21}^{19} + h_{21}^{17} + h_{21}^{15} + h_{21}^{13} + h_{21}^{11} + h_{21}^{5}).$$

But then the q-th power algorithm produces the integral closure:

$$\mathbf{F}_2[h_{16}, h_{15}, h_{13}, h_{12}, h_{11}, h_{10}, h_7]/I;$$

with I having Gröbner basis consisting of

$$h_{10}^2 + h_{13}h_7 + h_{11}h_7 + h_{10}h_7 + h_{15} + h_{13},$$

$$h_{11}h_{10} + h_7^3 + h_{13}h_7 + h_{15} + h_{13} + h_{11} + h_{10},$$

$$h_{11}^2 + h_{15}h_7 + h_{13}h_7 + h_{12}h_7 + h_{15} + h_{13} + h_{11} + h_{10},$$

$$h_{12}h_{10} + h_{15}h_7 + h_{13}h_7 + h_{12}h_7 + h_{12},$$

$$h_{12}h_{11} + h_{16}h_7 + h_{12}h_7 + h_{10}h_7,$$

$$h_{12}^2 + h_{10}h_7^2 + h_{16}h_7 + h_{15}h_7 + h_7^3 + h_{13}h_7 + h_{12}h_7 + h_{11}h_7 + h_{14} + h_{12} + h_7,$$

$$h_{13}h_{10} + h_{16}h_7 + h_{15}h_7 + h_{13}h_7 + h_{12}h_7 + h_{11}h_7 + h_7^2 + h_{12} + h_7,$$

$$h_{13}h_{11} + h_{10}h_7^2 + h_{16}h_7 + h_{11}h_7 + h_{13} + h_{10} + h_7 + 1,$$

$$h_{13}h_{12} + h_{11}h_7^2 + h_{15}h_7 + h_{12},$$

$$h_{13}^2 + h_{12}h_7^2 + h_{10}h_7^2 + h_{15}h_7 + h_{15}h_7^2 + 1,$$

$$h_{15}h_{10} + h_{11}h_7^2 + h_{13}h_7 + h_{15} + h_7,$$

$$h_{15}h_{11} + h_{12}h_7^2 + h_{11}h_7^2 + h_{10}h_7^2 + h_{15}h_7 + h_{13}h_7 + h_{15} + h_7^2 + h_7,$$

$$h_{15}h_{12} + h_{13}h_7^2 + h_{12}h_7^2 + h_{10}h_7^2 + h_{15}h_7,$$

$$h_{15}h_{13} + h_7^4 + h_{13}h_7^2 + h_{12}h_7^2 + h_{10}h_7^2 + h_{15}h_7 + h_{10}h_7 + h_7^2 + h_7,$$

$$h_{15}^2 + h_{16}h_7^2 + h_7^4 + h_{12}h_7^2 + h_{11}h_7^2 + h_{10}h_7^2 + h_{15}h_7 + h_{10}h_7 + h_{15} + h_7^2 + h_7,$$

$$h_{16}h_{10} + h_{12}h_7^2 + h_{11}h_7^2 + h_{13}h_7 + h_{16} + h_{10} + h_7 + 1,$$

$$h_{16}h_{11} + h_{13}h_7^2 + h_{11}h_7^2 + h_{15}h_7 + h_{13}h_7 + h_{12}h_7 + h_{16} + h_7^2 + h_{11} + h_7 + 1,$$

$$h_{16}h_{12} + h_7^4 + h_{12}h_7^2 + h_{11}h_7^2 + h_{10}h_7^2 + h_{16}h_7 + h_{12}h_7 + h_{12} + h_7,$$

$$h_{16}h_{13} + h_7^4 + h_{13}h_7^2 + h_{10}h_7^2 + h_{16}h_7 + h_{10}h_7 + h_{16} + h_{15} + h_7^2 + h_{13} + 1,$$

$$h_{16}h_{15} + h_{10}h_7^3 + h_7^4 + h_{12}h_7^2 + h_{11}h_7^2 + h_{10}h_7^2 + h_{15}h_7 + h_7^3 + h_{10}h_7 + h_7,$$

$$h_{16}^2 + h_{11}h_7^3 + h_{16}h_7^2 + h_{15}h_7^2 + h_7^4 + h_{13}h_7^2 + h_{15}h_7 + h_{12}h_7 + h_{10}h_7 + h_{16} + h_7^2 + h_7.$$

As a by-product, the smallest type I representation (relative to this choice of P_∞) would then be in terms of the single polynomial relating h_{10} and h_7:

$$h_{10}^7 + h_{10}^6 h_7 + h_{10}^5(h_7^2+1) + h_{10}^4(h_7+1) + h_{10}^3(h_7^5+h_7^4+h_7^2+1) + h_{10}^2(h_7^7+h_7^6+h_7^3+h_7^2+1)$$

$$+h_{10}(h_7^7+h_7^6+h_7^5+1) + (h_7^{10}+h_7^9+h_7^8+h_7^7+h_7^4+h_7^3+h_7^2+h_7+1).$$

So even to find a proper set of parity-check functions $h_i h_7^j$ for $i \in \{0, 10, 11, 12, 13, 15, 16\}$ it is necessary to compute Gröbner bases.

The best reference for further reading about AG codes is still Chapter 10 of the Handbook of Coding Theory, written by Høholdt, van Lint, and Pellikaan (with editors Pless and Huffman), Elsevier, 1998. This has an extensive bibliography pre-1998.

For a better intro to list-decoding of AG codes, the author prefers the paper by Høholdt and Nielsen, Decoding Hermitian Codes with Sudan's algorithm, AAECC-13, Springer, 1999;

For interesting reading on list-decoding, Forney functions, and other topics, try the last 5 or so years of IEEE Transactions on Information Theory.

For producing good codes start with the paper by Beelen, Garcia, and Stichtenoth, Towards a classification of recursive towers of function fields, in Finite Fields and their Applications, 2006. But to understand how to put these in a proper form for coding, try the paper by Leonard and Pellikaan, Integral closures and weight functions over finite fields, 2003 in the same journal.