A tutorial on AG code decoding

from a Gröbner basis perspective

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

1 Introduction

The notation and AG code description were set up in the author's previous chapter in this volume. While syndrome decoding of RS codes dates back at least to the 60's, the syndrome decoding of AG codes should be viewed in terms of Sakata's generalization of the Berlekamp-Massey algorithm (see his chapters of this volume) and Feng and Rao's majority voting scheme [2] to decode up to the designed minimum distance.

Sudan popularized list-decoding, but the important follow-up papers are [3] (for a much more readable introduction to Sudan's ideas), and [8], [9], and [1] for three differently flavored views on implementing these ideas.

2 Functional decoding of RS codes and AG codes using syndromes and error-locator ideals

Moving from RS codes to AG codes means moving theoretically from *univariate polynomial rings* to *multivariate polynomial rings*. In univariate polynomial rings all *ideals* are *principal* (that is, have a single generator), so finding generators for the *error-locator ideals* is equivalent to finding a single *error-locator polynomial*. The generalization to multivariate polynomial rings is to finding *Gröbner bases* for the error-locator ideals, that is ideal bases with leading monomials that divide leading monomials of any elements in the ideal.

Syndrome decoding algorithms recursively compute such Gröbner bases that are consistent with the initial part of the sequence of syndromes; that is, $\sum_{i=0}^{t} \sigma_i s_{i+j} = 0$. If there is an error of smallest weight $t \le e$, then the Δ-*set* produced by such algorithms will have size t, and the *variety* of the ideal will also have size t.

Let $\mathbf{F}_{2^4} := \mathbf{F}_2[\gamma]/\langle 1 + \gamma + \gamma^4 \rangle$. Consider the example syndrome vector (consisting of functions $\underline{e}Eval^T = \underline{r}Eval^T$ of the supposed error $\underline{e}$ of weight t at most 3:

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

relative to the underlying functions $(x^i : 0 \leq i \leq 5)$, which is a shiftable shorthand for the (backshifted or Hankel) syndrome matrix

$$S := Eval\Delta(\underline{r})Eval^T = \begin{pmatrix} 0 & \gamma^1 & \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 \\ \gamma^1 & \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 & \\ \gamma^1 & \gamma^2 & \gamma^{13} & \gamma^1 & & \\ \gamma^2 & \gamma^{13} & \gamma^1 & & & \\ \gamma^{13} & \gamma^1 & & & & \\ \gamma^1 & & & & & \end{pmatrix}$$

with (i,j)-th entry clearly of the form $\sum_P x^i(P)r(P)x^j(P)$. (In matrix terminology, an error-locator polynomial corresponds to a linear dependence $\underline{\sigma}$ among the rows of S; which can be gotten (inefficiently) by simple row-reduction techniques.

The *Berlekamp-Massey algorithm*, the *extended Euclidean algorithm*, or even the standard matrix row-reduction will produce recursively at least the sequence $1 + 0x$, $\gamma^4 + x + x^2$, and $\sigma(x) := \gamma^4 + \gamma^{14}x + \gamma^7x^2 + x^3$, consistent with initial parts of the total sequence of syndromes, with the former two being more efficient, in that they take advantage of the back-shifted nature of the matrix to avoid recalculating intermediate results.

The factorization $\sigma(x) = (x + \gamma^0)(x + \gamma^1)(x + \gamma^3)$ gives the variety $\{\gamma^0, \gamma^1, \gamma^3\}$ of *error positions* from which various other algorithms can be used to produce the *error magnitudes*.

Consider an example for the *Hermitian code* with affine definition given by the single generator $f := x_2^4 + x_2 - x_1^5$ having $1+16+2\cdot 6\sqrt{16} = 65 > 1+16$ projective points (equal to the Hasse-Weil bound) rational over $\mathbf{F}_{16}$, and genus $g = 6$.

Since $f_4 := x_1$ has pole order 4 and $f_5 := x_2$, pole order 5 at the projective point $P_\infty := (1 : 0 : 0)$ at which these rational functions have all their poles, there are functions of the form $f_5^{i_5} f_4^{i_4}$ of every pole order other than the $g = 6$ values $1, 2, 3, 6, 7, 11$.

$\mathcal{L}(m \cdot P_\infty)$ is given by an $\overline{\mathbf{F}_2}[f_4]$-*module basis* $(1, f_5, f_5^2, f_5^3)$, and the curve $\mathcal{X}$ is defined by the *quotient ring*

$$\mathcal{Q} := \overline{\mathbf{F}}_2[f_5, f_4]/\mathcal{I},\ \mathcal{I} := \langle f_5^4 + f_4^5 + f_5 \rangle$$

with the monomial order a weighted total-degree order relative to the weights $(5, 4)$, the pole orders of the variables.

Consider the original example Feng and Rao [2] used to exemplify majority voting to determine extra syndromes (also used by this author [4] to introduce the idea of an error-locator ideal and the computation of a basis for same). The syndrome "vector" (now a 2-dimensional array, given that

there are two variables involved)

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

with entries $\sum_P r(P) f_5^i(P) f_4^j(P)$ relative to the underlying functions $h_{i,j} := f_5^i f_4^j$:

$$\left(\begin{array}{ccccccccc} 1 & f_4 & f_4^2 & f_4^3 & f_4^4 & f_4^5 & f_4^6 & f_4^7 & f_4^8 & f_4^9 \\ f_5 & f_5 f_4 & f_5 f_4^2 & f_5 f_4^3 & f_5 f_4^4 & f_5 f_4^5 & f_5 f_4^6 & f_5 f_4^7 & & \\ f_5^2 & f_5^2 f_4 & f_5^2 f_4^2 & f_5^2 f_4^3 & f_5^2 f_4^4 & f_5^2 f_4^5 & f_5^2 f_4^6 & & & \\ f_5^3 & f_5^3 f_4 & f_5^3 f_4^2 & f_5^3 f_4^3 & f_5^3 f_4^4 & f_5^3 f_4^5 & & & & \\ \hline f_5^4 & f_5^4 f_4 & f_5^4 f_4^2 & f_5^4 f_4^3 & f_5^4 f_4^4 & & & & & \\ f_5^5 & & & & & & & & & \end{array}\right)$$

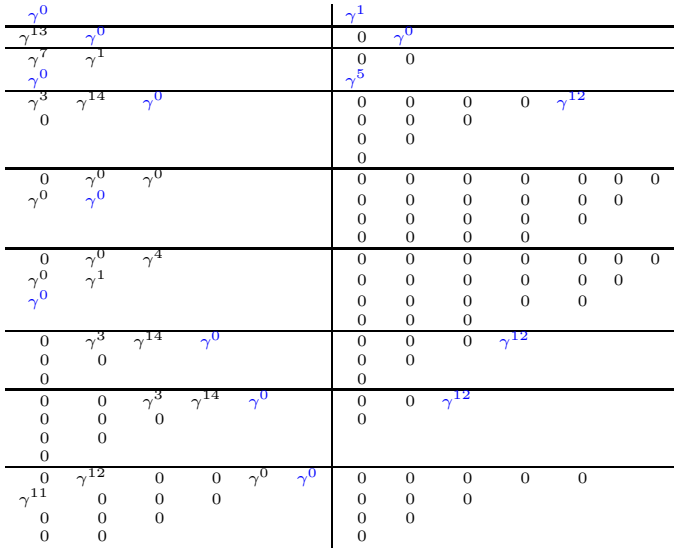
is a shorthand (shiftable in both directions) for the (almost backshifted) syndrome matrix $S := Eval\Delta(\underline{r})Eval^T = Eval\Delta(\underline{e})Eval^T$:

$$\begin{array}{cccccccccccccccccccccccc} \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^1 & \gamma^{12} & \gamma^5 & \gamma^{10} & \gamma^5 \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & \\ . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & & \\ \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}$$

with (4i+k,4j+l)-th entry clearly of the form $\sum_P f_5^k(P) f_4^{i-k}(P) r(P) f_5(P)^l f_4^{j-l}(P)$.

The algorithm producing the following computations of pairs, $(\sum_h \sigma_{f,h} h, \sum_h \sigma_{f,h} s_h)$, is simply a multi-dimensional row-reduction and shifting algorithm, a version of the *Berlekamp-Massey-Sakata algorithm* discussed elsewhere in this

volume:



The *minimal*, (*unreduced*) *Gröbner basis* for the error-locator ideal $\mathcal{I}$ can be read off from the left-hand side entries, with corresponding right-hand side zero as:

$$f_5 f_4 + f_4^2 + f_5 + f_4,\ f_5^2 + \gamma^1 f_5 f_4 + \gamma^4 f_4^2 + \gamma^0 f_5 + \gamma^0 f_4,\ f_4^5 + f_4^4 + \gamma^{11} f_5 + \gamma^{12} f_4$$

relative to the implicit *weighted total-degree* order induced by the pole orders. This is consistent with the syndromes computed from the received word (or those computed, given the extra assumption that the error weight and hence the rank of S is at most 6) in the sense that $\sum_h \sigma_{f,h} s_h = 0$ for each $\sigma_f := \sum_h \sigma_{f,h} h$ in the basis.

A *factored lex basis*

$$f_4(f_4+1)(f_4^4+f_4^3+1)\cdot 1,\ (f_4+1)\cdot(f_5+f_4),\ 1\cdot(f_5^2+\gamma^4 f_5+f_4^2+\gamma^4 f_4)$$

can be used to find the *variety* (of *error positions*) P_j with

$$(f_5(P_j), f_4(P_j)) \in \{(0,0),\ (\gamma,1),\ (\gamma^7,\gamma^7),\ (\gamma^{14},\gamma^{14}),\ (\gamma^{13},\gamma^{13}),\ (\gamma^{11},\gamma^{11})\},$$

$\{\gamma^7, \gamma^{14}, \gamma^{13}, \gamma^{11}\}$ being the set of roots of $x^4 + x^3 + 1$.

The following similar example in the handbook [7] is originally due to Sakata: The syndrome "vector" is

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

with $S =$

$$\begin{array}{cccccccccccccccccccccccccc}
\gamma^{9} & . & . & . & \gamma^{14} & 0 & . & . & \gamma^{5} & \gamma^{9} & \gamma^{9} & . & \gamma^{7} & \gamma^{14} & \gamma^{11} & \gamma^{6} & \gamma^{2} & \gamma^{12} & 0 & \gamma^{4} & \gamma^{5} & \gamma^{5} & \gamma^{12} & \gamma^{7} & \gamma^{0} & \gamma^{5} \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . \\
\gamma^{14} & . & . & . & \gamma^{5} & \gamma^{9} & . & . & \gamma^{7} & \gamma^{14} & \gamma^{11} & . & \gamma^{2} & \gamma^{12} & 0 & \gamma^{4} & \gamma^{5} & \gamma^{5} & \gamma^{12} & \gamma^{7} & \gamma^{0} & \gamma^{5} & & & & \\
0 & . & . & . & \gamma^{9} & \gamma^{9} & . & . & \gamma^{14} & \gamma^{11} & \gamma^{6} & . & \gamma^{12} & 0 & \gamma^{4} & \gamma^{5} & \gamma^{5} & \gamma^{12} & \gamma^{7} & \gamma^{7} & \gamma^{5} & & & & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & & & \\
\gamma^{5} & . & . & . & \gamma^{7} & \gamma^{14} & . & . & \gamma^{2} & \gamma^{12} & 0 & . & \gamma^{5} & \gamma^{5} & \gamma^{12} & \gamma^{7} & \gamma^{0} & \gamma^{5} & & & & & & & & \\
\gamma^{9} & . & . & . & \gamma^{14} & \gamma^{11} & . & . & \gamma^{12} & 0 & \gamma^{4} & . & \gamma^{5} & \gamma^{12} & \gamma^{7} & \gamma^{7} & \gamma^{5} & & & & & & & & & \\
\gamma^{9} & . & . & . & \gamma^{11} & \gamma^{6} & . & . & 0 & \gamma^{4} & \gamma^{5} & . & \gamma^{12} & \gamma^{7} & \gamma^{7} & \gamma^{6} & & & & & & & & & & \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & & & & & & & & & & & \\
\gamma^{7} & . & . & . & \gamma^{2} & \gamma^{12} & . & . & \gamma^{5} & \gamma^{5} & \gamma^{12} & . & \gamma^{0} & \gamma^{5} & & & & & & & & & & & & \\
\gamma^{14} & . & . & . & \gamma^{12} & 0 & . & . & \gamma^{5} & \gamma^{12} & \gamma^{7} & . & \gamma^{5} & & & & & & & & & & & & & \\
\gamma^{11} & . & . & . & 0 & \gamma^{4} & . & . & \gamma^{12} & \gamma^{7} & \gamma^{7} & . & & & & & & & & & & & & & & \\
\gamma^{6} & . & . & . & \gamma^{4} & \gamma^{5} & . & . & \gamma^{7} & \gamma^{7} & \gamma^{6} & & & & & & & & & & & & & & & \\
\gamma^{2} & . & . & . & \gamma^{5} & \gamma^{5} & . & . & \gamma^{0} & \gamma^{5} & & & & & & & & & & & & & & & & \\
\gamma^{12} & . & . & . & \gamma^{5} & \gamma^{12} & . & . & \gamma^{5} & & & & & & & & & & & & & & & & & \\
0 & . & . & . & \gamma^{12} & \gamma^{7} & . & . & & & & & & & & & & & & & & & & & & \\
\gamma^{4} & . & . & . & \gamma^{7} & \gamma^{7} & . & & & & & & & & & & & & & & & & & & & \\
\gamma^{5} & . & . & . & \gamma^{0} & \gamma^{5} & & & & & & & & & & & & & & & & & & & & \\
\gamma^{5} & . & . & . & \gamma^{5} & & & & & & & & & & & & & & & & & & & & & \\
\gamma^{12} & . & . & . & & & & & & & & & & & & & & & & & & & & & & \\
\gamma^{7} & . & . & & & & & & & & & & & & & & & & & & & & & & & \\
\gamma^{0} & . & & & & & & & & & & & & & & & & & & & & & & & & \\
\gamma^{5} & & & & & & & & & & & & & & & & & & & & & & & & & \\
\end{array}$$

The row-reduction computations are:

$$\begin{array}{cccccc|cccccccc}
\gamma^{0} & & & & & & \gamma^{9} & & & & & & & \\
\gamma^{5} & \gamma^{0} & & & & & 0 & \gamma^{8} & & & & & & \\
\hline
\gamma^{6} & \gamma^{1} & & & & & 0 & 0 & & & & & & \\
\gamma^{0} & & & & & & \gamma^{13} & & & & & & & \\
\hline
\gamma^{6} & \gamma^{11} & \gamma^{0} & & & & 0 & 0 & \gamma^{5} & & & & & \\
\gamma^{3} & & & & & & 0 & & & & & & & \\
\hline
\gamma^{1} & \gamma^{14} & 0 & & & & 0 & 0 & 0 & \gamma^{5} & & & & \\
\gamma^{13} & \gamma^{0} & & & & & 0 & 0 & & & & & & \\
 & & & & & & 0 & & & & & & & \\
\hline
\gamma^{11} & \gamma^{13} & 0 & & & & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\
\gamma^{13} & \gamma^{10} & & & & & 0 & 0 & 0 & 0 & 0 & 0 & & \\
\gamma^{0} & & & & & & 0 & 0 & 0 & 0 & 0 & & & \\
 & & & & & & 0 & 0 & 0 & & & & & \\
\hline
\gamma^{10} & 0 & \gamma^{5} & \gamma^{0} & & & 0 & 0 & 0 & & & & & \\
\gamma^{14} & \gamma^{3} & & & & & 0 & \gamma^{5} & & & & & & \\
0 & & & & & & & & & & & & & \\
\hline
\gamma^{4} & \gamma^{7} & \gamma^{3} & 0 & & & 0 & 0 & 0 & 0 & 0 & & & \\
\gamma^{1} & \gamma^{3} & \gamma^{0} & & & & 0 & 0 & 0 & & & & & \\
0 & & & & & & 0 & 0 & & & & & & \\
 & & & & & & 0 & & & & & & & \\
\hline
\gamma^{13} & \gamma^{3} & 0 & \gamma^{3} & \gamma^{0} & & 0 & 0 & 0 & 0 & & & & \\
\gamma^{2} & \gamma^{9} & 0 & \gamma^{3} & & & 0 & & & & & & & \\
0 & 0 & & & & & & & & & & & & \\
0 & & & & & & & & & & & & & \\
\hline
\gamma^{11} & 0 & 0 & 0 & 0 & \gamma^{0} & 0 & 0 & 0 & 0 & 0 & & & \\
\gamma^{11} & 0 & 0 & 0 & & & 0 & 0 & 0 & & & & & \\
0 & 0 & 0 & & & & 0 & 0 & & & & & & \\
0 & 0 & & & & & 0 & & & & & & & \\
\end{array}$$

so a minimal, reduced Gröbner basis for the error-locator ideal $\mathcal{I}$ is

$f_5^2+\gamma^{10}f_5f_4+\gamma^{13}f_5+\gamma^{13}f_4+\gamma^{11},\ f_5f_4^2+\gamma^4f_5f_4+\gamma^3f_4^2+\gamma^1f_5+\gamma^7f_4+\gamma^3,\ f_4^5\gamma^{11}f_5+\gamma^{11}.$

A factored lex basis is

$1\cdot(f_4+1)(f_4+\gamma^1)(f_4+\gamma^2)(f_4+\gamma^5)(f_4+\gamma^8)(f_4+\gamma^{11})(f_4+\gamma^{14}),\ (f_5+\gamma^4f_4^5+1)\cdot 1.$

and the variety (of error positions) is

$$(1,\gamma),\ (\gamma,\gamma^7),\ (\gamma^2,\gamma^3),\ (\gamma^5,\gamma^3),\ (\gamma^8,\gamma^3),\ (\gamma^{11},\gamma^3),\ (\gamma^{14},\gamma^3).$$

3 Interpolation to do list decoding for RS codes and AG codes

Sudan was first to suggest *list decoding* of a k-dimensional functionally-encoded RS code, by treating r and x as having weights $k-1$ and 1, respectively, in the polynomial ring $\mathbf{F}[r,x]$, interpolating the received pairs (r_i, x_i), and finding factors (linear in the variable r) of some resulting polynomial. For an example of such, consider the received word:

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

indexed by the elements of $\mathbf{F}_{16} := \mathbf{F}_2[\gamma]/\langle 1+\gamma+\gamma^4\rangle$:

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

for a functionally-encoded RS code with $k = 4$ (and $n = 16$). The MAGMA code

```
F16<c>:=FiniteField(16);
P<r,x>:=PolynomialRing(F16,2,"weight",[3,1,3,0]);
R:=[c^14,0  ,c^6,c^11,0  ,c^1,c^3,c^6,c^10,c^6,c^10,c^2 ,c^11,c^0 ,c^3 ,c^2];
X:=[c^0 ,c^1,c^2,c^3 ,c^4,c^5,c^6,c^7,c^8 ,c^9,c^10,c^11,c^12,c^13,c^14,0];
L<u,t>:=PolynomialRing(F16,2,"grevlex");
hpl:=function(i) return hom<P->L|R[i]+u,X[i]+t>; end function;
hlp:=function(i) return hom<L->P|u-R[i],t-X[i]>; end function;
tt:=function(f) return TrailingTerm(f); end function;
f_0_0:=(P!1)@hpl(1);0,0,1,tt(f_0_0);
f_0_1:=(f_0_0*t)@hlp(1)@hpl(2);0,1,2,tt(f_0_1);
f_0_2:=(f_0_1*t)@hlp(2)@hpl(3);0,2,3,tt(f_0_2);
f_0_3:=(f_0_2*t)@hlp(3)@hpl(4);0,3,4,tt(f_0_3);
f_1_0:=((((f_0_0*u)@hlp(1)@hpl(2)-c^14/c^4*f_0_1)@hlp(2)@hpl(3)
-c^13/c^13*f_0_2)@hlp(3)@hpl(4)-c^3/c^14*f_0_3)@hlp(4)@hpl(5);
1,0,5,tt(f_1_0);
f_0_4:=((f_0_3*t)@hlp(4)@hpl(5)-c^3/c^2*f_1_0)@hlp(5)@hpl(6);
0,4,6,tt(f_0_4);
f_1_1:=((f_1_0*t)@hlp(5)@hpl(6)-c^13/c^5*f_0_4)@hlp(6)@hpl(7);
1,1,7,tt(f_1_1);
f_0_5:=((f_0_4*t)@hlp(6)@hpl(7)-c^10/c*f_1_1)@hlp(7)@hpl(8);
0,5,8,tt(f_0_5);
f_1_2:=((f_1_1*t)@hlp(7)@hpl(8)-c^3/c*f_0_5)@hlp(8)@hpl(9);
1,2,9,tt(f_1_2);
f_0_6:=((f_0_5*t)@hlp(8)@hpl(9)-c^13/c^14*f_1_2)@hlp(9)@hpl(10);
0,6,10,tt(f_0_6);
f_1_3:=((f_1_2*t)@hlp(9)@hpl(10)-1/c^8*f_0_6)@hlp(10)@hpl(16);
1,3,16,tt(f_1_3);
f_2_0:=(((((((f_1_0*u)@hlp(5)@hpl(6)-c^6/c^5*f_0_4)@hlp(6)@hpl(7)
-c^11/c*f_1_1)@hlp(7)@hpl(8)-c^7/c*f_0_5)@hlp(8)@hpl(9)
-c^9/c^14*f_1_2)@hlp(9)@hpl(10)-c/c^8*f_0_6)@hlp(10)@hpl(16)
-c^3/c^3*f_1_3)@hlp(16);2,0,Factorization(f_2_0);
f_0_7:=(f_0_6*t)@hlp(10)@hpl(11);0,7,11,tt(f_0_7);
f_1_4:=(f_1_3*t)@hlp(16);1,4,Factorization(f_1_4);
f_0_8:=(f_0_7*t)@hlp(11)@hpl(12);0,8,12,tt(f_0_8);
f_0_9:=(f_0_8*t)@hlp(12)@hpl(13);0,9,13,tt(f_0_9);
f_0_10:=(f_0_9*t)@hlp(13)@hpl(14);0,10,14,tt(f_0_10);
f_0_11:=(f_0_10*t)@hlp(14)@hpl(15);0,11,15,tt(f_0_11);
f_0_12:=((f_0_11*t)@hlp(15)@hpl(16)-c^5/c^3*f_1_3)@hpl(16);
0,12;
```

produces output (slightly edited for readability)

$$f_{2,0} = r^2+crx^3+c^6x^6+c^{10}rx^2+c^{12}x^5+c^3rx+c^{12}x^4+c^6r+c^7x^3+c^{11}x^2+c^7x+c^5;$$

$$f_{1,4} := rx^4+c^{14}x^7+c^{13}rx^3+c^2x^6+c^2rx^2+c^{10}x^5+c^{12}rx+c^3x^4+c^{13}x^3+c^2x^2+x;$$

$$f_{0,12} := x^{12}+rx^8+c^2x^{11}+c^{11}rx^7+c^5x^{10}+c^9rx^6+c^7x^9+crx^5+c^{12}x^8+c^4rx^4$$

$$+c^{11}x^7 + c^4x^6 + crx^2 + c^{12}x^5 + c^7rx + c^3x^4 + c^{12}r + c^8x^3 + c^{14}$$

with weighted total degrees 6, 7, and 12 respectively. These form a Gröbner basis for the interpolating ideal. And any message with codeword at most 4 errors away from the received word must be a common root of the first two. Indeed,

$$f_{2,0} = (r + c^7x^3 + c^6x^2 + c^7x + c^2)(r + c^{14}x^3 + c^7x^2 + c^4x + c^3)$$

$$f_{1,4} = x(x + c^3)(x + c^4)(x + c^5)(r + c^{14}x^3 + c^7x^2 + c^4x + c^3)$$

with common root $M(x) = \gamma^{14}x^3 + \gamma^7x^2 + \gamma^4x + \gamma^3$; which interpolates all the pairs except possibly the four with $x \in \{\gamma^3, \gamma^4, \gamma^5, 0\}$. In general, it is necessary to use interpolation to some depth s greater than 1 to get *lists* of such messages that can correspond to nearest codewords, allowing decoding beyond the standard minimum distance bound $e < d/2$.

To generalize this to AG codes, as first suggested by Sudan and Guruswami, let $(f_0, f_\rho, \ldots, f_m)$ be a canonical vector-space basis (of size k) for $\mathcal{L}(m \cdot P_\infty)$ with increasing pole sizes $0, \rho, \ldots, m$ at P_∞ (and for $m > 2(g-1)$, this means $m + 1 = k + g$). It may be possible to directly recover a message $M := \sum_j m_j f_j$ from the received word $\underline{r} = (r_1, \ldots, r_n)$ by interpolation techniques. First extend the weighted total-degree ordering on $\mathcal{L}(m \cdot P_\infty)$ given by the matrix A to $\overline{A} := \begin{pmatrix} m & A \\ \underline{1}^T & \underline{0} \end{pmatrix}$ to extend it to an extra variable r representing the received word.

Since these f have all their poles at P_∞, the Laurent series at points $P_j \neq P_\infty$ must be just *power series*. So map $r \mapsto r(P_j) + u$ and each $f \in \mathcal{L}(m \cdot P_\infty)$ to its power series expansion, truncated to $t_j^i, i < s$ at P_j. *Depth-s interpolation* means finding functions with images having total degree (in u and t_j) at least s.

If $M(f_m, \ldots, f_0)$ is encoded as a codeword $\underline{c}$ at distance at most e from the received word $\underline{r}$ and $H(M(f_m, \ldots, f_0), f_m, \ldots, f_0) \in \mathcal{L}(((n-e)s-1) \cdot P_\infty)$, then $H(M(f_m, \ldots, f_0), f_m, \ldots, f_0)$ is a rational function with fewer than $(n-e)s$ poles but at least that many zeros. But that means that $H(M(f_m, \ldots, f_0), f_m, \ldots, f_0) \equiv 0$, so $r - M(f_m, \ldots, f_0) | H(r, f_m, \ldots, f_0)$. Thus any M that encodes to a word at most e errors away from r, will correspond to a common linear factor $r - M$ of all such H.

At each point P_j there are $\binom{s+1}{2}$ "bad" trailing terms $u^i t_j^\ell$, with $i + \ell < s$, so a total Δ-set of size $n\binom{s+1}{2}$. The smallest element $H(r, f_m, \ldots, f_0)$ of the interpolating Gröbner basis will be a combination of the first $1 + n\binom{s+1}{2}$ monomials in the order described by $\overline{A}$. There will be at least one such good function H guaranteed, interpolating $n - e$ of the n points, if interpolation to depth s is done, and there are more monomials $f \in \mathcal{L}(((n-e)s-1) \cdot P_\infty)$ than $n\binom{s+1}{2}$, the number of elements in the Δ-set. Simple combinatorial arguments can be used to determine the depth s needed to correct e errors

using this method. And some lists will have more than one entry when $e \geq d/2$, as in the example below with $d = 4$ and $e = 2$. (Initial papers on list decoding spent far too much time on this combinatorial aspect of the topic to the detriment of the more interesting interpolation and ideal-theoretic aspects.)

Consider the example from Høholdt and Nielsen [3] using the Hermitian curve with $q = 2$. This has 8 rational points $P_j := (x_2(P_j) : x_1(P_j) : 1)$ over $\mathbf{F}_4 := \mathbf{F}_2[\alpha]/\langle 1 + \alpha + \alpha^2 \rangle$ other than $P_\infty := (1 : 0 : 0)$. Let $f_2 := x_1$ and $f_3 := x_2$ to reflect the respective pole sizes at P_∞. Consider the values:

$f_2(P_j)$	0	0	1	1	α	α	α^2	α^2
$f_3(P_j)$	0	1	α	α^2	α	α^2	α	α^2
$r(P_j)$	α^2	0	0	α^2	0	0	0	0
$c_1(P_j)$	0	0	0	0	0	0	0	0
$c_2(P_j)$	α^2	α^2	α^2	α^2	0	0	0	0

for $M_1 := 0$ and $M_2 := \alpha^2(1 + f_2 + f_2^2)$. $A := \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix}$, so $\overline{A} := \begin{pmatrix} 4 & 3 & 2 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ for $m = 4$.

For $n = 8$ and $e = 2$, the size of the Δ-set and the number of monomials for various values of s are $\Delta(1) = 8 > 6$, $\Delta(2) = 24 > 21$, $\Delta(3) = 48 > 45$, $\Delta(4) = 80 > 78$, $\Delta(5) = 120 = 120$, and $\Delta(6) = 168 < 171$. For instance the standard monomials of weight less than 6 are $f_0, f_2, f_3, f_2^2, r, f_3 f_2$, and the others of weight less than 12 are

$$f_2^3, r f_2, f_3 f_2^2, r f_3, f_2^4, r f_2^2, r^2, f_3 f_2^3, r f_3 f_2, f_2^5, r f_2^3, r^2 f_2, f_3 f_2^4, r f_3 f_2^2, r^2 f_3.$$

So interpolating to depth 6 is guaranteed to produce at least 171-168=3 functions $H(r, f_3, f_2)$ for list decoding.

The functions f_2 and f_3 with pole orders 2 and 3 respectively at the point P_∞ at infinity, have series expansions $f_2 = x_1(P_j) + t_j$ and $f_3 = x_2(P) + \sum_{\ell=0}^{\infty}(x_1(P_j)^2 t_j + x_1(P_j) t_j^2 + t_j^3)^{2^\ell}$ at each other point P_j. But with $x_1(P_j) \in \mathbf{F}_4$ (so that $x_1(P_j)^4 + x_1(P_j) = 0$) and working $\mod t_j^6$, this reduces to $f_3 \equiv x_2(P_j) + x_1(P_j)^2 t_j + t_j^3$. So map r to $r(P_j) + u$ as well, and ask for functions with images having total degree (in u and t_j) at least 6. In this example there are $5 > 3$ $H(r, f_3, f_2)$'s, all with common roots $r = 0$ and $r = \alpha^2(1 + f_2 + f_2^2)$, the two messages listed above.

References

[1] D. Augot and L. Pecquet, "A Hensel lifting to replace factorization in list-decoding of algebraic-geometric and Reed-Solomon codes", IEEE Trans. Inform. Theory, vol. 46, pp. 2605-2614, Nov. 2000.

[2] G. L. Feng and T. R. N. Rao "Decoding of algebraic geometric codes up to the designed minimum distance", IEEE Trans. Inform. Theory, vol. 39, pp. 37-45, Jan. 1993.

[3] T. Høholdt and R. Nielsen "Decoding Hermitian codes with Sudan's algorithm", AAECC 13 (LNCS vol. 1719), N. Fossoeier, H. Imei, S. Lin, A. Polé, eds., Springer, Berlin, pp. 260-270, 1999.

[4] D. Leonard, "Error-locator ideals for algebraic-geometric codes", IEEE Trans. Inform. Theory, vol. 41, pp. 819-824, May, 1995.

[5]

[6] The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry. The University of Sydney Computational Algebra Group. `http://magma.maths.usyd.edu.au/magma`

[7] T. Høholdt, R. Pellikaan, and J. H. van Lint, Algebraic Geometry Codes, Handbook of Coding Theory, chapter 10, V. PLess and C. Huffman, eds., North Holland, Amsterdam, pp. 871-961, 1998.

[8] R. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance", IEEE Trans. Inform. Theory, vol. 46, pp. 246-257, Jan. 2000.

[9] X. W. Wu and P. H. Siegel, "Efficient root-finding algorithm with applications to list decoding of algebraic-geometric codes", IEEE Trans. Inform. Theory, vol. 47, pp. 2579-2586, Sept. 2001.