Finite Fields and Their Applications 18 (2012) 167–178

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Generic interpolation polynomial for list decoding

R.F. Lax

Department of Mathematics, LSU, Baton Rouge, LA 70803, United States

ARTICLE INFO

Article history:
Received 24 January 2011
Revised 16 May 2011
Accepted 17 July 2011
Available online 6 August 2011
Communicated by Shojiro Sakata

MSC:
94B27
94B30
14G50
13P10

Keywords:
List decoding
Interpolation polynomial
One-point AG code
Gröbner basis
Affine variety code

ABSTRACT

We extend results of K. Lee and M.E. O'Sullivan by showing how to use Gröbner bases to find the interpolation polynomial for list decoding a one-point AG code $C = C_L(rP, D)$ on any curve $\mathcal{X}$, where P is an $\mathbb{F}_q$-rational point on $\mathcal{X}$ and $D = P_1 + P_2 + \cdots + P_n$ is the sum of other $\mathbb{F}_q$-rational points on $\mathcal{X}$. We then define the generic interpolation polynomial for list decoding such a code. The generic interpolation polynomial should specialize to the interpolation polynomial for most received strings. We give an example of a family of Reed–Solomon 1-error correcting codes for which a single error can be decoded by a very simple process involving substituting into the generic interpolation polynomial.

1. Introduction

Let $\mathcal{X}$ be a nonsingular, absolutely irreducible, projective curve of genus g defined over the finite field $\mathbb{F}_q$. Let $C = C_L(rP, D)$ be a one-point algebraic geometry code such that P is an $\mathbb{F}_q$-rational point on $\mathcal{X}$ and $D = P_1 + P_2 + \cdots + P_n$ is the sum of other $\mathbb{F}_q$-rational points on $\mathcal{X}$. V. Guruswami and M. Sudan [11] gave an algorithm for list decoding C that, given a received string, requires the computation of an interpolation polynomial. Such a polynomial must vanish to certain multiplicities at certain points. This naturally gives rise to an ideal in a certain polynomial ring and the optimal interpolation polynomial can be characterized as an element in this ideal whose leading term is least with respect to a certain monomial order. This leads to a Gröbner basis approach to the determination of the interpolation polynomial, an approach that has been taken by H. O'Keeffe and P. Fitzpatrick [17]

E-mail address: lax@math.lsu.edu.

1071-5797/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2011.07.007

and K. Lee and M. E. O'Sullivan [12,13], among others. A recent survey article by E. Guerrini and A. Rimoldi [10] discusses Gröbner basis approaches to decoding, including list decoding.

Lee and O'Sullivan gave explicit generators for the above ideal in the case of Reed–Solomon codes and one-point Hermitian codes. We generalize their results by giving explicit generators for this ideal for any one-point code as above. It turns out that viewing the one-point code in the context of the affine variety codes of [6] is very helpful for this purpose. One could proceed to consider modules over this polynomial ring and use Gröbner bases for modules, as was done by O'Keeffe–Fitzpatrick, Lee–O'Sullivan, and P. Beelen and K. Brander [3], but we do not pursue that investigation here.

We go on to define a generic interpolation polynomial for C. This involves considering the components of a received string as *variables* instead of field elements. This is similar to the idea of considering syndromes as variables in the decoding of cyclic codes, an idea that goes back to A. Brinton Cooper [4]. This "Cooper philosophy" has been generalized and improved by several authors – see the recent papers [16] and [14] and the references cited therein. As an example, we give a family of 1-error correcting Reed–Solomon codes for which the generic interpolation polynomial may be easily computed. Using one of these codes, one can correct a single error by simply substituting into the generic interpolation polynomial to get the optimal interpolation polynomial for a given received string, solving some linear equations to find the "root" of this interpolation polynomial, and performing some evaluations to get the codeword associated to this root.

We thank William A. Adkins and James Oxley for very helpful conversations and the referees for their thoughtful comments.

2. List decoding for one-point AG codes

Let $\mathcal{X}$ be a nonsingular, absolutely irreducible, projective curve of genus g defined over $\mathbb{F}_q$. Let $C = C_L(rP, D)$ be a one-point AG code such that P is an $\mathbb{F}_q$-rational point on $\mathcal{X}$ and $D = P_1 + P_2 + \cdots + P_n$ is the sum of other $\mathbb{F}_q$-rational points on $\mathcal{X}$. We will assume that $\mathcal{X}$ is embedded in a projective space $\mathbb{P}^s_{\bar{\mathbb{F}}_q}$, where $\bar{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$, such that P is the only $\mathbb{F}_q$-rational point on the hyperplane at infinity. (One way to accomplish this is to embed the curve into a projective space using a linear system of the form $|NP|$, with $N \geqslant 2g + 1$.) Then the curve $\mathcal{X}_0 = \mathcal{X} \setminus \{P\}$ is an affine variety $V_{\bar{\mathbb{F}}_q}(J)$ for an ideal $J \subseteq \mathbb{F}_q[X_1, X_2, \ldots, X_s]$.

Put $A = \mathbb{F}_q[X_1, X_2, \ldots, X_s]$ and let $R = A/J$ denote the coordinate ring of $\mathcal{X}_0$. Then R is a Dedekind domain. Let $I \supseteq J$ be an ideal of A such that $V_{\mathbb{F}_q}(I) = \{P_1, P_2, \ldots, P_n\} = \operatorname{Supp}(D)$. We note that if D is the sum of all other $\mathbb{F}_q$-rational points on $\mathcal{X}$ besides P, then we can take $I = J$. Put

$$I_q = I + \langle X_1^q - X_1, X_2^q - X_2, \ldots, X_s^q - X_s \rangle \quad \text{and} \quad R_q = A/I_q.$$

Let $P_i = (a_{i1}, a_{i2}, \ldots, a_{is}), i = 1, 2, \ldots, n,$ and let $M_i = \langle X_1 - a_{i1}, X_2 - a_{i2}, \ldots, X_s - a_{is} \rangle, i = 1, 2, \ldots, n,$ denote the corresponding maximal ideals of A. Since I_q contains the polynomials $X_i^q - X_i, i = 1, 2, \ldots, s,$ it is an ideal of dimension 0, and we know, from Seidenberg's Lemma 92 ([18]; also see [2]), that it is a radical ideal, $V_{\bar{\mathbb{F}}_q}(I_q) = V_{\mathbb{F}_q}(I_q) = V_{\mathbb{F}_q}(I)$, and $I_q = \cap_{i=1}^n M_i$. It follows that the ring $R_q = A/I_q$ is an Artin ring of length n and that we have an isomorphism of $\mathbb{F}_q$-vector spaces

$$R_q \cong \oplus_{i=1}^n A/M_i.$$

We also have an isomorphism of $\mathbb{F}_q$-vector spaces

$$\phi : R_q \to \mathbb{A}^n,$$

$$\bar{f} \mapsto \bigl(f(P_1), f(P_2), \ldots, f(P_n)\bigr),$$

where f is any preimage of $\bar{f}$ in the polynomial ring A and $\mathbb{A}^n$ denotes the n-dimensional affine space over $\mathbb{F}_q$. The vector space $L(rP)$ may be identified with an $\mathbb{F}_q$-vector subspace L of R_q and the code C is then the image of L under the evaluation map ϕ. This amounts to viewing C as an affine variety code, as in [6] and [7]. A related ring-theoretic viewpoint for evaluation codes is also present in such articles as Matsumoto [15] and Geil and Pellikaan [8].

Example 1. In the case of the Reed–Solomon code of dimension k over $\mathbb{F}_q$, we have $R = \mathbb{F}_q[X], I = \langle X^{q-1} - 1\rangle, I_q = I$ and $L = L(kP)$ is the subspace with basis $\{1, x, x^2, \ldots, x^{k-1}\}$, where x denotes the residue class of X in R_q. If we take $I = \langle 0\rangle$ instead, then $I_q = \langle X^q - X\rangle, V(I_q) = \mathbb{A}^1$, and, with L as above, we get the extended Reed–Solomon code of dimension k.

In [6], we considered the decoding problem for affine variety codes. Under the assumption that there is a unique codeword within a given distance of a received string, we used Gröbner bases to solve equations arising from the syndrome of the received string. We also applied the "Cooper philosophy" (see [4] and [16]) to consider "universal" error locators obtained by treating syndromes as variables. These ideas were improved upon by Marcolla, Orsini, and Sala [14].

Here, we instead consider the problem of using a Gröbner basis to determine an interpolation polynomial for list decoding of a one-point AG code as above. Our work generalizes results of Lee and O'Sullivan [12,13] in the cases of Reed–Solomon codes and one-point Hermitian codes.

The first thing we need to do is to associate a polynomial to each n-tuple in $\mathbb{A}^n$. Fix polynomials $H_1, H_2, \ldots, H_n$ in A such that $H_i(P_j) = \delta_{ij}$. One way to do this would be to take

$$H_i(X_1, X_2, \ldots, X_s) = \prod_{j=1}^{s}\left[1 - (X_j - a_{ij})^{q-1}\right]. \tag{1}$$

In an application, one would like to find polynomials that have this property and have "small" degrees. Lee and O'Sullivan [13] give a formula in the Hermitian curve case for polynomials that have this property and have smaller degrees than the above H_i. Let h_i denote the residue class in R of H_i for $i = 1, 2, \ldots, n$. Following Lee and O'Sullivan, for $v = (v_1, v_2, \ldots, v_n) \in \mathbb{A}^n$, define

$$H_v = \sum_{i=1}^{n} v_i H_i$$

and let h_v denote the residue class of H_v in R. Note that $H_v(P_i) = v_i$ for $i = 1, 2, \ldots, n$.

Now, fix an n-tuple $v = (v_1, v_2, \ldots, v_n) \in \mathbb{A}^n$, which should be thought of as a received string. Put $P_{iv} = (a_{i1}, a_{i2}, \ldots, a_{is}, v_i)$ for $i = 1, 2, \ldots, n$. Let $M_{iv} = \langle X_1 - a_{i1}, X_2 - a_{i2}, \ldots, X_s - a_{is}, Z - v_i\rangle$ denote the maximal ideal in $A[Z]$ corresponding to P_{iv} for $i = 1, 2, \ldots, n$.

Proposition 2.

$$I_q + \langle Z - H_v\rangle = \cap_{i=1}^{n} M_{iv}.$$

Proof. If $f(X_1, \ldots, X_s) \in I_q$, then $f(P_{iv}) = f(P_i) = 0$ for $i = 1, 2, \ldots, n$. Also, $Z(P_{iv}) = H_v(P_{iv}) = v_i$ for $i = 1, 2, \ldots, n$. Hence, we have $I_q + \langle Z - H_v\rangle \subseteq \cap_{i=1}^{n} M_{iv}$. For the opposite inclusion, suppose $f(X_1, \ldots, X_s, Z) \in \cap_{i=1}^{n} M_{iv}$. Consider a lexicographic order on $A[Z]$ with Z greater than the X_i's and divide f by $Z - H_v$ to get $f = u(Z - H_v) + r$, with $u \in A[Z]$ and $r \in A$. Now, evaluate both sides at P_{iv}. Since $f \in \cap_{i=1}^{n} M_{iv}$, we have $f(P_{iv}) = 0$. Since $H_v(P_{iv}) = H_v(P_i) = v_i$, we have $(Z - H_v)(P_{iv}) = 0$. Hence $r(P_{iv}) = r(P_i) = 0$ for $i = 1, 2, \ldots, n$. Therefore, $r \in I_q$, since I_q is a radical ideal. □

Let $x_1, x_2, \dots, x_s$ denote the respective residue classes of $X_1, X_2, \dots, X_s$ in R. The maximal ideal M_{iv} in $A[Z]$ then corresponds to the maximal ideal $\overline{M}_{iv} = \langle x_1 - a_i1, \dots, x_s - a_is, Z - v_i\rangle$ in the ring $R[Z]$. It follows from the above proposition that in $R[Z]$ we have

$$(I/J)R[Z] + \langle x_1^q - x_1, x_2^q - x_2, \dots, x_s^q - x_s, Z - h_v\rangle = \cap_{i=1}^n \overline{M}_{iv}.$$

Put

$$\bar{I}_{m,v} = \left((I/J)R[Z] + \langle x_1^q - x_1, x_2^q - x_2, \dots, x_s^q - x_s, Z - h_v\rangle\right)^m.$$

Remark 3. In [13], the authors deal with one-point codes on the Hermitian curve $Y^q + Y = X^{q+1}$ over the field $\mathbb{F}_{q^2}$ and they consider the ideal $\langle x^{q^2} - x, Z - h_v\rangle^m$. In this case, we have $I = J = \langle Y^q + Y - X^{q+1}\rangle$ and notice that $Y^{q^2} - Y \in \langle Y^q + Y - X^{q+1}, X^{q^2} - X\rangle$ since

$$Y^{q^2} - Y = \left(Y^q + Y - X^{q+1}\right)^q - \left(Y^q + Y - X^{q+1}\right) + X^q\left(X^{q^2} - X\right).$$

It follows that in this case the ideal that they consider is the same as our ideal $\bar{I}_{m,v}$.

Corollary 4. *For any positive integer m,*

$$\bar{I}_{m,v} = \cap_{i=1}^n \overline{M}_{iv}^m.$$

Proof. From [1, Prop. 1.10], we know that the intersection of pairwise comaximal ideals equals the product of these ideals. It follows that

$$\cap_{i=1}^n \overline{M}_{iv}^m = \prod_{i=1}^n \overline{M}_{iv}^m = \left(\prod_{i=1}^n \overline{M}_{iv}\right)^m = \left(\cap_{i=1}^n \overline{M}_{iv}\right)^m = \bar{I}_{m,v}. \qquad \square$$

It then follows from the Chinese Remainder Theorem that we have an isomorphism of rings

$$R[Z]/\bar{I}_{m,v} \xrightarrow{\cong} \prod_{i=1}^n R[Z]/\overline{M}_{iv}^m. \tag{2}$$

We need the following lemma about ideals.

Lemma 5. *Let S be a commutative ring with identity and let $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ be ideals of S. If $\mathfrak{B}$ and $\mathfrak{C}$ are comaximal, then $\mathfrak{A} + (\mathfrak{B} \cap \mathfrak{C}) = (\mathfrak{A} + \mathfrak{B}) \cap (\mathfrak{A} + \mathfrak{C})$.*

Proof. Since $\mathfrak{A} + \mathfrak{B} \supseteq \mathfrak{A}$, the modular law implies that

$$(\mathfrak{A} + \mathfrak{B}) \cap (\mathfrak{A} + \mathfrak{C}) = \mathfrak{A} + \left((\mathfrak{A} + \mathfrak{B}) \cap \mathfrak{C}\right).$$

Since $\mathfrak{B}$ and $\mathfrak{C}$ are comaximal, so are $\mathfrak{A} + \mathfrak{B}$ and $\mathfrak{C}$. Therefore,

$$\mathfrak{A} + \left((\mathfrak{A} + \mathfrak{B}) \cap \mathfrak{C}\right) = \mathfrak{A} + (\mathfrak{A} + \mathfrak{B})\mathfrak{C} = \mathfrak{A} + \mathfrak{A}\mathfrak{C} + \mathfrak{B}\mathfrak{C} = \mathfrak{A} + \mathfrak{B}\mathfrak{C} = \mathfrak{A} + \mathfrak{B} \cap \mathfrak{C}. \qquad \square$$

Now, let $\psi \in L$. Let $c = (c_1, c_2, \dots, c_n) = \phi(\psi)$ denote the corresponding codeword of $C(rP, D)$. Let δ denote the Hamming distance between v and c. The following result generalizes Lemma 4 of [13]. Our proof does not involve power series or the Weierstrass Preparation Theorem, which were employed in [13].

Proposition 6. *The dimension of*

$$R[Z]/\big(\langle Z-\psi\rangle+\bar{I}_{m,v}\big)$$

as an $\mathbb{F}_q$-vector space is $m(n-\delta)$.

Proof. By Corollary 4 and successive applications of Lemma 5, we have

$$\langle Z-\psi\rangle+\bar{I}_{m,v}=\cap_{i=1}^{n}\big(\langle Z-\psi\rangle+\overline{M}_{iv}^{m}\big).$$

It then follows from the Chinese Remainder Theorem that we have an isomorphism

$$R[Z]/\big(\langle Z-\psi\rangle+\bar{I}_{m,v}\big)\xrightarrow{\cong}\prod_{i=1}^{n}R[Z]/\big(\langle Z-\psi\rangle+\overline{M}_{iv}^{m}\big). \tag{3}$$

Notice that the value of $Z-\psi$ at the point P_{iv} is v_i-c_i. There are two cases to consider. If $v_i\neq c_i$, then $Z-\psi$ does not belong to $\overline{M}_{iv}$. So, in this case, $\langle Z-\psi\rangle+\overline{M}_{iv}^{m}$ is all of $R[Z]$ and the corresponding factor in the product in (3) is zero.

On the other hand, if $v_i=c_i$, then we claim that

$$R[Z]/\big(\langle Z-\psi\rangle+\overline{M}_{iv}^{m}\big)\cong R/\overline{M}_{i}^{m},$$

where $\overline{M}_i=\langle x_1-a_{i1},x_2-a_{i2},\dots,x_s-a_{is}\rangle=\overline{M}_{iv}\cap R$ is the maximal ideal of R corresponding to the point P_i, $i=1,2,\dots,n$. Consider the ring homomorphism $\Theta: R[Z]\longrightarrow R/\overline{M}_i^{m}$ that is the composition of the ring homomorphism Ψ from $R[Z]$ to R that takes Z to ψ (and is the identity on R) and the canonical homomorphism from R to $R/\overline{M}_i^{m}$. Obviously, Θ is onto, so we need to see that $\mathrm{Ker}(\Theta)$ is $\langle Z-\psi\rangle+\overline{M}_{iv}^{m}$. Notice that $\Psi(Z-v_i)=\psi-v_i$, which vanishes at P_i since $c_i=v_i$. Hence, $\Psi(Z-v_i)\in\overline{M}_i$. It is then easy to see that $\Psi(\langle Z-\psi\rangle+\overline{M}_{iv}^{m})\subseteq\overline{M}_i^{m}$ and hence $\langle Z-\psi\rangle+\overline{M}_{iv}^{m}\subseteq\mathrm{Ker}(\Theta)$. Conversely, assume $g(Z)\in\mathrm{Ker}(\Theta)$. By taking a preimage of $g(Z)$ in $A[Z]$, dividing by $Z-\psi_0$, where ψ_0 denotes a preimage of ψ in A, as in the proof of Proposition 2, and then taking residue classes in R, we may write $g(Z)=s(Z)(Z-\psi)+\varphi$, where $s(Z)\in R[Z]$ and $\varphi\in R$. Then $\Psi(g(Z))=\varphi$ and, since $g(Z)\in\mathrm{Ker}(\Theta)$, we have that $\varphi\in\overline{M}_i^{m}$. It follows that $g(Z)\in\langle Z-\psi\rangle+\overline{M}_{iv}^{m}$.

Now, the Artin local ring $R/\overline{M}_i^{m}$ is isomorphic to $R_{\overline{M}_i}/\overline{M}_i^{m}R_{\overline{M}_i}$, where $R_{\overline{M}_i}$ denotes the localization of R at $\overline{M}_i$. Since R is a Dedekind domain, the local ring $R_{\overline{M}_i}$ is a discrete valuation ring, and its residue field is $\mathbb{F}_q$. Therefore, $R/\overline{M}_i^{m}$ has dimension m as an $\mathbb{F}_q$-vector space. It then follows from (3) that the dimension of $R[Z]/(\langle Z-\psi\rangle+\bar{I}_{m,v})$ as an $\mathbb{F}_q$-vector space is $m(n-\delta)$. □

We are now ready to generalize Theorem 6 of [13]. Our proof is virtually identical, but we include it for the sake of completeness. Let ν_P denote the valuation at the point P. If ψ is a nonzero element of R, then the order of the pole of ψ at P is $-\nu_P(\psi)=\dim_{\mathbb{F}_q}(R/\langle\psi\rangle)$ (cf. Lemma 5 of [13]). Given $p(Z)=\rho_l Z^l+\cdots+\rho_1 Z+\rho_0\in R[Z]$, define $\deg_r(p(Z))$, the r-weighted degree of $p(Z)$, by

$$\deg_r\big(p(Z)\big)=\max_{0\leqslant j\leqslant l}\big(-\nu_P(\rho_j)+rj\big).$$

Theorem 7. *Assume that $p(Z) \in \bar{I}_{m,v}$ has positive degree in Z. Put $\mu = \deg_r(p(Z))$. Let $c = \phi(\psi)$ be a codeword of $C(rP, D)$ such that the Hamming distance δ between c and v satisfies $\delta < n - (\mu/m)$. Then ψ is a root of $p(Z)$; i.e., $p(\psi) = 0$.*

Proof. Assume that $p(\psi) \neq 0$. Since $\psi \in L$, we have $\mu = \deg_r(p(Z)) \geqslant -\nu_P(p(\psi)) = \dim_{\mathbb{F}_q} R/\langle p(\psi)\rangle$. Now, it is easy to see that $R/\langle p(\psi)\rangle$ is isomorphic to $R[Z]/\langle p(Z), Z - \psi\rangle$. Hence, using the fact that $p(Z) \in \bar{I}_{m,v}$, we have

$$\begin{aligned}\mu &\geqslant \dim_{\mathbb{F}_q} R[Z]/\big\langle p(Z), Z - \psi\big\rangle \\ &\geqslant \dim_{\mathbb{F}_q} R[Z]/\big(\langle Z - \psi\rangle + \bar{I}_{m,v}\big) = m(n - \delta).\end{aligned}$$

Therefore, if $m(n - \delta) > \mu$, we must have $p(\psi) = 0$. □

Notice that because of the estimates used in the proof of Theorem 7, we may have $p(\psi) = 0$ even if $\delta \geqslant n - (\mu/m)$.

From now on, we will assume we are in one of the following two cases: (1) the divisor D is the sum of all rational points except for the point at infinity and, thus, we can assume $I = J$; or (2) $m = 1$. To apply Theorem 7 we can take a weighted monomial order on $A[Z]$ such that the weight of X_i is $-\nu_P(x_i)$ for $i = 1, 2, \ldots, s$, the weight of Z is r, and where we break ties by lexicographic order with Z the greatest variable. (We want Z to be the greatest variable so that our interpolation polynomial will have small powers of Z.) We then find the reduced Gröbner basis of the ideal $I + \langle X_1^q - X_1, \ldots, X_s^q - X_s, Z - H_v\rangle^m$ with respect to this order. From Theorem 7, the best choice for our interpolation polynomial is the residue class in $R[Z]$ of the least element in this Gröbner basis that has positive degree in Z. Let $Q_{m,v}(Z)$ denote the least element in this Gröbner basis that has positive degree in Z, and let $\overline{Q}_{m,v}$ denote the residue class of $Q_{m,v}(Z)$ in $R[Z]$. By slight abuse of language, we will refer to both $Q_{m,v}(Z)$ and $\overline{Q}_{m,v}(Z)$ as "the interpolation polynomial."

Example 8. We consider the curve $Y^4 + Y = X^5$ over the field $\mathbb{F}_4$ (not over the field $\mathbb{F}_{16}$, where this would be a Hermitian curve). There is a single point P at infinity and four other rational points: $P_1 = (0, 0)$, $P_2 = (0, 1)$, $P_3 = (0, \alpha)$, and $P_4 = (0, \alpha^2)$, where $\alpha^2 + \alpha + 1 = 0$. Let $C = C_L(5P, D)$, where $D = P_1 + P_2 + P_3 + P_4$. The vector space $L(5P)$ is identified with the $\mathbb{F}_4$-subspace of R_q generated by 1 and y, a generator matrix for C is

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix},$$

and C is a $(4, 2, 3)$ code over $\mathbb{F}_4$.

For our polynomials H_i, we can take $H_1 = 1 - Y^3, H_2 = 1 - (Y - 1)^3, H_3 = 1 - (Y - \alpha)^3$, and $H_4 = 1 - (Y - \alpha^2)^3$. These polynomials do not contain the unnecessary factor $(1 - X)$ that would be present if one used (1).

Notice that, in this example, our ideal $\bar{I}_{m,v}$ is not the same as the ideal $\langle x^4 - x, Z - h_v\rangle^m$ considered in [13]. Indeed, if we take $h_v = 0$, then the $\mathbb{F}_4$-vector space dimension of $R[Z]/\bar{I}_{1,v} = \mathbb{F}_4[X, Y]/I_q$ is 4, corresponding to the four rational points in the affine plane, while the $\mathbb{F}_4$-vector space dimension of $R[Z]/\langle x^4 - x, Z\rangle = \mathbb{F}_4[X, Y, Z]/\langle Y^4 + Y - X^5, X^4 - X, Z\rangle$ is 16.

Let the received string be $v = (1, 0, 1, \alpha)$. Then $H_v = \alpha Y^3 + \alpha^2 Y^2 + 1$. Now, we have $\nu_P(x) = -4$ and $\nu_P(y) = -5$. We then consider the weighted order on $\mathbb{F}_4[X, Y, Z]$ where the weight of X is 4, the weight of Y is 5, the weight of Z is 5 (since our code uses $L(5P)$), and where we break ties using a lexicographic order with $Z > Y > X$. If we take $m = 2$, then we need to find a Gröbner basis for the ideal

$$\big\langle Y^4 + Y - X^5\big\rangle + \big\langle X^4 - X, Y^4 - Y, Z - H_v\big\rangle^2$$

with respect to this order. We can use *Macaulay2* [9] and the following commands:

```
k=GF(ZZ/2[a]/(a^2+a+1));
R=k[X,Y,Z,MonomialOrder=>{Weights=>{4,5,5},RevLex}];
H=(1-Y^3)+(1-(Y-a)^3)+a*(1-(Y-a^2)^3);
B=ideal(Y^4+Y-X^5)+(ideal(X^4-X,Y^4-Y,Z-H))^2;
G=gens gb B.
```

We find that the least element in the reduced Gröbner basis with positive degree in Z is $Q_{2,v} = (XY+\alpha X)Z + XY^2 + \alpha^2 XY + \alpha X$. The interpolation polynomial in $R[Z]$ is then $(xy+\alpha x)Z + xy^2 + \alpha^2 xy + \alpha x$. Even though the r-weighted degree of this polynomial is $\mu = 14$ and $n - (\mu/m) = -3$, a check shows that the root in R of this polynomial is $Z = y+1$. Thus, we decode v as $c = \phi(y+1) = (1, 0, \alpha^2, \alpha)$, which is the correct nearest neighbor decoding. Actually, in this example, we can take $m = 1$. Doing that, the superfluous factor of x in the previous polynomial is removed, our interpolation polynomial turns out to be $(y+\alpha)Z + y^2 + \alpha^2 y + \alpha$, and again the root in R is $Z = y+1$. We did the calculation in the $m = 2$ case here to illustrate the case when $m > 1$.

If we put a limit on the size of the list of codewords that may be found in our list decoding, then, as in Lee and O'Sullivan [12,13], it may be possible to use Gröbner bases for modules instead of Gröbner bases for ideals. Specifically, if we desire no more than l possible codewords in the list corresponding to a given received string, then we can limit the degree in Z of our interpolation polynomial to at most l. Then, instead of viewing the interpolation polynomial as an element in $R[Z]$, we can view it as an element in the free R-module $R[Z]_l = \oplus_{j=0}^{l} RZ^j$. Assume $l \geqslant m$. Put $\bar{I}_{m,v,l} = \bar{I}_{m,v} \cap R[Z]_l$. Then it is not hard to see, as in Proposition 7 of [13], that $\bar{I}_{m,v,l}$ is generated as an R-module by

$$(Z - h_v)^a \prod_{i=1}^{s} \bigl(x_i^q - x_i\bigr)^{b_i}, \quad \text{where } 0 \leqslant a \leqslant m,\ \sum_{i=1}^{s} b_i = m - a, \text{ and } b_i \geqslant 0,$$

$$Z^{a-m}(Z - h_v)^m, \quad \text{where } m < a \leqslant l.$$

In [13], Lee and O'Sullivan made essential use of the facts that they were dealing with a plane curve and that $Y^q - Y$ was a power of X in constructing their algorithm. It is not clear if their algorithm can be generalized to the case of an arbitrary curve and we will not pursue this problem here. We note that P. Beelen and K. Brander [3] have also given a module-theoretic algorithm for computing an interpolation polynomial for a large class of plane curves (Miura–Kamiya curves).

3. Generic interpolation polynomial

We now apply "the Cooper philosophy" and "replace" the n-tuple $v = (v_1, v_2, \ldots, v_n)$ by an n-tuple of variables $t = (t_1, t_2, \ldots, t_n)$. So, instead of working over the field $\mathbb{F}_q$, we will work over the field $\mathbb{F}_q(t_1, t_2, \ldots, t_n)$. The idea is to obtain a polynomial in Z with coefficients in $R(t_1, t_2, \ldots, t_n)$ that will specialize to give the interpolation polynomial in $R[Z]$ for most received strings $(v_1, v_2, \ldots, v_n)$ when we substitute $t_i = v_i, i = 1, 2, \ldots, n$.

We keep the same notation as in the previous section and we assume throughout that either $I = J$ or $m = 1$. Let A_t denote the ring $\mathbb{F}_q(t_1, t_2, \ldots, t_n)[X_1, X_2, \ldots, X_s]$. Put $H_t = t_1 H_1 + t_2 H_2 + \cdots + t_n H_n$. Let h_t denote the residue class of H_t in $R(t_1, t_2, \ldots, t_n)$. Define the ideal $\mathcal{I}_{m,t}$ in $A_t[Z]$ by

$$\mathcal{I}_{m,t} = IA_t[Z] + \bigl\langle X_1^q - X_1, X_2^q - X_2, \ldots, X_s^q - X_s, Z - H_t\bigr\rangle^m.$$

Definition 9. Put the same weighted monomial order on $A_t[Z]$ as we put on $A[Z]$ in the previous section. Let $\mathcal{Q}_{m,t}(Z)$ denote the least element in the reduced Gröbner basis of the ideal $\mathcal{I}_{m,t}$ that has positive degree in Z. We call $\mathcal{Q}_{m,t}$ the mth *generic interpolation polynomial* for the code C.

This polynomial may depend on the choice of the H_i's and the representation of C as an affine variety code $C(I, L)$.

Theorem 10. *There is an algebraic variety $W \subseteq \mathbb{A}^n$ such that $\mathcal{Q}_{m,t}(Z)$ specializes to $Q_{m,v}(Z)$ for all specializations $(t_1, \ldots, t_n) \mapsto (v_1, \ldots, v_n) \in \mathbb{A}^n \setminus W$.*

Proof. We may assume that the generators of I are monic polynomials. However, note that the leading term of $Z - H_t$ need not be Z. From the definition of H_t, the leading coefficient of $Z - H_t$ may be $u = u(t_1, t_2, \ldots, t_n)$, an $\mathbb{F}_q$-linear combination of $t_1, t_2, \ldots, t_n$. In that case, the leading coefficient of some of the generators of $\mathcal{I}_{m,t}$ as given above will be a power of u. Dividing by powers of u when necessary, we can get to a set of monic polynomials

$$f_1, f_2, \ldots, f_\Lambda \in \mathbb{F}_q(t_1, t_2, \ldots, t_n)[X_1, X_2, \ldots, X_s, Z]$$

that generate $\mathcal{I}_{m,t}$. Let $g_1, g_2, \ldots, g_\Gamma$ be the reduced Gröbner basis for $\mathcal{I}_{m,t}$. Then there exist $B_{\gamma\lambda} \in A_t[Z]$ such that

$$g_\gamma = \sum_{\lambda=1}^{\Lambda} B_{\gamma\lambda} f_\lambda,$$

for $\gamma = 1, 2, \ldots, \Gamma$. If W' is the affine subvariety of $\mathbb{A}^n$ defined by the vanishing of $u(t_1, \ldots, t_n)$ and all the denominators that appear among the g_γ and $B_{\gamma\lambda}$, then $\{g_1, \ldots, g_\Gamma\}$ remains a Gröbner basis for $\langle f_1, \ldots, f_\Lambda \rangle$ under all specializations

$$(t_1, \ldots, t_n) \mapsto (v_1, \ldots, v_n) \in \mathbb{A}^n \setminus W'$$

by [5, pp. 288–289]. Let W'' be the subvariety of $\mathbb{A}^n$ such that $\mathcal{Q}_{m,t}(Z)$ specializes to a polynomial with positive degree in Z for all specializations $(t_1, \ldots, t_n) \mapsto (v_1, \ldots, v_n) \in \mathbb{A}^n \setminus W''$. It then follows that for specializations $(t_1, \ldots, t_n) \mapsto (v_1, \ldots, v_n)$ outside of $W = W' \cup W''$, the generic interpolation polynomial specializes to the interpolation polynomial for $(v_1, \ldots, v_n)$. □

While it is clear that the variety W in the above theorem is a proper subvariety of affine n-space over the algebraic closure of $\mathbb{F}_q$, it is not clear how many of the finite number of points in $\mathbb{A}^n$ may lie in W. We present some examples where the generic interpolation polynomial does specialize to the interpolation polynomial for "most" received strings.

Example 11. We return to the situation in Example 8 and compute the generic interpolation polynomial when $m = 2$. With *Macaulay2*, we can use the following commands:

```
k=GF(ZZ/2[a]/(a^2+a+1));
K=frac(k[t1,t2,t3,t4]);
R=K[X,Y,Z,MonomialOrder=>{Weights=>{4,5,5},RevLex}];
H=t1*(1-Y^3)+t2*(1-(Y-1)^3)+t3*(1-(Y-a)^3)+t4*(1-(Y-a^2)^3);
B=ideal(Y^4+Y-X^5)+(ideal(X^4-X,Y^4-Y,Z-H))^2;
G=gens gb B.
```

The least element of the reduced Gröbner basis with positive degree in Z is

$$\mathcal{Q}_{2,t}(Z) = \left(XY + \frac{t_2 + \alpha t_3 + \alpha^2 t_4}{t_1 + t_2 + t_3 + t_4} X\right) Z + \frac{t_1 t_2 + \alpha^2 t_1 t_3 + \alpha t_2 t_3 + \alpha t_1 t_4 + \alpha^2 t_2 t_4 + t_3 t_4}{t_1 + t_2 + t_3 + t_4} XY^2$$
$$+ \frac{t_1 t_2 + t_1 t_3 + t_2 t_3 + t_1 t_4 + t_2 t_4 + t_3 t_4}{t_1 + t_2 + t_3 + t_4} XY + \frac{t_1 t_2 + \alpha t_1 t_3 + \alpha^2 t_1 t_4}{t_1 + t_2 + t_3 + t_4} X.$$

When we substitute $t_1 = 1, t_2 = 0, t_3 = 1, t_4 = \alpha$ into $\mathcal{Q}_{2,t}(Z)$, we obtain the polynomial $Q_{2,v}(Z)$ in Example 8. Here, one can see that $\mathcal{Q}_{2,t}(Z)$ will specialize to the interpolation polynomial as long as $t_1 + t_2 + t_3 + t_4 \neq 0$. (Again, we can actually use $m = 1$ here and our generic interpolation polynomial will be $\mathcal{Q}_{1,t}(Z) = \mathcal{Q}_{2,t}(Z)/X$.) We note that for this code, if $c = (c_1, c_2, c_3, c_4)$ is any codeword, then $c_1 + c_2 + c_3 + c_4 = 0$. It follows that if $v = (v_1, v_2, v_3, v_4)$ is not a codeword and if $v_1 + v_2 + v_3 + v_4 = 0$, then the distance from v to any codeword is at least 2. Hence, the generic interpolation polynomial here can always be used to correct one error. Note that the generic interpolation polynomial becomes undefined when one specializes to any codeword.

As one can imagine, it is in general difficult to compute the generic interpolation polynomial. Indeed, using software like *Macaulay2* we have only been able to compute the generic interpolation polynomial in small examples. It is possible that techniques as in [14] might make the computations more manageable, or one may be able to extend the algorithms of Lee and O'Sullivan [12,13], or Beelen and Brander [3] to work over $\mathbb{F}_q(t_1, t_2, \ldots, t_n)$ to compute the generic interpolation polynomial in some cases. The advantage of having the generic interpolation polynomial is that, given most received words, one could then compute the interpolation polynomial by substitution, thus avoiding the update loop process in other algorithms. We will discuss this further in our final example in which we give a family of Reed–Solomon codes for which one can compute the generic interpolation polynomial "by hand." This is a family of codes of minimum distance 3 and falls into the "special case" $m = l = 1$ considered in the last section of [12]. An interesting feature of this example is that the finite field may be arbitrarily large (and, consequently, the code may be arbitrarily long).

Example 12. Assume $q \geqslant 5$. Let C denote the $[q-1, q-3, 3]$ Reed–Solomon code over $\mathbb{F}_q$. Then $I = \langle X^{q-1} - 1\rangle$, $J = \langle 0\rangle$, $L = L((q-4)P)$ is the $\mathbb{F}_q$-subspace of $\mathbb{F}_q[X]$ with basis $\{1, X, \ldots, X^{q-4}\}$, and we set $m = 1$. Denote the nonzero elements of $\mathbb{F}_q$ by $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$. Using Lagrange interpolation, we take

$$H_i(X) = \prod_{\substack{k=1 \\ k\neq i}}^{q-1} (\alpha_i - \alpha_k)^{-1}(X - \alpha_k)$$

for $i = 1, 2, \ldots, q-1$. Put $H_t = \sum_{i=1}^{q-1} t_i H_i$. Write

$$H_t = u_0 + u_1 X + \cdots + u_{q-2} X^{q-2}.$$

Put $K = \mathbb{F}_q(t_1, t_2, \ldots, t_{q-1})$. The ideal $\mathcal{I}_{1,t}$ of $K[X, Z]$ is given by

$$\mathcal{I}_{1,t} = \langle X^{q-1} - 1, Z - H_t\rangle.$$

Our weighted monomial order assigns a weight of 1 to X and a weight of $q-4$ to Z. Notice that the leading term of $Z - H_t$ is $-u_{q-2}X^{q-2}$. It is not hard to see that the S-polynomial of the two generators of $\mathcal{I}_{1,t}$ then reduces to the polynomial

$$\mathcal{Q}(X, Z) = XZ + \left(\frac{u_{q-3}^2}{u_{q-2}} - u_{q-4}\right)X^{q-3} - \frac{u_{q-3}}{u_{q-2}}Z + \sum_{k=1}^{q-4}\left(\frac{u_k u_{q-3}}{u_{q-2}} - u_{k-1}\right)X^k + \frac{u_{q-3}u_0}{u_{q-2}} - u_{q-2}.$$

Indeed, we have $\mathcal{Q}(X, Z) = u_{q-2}(X^{q-1} - 1) + (X - \frac{u_{q-3}}{u_{q-2}})(Z - H_t)$.

We claim that $\mathcal{Q}(X, Z)$ is the generic interpolation polynomial. This will follow from the next proposition. Before giving that result, we consider the number of multiplications in $\mathbb{F}_q$ that are needed to compute the interpolation polynomial from $\mathcal{Q}(X, Z)$ once a word is received. We assume that the nonzero field elements $\alpha_i, i = 1, 2, \ldots, q-1$ have been stored and do not need to be computed. Given field values $t_i = v_i$ for $i = 1, 2, \ldots, q-1$, it then requires $O(q)$ multiplications to compute each of the $u_i, i = 1, 2, \ldots, q-2$. Notice that in the above formula for $\mathcal{Q}(X, Z)$, the same element u_{q-3}/u_{q-2} appears in every term of the summation. (In particular, one only needs to invert the single element u_{q-2}.) It follows that all the terms in the polynomial $\mathcal{Q}(X, Z)$ may be computed using $O(q^2)$ multiplications. Step I2 in the algorithm in [12] (with $m = 1$) also requires $O(q^2)$ multiplications. However, because of the update loop, the algorithm in [12] might require as many as $O(q^4)$ multiplications to compute the interpolation polynomial (although that algorithm might perform better than that in this specific example).

Proposition 13. *There is no nonzero polynomial in $\mathcal{I}_{1,t}$ whose leading monomial is in $\{1, X, X^2, \ldots, X^{q-4}, Z, X^{q-3}\}$.*

Proof. We first claim that there is no nonzero polynomial solely in X of degree less than $q-1$ in $\mathcal{I}_{1,t}$. To see this, consider the homomorphism $\Psi : K[X, Z] \to K[X]$ such that $\Psi(X) = X$ and $\Psi(Z) = H_t$. The kernel of this homomorphism is easily seen to be $\langle Z - H_t\rangle$ and the image of $\mathcal{I}_{1,t}$ under this homomorphism is $\langle X^{q-1} - 1\rangle$. The claim then follows since there are no nonzero polynomials of degree less than $q-1$ in $\langle X^{q-1} - 1\rangle$.

Suppose there is a polynomial in $\mathcal{I}_{1,t}$ whose leading monomial is in $\{1, X, X^2, \ldots, X^{q-4}\}$. Then this would be a nonzero polynomial solely in X of degree less than $q-1$, which is a contradiction. Now suppose there is a polynomial $f(X, Z) \in \mathcal{I}_{1,t}$ whose leading monomial is Z. Then

$$f(X, Z) = aZ + \text{terms in } X \text{ of degree} \leqslant q-4,$$

for some $a \in K$. But then $f(X, Z) - a(Z - H_t) \in \mathcal{I}_{1,t}$ is a nonzero polynomial solely in X of degree less than $q-1$, which is a contradiction. Similarly, if there is a polynomial $g(X, Z) \in \mathcal{I}_{1,t}$ with leading monomial X^{q-3}, then $g(X, Z) = aX^{q-3} + bZ + \text{lower terms in } X$, and $g(X, Z) - b(Z - H_t)$ would be a nonzero polynomial solely in X of degree less than $q-1$. □

By the lemma, the least possible leading monomial of any nonzero polynomial in $\mathcal{I}_{1,t}$ is XZ. It follows that $\mathcal{Q}(X, Z)$ is the generic interpolation polynomial. We note that computations with *Macaulay2* indicate that the reduced Gröbner basis for $\mathcal{I}_{1,t}$ is given by

$$G = \left\{\mathcal{Q}(X, Z), \frac{-1}{u_{q-2}}(Z - H_t), T(X, Z)\right\},$$

where $T(X, Z)$ is a polynomial with leading term Z^2 that arises from reducing the S-polynomial of $\mathcal{Q}(X, Z)$ and $\frac{-1}{u_{q-2}}(Z - H_t)$.

To illustrate this example more explicitly, we consider the [7, 5, 3] Reed–Solomon code over $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$, where $\alpha^3 + \alpha + 1 = 0$. List the nonzero elements of $\mathbb{F}_8$ as $P_i = \alpha_i = \alpha^i$ for $i = 1, 2, \ldots, 7$. Then

$$H_1(X) = \alpha X^6 + \alpha^2 X^5 + \alpha^3 X^4 + \alpha^4 X^3 + \alpha^5 X^2 + \alpha^6 X + 1,$$
$$H_2(X) = \alpha^2 X^6 + \alpha^4 X^5 + \alpha^6 X^4 + \alpha X^3 + \alpha^3 X^2 + \alpha^5 X + 1,$$
$$H_3(X) = \alpha^3 X^6 + \alpha^6 X^5 + \alpha^2 X^4 + \alpha^5 X^3 + \alpha X^2 + \alpha^4 X + 1,$$
$$H_4(X) = \alpha^4 X^6 + \alpha X^5 + \alpha^5 X^4 + \alpha^2 X^3 + \alpha^6 X^2 + \alpha^3 X + 1,$$
$$H_5(X) = \alpha^5 X^6 + \alpha^3 X^5 + \alpha X^4 + \alpha^6 X^3 + \alpha^4 X^2 + \alpha^2 X + 1,$$
$$H_6(X) = \alpha^6 X^6 + \alpha^5 X^5 + \alpha^4 X^4 + \alpha^3 X^3 + \alpha^2 X^2 + \alpha X + 1,$$

$$H_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,$$

$$\begin{aligned} H_t(X) &= t_1H_1 + t_2H_2 + t_3H_3 + t_4H_4 + t_5H_5 + t_6H_6 + t_7H_7 \\ &= \sum_{j=0}^{6}\left(\sum_{i=1}^{7} t_i\alpha^{i(7-j)}\right)X^j. \end{aligned}$$

In particular, $u_6 = \sum_{i=1}^{7} t_i\alpha^i$. The generic interpolation polynomial in this case is

$$\mathcal{Q}(X, Z) = XZ + \left(\frac{u_5^2}{u_6} - u_4\right)X^5 - \frac{u_5}{u_6}Z + \sum_{k=1}^{4}\left(\frac{u_ku_5}{u_6} - u_{k-1}\right)X^k + \frac{u_5u_0}{u_6} - u_6.$$

We may use $\mathcal{Q}(X, Z)$ to correct one error in a received string $(v_1, v_2, \dots, v_7)$ as long as $\sum_{i=1}^{7} v_i\alpha^i \neq 0$. Note that, since our code is cyclic with α as one of its roots, if $(c_1, c_2, \dots, c_7)$ is any codeword, then $\sum_{i=1}^{7} c_i\alpha^i = 0$. It follows that if $(v_1, v_2, \dots, v_7)$ is a received string in which precisely one error has occurred, then $\sum_{i=1}^{7} v_i\alpha^i \neq 0$.

For example, assume the received string is $(\alpha^3, \alpha^4, \alpha^5, 0, 0, 0, 0)$. Substituting these values for the t_i's and computing the resulting u_i's, we find that the generic interpolation polynomial specializes to

$$Q(X, Z) = XZ + \alpha X^5 + \alpha^3 Z + \alpha^5 X^4 + \alpha X^3 + \alpha^6 X^2 + \alpha^6 X + \alpha^5.$$

Substituting $a_4X^4 + a_3X^3 + \cdots + a_0$ for Z in the equation $Q(X, Z) = 0$ and solving for the a_j's, we find that the root of $Q(X, Z)$ in $\mathbb{F}_8[X]$ is

$$f(X) = \alpha X^4 + X^3 + X^2 + \alpha^4 X + \alpha^2.$$

Evaluating f at the points P_i, we decode the received string as the codeword

$$\left(\alpha^3, \alpha^4, 1, 0, 0, 0, 0\right).$$

References

[1] M.F. Atiyah, I.G. MacDonald, Introduction to Commutative Algebra, Addison–Wesley, Reading, MA, 1969.

[2] T. Becker, V. Weispfenning, Gröbner Bases – A Computational Approach to Commutative Algebra, Springer-Verlag, New York, 1993.

[3] P. Beelen, K. Brander, Efficient list decoding of a class of algebraic–geometry codes, Adv. Math. Commun. 4 (4) (2010) 485–518.

[4] A.B. Cooper, Toward a new method of decoding algebraic codes using Gröbner bases, in: Transactions of the 10th Army Conference on Applied Mathematics and Computing, West Point, NY, 1992, U.S. Army Research Office, 1993, pp. 1–11.

[5] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, third edition, Springer-Verlag, New York, 2007.

[6] J. Fitzgerald, R.F. Lax, Decoding affine variety codes using Gröbner bases, Des. Codes Cryptogr. 13 (2) (1998) 147–158.

[7] O. Geil, Evaluation codes from an affine variety code perspective, in: Advances in Algebraic Geometry Codes, in: Ser. Coding Theory Cryptol., vol. 5, World Sci. Publ., 2008, pp. 153–180.

[8] O. Geil, R. Pellikaan, On the structure of order domains, Finite Fields Appl. 8 (3) (2002) 369–396.

[9] D.R. Grayson, M.E. Stillman, *Macaulay2*, available at http://www.math.uiuc.edu/Macaulay2/.

[10] E. Guerrini, A. Rimoldi, FGLM-like decoding: From Fitzpatrick's approach to recent developments, in: M. Sala, et al. (Eds.), Gröbner Bases, Coding, and Cryptography, Springer-Verlag, Heidelberg, 2009, pp. 197–218.

[11] V. Guruswami, M. Sudan, Improved decoding of Reed–Solomon codes and algebraic geometry codes, IEEE Trans. Inform. Theory 45 (6) (1999) 1757–1767.

[12] K. Lee, M.E. O'Sullivan, List decoding of Reed–Solomon codes from a Gröbner basis perspective, J. Symbolic Comput. 43 (9) (2008) 645–658.

[13] K. Lee, M.E. O'Sullivan, List decoding of Hermitian codes using Gröbner bases, J. Symbolic Comput. 44 (12) (2009) 1662–1675.

[14] C. Marcolla, E. Orsini, M. Sala, Improved decoding of affine-variety codes, http://arkiv.org/abs/1102.4186v2, 2011.

[15] R. Matsumoto, Miura's generalization of one-point AG codes is equivalent to Høholdt van Lint and Pellikaan's generalization, IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E82-A (10) (1999) 2007–2010.

[16] T. Mora, E. Orsini, Decoding cyclic codes: the Cooper philosophy, in: M. Sala, et al. (Eds.), Gröbner Bases, Coding, and Cryptography, Springer-Verlag, Heidelberg, 2009, pp. 69–92.

[17] H. O'Keeffe, P. Fitzpatrick, Gröbner basis approach to list decoding of algebraic geometry codes, Appl. Algebra Engrg. Comm. Comput. 18 (5) (2007) 445–466.

[18] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc. 197 (1974) 273–313.