J. Appl. Math. & Informatics Vol. **32**(2014), No. 1 - 2, pp. 83 - 98
http://dx.doi.org/10.14317/jami.2014.083

UNIQUE DECODING OF PLANE AG CODES REVISITED†

KWANKYU LEE

Abstract. We reformulate an interpolation-based unique decoding algorithm of AG codes, using the theory of Gröbner bases of modules on the coordinate ring of the base curve. The conceptual description of the reformulated algorithm lets us better understand the majority voting procedure, which is central in the interpolation-based unique decoding. Moreover the smaller Gröbner bases imply smaller space and time complexity of the algorithm.

AMS Mathematics Subject Classification: 94B35, 94B27.
Key words and phrases: Algebraic Geometry codes, interpolation decoding, Gröbner bases.

1. Introduction

Recently a new kind of unique decoding algorithm of algebraic geometry codes was presented [4]. The algorithm decodes the primal AG code that consists of codewords obtained by evaluation of functions at rational points of an algebraic curve, unlike the classical syndrome decoding algorithm that decodes the dual code. Based on Gröbner bases of modules over a univariate polynomial ring, the algorithm has a regular data and control structure that is suitable for parallel hardware implementation, like Kötter's algorithm for the syndrome decoding [3]. The ideas used can be traced back to [2, 1].

In this paper, we reformulate the previous algorithm, using the theory of Gröbner bases of modules on the coordinate ring of the base curve. This approach eliminates the technical complexity of the previous algorithm in a large degree, and results in a conceptually clean description of the algorithm which contributes to a better understanding of the majority voting procedure, which plays a central role in the interpolation-based unique decoding. Moreover the new approach allows the algorithm to work with smaller Gröbner bases so that

Received April 30, 2013. Revised October 25, 2013. Accepted November 2, 2013.
†This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(2013R1A1A2009714).

© 2014 Korean SIGCAM and KSCAM.

it can run faster and uses less space than the previous algorithm in a serial implementation.

Comparing with the well-known classical unique decoders of AG codes, Berlekamp-Massey-Sakata algorithm [7] and Kötter's algorithm [3], the features of the new algorithm put it in a unique place in the following table.

	C Interpolation-based	$C^\perp$ Syndrome-based
Gröbner on $\mathbb{F}[\mathcal{X}]$	New algorithm	BMS algorithm
Gröbner on $\mathbb{F}[x]$	Previous algorithm in [4]	Kötter's algorithm

That is, the new algorithm corrects the evaluation code C on a plane curve $\mathcal{X}$ working with the Gröbner bases on $\mathbb{F}[\mathcal{X}]$, the coordinate ring of $\mathcal{X}$. Thus we may view the new algorithm as a *dual* version of the BMS algorithm.

Let us briefly review basic facts about AG codes. Like the previous algorithm in [4] and the BMS decoding algorithm in [7], the new algorithm is formulated for the AG codes from the Miura-Kamiya curves [5], which include Hermitian curves as prominent special cases. A Miura-Kamiya curve $\mathcal{X}$ is an irreducible plane curve defined by the equation

$$E: \quad Y^a + \sum_{ai+bj<ab} c_{i,j} X^i Y^j + dX^b = 0 \tag{1}$$

over a field $\mathbb{F}$ with $\gcd(a,b) = 1$ and $0 \neq d \in \mathbb{F}$. It is well known that $\mathcal{X}$ has a unique point P_∞ at infinity and has a unique valuation v_{P_∞} associated with it. Let $\delta(f) = -v_{P_\infty}(f)$ for f in the coordinate ring R of $\mathcal{X}$. Then $\delta(x) = a$ and $\delta(y) = b$. By the equation of the curve, a function in the coordinate ring $R = \mathbb{F}[x,y] = \mathbb{F}[X,Y]/\langle E\rangle$ can be written as a unique $\mathbb{F}$-linear combination of the monomials $x^i y^j$ with $i \geq 0$ and $0 \leq j < a$, which we call *monomials of* R. The numerical semigroup of R at P_∞,

$$S = \{\delta(f) \mid f \in R\} = \{\delta(x^i y^j) \mid i \geq 0, 0 \leq j < a\} = \mathbb{N}a + \mathbb{N}b$$

is a subset of the Weierstrass semigroup at P_∞. See [6] for basic terminology about numerical semigroups. As $\gcd(a,b) = 1$, there is an integer b' such that $b'b \equiv 1 \pmod{a}$. If $s = ai + bj$ is a nongap, then $b's \bmod a = j$, $(s - bj)/a = i$, and therefore i and j are uniquely determined. Hence the monomials of R are in one-to-one correspondence with nongaps in S. For a nongap s, let φ_s denote the unique monomial with $\delta(\varphi_s) = s$.

Let $P_1, P_2, \ldots, P_n$ be nonsingular rational points of $\mathcal{X}$. The evaluation map ev from R to the Hamming space $\mathbb{F}^n$ is the $\mathbb{F}$-linear map defined by $\varphi \mapsto (\varphi(P_1), \varphi(P_2), \ldots, \varphi(P_n))$. Let u be a fixed positive integer less than n and define $L_u = \{f \in R \mid \delta(f) \leq u\} = \langle \varphi_s \mid s \in S, s \leq u\rangle$, where brackets denote the linear span over $\mathbb{F}$. Then the AG code C_u is defined as the image of L_u under ev. As $u < n$, ev is one-to-one on L_u. So the dimension of the linear code C_u equals $\dim_{\mathbb{F}} L_u = |\{s \in S \mid s \leq u\}|$.

In Section 2, we review the theory of the Gröbner bases of modules over the coordinate rings of algebraic curves, and outline the interpolation-based decoding algorithm. The algorithm operates by iterating two core steps, the Gröbner basis computation step and the message guessing step by the majority voting procedure. Sections 3 and 4 are devoted to these core steps. In Section 5, we demonstrate the algorithm with a Hermitian code. In the final section, we give some remarks about the complexity of the algorithm.

2. Interpolation decoding

We assume a codeword c in C_u is sent through a noisy communication channel and $v \in \mathbb{F}^n$ is the vector received from the channel. Let $v = c + e$ with the error vector e. Then $c = \mathrm{ev}(\mu)$ for a unique $\mu = \sum_{s \in S, s \leq u} \omega_s \varphi_s \in L_u$, $\omega_s \in \mathbb{F}$, where we assume that the vector $(\omega_s \mid s \in S, s \leq u)$ is the message encoded into the codeword c. The decoding problem is essentially to find ω_s for all nongap $s \leq u$ from the given vector v.

For $s \geq u$, let $v^{(s)} = v$, $c^{(s)} = c$, and $\mu^{(s)} = \mu$. For nongap $s \leq u$, let

$$\mu^{(s-1)} = \mu^{(s)} - \omega_s \varphi_s, \quad c^{(s-1)} = c^{(s)} - \mathrm{ev}(\omega_s \varphi_s), \quad v^{(s-1)} = v^{(s)} - \mathrm{ev}(\omega_s \varphi_s),$$

and for gap $s \leq u$, let $v^{(s-1)} = v^{(s)}$, $c^{(s-1)} = c^{(s)}$, and $\mu^{(s-1)} = \mu^{(s)}$. Note that

$$\mu^{(s)} \in L_s, \quad c^{(s)} = \mathrm{ev}(\mu^{(s)}) \in C_s, \quad v^{(s)} = c^{(s)} + e$$

for all s. Hence we see that we can find ω_s iteratively.

A polynomial in $R[z]$ defines a function on the product surface of $\mathcal{X}$ and the line $\mathbb{A}^1_{\mathbb{F}}$, and can be evaluated at a point (P, α) with $P \in \mathcal{X}, \alpha \in \mathbb{F}$. Hence we can define the *interpolation module*

$$I_v = \{f \in Rz \oplus R \mid f(P_i, v_i) = 0, 1 \leq i \leq n\}$$

for v and similarly for $v^{(s)}$. These interpolation modules are indeed modules over R, and finite-dimensional vector space over $\mathbb{F}$. Note that

$$I_v = R(z - h_v) + J \tag{2}$$

where $J = \bigcap_{1 \leq i \leq n} \mathfrak{m}_i$ and $\mathrm{ev}(h_v) = v$, and $\mathfrak{m}_i = \langle x - \alpha_i, y - \beta_i \rangle$ is the maximal ideal of R associated with $P_i = (\alpha_i, \beta_i)$. Recall that by Lagrange interpolation, h_v can be computed fast from v. We will see that the key to find ω_s is the Gröbner basis of $I_{v^{(s)}}$ with respect to a monomial order $>_s$, defined as follows.

Let s be an integer. For monomial $x^i y^j z^k \in R[z]$, let $\delta_s(x^i y^j z^k) = \delta(x^i y^j) + sk$. In particular, $\delta_s(x^i y^j z) = ai + bj + s$ and $\delta_s(x^i y^j) = \delta(x^i y^j) = ai + bj$. The order $>_s$ on $Rz \oplus R$ put the monomials in the order of their δ_s values, and breaks the tie with higher z-degree. For f in $Rz \oplus R$, the notations $\mathrm{lt}_s(f)$, $\mathrm{lm}_s(f)$, and $\mathrm{lc}_s(f)$ denote the leading term, the leading monomial, and the leading coefficient of f, respectively, with respect to $>_s$. Note that for $f \in Rz \oplus R$, there are unique f^U and $f^D \in R$ such that $f = f^U z + f^D$ (the superscripts U and D may be read "upstairs" and "downstairs", respectively, with z being the staircase). By the definitions, we have the following lemma.

Lemma 2.1. *Let $f = f^U z + f^D$ with $f^U, f^D \in R$. Then* $\mathrm{lm}_s(f) \in Rz \iff \delta(f^U) + s \geq \delta(f^D)$*, where equality holds if and only if* $\mathrm{lm}_s(f) \in Rz$ *and* $\mathrm{lm}_{s-1}(f) \in R$.

Now let M be a submodule of $Rz \oplus R$. A finite subset B of M is called a *Gröbner basis* with respect to $>_s$ if the leading term of every element of M is divided by the leading term of some element of B. We will write $B = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$ where $\mathcal{G}, \mathcal{F}$ are some index sets, with the understanding that each G_i is a basis element such that $\mathrm{lm}_s(G_i) \in R$ and each F_j is a basis element such that $\mathrm{lm}_s(F_j) \in Rz$. The *sigma set* $\Sigma_s = \Sigma_s(M)$ of M is the set of all leading monomials of the polynomials in M with respect to $>_s$. The *delta set* $\Delta_s = \Delta_s(M)$ of M is the complement of Σ_s in the set of all monomials of $Rz \oplus R$. For the case that M is an ideal of R, we may omit the superfluous s from the notations, and denote $>_s$ simply by $>$. Note that if $\mathrm{lm}_s(f) \in Rz$, then $\mathrm{lm}_s(f) = \mathrm{lm}(f^U)z$, and if $\mathrm{lm}_s(f) \in R$, then $\mathrm{lm}_s(f) = \mathrm{lm}(f^D)$. It is easy to see by the definition of Gröbner bases that

$$\begin{aligned}\dim_{\mathbb{F}}(Rz \oplus R/M) &= |\Delta_s| = |\Delta_s \cap Rz| + |\Delta_s \cap R| \\ &= |\Delta(\{F_j^U \mid j \in \mathcal{F}\})| + |\Delta(\{G_i^D \mid i \in \mathcal{G}\})|,\end{aligned}$$

where $\Sigma(T)$, $\Delta(T)$ with a set T of polynomials in R have natural definitions.

As J is an ideal of R, it has a Gröbner basis $\{\eta_i \mid i \in \mathcal{J}\}$ with respect to $>$, and $\dim_{\mathbb{F}} R/J = |\Delta(J)| = |\Delta(\{\eta_i \mid i \in \mathcal{J}\})| = n$ since J is the ideal associated with the sum of n rational points on $\mathcal{X}$. By (2), we see that $\dim_{\mathbb{F}}(Rz \oplus R/I_v) = \dim_{\mathbb{F}}(R/J) = n$. Let $N = \delta(h_v)$. The set $\{\eta_i \mid i \in \mathcal{J}\} \cup \{z - h_v\}$ is then a Gröbner basis of I_v with respect to $>_N$. Let us denote a Gröbner basis of $I_{v^{(s)}}$ with respect to $>_s$ by $B^{(s)} = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$. Observe that if s is a nongap $\leq u$, then the set $\tilde{B} = \{G_i(z + \omega_s\varphi_s) \mid i \in \mathcal{G}\} \cup \{F_j(z + \omega_s\varphi_s) \mid j \in \mathcal{F}\}$ is still a Gröbner basis of $I_{v^{(s-1)}}$ with respect to $>_s$, but not with respect to $>_{s-1}$ in general. These observations lead to the following interpolation decoding algorithm.

Interpolation Decoding Algorithm. Let v be the received vector.

- **Initialize:** Compute h_v. Let $B^{(N)} = \{\eta_i \mid i \in \mathcal{J}\} \cup \{z - h_v\}$ where $N = \delta(h_v)$.
- **Main:** Repeat the following for s from N to 0.
  - **M1:** If s is a nongap $\leq u$, then make a guess $w^{(s)}$ for ω_s, and let $\tilde{B} = \{G_i(z + w^{(s)}\varphi_s) \mid i \in \mathcal{G}\} \cup \{F_j(z + w^{(s)}\varphi_s) \mid j \in \mathcal{F}\}$. Otherwise, let $\tilde{B} = B^{(s)}$.
  - **M2:** Compute $B^{(s-1)}$ from $\tilde{B}$.
- **Finalize:** Output $(w^{(s)} \mid \text{nongap } s \leq u)$, where $w^{(s)} = 0$ for $N < s \leq u$.

In the next section, we will elaborate on the step **M2**. The results in the section will lay a foundation for Section 4, in which we give details of the main steps **M1** and **M2**.

3. Gröbner basis computation

First we review the concept of the lcm, least common multiple, for the monomials of R. For two monomials φ_s and φ_t, we say φ_s *divides* φ_t if there exists a unique monomial λ such that

$$\delta(\varphi_t - \lambda\varphi_s) < \delta(\varphi_t).$$

The unique monomial λ will be denoted by the quotient φ_t/φ_s. Note that φ_s divides φ_t if and only if $t-s$ is a nongap, and in this case, actually $\lambda = \varphi_{t-s}$. Therefore φ_s and φ_t do not divide each other if and only if $s+S$ and $t+S$ do not contain each other.

Proposition 3.1. *Suppose $s+S$ and $t+S$ do not contain each other. Then there are unique nongaps l_1 and l_2 such that*

$$(s+S)\cap(t+S) = (l_1+S)\cup(l_2+S).$$

Indeed we can take $l_1 = \min(s+\mathbb{N}a)\cap(t+\mathbb{N}b)$ and $l_2 = \min(s+\mathbb{N}b)\cap(t+\mathbb{N}a)$.

Proof. Recall that $S = \mathbb{N}a + \mathbb{N}b$. By the definitions of l_1 and l_2, the inclusions $l_1 + S \subset (s+S)\cap(t+S)$, $l_2+S \subset (s+S)\cap(t+S)$ are obvious. So it remains to show the reverse inclusion. Suppose $c \in (s+S)\cap(t+S)$. Then $c = s+s_1a+s_2b = t+t_1a+t_2b$ for some $s_1, s_2, t_1, t_2 \in \mathbb{N}$. By our assumption that $s+S$ and $t+S$ do not contain each other, we either have $s_1 \geq t_1, s_2 < t_2$ or $s_1 < t_1, s_2 \geq t_2$. In the former case, $s+(s_1-t_1)a = t+(t_2-s_2)b \in (s+\mathbb{N}a)\cap(t+\mathbb{N}b) \subset l_1+S$, and hence $c \in l_1+S$. In the latter case, similarly we have $c \in l_2+S$. This shows that $(s+S)\cap(t+S) \subset (l_1+S)\cup(l_2+S)$. □

By the definition, we call φ_{l_1} and φ_{l_2} the *lcms* of φ_s and φ_t. In the case when φ_s divides φ_t, we will call φ_t the lcm of φ_s and φ_t.

Let $B = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$ be a Gröbner basis of a submodule M of $Rz \oplus R$ with respect to $>_s$. We want to compute a Gröbner basis of the same module M with respect to $>_{s-1}$ from B. Note that while $\mathrm{lm}_{s-1}(G_i) = \mathrm{lm}_s(G_i) \in R$ for all $i \in \mathcal{G}$, we may have either $\mathrm{lm}_{s-1}(F_j) = \mathrm{lm}_s(F_j) \in Rz$ or $\mathrm{lm}_{s-1}(F_j) \in R$ depending on $j \in \mathcal{F}$. Let Σ_s and Δ_s denote the sigma set and the delta set of M with respect to $>_s$, respectively. Observe that $\Sigma_{s-1}\cap Rz \subset \Sigma_s \cap Rz$, $\Sigma_{s-1}\cap R \supset \Sigma_s \cap R$.

For those $j \in \mathcal{F}$ such that $\mathrm{lm}_{s-1}(F_j) = \mathrm{lm}_s(F_j) \in Rz$, define $\mathrm{spoly}(F_j) = \{F_j\}$. If $\mathrm{lm}_{s-1}(F_j) \in R\cap\Sigma_s$, then there is an $i \in \mathcal{G}$ such that $\mathrm{lm}_s(G_i) | \mathrm{lm}_{s-1}(F_j)$, and then, with one such i, define

$$\mathrm{spoly}(F_j) = \{\frac{1}{\mathrm{lc}_{s-1}(F_j)}F_j - \frac{\mathrm{lm}_{s-1}(F_j)}{\mathrm{lt}_s(G_i)}G_i\}.$$

Finally, if $\mathrm{lm}_{s-1}(F_j) \in R\cap\Delta_s$, then define

$$\begin{aligned}\mathrm{spoly}(F_j) = \{&\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i \mid \\ &\psi \text{ is an lcm of } \mathrm{lm}_{s-1}(F_j) \text{ and } \mathrm{lm}_s(G_i) \text{ for } i \in \mathcal{G}\},\end{aligned}$$

which is generally not a singleton set unlike the previous two cases.

Proposition 3.2. *For every $f \in \mathrm{spoly}(F_j)$, $\mathrm{lm}_{s-1}(f)$ is in Rz.*

Proof. Recall that $\mathrm{lm}_s(F_j) \in Rz$. Suppose $\mathrm{lm}_{s-1}(F_j) \in R$, and let ψ be an lcm of $\mathrm{lm}_{s-1}(F_j)$ and $\mathrm{lm}_s(G_i)$ for any $i \in \mathcal{G}$. Then by Lemma 2.1,

$$\delta(\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j^U) = \delta(\psi) - \delta(F_j^D) + \delta(F_j^U) = \delta(\psi) - s,$$
$$\delta(\frac{\psi}{\mathrm{lt}_s(G_i)}G_i^U) = \delta(\psi) - \delta(G_i^D) + \delta(G_i^U) < \delta(\psi) - s.$$

Therefore $\delta((\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i)^U) = \delta(\psi) - s$. On the other hand,

$$\delta(\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j^D) = \delta(\psi) - \delta(F_j^D) + \delta(F_j^D) = \delta(\psi),$$
$$\delta(\frac{\psi}{\mathrm{lt}_s(G_i)}G_i^D) = \delta(\psi) - \delta(G_i^D) + \delta(G_i^D) = \delta(\psi).$$

As the monic terms cancel each other, $\delta((\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i)^D) < \delta(\psi)$. Therefore $\delta((\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i)^U) + s - 1 \geq \delta((\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i)^D)$, and hence by Lemma 2.1,

$$\mathrm{lm}_{s-1}(\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i) = \mathrm{lm}(\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j^U)z \in Rz. \tag{3}$$

For the case when $\mathrm{lm}_{s-1}(F_j) \in R \cap \Sigma_s$, notice that $\mathrm{lm}_{s-1}(F_j)$ is the lcm. □

Proposition 3.3. *A monomial φ is in $R \cap \Sigma_{s-1}$ if and only if there exists an $i \in \mathcal{G}$ such that $\mathrm{lm}_{s-1}(G_i)|\varphi$ or there exists a $j \in \mathcal{F}$ such that $\mathrm{lm}_{s-1}(F_j) \in R \cap \Delta_s$ and $\mathrm{lm}_{s-1}(F_j)|\varphi$.*

Proof. Both $\mathrm{lm}_{s-1}(G_i)|\varphi$ and $\mathrm{lm}_{s-1}(F_j)|\varphi$ imply $\varphi \in R \cap \Sigma_{s-1}$. Let us show the converse. If $\varphi \in R \cap \Sigma_s$, then $\mathrm{lm}_s(G_i)|\varphi$ for some $i \in \mathcal{G}$, and therefore $\mathrm{lm}_{s-1}(G_i)|\varphi$. As $R \cap \Sigma_{s-1} \supset R \cap \Sigma_s$, it remains to consider the case when $\varphi \in R \cap (\Sigma_{s-1} \setminus \Sigma_s)$.

Suppose $f \in M$ is such that $\varphi = \mathrm{lm}_{s-1}(f) \in R \cap (\Sigma_{s-1} \setminus \Sigma_s)$. Since $\varphi \notin R \cap \Sigma_s$, we must have $\mathrm{lm}_s(f) \in Rz$, and hence by Lemma 2.1, $\delta(f^U) + s = \delta(f^D) = \delta(\varphi)$. Then $\mathrm{lm}_s(F_j)|\mathrm{lm}_s(f)$ for some $j \in \mathcal{F}$. As $\mathrm{lm}_s(F_j) \in Rz$, we have $\delta(F_j^U) + s \geq \delta(F_j^D)$, where actually equality holds as we will show now. Assume the contrary, that is, $\delta(F_j^U) + s > \delta(F_j^D)$. Then

$$\delta(\frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F_j^D) = \delta(f^U) - \delta(F_j^U) + \delta(F_j^D) < \delta(f^U) + s = \delta(f^D),$$
$$\delta(\frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F_j^U) = \delta(f^U) - \delta(F_j^U) + \delta(F_j^U) = \delta(f^U).$$

These imply $\mathrm{lm}_s(f - \frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F) = \mathrm{lm}(f^D) = \mathrm{lm}_{s-1}(f) = \varphi$, contradictory to the assumption $\varphi \notin R \cap \Sigma_s$. Hence $\delta(F_j^U) + s = \delta(F_j^D)$, and

$$\delta(\frac{\mathrm{lm}_s(f)}{\mathrm{lm}_s(F_j)}\mathrm{lm}_{s-1}(F_j)) = \delta(f^U) - \delta(F_j^U) + \delta(F_j^D) = \delta(f^U) + s = \delta(\varphi).$$

Therefore $\mathrm{lm}_{s-1}(F_j)|\varphi$, and $\mathrm{lm}_{s-1}(F_j) \in R \cap \Delta_s$. □

Proposition 3.4. *A monomial φ is in $Rz \cap \Sigma_{s-1}$ if and only if there exists a $j \in \mathcal{F}$ such that $\mathrm{lm}_{s-1}(f)|\varphi$ for some $f \in \mathrm{spoly}(F_j)$.*

Proof. By Proposition 3.2, the converse is clear. Let us assume $\varphi \in Rz \cap \Sigma_{s-1}$. Suppose $\varphi = \mathrm{lm}_{s-1}(f)$ for some $f \in M$. Then $\varphi = \mathrm{lm}_s(f)$, and there exists some $j \in \mathcal{F}$ such that $\mathrm{lm}_s(F_j)|\varphi$. If $\mathrm{lm}_{s-1}(F_j) \in Rz$, then $F_j \in \mathrm{spoly}(F_j)$ and $\mathrm{lm}_{s-1}(F_j) = \mathrm{lm}_s(F_j)|\varphi$.

Suppose $\mathrm{lm}_{s-1}(F_j) \in R\cap\Sigma_s$. Then there is an $i \in \mathcal{G}$ such that $\mathrm{lm}_s(G_i)|\mathrm{lm}_{s-1}(F_j)$ and $\frac{1}{\mathrm{lc}_{s-1}(F_j)}F_j - \frac{\mathrm{lm}_{s-1}(F_j)}{\mathrm{lt}_s(G_i)}G_i \in \mathrm{spoly}(F_j)$ and by (3),

$$\mathrm{lm}_{s-1}(\frac{1}{\mathrm{lc}_{s-1}(F_j)}F_j - \frac{\mathrm{lm}_{s-1}(F_j)}{\mathrm{lt}_s(G_i)}G_i) = \mathrm{lm}_s(F_j)|\varphi.$$

Suppose $\mathrm{lm}_{s-1}(F_j) \in R\cap\Delta_s$. Note that $\delta(f^U)+s > \delta(f^D)$, $\delta(F_j^U)+s = \delta(F_j^D)$, and hence

$$\delta(\frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F_j^U) = \delta(f^U) - \delta(F_j^U) + \delta(F_j^U) = \delta(f^U),$$

$$\delta(\frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F_j^D) = \delta(f^U) - \delta(F_j^U) + \delta(F_j^D) = \delta(f^U) + s > \delta(f^D).$$

Thus we see that $\mathrm{lm}_s(f - \frac{\mathrm{lt}_s(f)}{\mathrm{lt}_s(F_j)}F_j) = \frac{\mathrm{lm}_s(f)}{\mathrm{lm}_s(F_j)}\mathrm{lm}_{s-1}(F_j) \in R$ and hence there is an $i \in \mathcal{G}$ such that $\mathrm{lm}_s(G_i)|\frac{\mathrm{lm}_s(f)}{\mathrm{lm}_s(F_j)}\mathrm{lm}_{s-1}(F_j)$. Now there is an lcm ψ of $\mathrm{lm}_{s-1}(F_j)$ and $\mathrm{lm}_s(G_i)$ such that

$$\psi|\frac{\mathrm{lm}_s(f)}{\mathrm{lm}_s(F_j)}\mathrm{lm}_{s-1}(F_j), \tag{4}$$

and $\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i \in \mathrm{spoly}(F_j)$. By (3), $\mathrm{lm}_{s-1}(\frac{\psi}{\mathrm{lt}_{s-1}(F_j)}F_j - \frac{\psi}{\mathrm{lt}_s(G_i)}G_i) = \frac{\psi}{\mathrm{lm}_{s-1}(F_j)}\mathrm{lm}_s(F_j) \in Rz$ and finally from (4), $\frac{\psi}{\mathrm{lm}_{s-1}(F_j)}\mathrm{lm}_s(F_j)|\mathrm{lm}_s(f) = \varphi$. □

Combining the above results, we obtain

Theorem 3.5. *Suppose that $\{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$ is a Gröbner basis of M with respect to $>_s$. Then*

$$\{G_i, F_j \mid i \in \mathcal{G}, j \in \mathcal{F}, \mathrm{lm}_{s-1}(F_j) \in R \cap \Delta_s\} \cup \bigcup_{j\in\mathcal{F}} \mathrm{spoly}(F_j)$$

is a Gröbner basis of M with respect to $>_{s-1}$.

In general, the Gröbner basis may contain more elements than necessary. Indeed, we can reduce each set in the union by removing the redundant elements whose leading term is divisible by that of other elements in the set. We will denote this *reduced* Gröbner basis of M with respect to $>_{s-1}$ by

$$\{G_i, F_j \mid i \in \mathcal{G}, j \in \mathcal{F}, \mathrm{lm}_{s-1}(F_j) \in R \cap \Delta_s\}' \cup {\bigcup_{j\in\mathcal{F}}}' \mathrm{spoly}(F_j) \tag{5}$$

4. Message Selection

The ideal of the error vector e defined by $J_e = \bigcap_{e_i \neq 0} \mathfrak{m}_i$ has a Gröbner basis $\{\epsilon_i \mid i \in \mathcal{E}\}$ with respect to $>$, and

$$\dim_{\mathbb{F}} R/J_e = |\Delta(J_e)| = \mathrm{wt}(e). \tag{6}$$

Recall that $B^{(s)} = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$ is a Gröbner basis of $I_{v^{(s)}}$ with respect to $>_s$. Observe that $J_e(z - \mu^{(s)}) \subset I_{v^{(s)}}$, which results in $\Sigma(J_e)z \subset \Sigma_s(I_{v^{(s)}}) \cap Rz$, and hence $\Delta_s(I_{v^{(s)}}) \cap Rz \subset \Delta(J_e)z$. Therefore

$$|\Delta_s(I_{v^{(s)}}) \cap Rz| = |\Delta(F_j^U)| \leq \mathrm{wt}(e).$$

Now let s be a nongap $\leq u$. Let us consider the module

$$\tilde{I}_w = \{f(z + w\varphi_s) \mid f \in I_{v^{(s)}}\} \subset Rz \oplus R.$$

for $w \in \mathbb{F}$. Note that $\tilde{B} = \{G_i(z + w\varphi_s) \mid i \in \mathcal{G}\} \cup \{F_j(z + w\varphi_s) \mid j \in \mathcal{F}\}$ is a Gröbner basis of $\tilde{I}_w$ with respect to $>_s$ since $\mathrm{lm}_s(f(z + w\varphi_s)) = \mathrm{lm}_s(f)$ for all $f \in I_{v^{(s)}}$. For the same reason, $\Sigma_s(\tilde{I}_w) = \Sigma_s(I_{v^{(s)}})$, $\Delta_s(\tilde{I}_w) = \Delta_s(I_{v^{(s)}})$. Observe that $\tilde{I}_{\omega_s} = I_{v^{(s-1)}}$. Hence

$$|\Delta_{s-1}(\tilde{I}_{\omega_s}) \cap Rz| \leq \mathrm{wt}(e). \tag{7}$$

In Theorem 4.3 below, we will characterize ω_s as such a w that makes the value $|\Delta_{s-1}(\tilde{I}_w) \cap Rz|$ smallest, provided that $\mathrm{wt}(e)$ is not too large. Recall that $|\Delta_s(\tilde{I}_w) \cap R| + |\Delta_s(\tilde{I}_w) \cap Rz| = |\Delta_s(\tilde{I}_w)| = n$ in the following arguments.

Lemma 4.1. *For $w \neq \omega_s$, $|\Delta_{s-1}(\tilde{I}_w) \cap Rz| \geq n - |\Delta(J_e\varphi_s) \cap \Delta(J)|$.*

Proof. Observe that $J_e(z - (\omega_s - w)\varphi_s - \mu^{(s-1)}) \subset \tilde{I}_w$ and $J \subset \tilde{I}_w$. Therefore $\Sigma(J_e\varphi_s) \cup \Sigma(J) \subset \Sigma_{s-1}(\tilde{I}_w) \cap R$, and $\Delta_{s-1}(\tilde{I}_w) \cap R \subset \Delta(J_e\varphi_s) \cap \Delta(J)$. Hence $|\Delta_{s-1}(\tilde{I}_w) \cap R| \leq |\Delta(J_e\varphi_s) \cap \Delta(J)|$, equivalent to the second equality. $\square$

Lemma 4.2. $|\Delta(J_e\varphi_s)| = \mathrm{wt}(e) + s$.

Proof. Note that

$$\begin{aligned} |\Delta(J_e\varphi_s)| &= |\Sigma(R) \setminus \Sigma(J_e\varphi_s)| = |\Delta(J_e)| + |\Sigma(R) \setminus \Sigma(R\varphi_s)| \\ &= \mathrm{wt}(e) + |S \setminus (s + S)| = \mathrm{wt}(e) + s. \end{aligned}$$

The equality $|S \setminus (s + S)| = s$ holds for any numerical semigroup S, since S is closed under addition and contains all large enough integers. $\square$

Theorem 4.3. *The value* $|\Delta_{s-1}(\tilde{I}_w) \cap Rz|$ *is smallest for* $w = \omega_s$, *provided that* $|\Delta(J) \cup \Delta(R\varphi_s)| - s > 2\mathrm{wt}(e)$.

Proof. We need to show that for $w \neq \omega_s$, $|\Delta_{s-1}(\tilde{I}_w) \cap Rz| > |\Delta_{s-1}(\tilde{I}_{\omega_s}) \cap Rz|$. By (7) and the previous lemmas, a sufficient condition for the above is

$$\begin{aligned} & n - |\Delta(J) \cap \Delta(J_e\varphi_s)| > \mathrm{wt}(e) \\ \iff & n - |\Delta(J)| - |\Delta(J_e\varphi_s)| + |\Delta(J) \cup \Delta(J_e\varphi_s)| > \mathrm{wt}(e) \\ \iff & |\Delta(J) \cup \Delta(J_e\varphi_s)| - s > 2\mathrm{wt}(e) \end{aligned}$$

since $|\Delta(J)| = n$. Finally note that $|\Delta(J) \cup \Delta(J_e\varphi_s)| \geq |\Delta(J) \cup \Delta(R\varphi_s)|$. $\square$

Note that $|\Delta_{s-1}(\tilde{I}_w) \cap Rz|$ is smallest when so is

$$\begin{aligned} |\Delta_{s-1}(\tilde{I}_w) \cap Rz| - |\Delta_s(\tilde{I}_w) \cap Rz| &= |\Delta_s(\tilde{I}_w) \cap R| - |\Delta_{s-1}(\tilde{I}_w) \cap R| \\ &= |(\Delta_s(\tilde{I}_w) \setminus \Delta_{s-1}(\tilde{I}_w)) \cap R)| \\ &= |\Sigma_{s-1}(\tilde{I}_w) \cap \Delta_s(\tilde{I}_w) \cap R|. \end{aligned}$$

since $|\Delta_s(\tilde{I}_w) \cap Rz| = |\Delta_s(I_{v^{(s)}}) \cap Rz|$ is independent of w. The value $|\Sigma_{s-1}(\tilde{I}_w) \cap \Delta_s(\tilde{I}_w) \cap R|$ can be computed using the Gröbner bases of $\tilde{I}_w$ with respect to $>_s$ and $>_{s-1}$. As we saw in Section 3, the Gröbner basis of $\tilde{I}_w$ with respect to $>_{s-1}$ is determined from $\tilde{B}$, the Gröbner bases of $\tilde{I}_w$ with respect to $>_s$. Precisely, according to Proposition 3.3, the set $\Sigma_{s-1}(\tilde{I}_w) \cap \Delta_s(\tilde{I}_w) \cap R$ is determined by the monomials $\mathrm{lm}_{s-1}(F_j(z + w\varphi_s))$, $j \in \mathcal{F}$ that lies in $\Delta_s(\tilde{I}_w) \cap R$.

We note that for each $j \in \mathcal{F}$, there is a unique $w_j \in \mathbb{F}$ such that $\mathrm{lm}_{s-1}(F_j(z + w_j\varphi_s)) \in Rz$, and $\mathrm{lm}_{s-1}(F_j(z + w\varphi_s)) = \mathrm{lm}(F_j^U\varphi_s) \in R$ if and only if $w \neq w_j$. In fact, $w_j = -\frac{d}{\mathrm{lc}(F_j^U)}$, where d is the coefficient of the monomial $\mathrm{lm}(F_j^U\varphi_s)$ in F_j^D.

Proposition 4.4. *Let* $\sqcup$ *denote disjoint union. We have*

$$\begin{aligned} \Sigma_{s-1}(\tilde{I}_w) \cap \Delta_s(\tilde{I}_w) \cap R &= \bigcup_{j \in \mathcal{F}, w_j \neq w} \Sigma_{s-1}(F_j(z + w\varphi_s)) \cap \Delta_s(\tilde{I}_w) \\ &= \bigsqcup_{c \in \mathbb{F}, c \neq w} \bigcup_{j \in \mathcal{F}, w_j = c} \Sigma_{s-1}(F_j(z + w\varphi_s)) \cap \Delta_s(\tilde{I}_w). \end{aligned}$$

Proof. The first equality follows from Proposition 3.3. It remains to show that the second union is disjoint. Assume that for $c_1, c_2 \in \mathbb{F}$ with $c_1 \neq c_2$, there is a monomial $\varphi \in R$ such that φ is in the intersection of

$$\bigcup_{j \in \mathcal{F}, w_j = c_1} \Sigma_{s-1}(F_j(z + w\varphi_s)) \cap \Delta_s(\tilde{I}_w)$$

and

$$\bigcup_{j \in \mathcal{F}, w_j = c_2} \Sigma_{s-1}(F_j(z + w\varphi_s)) \cap \Delta_s(\tilde{I}_w).$$

Let $\varphi = \psi\mathrm{lm}_{s-1}(F_{j_1}(z+w\varphi_s)) = \chi\mathrm{lm}_{s-1}(F_{j_2}(z+w\varphi_s))$ with $w_{j_1} = c_1$, $w_{j_2} = c_2$, and monomials ψ, χ. Then we will show that

$$\mathrm{lm}_s(\frac{\psi}{\mathrm{lc}(F^U_{j_1})}F_{j_1}(z+w\varphi_s) - \frac{\chi}{\mathrm{lc}(F^U_{j_2})}F_{j_2}(z+w\varphi_s)) = \varphi, \tag{8}$$

contradicting the assumption that $\varphi \in \Delta_s(\tilde{I}_w)$. Indeed notice that $\varphi = \mathrm{lm}(\psi F^U_{j_1}\varphi_s) = \mathrm{lm}(\chi F^U_{j_2}\varphi_s)$. Hence the coefficient of the monomial φ in the first term of the polynomial in (8) is $\frac{1}{\mathrm{lc}(F^U_{j_1})}(w + d_1)$ where d_1 is the coefficient of the monomial $\mathrm{lm}(F^U_{j_1}\varphi_s)$ in $F^D_{j_1}$. In the same way, the coefficient of the monomial φ in the second term after the minus in (8) is $\frac{1}{\mathrm{lc}(F^U_{j_2})}(w + d_2)$ where d_2 is the coefficient of the monomial $\mathrm{lm}(F^U_{j_2}\varphi_s)$ in $F^D_{j_2}$. These two coefficients are different because we assumed

$$w_{j_1} = -\frac{d_1}{\mathrm{lc}(F^U_{j_1})} \neq w_{j_2} = -\frac{d_2}{\mathrm{lc}(F^U_{j_2})}.$$

Hence (8) follows. □

We observe that for $c, w \in \mathbb{F}$ with $w \neq c$,

$$\bigcup_{j\in\mathcal{F},w_j=c} \Sigma_{s-1}(F_j(z+w\varphi_s)) \cap \Delta_s(\tilde{I}_w) = \bigcup_{j\in\mathcal{F},w_j=c} \Sigma(F^U_j\varphi_s) \cap \Delta\{G^D_i \mid i \in \mathcal{G}\}.$$

Therefore this set is independent of w, and is determined by $B^{(s)}$. Let

$$d_c = \Big|\bigcup_{j\in\mathcal{F},w_j=c} \Sigma(F^U_j\varphi_s) \cap \Delta\{G^D_i \mid i \in \mathcal{G}\}\Big|.$$

Then Proposition 4.4 implies $|\Delta_{s-1}(\tilde{I}_w) \cap Rz| - |\Delta_s(\tilde{I}_w) \cap Rz| = \sum_{c\in\mathbb{F},c\neq w} d_c$ is smallest when $w = c$ with d_c largest. Now we elaborate the main steps of the interpolation decoding algorithm as follows.

- **M1:** If s is a nongap $\leq u$, then do the following. Otherwise let $\tilde{B} = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$.
  - **M1.1:** Compute the set $W = \{w_j \mid j \in \mathcal{F}\}$, where $w_j = -\frac{d}{\mathrm{lc}(F^U_j)}$, and d is the coefficient of the monomial $\mathrm{lm}(F^U_j\varphi_s)$ in F^D_j.
  - **M1.2:** Let $w^{(s)} = c \in W$ with largest $d_c = \Big|\bigcup_{w_j=c}\Sigma(F^U_j\varphi_s) \cap \Delta(\{G^D_i\})\Big|$.
  - **M1.3:** Let $\tilde{B} = \{G_i(z+w^{(s)}\varphi_s) \mid i \in \mathcal{G}\} \cup \{F_j(z+w^{(s)}\varphi_s) \mid j \in \mathcal{F}\}$.
- **M2:** Let $\tilde{B} = \{\tilde{G}_i \mid i \in \mathcal{G}\} \cup \{\tilde{F}_j \mid j \in \mathcal{F}\}$. Compute

$$B^{(s-1)} = \{\tilde{G}_i, \tilde{F}_j \mid i \in \mathcal{G}, j \in \mathcal{F}, \mathrm{lm}_{s-1}(\tilde{F}_j) \in R \cap \Delta_s\}' \cup \bigcup_{j\in\mathcal{F}}{}' \mathrm{spoly}(\tilde{F}_j).$$

Theorem 4.5. *The algorithm outputs $w^{(s)} = \omega_s$ for all $s \in S, s \leq u$ if*

$$d_u = \min_{s\in S,s\leq u} \nu(s) > 2\mathrm{wt}(e),$$

where $\nu(s) = |\Delta(J) \cup \Delta(R\varphi_s)| - s$ *for* $s \in S$. *Moreover* $d_u \geq n - u$.

Proof. By Theorem 4.3, the condition $d_u > 2\mathrm{wt}(e)$ implies that the algorithm computes $w^{(s)} = \omega_s$ for each iteration for nongap s from u to 0. To see $d_u \geq n-u$, notice that $|\Delta(J) \cup \Delta(R\varphi_s)| \geq |\Delta(J)| = n$. □

5. Decoding Hermitian Codes

Let us consider the Hermitian code C_u defined on the Hermitian curves with equation $Y^q + Y - X^{q+1} = 0$ over $\mathbb{F}_{q^2}$. There are q^3 rational points on the Hermitian curve, and $J = \langle x^{q^2} - x\rangle$. In Theorem 5.1, we determine the performance of the decoding algorithm for C_u. Recall that the same result was proved for the previous algorithm in Proposition 14 in [4], but the proof for the present algorithm is clearer and short.

Theorem 5.1. *For nongap* $u < q^3$, *let* $u = aq+b$, $0 \leq b < q$. *Then* $d_u = q^3 - aq$ *if* $b \leq a + q - q^2$ *and* $d_u = q^3 - u$ *if* $b > a + q - q^2$.

Proof. We first compute $\nu(s)$ for nongap $s = qs_1 + s_2 < q^3$. As

$$|\Delta(J) \cup \Delta(R\varphi_s)| = |\Sigma(J) \cap \Delta(R\varphi_s)| + |\Delta(J)| = |\{t \in S \mid q^3 + t \notin s + S\}| + q^3.$$

we have $\nu(s) = |\{t \in S \mid q^3 + t - s \notin S\}| + q^3 - s$. Note that $q^3 + t - s = q(q^2 + t_1 - s_1) + t_2 - s_2$ with $t = qt_1 + t_2$. Therefore $q^3 + t - s \notin S$ if and only if $t_2 - s_2 \geq 0$, $q^2 + t_1 - s_1 < t_2 - s_2$ or $t_2 - s_2 < 0$, $q^2 + t_1 - s_1 < q + 1 + t_2 - s_2$. The first case is actually impossible since $s_1 < q^2$. Hence

$$|\{t \in S \mid q^3 + t - s \notin S\}| = s_2 \max\{s_1 - s_2 + q + 1 - q^2, 0\}.$$

Thus $\nu(s) = s_2 \max\{s_1 - s_2 + q + 1 - q^2, 0\} + q^3 - s$ for $s = qs_1 + s_2 < q^3$. If $a-b+q-q^2 \geq 0$, then the minimum is attained at $s = aq$, and hence $d_u = q^3 - aq$ while if $a - b + q - q^2 < 0$, then the minimum is attained at $s = u$, and hence $d_u = q^3 - u$. □

Now we demonstrate the decoding algorithm, using the same example in [4] to facilitate a comparison with the previous algorithm. So we use the Hermitian curve $y^3 + y - x^4 = 0$ over $\mathbb{F}_9$, where $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ with $\alpha^2 - \alpha - 1 = 0$. There are 27 rational points on the affine part of the curve and a unique point P_∞ at infinity. As $\delta(x) = 3$ and $\delta(y) = 4$, the numerical semigroup of the coordinate ring R is $S = 3\mathbb{N} + 4\mathbb{N} = \{0, 3, 4, 6, 7, 8, 9, 10, \ldots\}$. Note that S has three gaps 1, 2, and 5. The monomials of R correspond to nongaps in S and are displayed in the diagram

y^2	xy^2	x^2y^2	x^3y^2	x^4y^2	x^5y^2	x^6y^2	x^7y^2	x^8y^2	x^9y^2	$\cdots$
y	xy	x^2y	x^3y	x^4y	x^5y	x^6y	x^7y	x^8y	x^9y	$\cdots$
1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	$\cdots$

Let $u = 16$. Then the Hermitian code C_{16} has dimension 14 and minimum distance 11, and the decoding algorithm can correct up to 5 errors. Suppose we received the vector

$$v = (0,0,0,\alpha^5,\alpha^2,\alpha,\alpha^6,\alpha^2,2,\alpha^5,2,\alpha^2,\alpha^5,\alpha^2,2,\alpha^5,2,\\ \alpha^2,\alpha^5,\alpha^5,\alpha^2,\alpha^5,\alpha^2,\alpha^2,\alpha^5,\alpha,2)$$

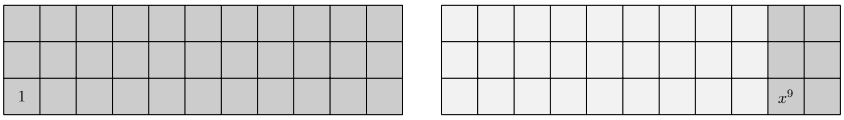
from a noisy channel. Let us follow the steps of the decoding algorithm.

The algorithm first compute the Lagrange interpolation of v,

$$h_v = \alpha^3x^8y^2 + x^7y^2 + \cdots + \alpha^2x^3 + \alpha^3xy + x.$$

The algorithm iterates the main steps for s from $N = \delta(h_v) = 32$ to 0. The ideal J has Gröbner basis $\{\eta_1 = x^9 - x\}$. Hence the Gröbner basis of $I_{v^{(32)}} = I_v$ is

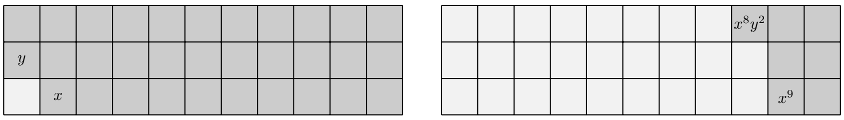
$$B^{(32)} = \left\{ \begin{array}{cccc} G_1 & = & 0\,z & + & x^9 - x \\ F_1 & = & 1\,z & + & \alpha^7x^8y^2 + \cdots \end{array} \right\}$$



Here the left diagram exhibits the monomials in $\Sigma_{32}(I_{v^{(32)}}) \cap Rz$ omitting the common z variable, while the right diagram shows the monomials in $\Sigma_{32}(I_{v^{(32)}}) \cap R$. The leading terms of the polynomials in the Gröbner basis are also shown.

For $s \geq u = 16$ or a gap s, as $\tilde{B} = B^{(s)} = \{G_i \mid i \in \mathcal{G}\} \cup \{F_j \mid j \in \mathcal{F}\}$ in the step **M1**, we will omit the tilde in the following. In the step **M2**, $\mathrm{lm}_{31}(F_1) = x^8y^2 \in \Delta_{32}(G_1) \cap R$, and the lcms of $\mathrm{lm}_{31}(F_1) = x^8y^2$ and $\mathrm{lm}_{32}(G_1) = x^9$ are x^9y^2 and x^{12}. Hence $\mathrm{spoly}(F_1) = \{\alpha xz + \alpha^5x^8y^2 + \cdots + \alpha^5x^2, \alpha yz + \alpha^5x^{11} + \cdots + \alpha^2xy\}$. Then the Gröbner basis of $I_{v^{(31)}}$ is

$$B^{(31)} = \left\{ \begin{array}{ccrcl} G_1 & = & 0\,z & + & x^9 + \cdots \\ G_2 & = & 1\,z & + & \alpha^7x^8y^2 + \cdots \\ F_1 & = & \alpha x\,z & + & \alpha^5x^8y^2 + \cdots \\ F_2 & = & \alpha y\,z & + & \alpha^5x^{11} + \cdots \end{array} \right\}$$



As $\mathrm{lm}_s(F_1), \mathrm{lm}_s(F_2) \in Rz$ for $s = 31, 30$, there is no change in the Gröbner basis. So we get to the unaltered Gröbner basis of $I_{v^{(29)}}$

$$B^{(29)} = \left\{ \begin{array}{ccrcl} G_1 & = & 0\,z & + & x^9 + \cdots \\ G_2 & = & 1\,z & + & \alpha^7x^8y^2 + \cdots \\ F_1 & = & \alpha x\,z & + & \alpha^5x^8y^2 + \cdots \\ F_2 & = & \alpha y\,z & + & \alpha^5x^{11} + \cdots \end{array} \right\}$$

Now since $\mathrm{lm}_{29}(G_2) = x^8y^2$ divides $\mathrm{lm}_{28}(F_1) = x^8y^2$ and $\mathrm{lm}_{29}(G_1) = x^9$ divides $\mathrm{lm}_{28}(F_2) = x^{11}$, both $\mathrm{lm}_{28}(F_1)$ and $\mathrm{lm}_{28}(F_2)$ are in $\Sigma_{29}(G_1, G_2) \cap R$

Thus

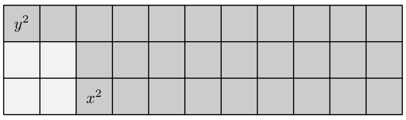
$$\begin{aligned}\mathrm{spoly}(F_1) &= \{2xz + \alpha^5 z + \alpha^6 x^9 y + \cdots + \alpha x\},\\ \mathrm{spoly}(F_2) &= \{2yz + \alpha^6 x^8 y^2 + \cdots + \alpha^5 xy\}.\end{aligned}$$

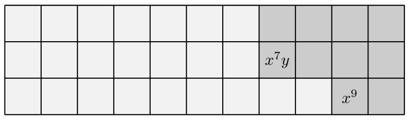
Hence the Gröbner basis of $I_{v^{(28)}}$ is

$$B^{(28)} = \left\{\begin{array}{ccrcl} G_1 & = & 0\,z & + & x^9 + \cdots \\ G_2 & = & 1\,z & + & \alpha^7 x^8 y^2 + \cdots \\ F_1 & = & (2x+\alpha^5)\,z & + & \alpha^6 x^9 y + \cdots \\ F_2 & = & 2y\,z & + & \alpha^6 x^8 y^2 + \cdots \end{array}\right\}$$

Similar steps are iterated. Eventually, we get to the Gröbner basis of $I_{v^{(16)}}$,

$$B^{(16)} = \left\{\begin{array}{ccrcl} G_1 & = & 0\,z & + & x^9 + \cdots \\ G_2 & = & (\alpha^2 xy + \dots)\,z & + & \alpha^2 x^7 y + \cdots \\ F_1 & = & (\alpha^2 x^2 + \cdots)\,z & + & \alpha^7 x^6 y + \cdots \\ F_2 & = & (\alpha^5 y^2 + \cdots)\,z & + & \alpha^7 x^8 + \cdots \end{array}\right\}$$

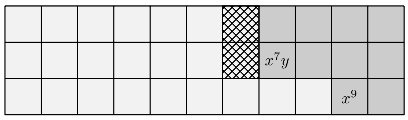




Now $s = 16$ is a nongap and $\leq u = 16$. So in the step **M1**, we proceed to select ω_{16} for the monomial $\varphi_{16} = x^4 y$. The leading coefficient of F_1 is α^2 and the coefficient of the monomial $x^6 y$ in F_1 is α^7, where $x^6 y$ is the leading monomial of $x^2\varphi_{16}$. Hence $w_1 = -(\alpha^7/\alpha^2) = \alpha$. The leading coefficient of F_2 is α^5 and the coefficient of the monomial x^8 in F_2 is α^7, where x^8 is the leading monomial of $y^2\varphi_{16}$. Hence $w_2 = -(\alpha^7/\alpha^5) = \alpha^6$. So $W = \{\alpha, \alpha^6\}$. The shape of

$$\bigcup_{j\in\mathcal{F}, w_j=\alpha} \Sigma(F_j^U \varphi_{16}) \cap \Delta(\{G_i^D \mid i \in \mathcal{G}\}) = \Sigma(x^6 y) \cap \Delta(x^9, x^7 y)$$

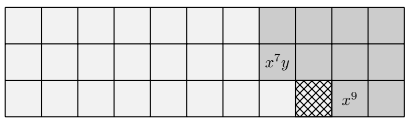
is



and thus $d_\alpha = 2$. On the other hand, the shape of

$$\bigcup_{j\in\mathcal{F}, w_j=\alpha^6} \Sigma(F_j^U \varphi_{16}) \cap \Delta(\{G_i^D \mid i \in \mathcal{G}\}) = \Sigma(x^8) \cap \Delta(x^9, x^7 y)$$

is



and thus $d_{\alpha^6} = 1$. Hence we take $w^{(16)} = \alpha$. Then

$$\tilde{B} = \left\{ \begin{array}{lcrcl} \tilde{G}_1 & = & 0\,z & + & x^9 + \cdots \\ \tilde{G}_2 & = & (\alpha^2 xy + \ldots)\,z & + & \alpha^2 x^7 y + \cdots \\ \tilde{F}_1 & = & (\alpha^2 x^2 + \cdots)\,z & + & 0 \\ \tilde{F}_2 & = & (\alpha^5 y^2 + \cdots)\,z & + & x^8 + \cdots \end{array} \right\}$$

In the step **M2**, $\mathrm{lm}_{15}(\tilde{F}_1) = x^2 z \in Rz$ and $\mathrm{lm}_{15}(\tilde{F}_2) = x^8 \in \Delta_{15}(\tilde{G}_1, \tilde{G}_2) \cap R$. So $\mathrm{spoly}(\tilde{F}_1) = \{\tilde{F}_1\}$, and since the lcm of $\mathrm{lm}_{15}(\tilde{F}_2) = x^8$ and $\mathrm{lm}_{15}(\tilde{G}_1) = x^9$ is x^9, and the lcms of $\mathrm{lm}_{15}(\tilde{F}_2)$ and $\mathrm{lm}_{15}(\tilde{G}_2) = x^7 y$ are $x^8 y$ and x^{11},

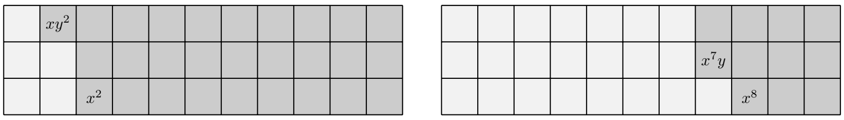
$$\mathrm{spoly}(\tilde{F}_2) = \{\alpha^5 xy^2 z + \cdots + x, \alpha^5 x^4 z + \cdots + x^2, \alpha^5 x^3 y^2 z + \cdots + \alpha^5 xy\}.$$

Removing redundant elements, we have

$$\{\tilde{G}_1, \tilde{G}_2, \tilde{F}_2\}' = \{\tilde{G}_2, \tilde{F}_2\},$$
$$(\mathrm{spoly}(\tilde{F}_1) \cup \mathrm{spoly}(\tilde{F}_2))' = \{\tilde{F}_1, \alpha^5 xy^2 z + \cdots + x\}.$$

Thus the Gröbner basis of $I_{v^{(15)}}$ is

$$B^{(15)} = \left\{ \begin{array}{lcrcl} G_1 & = & (\alpha^2 xy + \cdots)\,z & + & \alpha^2 x^7 y + \cdots \\ G_2 & = & (\alpha^5 y^2 + \cdots)\,z & + & x^8 + \cdots \\ F_1 & = & (\alpha^2 x^2 + \cdots)\,z & + & 0 \\ F_2 & = & (\alpha^5 xy^2 + \cdots)\,z & + & 2x^7 y + \cdots \end{array} \right\}$$



Continuing in this way, after the last iteration for $s = 0$, we get to the Gröbner basis of $I_{v^{(-1)}}$,

$$B^{(-1)} = \left\{ \begin{array}{lcrcl} G_1 & = & (\alpha^2 xy + \cdots)\,z & + & \alpha^2 x^7 y + \cdots \\ G_2 & = & (\alpha^5 y^2 + \cdots)\,z & + & x^8 + \cdots \\ F_1 & = & (\alpha^2 x^2 + \cdots)\,z & + & 0 \\ F_2 & = & (xy^2 + \cdots)\,z & + & 0 \end{array} \right\}$$

Finally, the algorithm output the recovered message

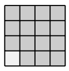
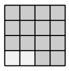
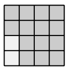
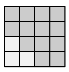
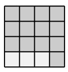
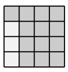
$$(0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \alpha).$$

6. Final Remarks

By carefully counting the number of finite field multiplication operations needed for an execution of the algorithm for the received vector with $\mathrm{wt}(e) \leq \tau$, we can estimate the complexity of the algorithm as $\mathcal{O}(a^4 b^3)$. With the assumptions $\mathcal{O}(n) = \mathcal{O}(a^3)$ and $\mathcal{O}(a) = \mathcal{O}(b)$, this is the same complexity $\mathcal{O}(n^{7/3})$ that Sakata et al. obtained for the algorithm in [7].

We now discuss on the advantages of the present algorithm compared with the previous one in [4], in terms of time and space complexity. First note that by the structure of both algorithms, the decoding time and the size of the required space are largely dictated by the number of polynomials that needs to be kept and updated by the algorithm through the iterations. Recall that the present algorithm works with the Gröbner bases of modules over the coordinate ring $\mathbb{F}[x, y]$, which is realized as the quotient ring of the two-variate polynomial ring modulo the curve equation (1), while the previous algorithm works with the Gröbner bases of the same modules but viewed as modules over $\mathbb{F}[x]$. Thus the previous algorithm, from the start, keeps and updates at each iteration $2a$ polynomials in $Rz \oplus R$. On the other hand, the present algorithm starts with at least 2 polynomials in $Rz \oplus R$, and keeps and updates polynomials whose number grows through the iterations to at most $2a$, the precise number depending on the "shape of the error", $\Delta(J_e)$.

For the example in Section 5 and also in Section IV of [4], where $a = 3$, the previous algorithm always keeps and updates 6 polynomials, and the present algorithm starts with 2 polynomials and ends with 4 polynomials. This difference gets amplified as we consider longer codes. For the $[64, 53, 8]$ Hermitian code C_{58} over $\mathbb{F}_{16}$, which has the largest dimension among the Hermitian codes of length 64 that can correct up to 3 errors, the following table shows the counts of the possible shapes of the errors.

wt(e)	shape of the error (number of error positions)	total number
1	 (64)	$\binom{64}{1} = 64$
2	 (1920)  (96)	$\binom{64}{2} = 2016$
3	 (39680)  (1920)  (64)	$\binom{64}{3} = 41664$

We can see from the table that the number of F_j in $B^{(s)}$ is bounded above by 2 when $\mathrm{wt}(e) = 1$ or 2, and by 3 when $\mathrm{wt}(e) = 3$. The number of G_i in $B^{(s)}$ is bounded above by 4 but usually comes close to the number of F_j, as observed in experiments. This contrasts with 8 polynomials kept and updated by the previous algorithm independent of the number of errors.

For a fair comparison, however, we should note that for the present algorithm to take full advantage of this smaller size of Gröbner bases, it needs to efficiently compute the reduced Gröbner basis (5) by avoiding to compute unnecessary polynomials in $\mathrm{spoly}(F_j)$, those that would be discarded anyway to reduce the Gröbner basis. To summarize, the present algorithm has the potential to run faster and use smaller space than the previous algorithm, but the final winner would depend on implementation details in software or hardware.

Finally the author thanks the anonymous referees for valuable comments.

References

1. Gui Liang Feng and T. T. N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. Inf. Theory **39** (1993), no. 1, 37–45.
2. Patrick Fitzpatrick, *On the key equation*, IEEE Trans. Inf. Theory **41** (1995), no. 5, 1290–1302.
3. Ralf Kötter, *A fast parallel implementation of a Berlekamp-Massey algorithm for algebraic-geometric codes*, IEEE Trans. Inf. Theory **44** (1998), no. 4, 1353–1368.
4. Kwankyu Lee, Maria Bras-Amorós, and Michael E. O'Sullivan, *Unique decoding of plane AG codes via interpolation*, IEEE Trans. Inf. Theory **58** (2012), no. 6, 3941–3950.
5. Shinji Miura, *Algebraic geometric codes on certain plane curves*, Electronics and Communications in Japan **76** (1993), no. 12, 1–13.
6. J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, vol. 20, Springer, New York, 2009.
7. S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt, *A fast decoding method of AG codes from Miura-Kamiya curves C_{ab} up to half the Feng-Rao bound*, Finite Fields and Their Applications **1** (1995), no. 1, 83–101.

Kwankyu Lee received the B.Sc., M.Sc., and Ph.D. degrees in mathematics in 1998, 2000, and 2005, respectively, from Sogang University in Korea. He is a professor at Chosun University since 2008. His research interests include algebraic coding theory, commutative algebra, and number theory.

Department of Mathematics and Education, Chosun University, Gwangju 501-759, Korea.
`e-mail: kwankyu@chosun.ac.kr`