Journal of Symbolic Computation 55 (2013) 1–9

Contents lists available at SciVerse ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Generalization of the Lee–O'Sullivan list decoding for one-point AG codes

Ryutaroh Matsumoto [a], Diego Ruano [b], Olav Geil [b]

[a] Department of Communications and Computer Engineering, Tokyo Institute of Technology, 152-8550 Japan
[b] Department of Mathematical Sciences, Aalborg University, Denmark

ARTICLE INFO

Article history:
Received 26 March 2012
Accepted 5 March 2013
Available online 7 March 2013

Keywords:
Algebraic geometry code
Gröbner basis
List decoding

ABSTRACT

We generalize the list decoding algorithm for Hermitian codes proposed by Lee and O'Sullivan (2009) based on Gröbner bases to general one-point AG codes, under an assumption weaker than one used by Beelen and Brander (2010). Our generalization enables us to apply the fast algorithm to compute a Gröbner basis of a module proposed by Lee and O'Sullivan (2009), which was not possible in another generalization by Lax (2012).

1. Introduction

We consider the list decoding problem of one-point algebraic geometry (AG) codes. Guruswami and Sudan (1999) proposed the well-known list decoding algorithm for one-point AG codes, which consists of the interpolation step and the factorization step. The interpolation step has large computational complexity and many researchers have proposed faster interpolation steps, see Beelen and Brander (2010, Figure 1). Lee and O'Sullivan (2009) proposed a faster interpolation step based on the Gröbner basis theory for one-point Hermitian codes. Beelen and Brander (2010) proposed the fastest interpolation procedure for the so-called C_{ab} curves (Miura, 1993) with an additional assumption (Beelen and Brander, 2010, Assumptions 1 and 2). Little (2011) generalized the method in Lee and O'Sullivan (2009) to codes defined using a curve satisfying the same assumption as Beelen and Brander (2010, Assumptions 1 and 2). Lax (2012) generalized part of Lee and O'Sullivan (2009), namely the interpolation ideal, to general algebraic curves, but he did not generalize the faster interpolation algorithm in Lee and O'Sullivan (2009). The aim of this paper is to generalize the faster interpolation algorithm (Lee and O'Sullivan, 2009) to an even wider class of algebraic curves than Little (2011). We shall compare our proposal with the previously known interpolation algorithms for the code on the Klein quartic in Example 12. As a byproduct of our argument, in Corollary 7 we also clarify the

E-mail addresses: ryutaroh@rmatsumoto.org (R. Matsumoto), diego@math.aau.dk (D. Ruano), olav@math.aau.dk (O. Geil).

0747-7171/$ – see front matter
http://dx.doi.org/10.1016/j.jsc.2013.03.001

relation between two different definitions of modules used by Sakata (2001), Lax (2012), and Lee and O'Sullivan (2009) for list decoding.

This paper is organized as follows: Section 2 introduces notations and relevant facts. Section 3 generalizes (Lee and O'Sullivan, 2009). Section 4 concludes the paper. The proposed algorithm in this paper was published without any proof of its correctness in Proc. 2012 IEEE International Symposium on Information Theory (Geil et al., 2012).

2. Notation and preliminary

Our study heavily relies on the standard form of algebraic curves introduced independently by Geil and Pellikaan (2002) and Miura (1998), which is an enhancement of earlier results (Miura, 1993; Saints and Heegard, 1995). Let $F/\mathbf{F}_q$ be an algebraic function field of one variable over a finite field $\mathbf{F}_q$ with q elements. Let g be the genus of F. Fix $n+1$ distinct places $Q, P_1, \ldots, P_n$ of degree one in F and a nonnegative integer u. We consider the following one-point algebraic geometry (AG) code

$$C_u = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(uQ)\}.$$

Suppose that the Weierstrass semigroup $H(Q)$ at Q is generated by $a_1, \ldots, a_t$, and choose t elements $x_1, \ldots, x_t$ in F whose pole divisors are $(x_i)_\infty = a_i Q$ for $i = 1, \ldots, t$. Without loss of generality we may assume the availability of such $x_1, \ldots, x_t$, because otherwise we cannot find a basis of C_u for every u, i.e. we cannot construct the code C_u. Then we have that $\mathcal{L}(\infty Q) = \bigcup_{i=1}^{\infty} \mathcal{L}(iQ)$ is equal to $\mathbf{F}_q[x_1, \ldots, x_t]$ (Saints and Heegard, 1995). We express $\mathcal{L}(\infty Q)$ as a residue class ring $\mathbf{F}_q[X_1, \ldots, X_t]/I$ of the polynomial ring $\mathbf{F}_q[X_1, \ldots, X_t]$, where $X_1, \ldots, X_t$ are transcendental over $\mathbf{F}_q$, and I is the kernel of the canonical homomorphism sending X_i to x_i. Geil and Pellikaan (2002) and Miura (1998) identified the following convenient representation of $\mathcal{L}(\infty Q)$ by using the Gröbner basis theory (Adams and Loustaunau, 1994). The following review is borrowed from Matsumoto and Miura (2000b). Hereafter, we assume that the reader is familiar with the Gröbner basis theory in Adams and Loustaunau (1994).

Let $\mathbf{N}_0$ be the set of nonnegative integers. For $(m_1, \ldots, m_t)$, $(n_1, \ldots, n_t) \in \mathbf{N}_0^t$, we define the weighted reverse lexicographic monomial order $\succ$ such that $(m_1, \ldots, m_t) \succ (n_1, \ldots, n_t)$ if $a_1 m_1 + \cdots + a_t m_t > a_1 n_1 + \cdots + a_t n_t$, or $a_1 m_1 + \cdots + a_t m_t = a_1 n_1 + \cdots + a_t n_t$, and $m_1 = n_1$, $m_2 = n_2$, ..., $m_{i-1} = n_{i-1}$, $m_i < n_i$, for some $1 \leqslant i \leqslant t$. Note that a Gröbner basis of I with respect to $\succ$ can be computed by Saints and Heegard (1995, Theorem 15), Schicho (1998), Tang (1998, Theorem 4.1) or Vasconcelos (1998, Proposition 2.17), starting from any affine defining equations of $F/\mathbf{F}_q$.

Example 1. According to Høholdt and Pellikaan (1995, Example 3.7),

$$u^3 v + v^3 + u = 0$$

is an affine defining equation for the Klein quartic over $\mathbf{F}_8$. There exists a unique $\mathbf{F}_8$-rational place Q such that $(v)_\infty = 3Q$, $(uv)_\infty = 5Q$, and $(u^2 v)_\infty = 7Q$. The numbers 3, 5 and 7 constitute the minimal generating set of the Weierstrass semigroup at Q. Choosing x_1 as v, x_2 as uv and x_3 as $u^2 v$, by Tang (1998, Theorem 4.1) we can see that the standard form of the Klein quartic is given by

$$X_2^2 + X_3 X_1, \qquad X_3 X_2 + X_1^4 + X_2, \qquad X_3^2 + X_2 X_1^3 + X_3,$$

which is the reduced Gröbner basis for I with respect to the monomial order $\succ$. We can see that $a_1 = 3$, $a_2 = 5$, and $a_3 = 7$.

For $i = 0, \ldots, a_1 - 1$, we define $b_i = \min\{m \in H(Q) \mid m \equiv i \pmod{a_1}\}$, and L_i to be the minimum element $(m_1, \ldots, m_t) \in \mathbf{N}_0^t$ with respect to $\prec$ such that $a_1 m_1 + \cdots + a_t m_t = b_i$. Note that the set of b_i's is the well-known Apéry set (Apéry, 1946; Rosales and García-Sánchez, 2009, Lemmas 2.4 and 2.6) of the numerical semigroup $H(Q)$. Then we have $\ell_1 = 0$ if we write L_i as $(\ell_1, \ldots, \ell_t)$. For each $L_i = (0, \ell_{i2}, \ldots, \ell_{it})$, define $y_i = x_2^{\ell_{i2}} \cdots x_t^{\ell_{it}} \in \mathcal{L}(\infty Q)$.

The footprint of I, denoted by $\Delta(I)$, is $\{(m_1, \ldots, m_t) \in \mathbf{N}_0^t \mid X_1^{m_1} \cdots X_t^{m_t}$ is not the leading monomial of any nonzero polynomial in I with respect to $\prec\}$, and define $B = \{x_1^{m_1} \cdots x_t^{m_t} \mid (m_1, \ldots, m_t) \in \Delta(I)\}$.

Then B is a basis of $\mathcal{L}(\infty Q)$ as an $\mathbf{F}_q$-linear space (Adams and Loustaunau, 1994), two distinct elements in B have different pole orders at Q, and

$$\begin{aligned} B &= \left\{x_1^m x_2^{\ell_2}\cdots, x_t^{\ell_t} \;\middle|\; m \in \mathbf{N}_0, (0, \ell_2, \ldots, \ell_t) \in \{L_0, \ldots, L_{a_1-1}\}\right\} \\ &= \left\{x_1^m y_i \mid m \in \mathbf{N}_0, i = 0, \ldots, a_1 - 1\right\}. \end{aligned} \tag{1}$$

Eq. (1) shows that $\mathcal{L}(\infty Q)$ is a free $\mathbf{F}_q[x_1]$-module with a basis $\{y_0, \ldots, y_{a_1-1}\}$. Note that the above structured shape of B reflects the well-known property of every weighted reverse lexicographic monomial order, see the paragraph preceding to Eisenbud (1995, Proposition 15.12).

Example 2. For the curve in Example 1, we have $y_0 = 1$, $y_1 = x_3$, $y_2 = x_2$.

Let v_Q be the unique valuation in F associated with the place Q. The semigroup $H(Q)$ is equal to $\{ia_1 - v_Q(y_j) \mid 0 \leqslant i,\ 0 \leqslant j < a_1\}$ (Rosales and García-Sánchez, 2009, Lemma 2.6).

3. Generalization of Lee–O'Sullivan's list decoding to general one-point AG codes

3.1. Background on Lee–O'Sullivan's algorithm

In the famous list decoding algorithm for the one-point AG codes in Guruswami and Sudan (1999), we have to compute the univariate interpolation polynomial whose coefficients belong to $\mathcal{L}(\infty Q)$. Lee and O'Sullivan (2009) proposed a faster algorithm to compute the interpolation polynomial for the Hermitian one-point codes. Their algorithm was sped up and generalized to one-point AG codes over the so-called C_{ab} curves (Miura, 1993) by Beelen and Brander (2010) with an additional assumption. In this section we generalize Lee–O'Sullivan's procedure to general one-point AG codes with an assumption weaker than Beelen and Brander (2010, Assumption 2), which will be introduced in and used after Assumption 9. The argument before Assumption 9 is true without Assumption 9.

Let m be the multiplicity parameter in Guruswami and Sudan (1999). Lee and O'Sullivan (2009) introduced the ideal $I_{\vec{r},m}$ for Hermitian curves containing the interpolation polynomial corresponding to the received word $\vec{r}$ and the multiplicity m. The ideal $I_{\vec{r},m}$ contains the interpolation polynomial as its nonzero element minimal with respect to the weighted reverse lexicographic monomial order $\prec_u$ to be introduced in Section 3.3. We will give a generalization of $I_{\vec{r},m}$ for general algebraic curves.

3.2. Generalization of the interpolation ideal

Let $\vec{r} = (r_1, \ldots, r_n) \in \mathbf{F}_q^n$ be the received word. For a divisor G of F, we define $\mathcal{L}(-G + \infty Q) = \bigcup_{i=1}^{\infty} \mathcal{L}(-G + iQ)$. We see that $\mathcal{L}(-G + \infty Q)$ is an ideal of $\mathcal{L}(\infty Q)$ (Matsumoto and Miura, 2000a).

Let $h_{\vec{r}} \in \mathcal{L}(\infty Q)$ such that $h_{\vec{r}}(P_i) = r_i$. Computation of such $h_{\vec{r}}$ can be easily done as follows provided that we can construct generator matrices for C_u for all u. For $1 \leqslant j \leqslant n$, define $\psi_j \in B$ such that $\dim C_{-v_Q(\psi_j)} = j$, and let

$$\begin{pmatrix} i_1 \\ \vdots \\ i_n \end{pmatrix} = \begin{pmatrix} \psi_1(P_1) & \cdots & \psi_1(P_n) \\ \vdots & \vdots & \vdots \\ \psi_n(P_1) & \cdots & \psi_n(P_n) \end{pmatrix}^{-1} \vec{r}.$$

We find that $h_{\vec{r}} = \sum_{j=1}^{n} i_j \psi_j$ satisfies the required condition for $h_{\vec{r}}$. Since $-v_Q(\psi_n) \leqslant n + 2g - 1$, we can choose $h_{\vec{r}}$ so that $-v_Q(h_{\vec{r}}) \leqslant n + 2g - 1$.

Let Z be transcendental over $\mathcal{L}(\infty Q)$, and $D = P_1 + \cdots + P_n$. $\mathcal{L}(\infty Q)[Z]$ denotes the univariate polynomial ring of Z over $\mathcal{L}(\infty Q)$. For a divisor G we denote by $\mathcal{L}_Z(-G + \infty Q)$ the ideal of $\mathcal{L}(\infty Q)[Z]$ generated by $\mathcal{L}(-G + \infty Q) \subset \mathcal{L}(\infty Q)$. Define the ideal $I_{\vec{r},m}$ of $\mathcal{L}(\infty Q)[Z]$ as

$$\begin{aligned} I_{\vec{r},m} &= \mathcal{L}_Z(-mD + \infty Q) + \mathcal{L}_Z(-(m-1)D + \infty Q)\langle Z - h_{\vec{r}}\rangle + \cdots \\ &\quad + \mathcal{L}_Z(-D + \infty Q)\langle Z - h_{\vec{r}}\rangle^{m-1} + \langle Z - h_{\vec{r}}\rangle^m, \end{aligned} \tag{2}$$

where $\langle\cdot\rangle$ denotes the ideal generated by $\cdot$, the plus sign $+$ denotes the sum of ideals, and $\mathcal{L}_Z(-iD+\infty Q)\langle Z-h_{\vec{r}}\rangle^{m-i}$ denotes the product of two ideals $\mathcal{L}_Z(-iD+\infty Q)$ and $\langle Z-h_{\vec{r}}\rangle^{m-i}$. We remark that the above $I_{\vec{r},m}$ is equal to $\bar{I}_{m,v}$ defined by Lax (2012). Note that our definition does not involve coordinate variables $x_1, x_2, \dots$ of the defining equations as used by Lax (2012). For $Q(Z) \in \mathcal{L}(\infty Q)[Z]$, we say $Q(Z)$ has multiplicity m at (P_i, r_i) if

$$Q(Z+r_i) = \sum_j \alpha_j Z^j \tag{3}$$

with $\alpha_j \in \mathcal{L}(\infty Q)$ satisfies $v_{P_i}(\alpha_j) \geqslant m-j$ for all j. Sakata (2001, Section 3.2) introduced a special case of the following set for Hermitian curves. We give a more general definition (for any curve) as follows:

$$I'_{\vec{r},m} = \{Q(Z) \in \mathcal{L}(\infty Q)[Z] \mid Q(Z) \text{ has multiplicity } m \text{ for all } (P_i, r_i)\}.$$

This definition of the multiplicity is the same as Guruswami and Sudan (1999). Therefore, we can find the interpolation polynomial used in Guruswami and Sudan (1999) from $I'_{\vec{r},m}$. We shall explain how to find efficiently the interpolation polynomial from $I'_{\vec{r},m}$, after clarifying the relation between $I_{\vec{r},m}$ and $I'_{\vec{r},m}$.

Lemma 3. *We have $I_{\vec{r},m} \subseteq I'_{\vec{r},m}$.*

Proof. Observe that $I'_{\vec{r},m}$ is an ideal of $\mathcal{L}(\infty Q)[Z]$. Let $\alpha(Z-h_{\vec{r}})^j \in \mathcal{L}_Z(-(m-j)D+\infty Q)\langle Z-h_{\vec{r}}\rangle^j$ such that $\alpha \in \mathcal{L}(-(m-j)D+\infty Q)$. Then we have

$$\alpha(Z+r_i-h_{\vec{r}})^j = \alpha\big(Z-(h_{\vec{r}}-r_i)\big)^j = \sum_{k=0}^{j} \alpha_k (h_{\vec{r}}-r_i)^{j-k} Z^k,$$

where $\alpha_k \in \mathcal{L}(-(m-j)D+\infty Q)$. We can see that $\alpha_k(h_{\vec{r}}-r_i)^{j-k} \in \mathcal{L}(-(m-k)P_i+\infty Q)$ and that $\mathcal{L}(-(m-j)D+\infty Q)\langle Z-h_{\vec{r}}\rangle^j \subseteq I'_{\vec{r},m}$, because $\mathcal{L}_Z(-(m-j)D+\infty Q)\langle Z-h_{\vec{r}}\rangle^j$ is generated by $\{\alpha(Z-h_{\vec{r}})^j \mid \alpha \in \mathcal{L}(-(m-j)D+\infty Q)\}$ as an ideal of $\mathcal{L}(\infty Q)[Z]$. Since $I'_{\vec{r},m}$ is an ideal, it follows that $I_{\vec{r},m} \subseteq I'_{\vec{r},m}$. $\square$

The following Proposition 4 will be used in the proof of Proposition 6.

Proposition 4. *(See Guruswami and Sudan, 1999.)* $\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)[Z]/I'_{\vec{r},m} = n\binom{m+1}{2}$.

Lemma 5. *Let G be a divisor $\geqslant 0$ whose support is disjoint from Q. If $\deg P = 1$ for all $P \in \operatorname{supp}(G)$ then we have*

$$\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)/\mathcal{L}(-G+\infty Q) = \deg G.$$

Proof. Let $n()$ be a mapping from $\operatorname{supp}(G)$ to the set of nonnegative integers. Let $\mathcal{N}$ be the set of those functions such that $n(P) < v_P(G)$ for all $P \in \operatorname{supp}(G)$. By the strong approximation theorem (Stichtenoth, 1993, Theorem I.6.4) we can choose an $f_{n()} \in \mathcal{L}(\infty Q)$ such that $v_P(f_{n()}) = n(P)$ for every $P \in \operatorname{supp}(G)$. Any element in $\mathcal{L}(\infty Q) \setminus \mathcal{L}(-G+\infty Q)$ can be written as the sum of an element $g \in \mathcal{L}(-G+\infty Q)$ plus an $\mathbf{F}_q$-linear combination of $f_{n()}$'s by the assumption $\deg P = 1$ for all $P \in \operatorname{supp}(G)$, which completes the proof. $\square$

The following proposition is equivalent to Lax (2012, Proposition 6), but we include its proof because our definition of $I_{\vec{r},m}$ is apparently very different from that of $\bar{I}_{m,v}$ by Lax (2012).

Proposition 6. $\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)[Z]/I_{\vec{r},m} = n\binom{m+1}{2}$.

Proof. Recall that I is an ideal of $\mathbf{F}_q[X_1, \dots, X_t]$ such that $\mathcal{L}(\infty Q) = \mathbf{F}_q[X_1, \dots, X_t]/I$ as introduced in Section 2. Let G_i be a Gröbner basis of the preimage of $\mathcal{L}(-iD + \infty Q)$ in $\mathbf{F}_q[X_1, \dots, X_t]$, and $H_{\vec{r}}$ be the coset representative of $h_{\vec{r}}$ written as a sum of monomials whose exponents belong to $\Delta(I)$. In this proof, the footprint $\Delta(\cdot)$ is always considered for $\mathbf{F}_q[X_1, \dots, X_t]$ excluding the variable Z. Then

$$G = \bigcup_{i=0}^{m} \left\{ F(Z - H_{\vec{r}})^{m-i} \mid F \in G_i \right\}$$

is a Gröbner basis of the preimage of $I_{\vec{r},m}$ in $\mathbf{F}_q[Z, X_1, \dots, X_t]$ with the elimination monomial order with Z greater than X_i's and refining the monomial order $\succ$ defined in Section 2. Please refer to Eisenbud (1995, Section 15.2) for refining monomial orders. A remainder of division by G can always be written as

$$F_{m-1}Z^{m-1} + F_{m-2}Z^{m-2} + \cdots + F_0$$

with $F_i \in \mathbf{F}_q[X_1, \dots, X_t]$. Then F_{m-i} must be written as a sum of monomials whose exponents belong to the footprint $\Delta(G_i)$ of G_i, for $i = 1, \dots, m$. This shows that

$$\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)[Z]/I_{\vec{r},m} \leqslant \sum_{i=1}^{m} \sharp\Delta(G_i).$$

On the other hand, by Lemma 5,

$$\sharp\Delta(G_i) = \dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)/\mathcal{L}(-iD + \infty Q) = ni.$$

This implies

$$\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)[Z]/I_{\vec{r},m} \leqslant n\binom{m+1}{2}.$$

By Proposition 4 and Lemma 3, we see

$$\dim_{\mathbf{F}_q} \mathcal{L}(\infty Q)[Z]/I_{\vec{r},m} = n\binom{m+1}{2}. \qquad \square$$

The following corollary clarifies the relation between the module $I'_{\vec{r},m}$ used by Sakata (2001) and $I_{\vec{r},m}$ used by Lax (2012), Lee and O'Sullivan (2009), which was not explicit in previous literature.

Corollary 7. $I'_{\vec{r},m} = I_{\vec{r},m}$.

Since $I'_{\vec{r},m}$ is the ideal used in Guruswami and Sudan (1999), we can find the required interpolation polynomial directly from an $\mathbf{F}_q[x_1]$-submodule of $I_{\vec{r},m} = I'_{\vec{r},m}$ as explained in Section 3.3.

For $i = 0, \dots, m$ and $j = 0, \dots, a_1 - 1$, let $\eta_{i,j}$ be an element in $\mathcal{L}(-iD + \infty Q)$ such that $-v_Q(\eta_{i,j})$ is the minimum among $\{-v_Q(\eta) \mid \eta \in \mathcal{L}(-iD + \infty Q),\ -v_Q(\eta) \equiv j \pmod{a_1}\}$. Such elements $\eta_{i,j}$ can be computed by Matsumoto and Miura (2000a) before receiving $\vec{r}$. It was also shown (Matsumoto and Miura, 2000a) that $\{\eta_{i,j} \mid j = 0, \dots, a_1 - 1\}$ generates $\mathcal{L}(-iD + \infty Q)$ as an $\mathbf{F}_q[x_1]$-module. Note also that we can choose $\eta_{0,i} = y_i$ defined in Section 2. By Eq. (1), all $\eta_{i,j}$ and $h_{\vec{r}}$ can be expressed as polynomials in x_1 and $y_0, \dots, y_{a_1-1}$. Thus we have

Theorem 8. *(Generalization of Beelen and Brander, 2010, Proposition 6 and Little, 2011.) Let $\ell \geqslant m$. One has that*

$$\begin{aligned} &\left\{ (Z - h_{\vec{r}})^{m-i}\eta_{i,j} \,\middle|\, i = 0, \dots, m,\ j = 0, \dots, a_1 - 1 \right\} \\ &\quad \cup \left\{ Z^{\ell-m}(Z - h_{\vec{r}})^{m}\eta_{0,j} \,\middle|\, \ell = 1, \dots,\ j = 0, \dots, a_1 - 1 \right\} \end{aligned}$$

generates

$$I_{\vec{r},m,\ell} = I_{\vec{r},m} \cap \{Q(Z) \in \mathcal{L}(\infty Q)[Z] \mid \deg_Z Q(Z) \leqslant \ell\}$$

as an $\mathbf{F}_q[x_1]$*-module.*

Proof. Let $e \in I_{\vec{r},m}$ and E be its preimage in $\mathbf{F}_q[Z, X_1, \ldots, X_t]$. By dividing E by the Gröbner basis G introduced in the proof of Proposition 6, we can see that e is expressed as

$$e = \sum_{\ell=1} \alpha_{-\ell} Z^\ell (Z - h_{\vec{r}})^m + \sum_{i=0}^{m} \alpha_i (Z - h_{\vec{r}})^{m-i}$$

with $\alpha_i \in \mathcal{L}(-\max\{i, 0\}D + \infty Q)$, from which the assertion follows. $\square$

3.3. *Computation of the interpolated polynomial from the interpolation ideal* $I_{\vec{r},m}$

For $(m_1, \ldots, m_t, m_{t+1}), (n_1, \ldots, n_t, n_{t+1}) \in \mathbf{N}_0^{t+1}$, we define the other weighted reverse lexicographic monomial order $\succ_u$ in $\mathbf{F}_q[X_1, \ldots, X_t, Z]$ such that $(m_1, \ldots, m_t, m_{t+1}) \succ_u (n_1, \ldots, n_t, n_{t+1})$ if $a_1 m_1 + \cdots + a_t m_t + u m_{t+1} > a_1 n_1 + \cdots + a_t n_t + u n_{t+1}$, or $a_1 m_1 + \cdots + a_t m_t + u m_{t+1} = a_1 n_1 + \cdots + a_t n_t + u n_{t+1}$, and $m_1 = n_1$, $m_2 = n_2$, ..., $m_{i-1} = n_{i-1}$, $m_i < n_i$, for some $1 \leqslant i \leqslant t+1$. As done in Lee and O'Sullivan (2009), the interpolation polynomial is the smallest nonzero polynomial with respect to $\succ_u$ in the preimage of $I_{\vec{r},m}$. Such a smallest element can be found from a Gröbner basis of the $\mathbf{F}_q[x_1]$-module $I_{\vec{r},m,\ell}$ in Theorem 8. To find such a Gröbner basis, Lee and O'Sullivan proposed the following general purpose algorithm as Lee and O'Sullivan (2009, Algorithm G).

Their algorithm (Lee and O'Sullivan, 2009, Algorithm G) efficiently finds a Gröbner basis of submodules of $\mathbf{F}_q[x_1]^s$ for a special kind of generating set and monomial orders. Please refer to Adams and Loustaunau (1994) for Gröbner bases for modules. Let $\mathbf{e}_1, \ldots, \mathbf{e}_s$ be the standard basis of $\mathbf{F}_q[x_1]^s$. Let $u_x, u_1, \ldots, u_s$ be positive integers. Define the monomial order in the $\mathbf{F}_q[x_1]$-module $\mathbf{F}_q[x_1]^s$ such that $x_1^{n_1}\mathbf{e}_i \succ_{\mathrm{LO}} x_1^{n_2}\mathbf{e}_j$ if $n_1 u_x + u_i > n_2 u_x + u_j$ or $n_1 u_x + u_i = n_2 u_x + u_j$ and $i > j$. For $f = \sum_{i=1}^{s} f_i(x_1)\mathbf{e}_i \in \mathbf{F}_q[x_1]^s$, define $\mathrm{ind}(f) = \max\{i \mid f_i(x_1) \neq 0\}$, where $f_i(x_1)$ denotes a univariate polynomial in x_1 over $\mathbf{F}_q$. Their algorithm (Lee and O'Sullivan, 2009, Algorithm G) efficiently computes a Gröbner basis with respect to $\succ_{\mathrm{LO}}$ of a module generated by $g_1, \ldots, g_s \in \mathbf{F}_q[x_1]^s$ such that $\mathrm{ind}(g_i) = i$. The computational complexity is also evaluated in Lee and O'Sullivan (2009, Proposition 16).

Let ℓ be the maximum Z-degree of the interpolation polynomial in Guruswami and Sudan (1999). The set $I_{\vec{r},m,\ell}$ in Theorem 8 is an $\mathbf{F}_q[x_1]$-submodule of $\mathbf{F}_q[x_1]^{a_1(\ell+1)}$ with the module basis $\{y_j Z^k \mid j = 0, \ldots, a_1 - 1,\ k = 0, \ldots, \ell\}$.

Assumption 9. We assume that there exists $f \in \mathcal{L}(\infty Q)$ whose zero divisor $(f)_0 = D$.

By the algorithm of Matsumoto and Miura (2000a), we can find f in Assumption 9 if it exists.

The assumptions in Beelen and Brander (2010) are

- The function field F was defined by a nonsingular affine algebraic curve of the form

$$\gamma_{a_2,0} X_1^{a_2} + \gamma_{0,a_1} X_2^{a_1} + \sum_{i a_2 + j a_1 < a_1 a_2} \gamma_{i,j} X_1^i X_2^j \tag{4}$$

  with $\gcd(a_1, a_2) = 1$, $\gamma_{a_2,0} \neq 0$ and $\gamma_{0,a_1} \neq 0$,
- and Assumption 9 above.

Since the function field can be defined in the form (4) if the Weierstrass semigroup $H(Q)$ is generated by relatively prime positive integers a_1 and a_2 (Matsumoto and Miura, 2000b), we can see that Assumption 9 is implied by Beelen and Brander (2010, Assumption 2) and is weaker than Beelen and Brander (2010, Assumption 2).

Let $\langle f\rangle$ be the ideal of $\mathcal{L}(\infty Q)$ generated by f. By Matsumoto and Miura (2000a, Corollary 2.3) we have $\mathcal{L}(-D+\infty Q)=\langle f\rangle$. By Matsumoto and Miura (2000a, Corollary 2.5) we have $\mathcal{L}(-iD+\infty Q)=\langle f^i\rangle$.

Example 10. This is continuation of Example 2. Let $f=x_1^7+1$. We see that $-v_Q(f)=21$ and that there exist 21 distinct $\mathbf{F}_8$-rational places $P_1,\ldots,P_{21}$, such that $f(P_i)=0$ for $i=1,\ldots,21$ by straightforward computation. By setting $D=P_1+\cdots+P_{21}$ Assumption 9 is satisfied.

We remark that we have $-v_Q(x_1^8+x_1)=24$ but there exist only 23 $\mathbf{F}_8$-rational places P such that $(x_1^8+x_1)(P)=0$, other than Q, and that $(x_1^8+x_1)$ does not satisfy Assumption 9.

Without loss of generality we may assume existence of $x'\in\mathcal{L}(\infty Q)$ such that $f\in\mathbf{F}_q[x']$, because we can set $x'=f$. By changing the choice of $x_1,\ldots,x_t$ if necessary, we may assume $x_1=x'$ and $f\in\mathbf{F}_q[x_1]$ without loss of generality, while it is better to make $-v_Q(x_1)$ as small as possible in order to reduce the computational complexity. Under the assumption $f\in\mathbf{F}_q[x_1]$, f^iy_j satisfies the required condition for $\eta_{i,j}$ in Theorem 8. By naming y_jZ^k as $\mathbf{e}_{1+j+ku}$, the generators in Theorem 8 satisfy the assumption in Lee and O'Sullivan (2009, Algorithm G). In the following, we assign weight $-iv_Q(x_1)-v_Q(y_j)+ku$ to the module element $x_1^iy_jZ^k$. With this assignment of weights, the monomial order $\succ_{\mathrm{LO}}$ is the restriction of $\succ_u$ to the $\mathbf{F}_q[x_1]$-submodule of $\mathcal{L}(\infty Q)[Z]$ generated by $\{y_jZ^k \mid j=0,\ldots,a_1-1,\ k=0,\ldots,\ell\}$. We can efficiently compute a Gröbner basis of the $\mathbf{F}_q[x_1]$-module $I_{\vec{r},m,\ell}$ by Lee and O'Sullivan (2009, Algorithm G). After that we find the interpolation polynomial required in the list decoding algorithm by Guruswami and Sudan (1999) as the minimal element with respect to $\succ_{\mathrm{LO}}$ in the computed Gröbner basis.

Proposition 11. *Suppose that we use Lee and O'Sullivan (2009, Algorithm G) to find the Gröbner basis of $I_{\vec{r},m,\ell}$ with respect to $\succ_{\mathrm{LO}}$. Under Assumption 9, the number of multiplications in Lee and O'Sullivan (2009, Algorithm G) with the generators in Theorem 8 is at most*

$$\Big[\max_j\big\{-v_Q(y_j)\big\}+m(n+2g-1)+u(\ell-m)\Big]^2 a_1^{-1}\sum_{i=1}^{a_1(\ell+1)} i^2. \tag{5}$$

Proof. What we shall do in this proof is substitution of variables in the general complexity formula in Lee and O'Sullivan (2009) by specific values. The number of generators is $a_1(\ell+1)$, which is denoted by m in Lee and O'Sullivan (2009, Proposition 16). We have $-v_Q(f)\leqslant n+g$ and $-v_Q(h_{\vec{r}})\leqslant n+2g-1$. We can assume $u\leqslant n+2g-1$. Thus, the maximum weight of the generators is upper bounded by

$$\max_j\big\{-v_Q(y_j)\big\}+m(n+2g-1)+u(\ell-m).$$

By Lee and O'Sullivan (2009, Proof of Proposition 16), the number of multiplications is upper bounded by Eq. (5). □

Example 12. Consider the $[21,10]$ code C_{12} over the Klein quartic considered in Examples 1, 2 and 10. Its Goppa bound is $n-u=21-12=9$. The equivalent algorithms by Beelen and Høholdt (2008), Guruswami and Sudan (1999) can correct 5 errors with $m=40$ and $\ell=54$. An advantage of Beelen and Høholdt (2008) over Guruswami and Sudan (1999) is that the former solves a smaller system of linear equations by utilizing the structure of the equations, and thus is faster than the latter.

We shall evaluate the number of multiplications and divisions by the method in Beelen and Høholdt (2008). One can choose the divisor A in Beelen and Høholdt (2008, Section 2.6) as $(m(n-5)-1)Q=639Q$. The algorithm by Beelen and Høholdt (2008) solves a system of

$$\sum_{i=0}^{m}\big((m-i)n-\dim(A-iuQ)+\dim\big(-(m-i)D+A-iuQ\big)\big)$$

$$
\begin{aligned}
&= \sum_{i=0}^{40} 21(40-i) - \dim(639-12i)Q + \dim\bigl(-(40-i)D + (639-12i)Q\bigr) \\
&= 2392
\end{aligned}
$$

linear equations with

$$
\begin{aligned}
&\sum_{i=m+1}^{\ell} \dim(A - iuQ) + \sum_{i=0}^{m} \dim\bigl(-(m-i)D + A - iuQ\bigr) \\
&\quad = \sum_{i=41}^{54} \dim(639-12i)Q + \sum_{i=0}^{40} \dim\bigl(-(40-i)D + (639-12i)Q\bigr) \\
&\quad = 2399
\end{aligned}
$$

unknowns. The number of multiplications and divisions is about $2399^3/3 \simeq 4.6 \times 10^9$.

On the other hand, the original algorithm by Guruswami and Sudan (1999) requires us to solve a system of $21 \times \binom{40+1}{2} = 17{,}220$ linear equations. Solving such a system needs roughly $17{,}220^3/3 \simeq 1.7 \times 10^{12}$ multiplications and divisions in $\mathbf{F}_8$.

The value of Eq. (5) is given by

$$
\begin{aligned}
&\Bigl[\max_j\bigl\{-v_Q(y_j)\bigr\} + m(n+2g-1) + u(\ell-m)\Bigr]^2 a_1^{-1} \sum_{i=1}^{a_1(\ell+1)} i^2 \\
&\quad = \bigl[7 + 40\cdot 26 + 12(54-40)\bigr]^2/3 \times \sum_{i=1}^{3\cdot 55} i^2 \\
&\quad = 28{,}038{,}433{,}500 \simeq 2.8 \times 10^{10}.
\end{aligned}
$$

We see that the proposed method can solve the interpolation step faster than Guruswami and Sudan (1999), but the method by Beelen and Høholdt (2008) is even faster.

4. Concluding remarks

The interpolation step in Guruswami and Sudan (1999) is computationally costly and many researchers proposed faster interpolation methods, as summarized by Beelen and Brander (2010, Figure 1). However, except Beelen and Høholdt (2008), those researches assumed either Hermitian curves, e.g. Lee and O'Sullivan (2009), Sakata (2001) or C_{ab} curves, e.g. Beelen and Brander (2010), Little (2011). Our argument used no assumption until Assumption 9 that seems indispensable with application of Algorithm G in Lee and O'Sullivan (2009). The Klein quartic is the well-known family for constructing AG codes. In Example 12 we demonstrated that the proposed interpolation procedure is faster than the original (Guruswami and Sudan, 1999) and comparable to Beelen and Høholdt (2008) for codes on the Klein quartic.

Acknowledgements

The authors would like to thank an anonymous reviewer for his/her very careful reading of the initial manuscript, and Prof. Robert Lax for pointing out its errors. This research was partly supported by the MEXT Grant-in-Aid for Scientific Research (A) No. 23246071, the Villum Foundation through their VELUX Visiting Professor Programme 2011–2012, the Danish National Research Foundation and the National Science Foundation of China (Grant No. 11061130539) for the Danish–Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography, the Spanish grant MTM2007-64704, and the Spanish MINECO grant No. MTM2012-36917-C03-03.

References

Adams, W.W., Loustaunau, P., 1994. An Introduction to Gröbner Bases. Graduate Studies in Mathematics, vol. 3. American Mathematical Society, Providence, RI.

Apéry, R., 1946. Sur les branches superlinéaires des courbes algébriques. C. R. Acad. Sci. Paris 222, 1198–1200.

Beelen, P., Brander, K., 2010. Efficient list decoding of a class of algebraic-geometry codes. Adv. Math. Commun. 4, 485–518, http://dx.doi.org/10.3934/amc.2010.4.485.

Beelen, P., Høholdt, T., 2008. The decoding of algebraic geometry codes. In: Martínez-Moro, E., Munuera, C., Ruano, D. (Eds.), Advances in Algebraic Geometry Codes. In: Coding Theory and Cryptology, vol. 5. World Scientific, pp. 49–98.

Eisenbud, D., 1995. Commutative Algebra with a View Toward Algebraic Geometry. Graduate Texts in Mathematics, vol. 150. Springer-Verlag, Berlin.

Geil, O., Matsumoto, R., Ruano, D., 2012. List decoding algorithms based on Gröbner bases for general one-point AG codes. In: Proc. ISIT 2012, Cambridge, MA, USA, pp. 86–90, http://dx.doi.org/10.1109/ISIT.2012.6284685.

Geil, O., Pellikaan, R., 2002. On the structure of order domains. Finite Fields Appl. 8, 369–396, http://dx.doi.org/10.1006/ffta.2001.0347.

Guruswami, V., Sudan, M., 1999. Improved decoding of Reed–Solomon and algebraic-geometry codes. IEEE Trans. Inform. Theory 45, 1757–1767, http://dx.doi.org/10.1109/18.782097.

Høholdt, T., Pellikaan, R., 1995. On the decoding of algebraic-geometric codes. IEEE Trans. Inform. Theory 41, 1589–1614, http://dx.doi.org/10.1109/18.476214.

Lax, R.F., 2012. Generic interpolation polynomial for list decoding. Finite Fields Appl. 18, 167–178, http://dx.doi.org/10.1016/j.ffa.2011.07.007.

Lee, K., O'Sullivan, M.E., 2009. List decoding of Hermitian codes using Gröbner bases. J. Symbolic Comput. 44, 1662–1675, http://dx.doi.org/10.1016/j.jsc.2007.12.004.

Little, J.B., 2011. List decoding for AG codes using Gröbner bases. In: SIAM Conference on Applied Algebraic Geometry, North Carolina State University, NC, USA.

Matsumoto, R., Miura, S., 2000a. Finding a basis of a linear system with pairwise distinct discrete valuations on an algebraic curve. J. Symbolic Comput. 30, 309–323, http://dx.doi.org/10.1006/jsco.2000.0372.

Matsumoto, R., Miura, S., 2000b. On construction and generalization of algebraic geometry codes. In: Katsura, T., et al. (Eds.), Proc. Algebraic Geometry, Number Theory, Coding Theory, and Cryptography. Univ. Tokyo, Japan, pp. 3–15. http://www.rmatsumoto.org/repository/weight-construct.pdf.

Miura, S., 1993. Algebraic geometric codes on certain plane curves. Electron. Commun. Jpn., Part III: Fundam. Electron. Sci. 76, 1–13, http://dx.doi.org/10.1002/ecjc.4430761201. Original Japanese version published as Trans. IEICE J75-A (11) (1992) 1735–1745.

Miura, S., 1998. Linear codes on affine algebraic curves. Trans. IEICE J81-A, 1398–1421.

Rosales, J.C., García-Sánchez, P.A., 2009. Numerical Semigroups. Developments in Mathematics, vol. 20. Springer, New York.

Saints, K., Heegard, C., 1995. Algebraic-geometric codes and multidimensional cyclic codes: A unified theory and algorithms for decoding using Gröbner bases. IEEE Trans. Inform. Theory 41, 1733–1751, http://dx.doi.org/10.1109/18.476246.

Sakata, S., 2001. On fast interpolation method for Guruswami–Sudan list decoding of one-point algebraic-geometry codes. In: Boztaş, S., Shparlinski, I.E. (Eds.), Proc. AAECC-14. Springer-Verlag, Melbourne, Australia, pp. 172–181.

Schicho, J., 1998. Inversion of birational maps with Gröbner bases. In: Buchberger, B., Winkler, F. (Eds.), Gröbner Bases and Applications. In: London Mathematical Society Lecture Note Series, vol. 251. Cambridge University Press, pp. 495–503.

Stichtenoth, H., 1993. Algebraic Function Fields and Codes. Springer-Verlag, Berlin.

Tang, L.Z., 1998. A Gröbner basis criterion for birational equivalence of affine varieties. J. Pure Appl. Algebra 123, 275–283, http://dx.doi.org/10.1016/S0022-4049(97)00139-4.

Vasconcelos, W.V., 1998. Computational Methods in Commutative Algebra and Algebraic Geometry. Algorithms and Computation in Mathematics, vol. 2. Springer-Verlag, Berlin.