Faster List Decoding of AG Codes

Peter Beelen, Vincent Neiger

Faster List Decoding of AG Codes

Peter Beelen* Vincent Neiger†

Abstract

In this article, we present a fast algorithm performing an instance of the Guruswami-Sudan list decoder for algebraic geometry codes. We show that any such code can be decoded in $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g)+\ell^\omega\mu^\omega)$ operations in the underlying finite field, where n is the code length, g is the genus of the function field used to construct the code, s is the multiplicity parameter, ℓ is the designed list size and μ is the smallest positive element in the Weierstrass semigroup of some chosen place.

1 Introduction

Context and main result. Algebraic geometry (AG) codes form a large class of error-correcting codes that became famous for providing asymptotically good families of codes surpassing the Gilbert-Varshamov bound. Such codes are constructed using algebraic curves defined over a finite field, say $\mathbb{F}_q$ where q is the cardinality of the field. Instead of considering algebraic curves defined over $\mathbb{F}_q$, one can also use the language of function fields with full constant field $\mathbb{F}_q$; we follow the latter viewpoint in this article. Section 2 gives some more background on AG codes and function fields; for a detailed introduction, the reader may refer to [17].

Decoding algorithms for AG codes have been studied since the late 80's. One important such decoder is the well-known Guruswami-Sudan (GS) list-decoder, that can be used to decode any AG code.

Consider an AG code constructed from a function field F of genus g, with underlying finite field $\mathbb{F}_q$ and code length n. The design of the GS decoder further asks that one chooses a *list size* ℓ and *multiplicity* parameter s, which are such that $s \leq \ell$. It was shown in [2] that such an AG code can be decoded using a particular instance of the GS decoder using $\tilde{\mathcal{O}}(s\ell^\omega\mu^{\omega-1}(n+g))$ operations in $\mathbb{F}_q$, where μ is the smallest positive element in the Weierstrass semigroup at some chosen rational place P_∞ of F. Here, the "soft-O" notation $\tilde{\mathcal{O}}(\cdot)$ is similar to the "big-O" notation $\mathcal{O}(\cdot)$, but hides factors logarithmic in the parameters s, ℓ, μ, n, g. This complexity result is achieved under the mild assumption that

*Department of Applied Mathematics and Computer Science, Technical University of Denmark, Lyngby, Denmark.

†Sorbonne Université, CNRS, LIP6, F-75005 Paris, France.

one has already carried out some precomputations, yielding objects which depend on the code but not on the received word. These objects can therefore be reused as such, with no additional computation, in each subsequent call to the decoder (see [2, Section VI] for more details).

To the best of our knowledge, this complexity result is the best known one for this decoding task in general. More precisely, any other implementation of the GS decoder has a complexity bound which is similar or worse, with one exception in the specific context of Reed-Solomon (RS) codes. Indeed, in this case the above complexity from [2] becomes $\tilde{\mathcal{O}}(s\ell^{\omega}n)$, while there are known list decoders for these codes whose complexity is in $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}n)$ [4, Section IV] [9, Sections 2.4 to 2.6]; recall that $s \leq \ell$.

The main goal of this paper is to refine the exploitation of efficient univariate polynomial matrix computations in the algorithmic framework from [2]. We will show that this indeed is possible, leading to our main result: any AG code can be list decoded, using an instance of the GS list decoder, in complexity $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g)+\ell^{\omega}\mu^{\omega})$. This complexity bound holds under mild assumptions about precomputations, similar to those of [2] mentioned above. Since $\mu \leq g+1$, the term $\ell^{\omega}\mu^{\omega}$ is in $\mathcal{O}(\ell^{\omega}\mu^{\omega-1}g)$, and therefore this new complexity bound improves upon the best previously known bound $\tilde{\mathcal{O}}(s\ell^{\omega}\mu^{\omega-1}(n+g))$. Moreover, for Reed-Solomon codes one has $\mu = g+1 = 1$ and also $\ell \leq sn$, so that the new complexity bound becomes $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}n)$, matching the best previously known bound in this specific case.

Overview of the approach. The GS list decoding algorithm consists of two main steps: the interpolation step, in which one seeks a polynomial $Q(z) \in F[z]$ satisfying certain interpolation properties; and the root finding step, in which one computes roots of the polynomial $Q(z)$. The second step is generally considered as computationally easier than the first step. In this paper, we keep the root finding algorithm described in [2, Algorithm 6], yet with a minor refinement of the complexity analysis to ensure that it does not become the dominant step after our improvement of the interpolation step. Specifically, Section 5.2 shows a simple modification of the analysis from [2] leading to the complexity estimate $\tilde{\mathcal{O}}(s\ell\mu^{\omega-1}(n+g))$, improving upon the one $\tilde{\mathcal{O}}(\ell^2\mu^{\omega-1}(n+g))$ reported in [2].

We also keep the overall structure of the interpolation step [2, Algorithm 7, Steps 1 to 9], which performs two main tasks: first build a basis $\boldsymbol{B}$ of some $\mathbb{F}_q[x]$-module of interpolant polynomials, and then find a small degree such interpolant $Q(z)$ thanks to a suitable $\mathbb{F}_q[x]$-module basis reduction procedure. The main novel ideas for obtaining our result are the following:

- For applying basis reduction to $\boldsymbol{B}$, we rely on the algorithm from [14] for computing so-called shifted Popov forms. The same choice was made in [2], where it was motivated by the fact that this algorithm supports any shift, whereas earlier similarly efficient algorithms [5, 16, 6] focus on the unshifted case. Here, we have an additional motivation for this choice: a key towards our complexity improvement lies in the fact that

the complexity of this basis reduction algorithm is sensitive to some type of *average degree* of the input polynomial matrix.

- We describe a new algorithm to build a polynomial matrix $\boldsymbol{B}$ whose average degree is small, and whose rows generate all possible interpolating polynomials $Q(z)$. Our construction directly provides a matrix whose rows are $\mathbb{F}_q[x]$-linearly independent, whereas the matrix built in [2] has redundant rows and therefore requires additional computations to obtain a basis of its $\mathbb{F}_q[x]$-row space, which furthermore typically does not have small average degree. In our case, this small average degree is ensured through the combination of two ingredients. The first one is a new description of a generating set of the module of interpolants (see Sections 3.1 to 3.3) which leads to a matrix $\boldsymbol{B}$ with many zero entries in each row (like in [2]), and also such that the nonzero entries are restricted to the first μs columns (unlike in [2] where they can be found in all columns). The second ingredient is an iterative computation of blocks of rows of $\boldsymbol{B}$, avoiding any degree growth at each stage via the computation of matrix remainders in polynomial matrix divisions by well-chosen matrix quotients (see Sections 3.4 and 4.2).

- A core tool in our construction of $\boldsymbol{B}$ is a generalization of [2, Algorithm 4] which, given some function $a \in \mathcal{R}(A)$, finds a polynomial matrix representation of the multiplication map $f \in \mathcal{R}(B) \mapsto af \in \mathcal{R}(A+B)$ (see Section 2 for definitions and notation). The version in [2] was for $A = 0$, and we show how to generalize it to any divisor A without impacting the asymptotic complexity.

Outline. Section 2 presents the main definitions and preliminary results used throughout the paper. Section 3 focuses on bases for the module of interpolant polynomials, starting with a versatile description of a family of such bases, then showing a polynomial matrix representation of an explicit choice of such a basis, and finally gathering some properties that constructively prove the existence a basis matrix $\boldsymbol{B}$ with small average degree. Section 4 describes the above-mentioned generalization of [2, Algorithm 4], and a complete algorithm for efficiently constructing $\boldsymbol{B}$. Finally, Section 5 summarizes the resulting list decoder and proves the announced overall complexity bound.

Perspectives. After this work, the obvious perspective is to seek further complexity improvements beyond $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g)+\ell^\omega\mu^\omega)$. Remark that any improvement concerning the exponents of ℓ, s, or n would directly imply an improvement of the state-of-the-art complexity for the case of Reed-Solomon codes; a perhaps more accessible target would be to reduce the dependency on the genus g or on the quantity μ. Although our emphasis here is on the complexity of the decoder for a fixed code, allowing to perform some precomputations that depend only on this code, another natural direction for further

work is to carry out a complexity analysis for these precomputations. This involves notably the computation of Apéry systems as introduced in [12], which relates directly to active research topics such as the computation of bases of Riemann-Roch spaces (see for example [8] and the literature overview in [3, Section 7]).

2 Preliminaries

In this section we review some necessary concepts and notations about function fields, AG codes, the GS list decoder, and algorithms for polynomial matrices (i.e. matrices over $\mathbb{F}_q[x]$). We largely use the same notation as in [2] and definitions from [17].

2.1 Function fields and AG codes

Let a function field F of genus g and full constant field $\mathbb{F}_q$ be given. A divisor $A = \sum_i n_i A_i$ of F is a formal $\mathbb{Z}$-linear combination of places A_i of F, such that finitely many of these places have a nonzero coefficient. Then the support of A, denoted by $\mathrm{supp}(A)$ is the set of all places A_i of F such that $n_i \neq 0$. A divisor A is called effective if for all i it holds $n_i \geq 0$. This is commonly denoted by $A \geq 0$. The degree of a place A_i of F is defined as the dimension of the residue field F_{A_i} of the place A_i, viewed as an $\mathbb{F}_q$-vector space. If a place of F has degree one, it is called a rational place of F. The degree of a divisor $A = \sum_i n_i A_i$, is then simply defined as $\deg(A) = \sum_i n_i \deg(A_i)$, where $\deg(A_i)$ denotes the degree of the place A_i.

The Riemann-Roch space of a divisor A is given by

$$\mathcal{L}(A) = \{f \in F \setminus \{0\} \mid (f) + A \geq 0\} \cup \{0\},$$

where (f) denotes the divisor of f. Divisors of nonzero functions are called principal divisors. The Riemann-Roch space $\mathcal{L}(A)$ is a finite dimensional vector space over $\mathbb{F}_q$, whose dimension will be denoted by $l(A)$. The dimension of $\mathcal{L}(A)$ is the topic of the theorem of Riemann-Roch [17, Theorem 1.5.15]. In particular, it implies that $l(A) \geq \deg(A)+1-g$ and that equality holds whenever $\deg(A) \geq 2g-1$. Moreover $l(A) = 0$ if $\deg(A) < 0$ since the degree of a principal divisor is zero.

Now let $P_1, \ldots, P_n$ be distinct rational places of F and write $D = P_1 + \cdots + P_n$. Given any divisor G such that $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \emptyset$, one defines the AG code

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathcal{L}(G)\},$$

where $\mathcal{L}(G)$ denotes the Riemann-Roch space of the divisor G. The dimension of the code equals $l(G) - l(G-D)$, the functions in $\mathcal{L}(G-D)$ being precisely all function in $\mathcal{L}(G)$ that give rise to the zero codeword. In particular, $\mathcal{C}_{\mathcal{L}}(D, G)$ is the zero code if $\deg(G) < 0$. Moreover, the theorem of Riemann-Roch implies that $\dim(\mathcal{C}_{\mathcal{L}}(D, G)) = n$, i.e. $\mathcal{C}_{\mathcal{L}}(D, G) = \mathbb{F}_q^n$, whenever $\deg(G) \geq n + 2g - 1$.

Because of this, we may assume $0 \leq \deg(G) \leq n + 2g - 1$ and in particular $\deg(G) \in \mathcal{O}(n + g)$.

Further we denote by P_∞ an additional rational place of F not occurring in the divisor D. (At first sight this seems to restrict the length of the AG code $C_{\mathcal{L}}(D, G)$, since apparently not all rational places can occur in D, but as explained in [2, Section II.B] this is not the case: if needed, a small degree extension of the constant field will always produce "new" rational places from which P_∞ can be chosen; a similar observation about P_∞ was made independently in [11].) We denote by $\mu \in \mathbb{Z}_{>0}$ the smallest positive element in the Weierstrass semigroup of P_∞ and by $x \in F$ a function that has pole order μ at P_∞, but otherwise is without poles. Note that $\mu \leq g+1$, since the Weierstrass semigroup has g gaps; in fact $\mu \leq g$ as soon as the set of these gaps is not $\{1, \ldots, g\}$.

For any divisor A of F, let $\mathcal{A}(A) = \bigcup_{m=-\infty}^{\infty} \mathcal{L}(mP_\infty + A)$ and let $\mathcal{A} = \mathcal{A}(0)$. As in [12], for any nonzero $a \in \mathcal{A}(A)$ we denote by $\delta_A(a)$ the smallest integer m such that $a \in \mathcal{L}(mP_\infty + A)$, i.e. $\delta_A(a) = -v_{P_\infty}(a) - v_{P_\infty}(A)$ and let $\delta(a) = \delta_0(a) = -v_{P_\infty}(a)$. We will take as convention that $\delta_A(0) = -\infty$. Note that for any $a \in \mathcal{A}(A)$ and $b \in \mathcal{A}(B)$, one has $\delta_{A+B}(ab) = \delta_A(a) + \delta_B(b)$. We will use the quantity $\delta_A(a)$ to indicate the "size" of an element $a \in \mathcal{A}(A)$; it generalizes the degree of a univariate polynomial. For example, the following known result, see for example [2, Lemma V.3] for a proof, indicates the size of interpolating functions in $\mathcal{A}(A)$:

Lemma 2.1 ([2, Lemma V.3])**.** *Let A be a divisor and $E = E_1 + \cdots + E_N$ for distinct rational places $E_1, \ldots, E_N$ of F different from P_∞ such that* $\operatorname{supp}(A) \cap \operatorname{supp}(E) = \emptyset$. *For any $(w_1, \ldots, w_N) \in \mathbb{F}_q^N$ there exists an $a \in \mathcal{A}(A)$ with*

$$\delta_A(a) \leq \deg(E) + 2g - 1 - \deg(A)$$

such that $a(E_j) = w_j$ for $j = 1, \ldots, N$.

Since by definition, the function x only has a pole in P_∞, we have $x \in \mathcal{A} \setminus \mathbb{F}_q$. Hence, we can view $\mathcal{A}(A)$ as a free $\mathbb{F}_q[x]$-module. Following [12] and using the same notation as in [2], we consider a specific kind of basis of $\mathcal{A}(A)$ as $\mathbb{F}_q[x]$-module, called an Apéry system of $\mathcal{A}(A)$.

Definition 2.2. *For a divisor A and an integer $i = 0, \ldots, \mu-1$, let $y_i^{(A)} \in \mathcal{A}(A)$ be a function satisfying:*

1. $\delta_A(y_i^{(A)}) \equiv i \mod \mu$,
2. *if $a \in \mathcal{A}(A)$ and $\delta_A(a) \equiv i \mod \mu$, then $\delta_A(y_i^{(A)}) \leq \delta_A(a)$.*

Further we define $y_i = y_i^{(0)}$.

Using the theorem of Riemann-Roch, it is not hard to show the following lemma, see for example [2, Lemma III.3] for details:

Lemma 2.3 ([2, Lemma III.3])**.** *For any divisor A it holds that*

$$-\deg(A) \leq \delta_A(y_i^{(A)}) \leq 2g - 1 - \deg(A) + \mu,$$

for $i = 0, \ldots, \mu - 1$.

As mentioned in [12], $y_0^{(A)}, \ldots, y_{\mu-1}^{(A)}$ is an $\mathbb{F}_q[x]$-basis of $\mathcal{A}(A)$. Given $a \in \mathcal{A}(A)$, it is therefore possible to write a as an $\mathbb{F}_q[x]$-linear combination of these basis elements, and in fact the $\mathbb{F}_q[x]$-coefficients of this combination are unique. As demonstrated in [2, Lemma III.4], there is a very explicit upper bound for the degree of these occurring coefficient polynomials:

Lemma 2.4 ([2, Lemma III.4]). *If $a = \sum_{i=0}^{\mu-1} a_i y_i^{(A)} \in \mathcal{A}(A)$, where $a_i \in \mathbb{F}_q[x]$ and A is a divisor, then*

$$\deg(a_i) \leq \frac{1}{\mu}\Big(\delta_A(a) - \delta_A(y_i^{(A)})\Big) \leq \frac{1}{\mu}\Big(\delta_A(a) + \deg(A)\Big) \ .$$

2.2 The Guruswami-Sudan list decoder

The key idea in the Guruswami-Sudan list decoding algorithm for $\mathcal{C}_{\mathcal{L}}(D, G)$ [7] is to find a polynomial $Q(z) = \sum_{t=0}^{\ell} z^t Q_t \in F[z]$, nonzero of degree at most ℓ, that vanishes with multiplicity at least s at each point (P_i, r_i), where $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$ is the received word. The idea is that if the coefficients $Q_t \in F$ are chosen in suitable subspaces of F and $\boldsymbol{r}$ has small enough Hamming distance from the sent codeword $(f(P_1), \ldots, f(P_n))$, then $Q(f)$ is the zero element in F (see Theorem 2.5). This can then be used to recover f from Q by finding the roots of Q in F.

For the remainder of this paper fix $s, \ell \in \mathbb{Z}_{>0}$ with $s \leq \ell$, where s is the multiplicity parameter and ℓ the designed list size of the Guruswami-Sudan list decoder. The corresponding list decoding radius will be denoted by τ.

More specifically, as in [2], we restrict ourselves to the setting where $Q = \sum_{t=0}^{\ell} z^t Q_t$ with $Q_t \in \mathcal{A}(-tG)$ and define $\delta_G(Q) = \max_t \delta_{-tG}(Q_t)$. Further, given a received word $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$, we define

$$\begin{aligned} \mathcal{M}_{s,\ell,\boldsymbol{r}} = \Bigg\{ Q = \sum_{t=0}^{\ell} z^t Q_t \in F[z] \;\Big|\; & Q_t \in \mathcal{A}(-tG), \\ & Q \text{ has a root of multiplicity at least } s \text{ at } (P_j, r_j) \text{ for all } j \Bigg\}. \end{aligned} \tag{2.1}$$

In this setting, one has the following result, which is the crux of the correctness of the Guruswami-Sudan list decoder [7]:

Theorem 2.5 (Instance of Guruswami-Sudan). *Let $\boldsymbol{r} \in \mathbb{F}_q^n$ be a received word and $Q \in \mathcal{M}_{s,\ell,\boldsymbol{r}}$ with $\delta_G(Q) < s(n - \tau)$. If $f \in \mathcal{L}(G)$ is such that the Hamming distance between $\boldsymbol{r}$ and $(f(P_1), \ldots, f(P_n))$ is at most τ, then $Q(f) = 0$.*

For algorithmic purposes, it is convenient to give a description of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ that is as explicit as possible. For the remainder of this article let $G_t = (t-s)D - tG$ for $0 \leq t < s$ and $G_t = -tG$ for $s \leq t \leq \ell$. From [2] we quote the following:

Theorem 2.6 ([2, Theorem IV.4 and Remark IV.7]). *Let $R \in \mathcal{R}(G)$ be such that $R(P_j) = r_j$ for $1 \le j \le n$. Then*

$$\mathcal{M}_{s,\ell,\boldsymbol{r}} = \bigoplus_{t=0}^{\ell} (z-R)^t \mathcal{R}(G_t) \tag{2.2}$$

$$= \bigoplus_{t=0}^{s-1} (z-R)^t \mathcal{R}(G_t) \oplus \bigoplus_{t=s}^{\ell} z^{t-s}(z-R)^s \mathcal{R}(G_t). \tag{2.3}$$

In [2], the first description (Equation (2.2)) was used to obtain a decoding algorithm for $\mathcal{C}_{\mathcal{L}}(D,G)$ with complexity $\tilde{\mathcal{O}}(\ell^{\omega+1}\mu^{\omega-1}(n+g))$, while the second description (Equation (2.3)) improved this to $\tilde{\mathcal{O}}(s\ell^{\omega}\mu^{\omega-1}(n+g))$. We will see in Section 3 that one ingredient in our improvement is to use yet another description of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$.

2.3 Reminders on univariate polynomial matrices

In this paper, we will make use of a few classical notions on univariate polynomial matrices. For brevity, since only the univariate case will be encountered, we will just write "polynomial matrix".

For a polynomial matrix $\boldsymbol{A} = [a_{i,j}]_{i,j} \in \mathbb{F}_q[x]^{m\times\nu}$, its *degree* is defined as $\max_{i,j} \deg(a_{i,j})$ and denoted by $\deg(\boldsymbol{A})$; its column degrees is the tuple formed by the degrees of each of its columns. In the square case $m = \nu$, the matrix $\boldsymbol{A}$ is said to be *nonsingular* if $\det(\boldsymbol{A}) \neq 0$, and *unimodular* if $\det(\boldsymbol{A}) \in \mathbb{F}_q \setminus \{0\}$.

We refer to [10, 1] for the classical notions of Popov forms and reduced forms, row degrees and pivot indices, as well as their shifted generalizations.

We will use the following result on the feasibility of polynomial matrix division with remainder, and on the complexity of performing such divisions using a Newton iteration-based approach.

Lemma 2.7. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be matrices in $\mathbb{F}_q[x]^{m\times m}$ with $\boldsymbol{B}$ nonsingular. Then there exists a matrix $\boldsymbol{R} \in \mathbb{F}_q[x]^{m\times m}$ such that $\boldsymbol{A} - \boldsymbol{R}$ is a left multiple of $\boldsymbol{B}$ and $\deg(\boldsymbol{R}) < \deg(\boldsymbol{B})$. There is an algorithm* PM-Rem *which, on input $\boldsymbol{A}$ and $\boldsymbol{B}$, returns such a matrix $\boldsymbol{R}$ using $\tilde{\mathcal{O}}(m^{\omega}(\deg(\boldsymbol{A}) + \deg(\boldsymbol{B})))$ operations in $\mathbb{F}_q$.*

Proof. The existence of $\boldsymbol{R}$ such that $\boldsymbol{A} - \boldsymbol{R}$ is a left multiple of $\boldsymbol{B}$ is proved in [10, Theorem 6.3-15, page 389]. This reference also ensures that $\boldsymbol{B}^{-1}\boldsymbol{R}$ is a so-called *strictly proper* matrix fraction, which implies $\deg(\boldsymbol{R}) < \deg(\boldsymbol{B})$ as showed for example in [10, Lemma 6.3-10, page 383]. To find $\boldsymbol{R}$, one may start with computing a Popov form $\boldsymbol{P} \in \mathbb{F}_q[x]^{m\times m}$ of $\boldsymbol{B}$, which costs $\tilde{\mathcal{O}}(m^{\omega}\deg(\boldsymbol{B}))$ [16, Theorem 21]. In particular, $\boldsymbol{B}$ and $\boldsymbol{P}$ are left-unimodularly equivalent, so that left multiples of $\boldsymbol{B}$ are the same as left multiples of $\boldsymbol{P}$. Thus $\boldsymbol{R}$ can be found as a remainder in the division of $\boldsymbol{A}$ by $\boldsymbol{P}$, since $\deg(\boldsymbol{P}) \le \deg(\boldsymbol{B})$. Since $\boldsymbol{P}$ is column reduced, to find this remainder we can apply [14, Algorithm 1]: this boils down to one truncated expansion at order $\mathcal{O}(\deg(\boldsymbol{A}))$ of the inverse of an $m\times m$ matrix (whose constant term is invertible), and two multiplications of two $m\times m$ matrices of degree in $\mathcal{O}(\deg(\boldsymbol{A})+\deg(\boldsymbol{P}))$. Hence the total cost $\tilde{\mathcal{O}}(m^{\omega}(\deg(\boldsymbol{A})+\deg(\boldsymbol{P})))$, which concludes the proof since $\deg(\boldsymbol{P}) \le \deg(\boldsymbol{B})$. □

3 The interpolant module $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ and polynomial matrix representations of it

We now study the module $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ more in depth. First we generalize Theorem 2.6 to get more flexibility on the choice of generators for $\mathcal{M}_{s,\ell,\boldsymbol{r}}$, and we make such an explicit choice (Section 3.1). Then we introduce several maps and the corresponding $\mathbb{F}_q[x]$-matrices (Section 3.2). This allows us to describe a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as an $\mathbb{F}_q[x]$-module, and to represent this module as the $\mathbb{F}_q[x]$-row space of an explicit polynomial matrix $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ in $\mathbb{F}_q[x]^{m\times m}$, for $m = \mu(\ell+1)$ (Section 3.3). Finally, in Section 3.4, we deduce another basis matrix $\boldsymbol{P}_{s,\ell,\boldsymbol{r}}$ which is less explicit than $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$, but computationally easier to construct and manipulate. Throughout, it is assumed that the received vector is $\boldsymbol{r} = (r_1, \ldots, r_n) \in \mathbb{F}_q^n$ and that $R \in \mathcal{R}(G)$ is a function satisfying $R(P_j) = r_j$ for $1 \le j \le n$ as well as the bound from Lemma 2.1, $\delta_G(R) \le n + 2g - 1 - \deg(G)$.

3.1 A more flexible description of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$

In Theorem 2.6, two ways to describe the module $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ were given. We now indicate a more general shape for alternative descriptions for $\mathcal{M}_{s,\ell,\boldsymbol{r}}$.

Theorem 3.1. *For $s \le t \le \ell$, let $f_t(z) = \sum_{i=0}^{t-s} f_{ti} z^{t-s-i} \in F[z]$, where $f_{ti} \in \mathcal{R}(iG)$ and $\deg_z(f_t) = t - s$, hence in particular $f_{t0} \in \mathbb{F}_q \setminus \{0\}$. Then*

$$\mathcal{M}_{s,\ell,\boldsymbol{r}} = \bigoplus_{t=0}^{s-1} (z-R)^t \mathcal{R}(G_t) \oplus \bigoplus_{t=s}^{\ell} f_t(z)(z-R)^s \mathcal{R}(G_t).$$

Proof. Using Equation (2.2) in Theorem 2.6, and since by definition $G_t = -tG$ for $t \ge s$, it is sufficient to show that

$$\mathcal{M}_{s,\ell,\boldsymbol{r}} = \bigoplus_{t=0}^{s-1} (z-R)^t \mathcal{R}(G_t) \oplus \bigoplus_{t=s}^{\ell} (z-R)^t \mathcal{R}(-tG)$$

is equal to

$$\mathcal{M} := \bigoplus_{t=0}^{s-1} (z-R)^t \mathcal{R}(G_t) \oplus \bigoplus_{t=s}^{\ell} f_t(z)(z-R)^s \mathcal{R}(-tG).$$

We first prove the inclusion "$\mathcal{M}_{s,\ell,\boldsymbol{r}} \supseteq \mathcal{M}$". For this we show, for $t = s, \ldots, \ell$, the inclusion $f_t(z)(z-R)^s \mathcal{R}(-tG) \subseteq \bigoplus_{k=s}^{t} (z-R)^k \mathcal{R}(-kG)$. This follows from $f_t(z) \in \bigoplus_{k=s}^{t} (z-R)^{k-s} \mathcal{R}((t-k)G)$, which itself comes from using the binomial formula on $f_t(z) = \sum_{j=0}^{t-s} (z - R + R)^{t-s-j} f_{tj}$. Indeed, this yields $f_t(z) = \sum_{k=s}^{t} (z-R)^{k-s} \tilde{f}_{tk}$ where, for $s \le k \le t$, $\tilde{f}_{tk} = \sum_{j=0}^{t-k} \binom{t-s-j}{k-s} R^{t-k-j} f_{tj}$ is in $\mathcal{R}((t-k)G)$.

Now we prove the inclusion "$\mathcal{M}_{s,\ell,\boldsymbol{r}} \subseteq \mathcal{M}$". For this we show, for each $t = s, \ldots, \ell$, the inclusion $(z-R)^t \mathcal{R}(-tG) \subseteq \bigoplus_{k=s}^{t} f_k(z)(z-R)^s \mathcal{R}(-kG)$. Similarly

to the above, it is enough to prove $(z-R)^{t-s} \in \bigoplus_{k=s}^{t} f_k(z)\mathcal{R}((t-k)G)$. We proceed by induction on $t \in \{s, \dots, \ell\}$, showing that $(z-R)^{t-s} = \sum_{k=s}^{t} f_k(z)\alpha_{tk}$ for certain $\alpha_{tk} \in \mathcal{R}((t-k)G)$. The property is obvious for $t = s$, since $f_s(z) = f_{s0} \in \mathbb{F}_q \setminus \{0\}$. Let $t \in \{s+1, \dots, \ell\}$ and assume the property holds from s to $t-1$. Then

$$\begin{aligned}(z-R)^{t-s} &= \frac{1}{\tilde{f}_{tt}} \left(f_t(z) - \sum_{j=s}^{t-1} (z-R)^{j-s} \tilde{f}_{tj} \right) \\ &= \frac{1}{\tilde{f}_{tt}} f_t(z) + \sum_{k=s}^{t-1} f_k(z) \left(\frac{-1}{\tilde{f}_{tt}} \sum_{j=k}^{t-1} \alpha_{jk} \tilde{f}_{tj} \right)\end{aligned}$$

which proves the property for t, since $\tilde{f}_{tt} \in \mathbb{F}_q \setminus \{0\}$ and $\alpha_{jk}\tilde{f}_{tj} \in \mathcal{R}((t-k)G)$. □

As a first observation, the second description in Theorem 2.6 is now an easy consequence of Theorem 3.1 (which we proved using only the first description in Theorem 2.6). To obtain a faster decoder, we will start from the following description of the interpolant module.

Corollary 3.2. *For $s \le t \le \ell$, let $g_t(z) = \sum_{i=0}^{t-s} \binom{i+s-1}{i} R^i z^{t-s-i} \in F[z]$. Then $\mathcal{M}_{s,\ell,\boldsymbol{r}} = \bigoplus_{t=0}^{s-1} (z-R)^t \mathcal{R}(G_t) \oplus \bigoplus_{t=s}^{\ell} g_t(z)(z-R)^s \mathcal{R}(G_t)$.*

Proof. We only need to check that $f_t(z) = g_t(z)$ is a valid choice in Theorem 3.1. The first condition $\binom{i+s-1}{i} R^i \in \mathcal{R}(iG)$ follows from $R \in \mathcal{R}(G)$. The second condition $\deg_z(g_t(z)) = t - s$ is obvious. □

In this description, the polynomial $g_t(z)(z-R)^s$ has at most $s+1$ nonzero coefficients, as we will see in the next lemma (Lemma 3.3) which gives an explicit formula for these coefficients. In fact, looking back at the description in Equation (2.3), the polynomial $z^{t-s}(z-R)^s$ also has at most $s+1$ nonzero coefficients. Yet, the advantage of $g_t(z)(z-R)^s$ over $z^{t-s}(z-R)^s$ is the range of monomials that may appear with nonzero coefficients. Apart from the common leading term z^t, for the latter these monomials are $z^{t-s}, z^{t-s+1}, \dots, z^{t-1}$, whereas for the former they are $1, z, \dots, z^{s-1}$ independently of t. As we will see in Sections 3.3 and 3.4, this particular location of nonzero coefficients is instrumental in our approach for building an $\mathbb{F}_q[x]$-basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ which has small average column degree.

Lemma 3.3. *For $s \le t \le \ell$, let $g_t(z) = \sum_{i=0}^{t-s} \binom{i+s-1}{i} R^i z^{t-s-i}$. Then $z^t - g_t(z)(z-R)^s$ has degree at most $s-1$. Moreover, for $0 \le j < s$, the coefficient of z^j in $g_t(z)(z-R)^s$ equals $\gamma_{t,j} R^{t-j}$, where*

$$\gamma_{t,j} = \sum_{i=s-j}^{s} \binom{s}{i} \binom{t-j-i+s-1}{s-1} (-1)^i. \tag{3.1}$$

Proof. Using a classical power series expansion formula in z^{-1}, we obtain that

$$z^t = (z-R)^s z^{t-s}\left(1-\frac{R}{z}\right)^{-s} = (z-R)^s \sum_{i\geq 0}\binom{i+s-1}{i} R^i z^{t-s-i}.$$

This shows that

$$z^t - g_t(z)(z-R)^s = z^t - (z-R)^s \sum_{i\geq t-s+1}\binom{i+s-1}{i} R^i z^{t-s-i},$$

Hence the polynomial $z^t - g_t(z)(z-R)^s$ has degree at most $s-1$. To prove the second part of the lemma, one can simply expand the product $g_t(z)(z-R)^s$, yielding that for $0 \leq j < s$ the coefficient of z^j in $g_t(z)(z-R)^s$ equals $\gamma_{t,j}R^{t-j}$, just as indicated. □

3.2 Inclusion and multiplication maps, and their matrices

In this subsection we study two types of $\mathbb{F}_q[x]$-module homomorphisms: the first type are inclusion maps of submodules in a module, while the second type are maps of multiplication by some $R \in \mathcal{R}(G)$.

We will also consider matrices over $\mathbb{F}_q[x]$ which represent these maps, as this will help us describe and compute bases of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as an $\mathbb{F}_q[x]$-module. Note that, if the ranks as $\mathbb{F}_q[x]$-modules of the domain and codomain of the considered map are the same, then this map can, after choosing bases, be represented by a square $\mathbb{F}_q[x]$-matrix.

We start with the maps derived from the inclusions $\mathcal{R}(G_t) \subseteq \mathcal{R}(-tG)$ for $0 \leq t < s$; these inclusions follow from $G_t = (t-s)D - tG \leq -tG$.

Definition 3.4. *For $0 \leq t < s$, the map $\imath_t : \mathcal{R}(G_t) \to \mathcal{R}(-tG)$ is defined as the natural inclusion map of $\mathcal{R}(G_t)$ in $\mathcal{R}(-tG)$. We denote by $\boldsymbol{D}_t \in \mathbb{F}_q[x]^{\mu\times\mu}$ the matrix of $\imath_t$ with respect to the ordered $\mathbb{F}_q[x]$-bases $(y_0^{(G_t)}, \ldots, y_{\mu-1}^{(G_t)})$ for $\mathcal{R}(G_t)$ and $(y_0^{(-tG)}, \ldots, y_{\mu-1}^{(-tG)})$ for $\mathcal{R}(-tG)$.*

Remark 3.5. *In this paper, such matrices of maps are considered in a row-wise manner. For example, in this definition, the ith* row *of $\boldsymbol{D}_t$ yields the expression of $\imath_t(y_i^{(G_t)})$ as an $\mathbb{F}_q[x]$-linear combination of the mentioned basis of $\mathcal{R}(-tG)$.*

For deriving complexity estimates, we will use the following bound on the degree of any single entry of $\boldsymbol{D}_t$.

Lemma 3.6. *The matrix $\boldsymbol{D}_t$ is nonsingular and $\deg(\boldsymbol{D}_t)$ is in $\mathcal{O}(s(n+g)/\mu)$.*

Proof. Since $\imath_t$ is an injection, $\boldsymbol{D}_t$ is nonsingular. Let $[p_{ij}]_{0\leq i,j<\mu}$ be the entries of $\boldsymbol{D}_t$, so that $y_i^{(G_t)} = \sum_{j=0}^{\mu-1} p_{ij} y_j^{(-tG)}$ for $0 \leq i < \mu$ and $\deg(\boldsymbol{D}_t) =$

$\max_{ij} \deg(p_{ij})$. Using Lemmas 2.3 and 2.4 we see that

$$\begin{aligned}\deg(p_{ij}) &\leq \frac{1}{\mu}(\delta_{-tG}(y_i^{(G_t)}) - t\deg(G)) \\ &\leq \frac{1}{\mu}(\delta_{G_t}(y_i^{(G_t)}) - t\deg(G)) \\ &\leq \frac{1}{\mu}(2g-1+\mu-\deg(G_t) - t\deg(G)) \\ &= \frac{1}{\mu}(2g-1+\mu+(s-t)n) \quad \in \mathcal{O}(s(n+g)/\mu). \end{aligned}$$ □

We will also use the following, similarly defined inclusion maps and matrices, where we have defined $H_t = -sD - tG$ for $0 \leq t < s$.

Definition 3.7. *For $0 \leq t < s$, the map $\jmath_t : \mathcal{A}(H_t) \to \mathcal{A}(-tG)$ is defined as the natural inclusion map of $\mathcal{A}(H_t)$ in $\mathcal{A}(-tG)$. We denote by $\boldsymbol{E}_t \in \mathbb{F}_q[x]^{\mu\times\mu}$ the matrix of $\jmath_t$ with respect to the $\mathbb{F}_q[x]$-bases $(y_0^{(H_t)}, \ldots, y_{\mu-1}^{(H_t)})$ for $\mathcal{A}(H_t)$ and $(y_0^{(-tG)}, \ldots, y_{\mu-1}^{(-tG)})$ for $\mathcal{A}(-tG)$.*

This matrix $\boldsymbol{E}_t$ satisfies properties similar to those of $\boldsymbol{D}_t$.

Lemma 3.8. *The matrix $\boldsymbol{E}_t$ is nonsingular and $\deg(\boldsymbol{E}_t)$ is in $\mathcal{O}(s(n+g)/\mu)$.*

Proof. The proof can be directly adapted from that of Lemma 3.6. □

We now turn our attention to the maps of multiplication by some $R \in \mathcal{A}(G)$.

Definition 3.9. *For $1 \leq t \leq \ell$, we let the multiplication map $R_t : \mathcal{A}(-tG) \to \mathcal{A}(-(t-1)G)$ be defined by $R_t : f \mapsto Rf$. We denote by $\boldsymbol{R}_t \in \mathbb{F}_q[x]^{\mu\times\mu}$ the matrix of R_t with respect to the ordered $\mathbb{F}_q[x]$-bases $(y_0^{(-tG)}, \ldots, y_{\mu-1}^{(-tG)})$ for $\mathcal{A}(-tG)$ and $(y_0^{(-(t-1)G)}, \ldots, y_{\mu-1}^{(-(t-1)G)})$ for $\mathcal{A}(-(t-1)G)$.*

Although this definition is valid for any $R \in \mathcal{A}(G)$, recall that here we consider specifically R such that $\delta_G(R) \leq n + 2g - 1 - \deg(G)$. This allows us to bound the degree of any single entry of $\boldsymbol{R}_t$, as follows.

Lemma 3.10. *The matrix degree of $\boldsymbol{R}_t$ is in $\mathcal{O}((n+g)/\mu)$.*

Proof. Using Lemma 2.3, we see that for any $0 \leq i, t < \mu$,

$$\delta_{-(t-1)G}(Ry_i^{(-tG)}) = \delta_G(R) + \delta_{-tG}(y_i^{(-tG)}) \leq \delta_G(R) + 2g - 1 + t\deg(G) + \mu.$$

Let $[p_{ij}]_{0\leq i,j<\mu}$ be the entries of $\boldsymbol{R}_t$, so that $Ry_i^{(-tG)} = \sum_{j=0}^{\mu-1} p_{ij} y_j^{(-(t-1)G)}$ for $0 \leq i < \mu$ and $\deg(\boldsymbol{R}_t) = \max_{ij} \deg(p_{ij})$. Then from Lemma 2.4 and the fact that $\delta_G(R) \leq n + 2g - 1 - \deg(G)$, we obtain

$$\begin{aligned}\deg(p_{ij}) &\leq \frac{1}{\mu}\left(\delta_{-(t-1)G}(Ry_i^{(-tG)}) + \deg(-(t-1)G)\right) \\ &\leq \frac{1}{\mu}\left(\delta_G(R) + 2g - 1 + t\deg(G) + \mu - (t-1)\deg(G)\right) \\ &= 1 + \frac{1}{\mu}\left(\delta_G(R) + 2g - 1 + \deg(G)\right) \leq 1 + \frac{1}{\mu}\left(n + 4g - 2\right). \end{aligned}$$ □

In what follows we will also use this notation:

Definition 3.11. *For $0 \leq t \leq \ell$ and $0 \leq j \leq \ell$, the matrix $\boldsymbol{R}^{(t,j)} \in \mathbb{F}_q[x]^{\mu \times \mu}$ is defined as*

$$\boldsymbol{R}^{(t,j)} = \begin{cases} \boldsymbol{R}_t \boldsymbol{R}_{t-1} \cdots \boldsymbol{R}_{j+1} \text{ for } 0 \leq j < t; \\ \text{the } \mu \times \mu \text{ identity matrix } \boldsymbol{I} \text{ for } j = t; \\ \text{the } \mu \times \mu \text{ zero matrix } \boldsymbol{0} \text{ for } t < j \leq \ell. \end{cases}$$

The definition of the $\boldsymbol{R}_t$'s implies that, for $0 \leq j \leq t$, $\boldsymbol{R}^{(t,j)}$ is the matrix of the following map of multiplication by R^{t-j}:

$$R_{j+1} \circ R_{j+2} \circ \cdots \circ R_t : \mathit{Я}(-tG) \to \mathit{Я}(-jG), f \mapsto R^{t-j} f,$$

in the ordered bases $(y_0^{(-tG)}, \ldots, y_{\mu-1}^{(-tG)})$ for $\mathit{Я}(-tG)$ and $(y_0^{(-jG)}, \ldots, y_{\mu-1}^{(-jG)})$ for $\mathit{Я}(-jG)$. Similarly if $j \leq t < s$, then $\boldsymbol{D}_t \boldsymbol{R}^{(t,j)}$ is the matrix of the map

$$R_{j+1} \circ R_{j+2} \circ \cdots \circ R_t \circ \imath_t : \mathit{Я}(G_t) \to \mathit{Я}(-jG), f \mapsto R^{t-j} f,$$

in the ordered bases $(y_0^{(G_t)}, \ldots, y_{\mu-1}^{(G_t)})$ for $\mathit{Я}(G_t)$ and $(y_0^{(-jG)}, \ldots, y_{\mu-1}^{(-jG)})$ for $\mathit{Я}(-jG)$.

3.3 A first polynomial matrix basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$

From Theorem 3.1, one may deduce a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as an $\mathbb{F}_q[x]$-module.

Lemma 3.12. *$\mathcal{M}_{s,\ell,\boldsymbol{r}}$ is an $\mathbb{F}_q[x]$-module of rank $m := \mu(\ell+1)$, and admits the following basis:*

$$\left\{(z-R)^t y_i^{(G_t)} \mid 0 \leq t < s, 0 \leq i < \mu\right\} \bigcup \left\{f_t(z)(z-R)^s y_i^{(G_t)} \mid s \leq t \leq \ell, 0 \leq i < \mu\right\},$$

for any family of polynomials $\{f_t(z) \in F[z] \mid s \leq t \leq \ell\}$ as in Theorem 3.1.

Proof. Let $\mathcal{B}$ be the claimed basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$. Since $\langle y_0^{(G_t)}, \ldots, y_{\mu-1}^{(G_t)} \rangle_{\mathbb{F}_q[x]} = \mathit{Я}(G_t)$ for $0 \leq t \leq \ell$, from Theorem 3.1 it follows both that $\mathcal{B} \subseteq \mathcal{M}_{s,\ell,\boldsymbol{r}}$ and that any element of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ is an $\mathbb{F}_q[x]$-linear combination of polynomials in $\mathcal{B}$; whence $\langle \mathcal{B} \rangle_{\mathbb{F}_q[x]} = \mathcal{M}_{s,\ell,\boldsymbol{r}}$. To prove that $\mathcal{B}$ is a basis, it remains to show that its elements are $\mathbb{F}_q[x]$-linearly independent. Let $(\alpha_{t,i})_{0 \leq i < \mu, 0 \leq t < k} \in \mathbb{F}_q[x]^m$ be a tuple such that

$$\sum_{0 \leq t < s, 0 \leq i < \mu} \alpha_{t,i} (z-R)^t y_i^{(G_t)} + \sum_{s \leq t \leq \ell, 0 \leq i < \mu} \alpha_{t,i} f_t(z) (z-R)^s y_i^{(G_t)} = 0.$$

Since $f_t(z)(z-R)^s$ has degree t, the polynomials $\{(z-R)^t \mid 0 \leq t < s\} \cup \{f_t(z)(z-R)^s \mid s \leq t \leq \ell\}$ form a basis of the F-vector space $F[z]_{\deg_z \leq \ell}$. Thus, from the above identity we deduce that $\sum_{0 \leq i < \mu} \alpha_{t,i} y_i^{(G_t)} = 0$ for $0 \leq t \leq \ell$. By definition of the $y_i^{(G_t)}$'s, this implies $\alpha_{t,i} = 0$ for all t and i. Hence the rows of $\mathcal{B}$ form a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$, and the rank of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ is the cardinality m of $\mathcal{B}$. □

To represent such a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as a matrix $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ over $\mathbb{F}_q[x]$, we see $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as a submodule of the free $\mathbb{F}_q[x]$-module $\bigoplus_{0\le t\le \ell} z^t \mathcal{R}(-tG)$ of rank m, with basis $z^j y_k^{(-tG)}, 0 \le t \le \ell, 0 \le k < \mu$. The following $\mathbb{F}_q[x]$-module isomorphism will be useful for describing $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$:

$$\begin{array}{rccl} \varphi_\ell : & \mathbb{F}_q[x]^{1\times m} & \to & \displaystyle\bigoplus_{t=0}^{\ell} z^t \mathcal{R}(-tG) \\ & [p_{0,0}\cdots p_{0,\mu-1} \mid \cdots \mid p_{\ell,0}\cdots p_{\ell,\mu-1}] & \mapsto & \displaystyle\sum_{t=0}^{\ell}\sum_{k=0}^{\mu-1} p_{t,k} y_k^{(-tG)} z^t \end{array} . \tag{3.2}$$

Then, the rows of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ are the preimages by φ_ℓ of the elements of the basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ described in Lemma 3.12. Choosing specifically for $f_t(z)$ the polynomial $g_t(z)$ described in Section 3.1, and using the maps and matrices defined in Section 3.2, we obtain the following explicit description of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$.

Definition 3.13. *Let $m = \mu(\ell+1)$. The matrix $\boldsymbol{B}_{s,\ell,\boldsymbol{r}} \in \mathbb{F}_q[x]^{m\times m}$ is defined by blocks as $\boldsymbol{B}_{s,\ell,\boldsymbol{r}} = \left[\begin{smallmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \boldsymbol{R} & \boldsymbol{I} \end{smallmatrix}\right]$ where*

- *$\boldsymbol{I}$ is the $(m-\mu s)\times(m-\mu s)$ identity matrix;*
- *$\boldsymbol{0}$ is the $(\mu s)\times(m-\mu s)$ zero matrix;*
- *$\boldsymbol{D} \in \mathbb{F}_q[x]^{(\mu s)\times(\mu s)}$ is defined by blocks as*

$$\boldsymbol{D} = \left[\gamma_{t,j}\boldsymbol{D}_t\boldsymbol{R}^{(t,j)}\right]_{0\le t<s, 0\le j<s} = \begin{bmatrix} \boldsymbol{D}_0 & & & \\ -\boldsymbol{D}_1\boldsymbol{R}_1 & \boldsymbol{D}_1 & & \\ \boldsymbol{D}_2\boldsymbol{R}_2\boldsymbol{R}_1 & -2\boldsymbol{D}_2\boldsymbol{R}_2 & \boldsymbol{D}_2 & \\ \vdots & & & \ddots \end{bmatrix}$$

  where $\gamma_{t,j} = (-1)^{t-j}\binom{t}{j}$ for $0 \le t < s$, $0 \le j < s$;

- *$\boldsymbol{R} \in \mathbb{F}_q[x]^{(m-\mu s)\times(\mu s)}$ is defined by blocks as*

$$\boldsymbol{R} = \left[\gamma_{t,j}\boldsymbol{R}^{(t,j)}\right]_{s\le t\le \ell, 0\le j<s} = \begin{bmatrix} \gamma_{s,0}\boldsymbol{R}^{(s,0)} & \cdots & \gamma_{s,s-1}\boldsymbol{R}^{(s,s-1)} \\ \vdots & & \vdots \\ \gamma_{\ell,0}\boldsymbol{R}^{(\ell,0)} & \cdots & \gamma_{\ell,s-1}\boldsymbol{R}^{(\ell,s-1)} \end{bmatrix}$$

  where $\gamma_{t,j}$ for $s \le t \le \ell, 0 \le j < s$ is defined in Equation (3.1).

Theorem 3.14. *The matrix $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ from Definition 3.13 is a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$, seen as an $\mathbb{F}_q[x]$-submodule of $\bigoplus_{0\le t\le \ell} z^t \mathcal{R}(-tG)$. More precisely, indexing the rows of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ from 0 to $m-1$, for $0 \le t \le \ell$ and $0 \le i < \mu$ its row at index $t\mu + i$ is $\varphi_\ell^{-1}((z-R)^t y_i^{(G_t)})$ if $t < s$, and $\varphi_\ell^{-1}(g_t(z)(z-R)^s y_i^{(G_t)})$ if $s \le t \le \ell$.*

Proof. This follows directly from the construction of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ and from the definition of $\boldsymbol{D}_t$ and $\boldsymbol{R}^{(t,j)}$ in Section 3.2. Indeed, for $0 \le t \le \ell$ and $0 \le i < \mu$, the image by φ_ℓ of the row $t\mu + i$ of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ as built in Definition 3.13 is

$$\sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} R^{t-j} y_i^{(G_t)} z^j = (z-R)^t y_i^{(G_t)} \text{ if } t < s,$$

$$\text{and } z^t y_i^{(-tG)} + \sum_{j=0}^{s-1} \gamma_{t,j} R^{t-j} y_i^{(-tG)} z^j = g_t(z)(z-R)^s y_i^{(-tG)} \text{ if } s \le t \le \ell,$$

where the last identity comes from Lemma 3.3. □

Observe in particular the effect of our choice of polynomials $g_t(z)$ from Section 3.1: only the left μs columns $\left[\begin{smallmatrix} \boldsymbol{D} \\ \boldsymbol{R} \end{smallmatrix}\right]$ of $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ are nontrivial, while the remaining columns $\left[\begin{smallmatrix} \boldsymbol{0} \\ \boldsymbol{I} \end{smallmatrix}\right]$ are standard basis vectors. A parallel can be drawn with the remark on the monomials appearing in $g_t(z)(z-R)^s$, in Section 3.1. In contrast, the two descriptions from [2] recalled in Theorem 2.6 lead to matrices which are block-triangular as well, but with a lower triangular part which is either dense (if using Equation (2.2)) or is a band matrix (if using Equation (2.3)). Although in the latter case the number of nonzero blocks is the same as in $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$, the fact that these nonzero blocks are confined to the leftmost columns brings us closer to knowing an $\mathbb{F}_q[x]$-basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ with small average column degree, as we are going to see in the next subsection.

3.4 A small-degree polynomial matrix basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$

Keeping the same notation as in the previous subsection, we deduce from the matrix $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ a whole collection of suitable matrices for representing bases of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ as an $\mathbb{F}_q[x]$-module, which all share the property that their rightmost $m - \mu s$ columns are the standard basis vectors $\left[\begin{smallmatrix} \boldsymbol{0} \\ \boldsymbol{I} \end{smallmatrix}\right]$. It is within this collection that we will find a $\mathbb{F}_q[x]$-basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ with small average column degree, which means that its shifted Popov form can be computed efficiently.

Theorem 3.15. *For any matrix $\bar{\boldsymbol{R}} \in \mathbb{F}_q[x]^{(m-\mu s)\times(\mu s)}$ such that $\boldsymbol{R} - \bar{\boldsymbol{R}}$ is a left multiple of $\boldsymbol{D}$, the matrix $\boldsymbol{M}_{s,\ell,\boldsymbol{r}} := \left[\begin{smallmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \bar{\boldsymbol{R}} & \boldsymbol{I} \end{smallmatrix}\right] \in \mathbb{F}_q[x]^{m\times m}$ is a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$, seen as an $\mathbb{F}_q[x]$-submodule of $\bigoplus_{0\le t\le \ell} z^t \mathcal{R}(-tG)$. In particular, if $\bar{\boldsymbol{R}}$ has degree in $\mathcal{O}(s(n+g)/\mu)$, then the sum of column degrees of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ is in $\mathcal{O}(s^2(n+g))$, and the $\boldsymbol{d}$-Popov form of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ can be computed in $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g) + \ell^\omega\mu^\omega)$ operations in $\mathbb{F}_q$ for any shift $\boldsymbol{d} \in \frac{1}{\mu}\mathbb{Z}^{(\ell+1)\mu}$.*

Proof. The matrices $\boldsymbol{B}_{s,\ell,\boldsymbol{r}}$ and $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ are left-unimodularly equivalent, since

$$\begin{bmatrix} \boldsymbol{I} & \boldsymbol{0} \\ -\boldsymbol{Q} & \boldsymbol{I} \end{bmatrix} \begin{bmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \boldsymbol{R} & \boldsymbol{I} \end{bmatrix} = \begin{bmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \bar{\boldsymbol{R}} & \boldsymbol{I} \end{bmatrix}$$

where $\boldsymbol{Q} \in \mathbb{F}_q[x]^{(m-\mu s)\times(\mu s)}$ is the quotient matrix such that $\boldsymbol{R} = \boldsymbol{Q}\boldsymbol{D} + \bar{\boldsymbol{R}}$. Hence the rows of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ form a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$.

The degree bounds in Section 3.2 and the construction of $\boldsymbol{R}^{(t,j)}$ show that, for $0 \le t < s$ and $0 \le j < s$, both $\deg(\boldsymbol{D}_t)$ and $\deg(\boldsymbol{R}^{(t,j)})$ are in $\mathcal{O}(s(n+g)/\mu)$. Therefore the degree of $\boldsymbol{D} = [\gamma_{t,j}\boldsymbol{D}_t\boldsymbol{R}^{(t,j)}]_{0\le t<s, 0\le j<s}$ is also in $\mathcal{O}(s(n+g)/\mu)$. Then, under the assumption on $\deg(\bar{\boldsymbol{R}})$ stated in the theorem, the first μs columns of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ have degree in $\mathcal{O}(s(n+g)/\mu)$, whereas its last $m-\mu s$ columns have degree 0. The claimed bound on the column degrees of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ follows.

Computing the shifted Popov form of $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$, for any integer shift $\boldsymbol{d} \in \mathbb{Z}^{(\ell+1)\mu}$, can then be performed in $\tilde{\mathcal{O}}(\ell^\omega \mu^\omega \lceil \frac{s^2(n+g)}{\ell\mu} \rceil)$ operations in $\mathbb{F}_q$ [14, Theorem 1.3]. It has been showed that the case of a shift $\boldsymbol{d}$ with fractional entries in $\frac{1}{\mu}\mathbb{Z}^{(\ell+1)\mu}$ directly reduces to the case of an integer shift by both permuting the matrix columns appropriately and rounding down the entries of $\boldsymbol{d}$ to integers; see [15, Section III.A] [2, Theorem V.9] for the present case, and [13, Section 1.3.4] for transforming more generally any module monomial ordering on $\mathbb{F}_q[x]^{(\ell+1)s}$ into a corresponding shift in $\mathbb{Z}^{(\ell+1)\mu}$. The inequality $\lceil \frac{s^2(n+g)}{\ell\mu} \rceil < \frac{s^2(n+g)}{\ell\mu} + 1$ leads to the cost bound stated in the theorem. □

Finally, in Theorem 3.17 we will make the above result more effective by describing an explicit construction of such a small-degree matrix $\bar{\boldsymbol{R}}$, using remainders in the matrix division of $\boldsymbol{R}$ modulo the matrices $\boldsymbol{E}_0, \ldots, \boldsymbol{E}_{s-1}$ defined in Section 3.2. Here are some explanations why such a degree reduction is needed, and not straightforward.

Remark 3.16. *Observe that the matrix $\boldsymbol{R}$, as defined in Section 3.3, may have degrees too large for our purpose; that is, simply taking $\bar{\boldsymbol{R}} = \boldsymbol{R}$ in the above theorem is not interesting as $\deg(\boldsymbol{R})$ is most likely not in $\mathcal{O}(s(n+g)/\mu)$. In fact, by definition $\boldsymbol{R}$ has $\ell+1-s$ blocks of μ rows each with $s\mu$ columns, and the degree of the ith block of rows is in $\mathcal{O}((s+i)\frac{n+g}{\mu})$. In total, the dense representation of $\boldsymbol{R}$ therefore uses*

$$\mathcal{O}\left(\sum_{1\le i\le \ell+1-s} \mu(\mu s)(s+i)\frac{n+g}{\mu}\right) \subseteq \mathcal{O}\left(\ell^2 s\mu(n+g)\right)$$

coefficients from $\mathbb{F}_q$, and this asymptotic bound can be reached. Indeed, it is reached already in the case of Reed-Solomon codes, where $\boldsymbol{R}^{(t,j)}$ is a polynomial in $\mathbb{F}_q[x]$, which is the power R^{t-j} of some polynomial $R \in \mathbb{F}_q[x]$ whose degree is $n-1$ generically. Thus, simply the size of the storage of $\boldsymbol{R}$ can already be in conflict with our target complexity. This also implies that we must aim to compute a smaller degree $\bar{\boldsymbol{R}}$ without computing all of $\boldsymbol{R}$.

Theorem 3.17. *For each $s \le t \le \ell$ and $0 \le j < s$, there exists a matrix $\bar{\boldsymbol{R}}^{(t,j)}$ such that $\boldsymbol{R}^{(t,j)} - \bar{\boldsymbol{R}}^{(t,j)}$ is a left multiple of $\boldsymbol{E}_j$ and $\deg(\bar{\boldsymbol{R}}^{(t,j)}) < \deg(\boldsymbol{E}_j)$. Then, the matrix $\bar{\boldsymbol{R}} = [\gamma_{t,j}\bar{\boldsymbol{R}}^{(t,j)}]_{s\le t\le \ell, 0\le j<s} \in \mathbb{F}_q[x]^{(m-\mu s)\times(\mu s)}$ has degree in $\mathcal{O}(s(n+g)/\mu)$ and is such that $\boldsymbol{R} - \bar{\boldsymbol{R}}$ is a left multiple of $\boldsymbol{D}$.*

Proof. The existence of $\bar{\boldsymbol{R}}^{(t,j)}$ with the specified properties follows directly from Lemma 2.7. The bound on $\deg(\bar{\boldsymbol{R}})$ follows from $\deg(\boldsymbol{E}_j) \in \mathcal{O}(s(n+g)/\mu)$, proved

in Lemma 3.8. By construction, $\boldsymbol{R} - \bar{\boldsymbol{R}} = [\gamma_{t,j}(\boldsymbol{R}^{(t,j)} - \bar{\boldsymbol{R}}^{(t,j)})]_{s \le t \le \ell, 0 \le j < s}$ is a left multiple of

$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{E}_0 & & & \\ & \boldsymbol{E}_1 & & \\ & & \ddots & \\ & & & \boldsymbol{E}_{s-1} \end{bmatrix} \in \mathbb{F}_q[x]^{(\mu s)\times(\mu s)},$$

hence it remains to prove that $\boldsymbol{E}$ is itself a left multiple of $\boldsymbol{D}$.

We now show that each row of $\boldsymbol{E}$ is a left multiple of $\boldsymbol{D}$. Let $0 \le i < \mu$ and $0 \le t < s$. Similarly to the considerations in Section 3.3, we observe that the row $t\mu + i$ of $\boldsymbol{E}$ corresponds to the polynomial $z^t y_i^{(H_t)} \in z^t \mathcal{R}(H_t)$, which is in $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ since any function in $\mathcal{R}(H_t) = \mathcal{R}(-sD - tG)$ has valuation at least s at each of the places $P_1, \dots, P_n$. Since $z^t y_i^{(H_t)}$ has z-degree less than s, by Theorem 2.6 it is in $\bigoplus_{0 \le j < s} (z-R)^j \mathcal{R}(G_j)$, which means that the row $t\mu + i$ of $\boldsymbol{E}$ is a left multiple of $\boldsymbol{D}$. □

4 Efficient construction of a polynomial matrix basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$

4.1 Computing multiplication maps

Consider the following problem: given two divisors A and B and a function $a \in \mathcal{R}(A)$, compute the products $y_0^{(B)}a, \dots, y_{\mu-1}^{(B)}a \in \mathcal{R}(A+B)$, expressed in the basis $y_0^{(A+B)}, \dots, y_{\mu-1}^{(A+B)}$. In order to do this, we generalize [2, Algorithm 4]. We follow the same approach as in [2] for showing the correctness and complexity of this generalization.

Definition 4.1. *For any $Q(z) \in F[z]$, for any rational place $P \in \mathbb{P}_F$ that is not a pole of any of the coefficients of $Q(z)$, and for $\alpha \in \mathbb{F}_q$, we denote by $Q(P, \alpha)$ the evaluation of $Q(\alpha) \in F$ at P.*

Definition 4.2. *Let A, B be divisors and let $E = E_1 + \cdots + E_N$ for distinct rational places $E_1, \dots, E_N$ of F different from P_∞ such that $\operatorname{supp}(A) \cap \operatorname{supp}(E) = \emptyset$ and $\operatorname{supp}(B) \cap \operatorname{supp}(E) = \emptyset$. For $a \in \mathcal{R}(A)$, we define the $\mathbb{F}_q[x]$-module*

$$\begin{aligned} \mathcal{N}_{A,B,E}(a) = \{&Q = Q_0 + Q_1 z \in \mathcal{R}(A+B) \oplus z\mathcal{R}(B) \\ &\text{such that } Q(P, a(P)) = 0 \text{ for all } P \in \operatorname{supp}(E)\}. \end{aligned}$$

In the following lemmas, we use the same notation A, B, E as in Definition 4.2.

Lemma 4.3. *Let $a \in \mathcal{R}(A)$. If $Q = Q_0 + zQ_1 \in \mathcal{N}_{A,B,E}(a)$ with*

$$\max\{\delta_{A+B}(Q_0), \delta_B(Q_1) + \delta_A(a)\} < \deg(E) - \deg(A+B),$$

then $Q(a) = 0$, i.e. $Q \in (z-a)\mathcal{R}(B)$.

Proof. Since $Q \in \mathcal{N}_{A,B,E}(a)$, we have $Q(a) \in \mathcal{R}(A+B)$. Hence by definition of δ_{A+B}, we have $Q(a) \in \mathcal{L}(\delta_{A+B}(Q(a))P_\infty + A + B)$. Since for all $E_j \in \mathrm{supp}(E)$, we have $Q(a)(E_j) = 0$ and $\mathrm{supp}(E) \cap (\mathrm{supp}(A) \cup \mathrm{supp}(B) \cup \{P_\infty\}) = \emptyset$, we conclude that $Q(a) \in \mathcal{L}(\delta_{A+B}(Q(a))P_\infty + A + B - E)$. Moreover,

$$\begin{aligned} \delta_{A+B}(Q(a)) &\leq \max\{\delta_{A+B}(Q_0), \delta_{A+B}(Q_1 a)\} \\ &= \max\{\delta_{A+B}(Q_0), \delta_B(Q_1) + \delta_A(a)\} \\ &< \deg(E) - \deg(A+B), \end{aligned}$$

which ensures that the aforementioned Riemann-Roch space is trivial. □

Like in [2], our generalization will use the notion of an *x-partition* of E. We recall the definition, see also [2, Definition V.4]; the existence of an x-partition of E was shown in [2, Lemma V.6].

Definition 4.4. *If $E = E_1 + \cdots + E_N$, where $E_1, \ldots, E_N$ are distinct rational places different from P_∞, and $U_0, \ldots, U_{\mu-1}$ are effective divisors satisfying*

1. *$E = U_0 + \cdots + U_{\mu-1}$,*
2. *$\mathrm{supp}(U_i) \cap \mathrm{supp}(U_j) = \emptyset$ for all $i \neq j$,*
3. *$|\deg(U_i) - \deg(U_j)| \leq 1$ for all i, j,*
4. *for any $E_j, E_k \in \mathrm{supp}(U_i)$ it holds that $x(E_j) = x(E_k) \Leftrightarrow E_j = E_k$,*

*then we will say that $U_0, \ldots, U_{\mu-1}$ is an x-*partition *of E.*

Definition 4.5. *For a polynomial matrix $\boldsymbol{A} \in \mathbb{F}_q[x]^{2\mu \times \mu}$ and nonzero polynomials $u_0, \ldots, u_{\mu-1} \in \mathbb{F}_q[x] \setminus \{0\}$, we define*

$$\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A}) = \Big\{ \boldsymbol{v} \in \mathbb{F}_q[x]^{1\times 2\mu} \mid \boldsymbol{v}\boldsymbol{A}_{*,k} = 0 \bmod u_k \quad \text{for } 0 \leq k < \mu \Big\},$$

where $\boldsymbol{A}_{*,k}$ is the column k of $\boldsymbol{A}$.

Note that we have the following inclusion of $\mathbb{F}_q[x]$-submodules:

$$(\textstyle\prod_{0\leq k<\mu} u_k)\mathbb{F}_q[x]^{1\times 2\mu} \;\subseteq\; \mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A}) \;\subseteq\; \mathbb{F}_q[x]^{1\times 2\mu}.$$

In particular, $\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A})$ is a free $\mathbb{F}_q[x]$-module of rank 2μ, and each of its bases can be represented as a nonsingular $2\mu \times 2\mu$ matrix over $\mathbb{F}_q[x]$.

Lemma 4.6. *Let $a \in \mathcal{R}(A)$. Let $U_0, \ldots, U_{\mu-1}$ be an x-partition of E, and let $\boldsymbol{S} = [S_{i,k}]$ and $\boldsymbol{T} = [T_{i,k}]$ be matrices in $\mathbb{F}_q[x]^{\mu\times\mu}$ such that*

$$S_{i,k}(x(E_j)) = y_i^{(A+B)}(E_j) \text{ and } T_{i,k}(x(E_j)) = a(E_j) y_i^{(B)}(E_j) \text{ for } E_j \in U_k.$$

If $\boldsymbol{u} = (u_0, \ldots, u_{\mu-1}) \in \mathbb{F}_q[x]^\mu$, where $u_k = \prod_{E_j \in \mathrm{supp}(U_k)} (x - x(E_j))$, then the map

$$\psi : \sum_{i=0}^{\mu-1} (s_i y_i^{(A+B)} + t_i z y_i^{(B)}) \mapsto (s_0, \ldots, s_{\mu-1}, t_0, \ldots, t_{\mu-1})$$

is an $\mathbb{F}_q[x]$-isomorphism between $\mathcal{N}_{A,B,E}(a)$ and $\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A})$, where

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{S} \\ \boldsymbol{T} \end{bmatrix} \in \mathbb{F}_q[x]^{2\mu \times \mu}.$$

Proof. Clearly ψ is an $\mathbb{F}_q[x]$-isomorphism between $\mathcal{R}(A+B) \oplus z\mathcal{R}(B)$ and $\mathbb{F}_q[x]^{2\mu}$, therefore it suffices to show that for any $Q \in \mathcal{R}(A+B) \oplus z\mathcal{R}(B)$ it holds that $Q \in \mathcal{N}_{A,B,E}(a)$ if and only if $\psi(Q) \in \mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A})$, i.e. that for all $k = 0, \ldots, \mu-1$, $Q(E_j, a(E_j)) = 0$ for all $E_j \in \operatorname{supp}(U_k)$ if and only if $\psi(Q) \cdot \boldsymbol{A}_{*,k} = 0 \bmod u_k$. This is true since for every $E_j \in U_k$ the following identity holds, where $\alpha = x(E_j)$:

$$\begin{aligned} Q(E_j, a(E_j)) &= \sum_{i=0}^{\mu-1} \left(s_i(\alpha) y_i^{(A+B)}(E_j) + a(E_j) t_i(\alpha) y_i^{(B)}(E_j) \right) \\ &= \sum_{i=0}^{\mu-1} \left(s_i(\alpha) S_{i,k}(\alpha) + t_i(\alpha) T_{i,k}(\alpha) \right) = (\psi(Q) \cdot \boldsymbol{A}_{*,k})(\alpha). \qquad \square \end{aligned}$$

Lemma 4.7. *In the context of Lemma 4.6, if $\boldsymbol{P} \in \mathbb{F}_q[x]^{(2\mu)\times(2\mu)}$ is the $\boldsymbol{d}$-Popov basis of $\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A}) = \psi(\mathcal{N}_{A,B,E}(a))$, where $\deg(E) \geq 2g + \mu + \delta_A(a) + \deg(A)$ and*

$$\begin{aligned} \boldsymbol{d} = \frac{1}{\mu} \Big(& \delta_{A+B}(y_0^{(A+B)}) + \deg(B), \ldots, \delta_{A+B}(y_{\mu-1}^{(A+B)}) + \deg(B), \\ & \delta_B(y_0^{(B)}) + \delta_A(a) + \deg(B), \ldots, \delta_B(y_{\mu-1}^{(B)}) + \delta_A(a) + \deg(B) \Big) \in \tfrac{1}{\mu}\mathbb{Z}^{2\mu}, \end{aligned}$$

then exactly μ rows of $\boldsymbol{P}$ have $\boldsymbol{d}$-degree less than $\frac{1}{\mu}(\deg(E) - \deg(A))$. Furthermore, if $\tilde{\boldsymbol{P}} \in \mathbb{F}_q[x]^{\mu\times(2\mu)}$ is the submatrix of $\boldsymbol{P}$ consisting of these rows, then for $k = 0, \ldots, \mu-1$ the row k of $\tilde{\boldsymbol{P}}$ is $\psi(Y_k)$, where

$$Y_k = -a y_k^{(B)} + z y_k^{(B)} \in (z-a)\mathcal{R}(B) \subset \mathcal{N}_{A,B,E}(a).$$

Consequently, if $\tilde{\boldsymbol{P}} = [\boldsymbol{P}_1 \;\; \boldsymbol{P}_2]$, where $\boldsymbol{P}_1$ and $\boldsymbol{P}_2$ are in $\mathbb{F}_q[x]^{\mu\times\mu}$, then $a y_k^{(B)} = \sum_{i=0}^{\mu-1} p_{k,i} y_i^{(A+B)}$, where $(p_{k,0}, \ldots, p_{k,\mu-1})$ is the row k of $-\boldsymbol{P}_1$.

Proof. We start with some observations on the matrix whose rows are $\psi(Y_k)$ for $k = 0, \ldots, \mu-1$. This is a $\mu \times (2\mu)$ matrix over $\mathbb{F}_q[x]$, whose rank is μ since $Y_0, \ldots, Y_{\mu-1}$ are $\mathbb{F}_q[x]$-linearly independent. By construction, its $\mu\times\mu$ rightmost submatrix is the identity matrix. Writing $Y_k = -\sum_{i=0}^{\mu-1} w_i y_i^{(A+B)} + z y_k^{(B)}$, where $w_i \in \mathbb{F}_q[x]$, the fact that $Y_k(a) = 0$ implies

$$\begin{aligned} \max_i \delta_{A+B}(w_i y_i^{(A+B)}) &= \delta_{A+B}\left(\sum_{i=0}^{\mu-1} w_i y_i^{(A+B)} \right) \\ &= \delta_{A+B}(a y_k^{(B)}) = \delta_B(y_k^{(B)}) + \delta_A(a). \end{aligned}$$

Consequently, $\deg_{\boldsymbol{d}}(\psi(Y_k)) = \frac{1}{\mu}(\delta_B(y_k^{(B)}) + \delta_A(a) + \deg(B))$, and this $\boldsymbol{d}$-degree is reached at index $\mu + k$. This shows that $\mu + k$ is the $\boldsymbol{d}$-pivot index of the row $\psi(Y_k)$. This property combined with the special shape (with an identity submatrix) of the matrix formed by the $\psi(Y_k)$'s ensure that this matrix is in $\boldsymbol{d}$-Popov form.

Furthermore, since for $k = 0, \ldots, \mu - 1$, $\psi(Y_k)$ is in $\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A})$ with

$$\deg_{\boldsymbol{d}}(\psi(Y_k)) < \frac{1}{\mu}(\delta_A(a) + 2g + \mu) \leq \frac{1}{\mu}(\deg(E) - \deg(A)),$$

where the strict inequality is due to Lemma 2.3, then at least μ rows of $\boldsymbol{P}$ have $\boldsymbol{d}$-degree less than $\frac{1}{\mu}(\deg(E) - \deg(A))$, because $\boldsymbol{P}$ is $\boldsymbol{d}$-row reduced.

Now, for any $Q = Q_0 + zQ_1 \in \mathcal{N}_{A,B,E}(a)$, where $Q_0 = \sum_{i=0}^{\mu-1} s_i y_i^{(A+B)} \in \mathcal{R}(A+B)$ and $Q_1 = \sum_{i=0}^{\mu-1} t_i y_i^{(B)} \in \mathcal{R}(B)$ with $s_i, t_i \in \mathbb{F}_q[x]$, it holds that

$$\begin{aligned}\deg_{\boldsymbol{d}}(\psi(Q)) &= \max\left\{ \max_i \left(\deg(s_i) + \frac{\delta_{A+B}(y_i^{(A+B)}) + \deg(B)}{\mu} \right), \right. \\ &\qquad \left. \max_i \left(\deg(t_i) + \frac{\delta_B(y_i^{(B)}) + \delta_A(a) + \deg(B)}{\mu} \right) \right\} \\ &= \frac{1}{\mu} \max\{\delta_{A+B}(Q_0) + \deg(B), \delta_B(Q_1) + \delta_A(a) + \deg(B)\}.\end{aligned}$$

It then follows from Lemma 4.3 that

$$\deg_{\boldsymbol{d}}(\psi(Q)) < \frac{1}{\mu}(\deg(E) - \deg(A)) \implies Q \in (z-a)\mathcal{R}(B),$$

which means that at most μ rows of $\boldsymbol{P}$ can have $\boldsymbol{d}$-degree less than $\frac{1}{\mu}(\deg(E) - \deg(A))$, because $(z-a)\mathcal{R}(B)$ has rank μ as an $\mathbb{F}_q[x]$-module.

Thus, exactly μ rows of $\boldsymbol{P}$ have $\boldsymbol{d}$-degree less than $\frac{1}{\mu}(\deg(E) - \deg(A))$, which proves the first claim of the lemma. For the second claim, the above observations show that the matrix formed by the $\psi(Y_k)$'s is a left multiple $\boldsymbol{U}\tilde{\boldsymbol{P}}$ by a nonsingular $\mu \times \mu$ matrix $\boldsymbol{U}$. Yet, since both $\tilde{\boldsymbol{P}}$ and the matrix whose rows are the $\psi(Y_k)$'s are in $\boldsymbol{d}$-Popov form, and since the rightmost $\mu \times \mu$ submatrix of the latter is the identity matrix, the only possibility is $\boldsymbol{U} = \boldsymbol{I}_\mu$, proving the second claim. The last claim is obvious. □

Theorem 4.8. *Algorithm 1 is correct and costs $\tilde{\mathcal{O}}(\mu^{\omega-1}(N + |\deg(A)|))$ operations in $\mathbb{F}_q$.*

Proof. Correctness is given by Lemma 4.7. For complexity, simply note that the computational bottleneck lies in Step 8, in which case $\delta_A(a) \geq -\deg(A)$ because a is nonzero and $a \in \mathcal{L}(\delta_A(a)P_\infty + A)$. By assumption, we have that $N = \deg(E) \geq \deg(A) + \delta_A(a) + 2g + \mu$, hence by Lemma 2.3

$$\begin{aligned}-\deg(A) \leq \delta_{A+B}(y_i^{(A+B)}) + \deg(B) &\leq 2g - 1 - \deg(A) + \mu \\ &< \deg(E) - 2\deg(A) - \delta_A(a) \\ &\leq \deg(E) - \deg(A) = N - \deg(A)\end{aligned}$$

Algorithm 1 BasisProducts$(A, B, E, \boldsymbol{a}, \boldsymbol{x}, \boldsymbol{y}^{(A+B)}, \boldsymbol{y}^{(B)})$

Input:

- divisors A and B,
- a divisor $E = E_1 + \cdots + E_N$, where $E_1, \ldots, E_N$ are pairwise distinct rational places such that $\operatorname{supp}(E) \cap (\operatorname{supp}(A) \cup \operatorname{supp}(B) \cup \{P_\infty\}) = \emptyset$
- evaluations $\boldsymbol{a} = (a_j)_{j=1,\ldots,N}$, where $a_j = a(E_j)$ for a function $a \in \mathcal{H}(A)$ with known $\delta_A(a)$ and such that $\deg(E) \geq \deg(A) + \delta_A(a) + 2g + \mu$,
- evaluations $\boldsymbol{x} = (x_j)_{j=1,\ldots,N}$, where $x_j = x(E_j) \in \mathbb{F}_q$,
- evaluations $\boldsymbol{y}^{(A+B)} = (y_{i,j}^{(A+B)})_{j=1,\ldots,N}^{i=0,\ldots,\mu-1}$, where $y_{i,j}^{(A+B)} = y_i^{(A+B)}(E_j) \in \mathbb{F}_q$,
- evaluations $\boldsymbol{y}^{(B)} = (y_{i,j}^{(B)})_{j=1,\ldots,N}^{i=0,\ldots,\mu-1}$, where $y_{i,j}^{(B)} = y_i^{(B)}(E_j) \in \mathbb{F}_q$.

Output: matrix $[p_{k,i}] \in \mathbb{F}_q[x]^{\mu\times\mu}$ of the $\mathbb{F}_q[x]$-linear map $f \in \mathcal{H}(B) \mapsto af \in \mathcal{H}(A+B)$ with respect to the ordered $\mathbb{F}_q[x]$-bases $(y_0^{(B)}, \ldots, y_{\mu-1}^{(B)})$ for $\mathcal{H}(B)$ and $(y_0^{(A+B)}, \ldots, y_{\mu-1}^{(A+B)})$ for $\mathcal{H}(A+B)$, meaning $ay_k^{(B)} = \sum_{i=0}^{\mu-1} p_{k,i} y_i^{(A+B)}$ for all $k \in \{0, \ldots, \mu-1\}$.

1: **if** $\boldsymbol{a} = \boldsymbol{0}$ **then return** matrix $\boldsymbol{0} \in \mathbb{F}_q[x]^{\mu\times\mu}$
2: $U_0, \ldots, U_{\mu-1} \leftarrow$ an x-partition of E
3: $\boldsymbol{S} = [S_{i,k}] \in \mathbb{F}_q[x]^{\mu\times\mu} \leftarrow$ matrix with $S_{i,k}(x_j) = y_{i,j}^{(A+B)}$ for $E_j \in U_k$
4: $\boldsymbol{T} = [T_{i,k}] \in \mathbb{F}_q[x]^{\mu\times\mu} \leftarrow$ matrix with $T_{i,k}(x_j) = a_j\, y_{i,j}^{(B)}$ for $E_j \in U_k$
5: $\boldsymbol{u} = [u_0, \ldots, u_{\mu-1}] \in \mathbb{F}_q[x]^\mu \leftarrow$ vector with $u_k = \prod_{E_j \in U_k} (x - x_j)$
6: $\boldsymbol{d} \in \frac{1}{\mu}\mathbb{Z}^{2\mu} \leftarrow \frac{1}{\mu}\big(\delta_{A+B}(y_0^{(A+B)}) + \deg(B), \ldots, \delta_{A+B}(y_{\mu-1}^{(A+B)}) + \deg(B),$ $\delta_B(y_0^{(B)}) + \delta_A(a) + \deg(B), \ldots, \delta_B(y_{\mu-1}^{(B)}) + \delta_A(a) + \deg(B)\big)$
7: $\boldsymbol{P} \in \mathbb{F}_q[x]^{(2\mu)\times(2\mu)} \leftarrow \boldsymbol{d}$-Popov basis of $\mathcal{H}_{\boldsymbol{u}}(\boldsymbol{A})$ where $\boldsymbol{A} = \left[\begin{smallmatrix} \boldsymbol{S} \\ \boldsymbol{T} \end{smallmatrix}\right] \in \mathbb{F}_q[x]^{(2\mu)\times\mu}$
8: $[\boldsymbol{P}_1 \;\; \boldsymbol{P}_2] \in \mathbb{F}_q[x]^{\mu\times(2\mu)} \leftarrow$ the submatrix of $\boldsymbol{P}$ consisting of all rows with $\boldsymbol{d}$-degree less than $\frac{1}{\mu}(\deg(E) - \deg(A))$, where $\boldsymbol{P}_1, \boldsymbol{P}_2 \in \mathbb{F}_q[x]^{\mu\times\mu}$
9: **return** $-\boldsymbol{P}_1$

and

$$\begin{aligned} -\deg(A) &\le \delta_A(a) \le \delta_B(y_i^{(B)}) + \delta_A(a) + \deg(B) \\ &\le 2g - 1 + \mu + \delta_A(a) \\ &\le -1 + \deg(E) - \deg(A) < N - \deg(A). \end{aligned}$$

Since $\deg(u_k) \le N/\mu$ for $k = 0, \dots, \mu - 1$, then the total complexity of the algorithm is given by [2, Cor. V.10] as

$$\begin{aligned} &\tilde{\mathcal{O}}\big(\mu^{\omega-1} \max\{|\deg(E)|, |\deg(E) - \deg(A)|, |\deg(A)|\}\big) \\ &\subseteq \tilde{\mathcal{O}}(\mu^{\omega-1}(N + |\deg(A)|)) \end{aligned}$$

operations in $\mathbb{F}_q$. □

4.2 Computing a small-degree $\mathbb{F}_q[x]$-basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$

Theorem 4.9. *Algorithm 2 is correct and costs $\tilde{\mathcal{O}}(\ell\mu^{\omega-1}N + s^2\ell\mu^{\omega-1}(n+g))$ operations in $\mathbb{F}_q$.*

Proof. The correctness follows from the correctness of the called algorithms and from the results in Section 3.4.

For complexity, let us first consider the total cost of the calls to BasisProducts; for completeness we also give at the same time the detailed verification that the constraint on $\deg(E)$ required in the input of this algorithm is satisfied.

- For $t = 0, \dots, s-1$, the call at Line 3 is for the divisor $A = (s-t)D$ and the function $a = 1$, and therefore costs $\tilde{\mathcal{O}}(\mu^{\omega-1}(N + |\deg((s-t)D)|)) = \tilde{\mathcal{O}}(\mu^{\omega-1}(N + (s-t)n))$ according to Theorem 4.8. Over the s iterations, this cost is in $\tilde{\mathcal{O}}(s\mu^{\omega-1}N + s^2\mu^{\omega-1}n)$. Furthermore the input requirements of BasisProducts impose $\deg(E) \ge \deg((s-t)D) + \delta_{(s-t)D}(1) + 2g + \mu$ for all $t = 0, \dots, s-1$, hence we must ensure $\deg(E) \ge sn + 2g + \mu$; this is implied by the input requirements of InterpolantPolMatBasis.

- The calls at Line 4 are for the divisor $A = (s-t)D$ and the function $a = 1$. Thus their total complexity fits within the one in the previous item, and these calls do not bring any additional restriction on $\deg(E)$.

- Finally, the calls to BasisProducts at Line 9 are for the divisor $A = G$ and the function $a = R$, for each of the ℓ iterations. In total, this costs $\tilde{\mathcal{O}}(\ell\mu^{\omega-1}(N + |\deg(G)|)) = \tilde{\mathcal{O}}(\ell\mu^{\omega-1}N + \ell\mu^{\omega-1}(n+g))$. These calls all add the same constraint on $\deg(E)$, namely $\deg(E) \ge \deg(G) + \delta_G(R) + 2g + \mu$. Since $\delta_G(R) \le n + 2g - 1 - \deg(G)$ holds by construction of R (see the output specification of [2, Algorithm 2]), this constraint is satisfied when $\deg(E) \ge n + 4g + \mu - 1$, and this inequality is indeed implied by the input requirements of InterpolantPolMatBasis.

Algorithm 2 InterpolantPolMatBasis$(\boldsymbol{r}, D, G, E, \boldsymbol{x}, \boldsymbol{y}^{(-tG)}, \boldsymbol{y}^{(G_t)}, \boldsymbol{y}^{(H_t)})$

Input:

- received word $\boldsymbol{r} \in \mathbb{F}_q^n$,
- the code divisors D and G,
- a divisor $E = E_1 + \cdots + E_N$, where $E_1, \ldots, E_N$ are pairwise distinct rational places not in $\{P_\infty\} \cup \operatorname{supp}(G)$, with $\deg(E) \geq sn + 4g + \mu - 1$,
- evaluations $\boldsymbol{x} = (x_j)_{j=1,\ldots,N}$, where $x_j = x(E_j) \in \mathbb{F}_q$,
- evaluations $\boldsymbol{y}^{(-tG)} = (y_{i,j}^{(-tG)})_{j=1,\ldots,N}^{i=0,\ldots,\mu-1}$ for $t = -1, 0, \ldots, \ell$, where $y_{i,j}^{(-tG)} = y_i^{(-tG)}(E_j) \in \mathbb{F}_q$,
- evaluations $\boldsymbol{y}^{(G_t)} = (y_{i,j}^{(G_t)})_{j=1,\ldots,N}^{i=0,\ldots,\mu-1}$ for $t = 0, \ldots, s-1$, where $G_t = (t-s)D - tG$ and $y_{i,j}^{(G_t)} = y_i^{(G_t)}(E_j) \in \mathbb{F}_q$,
- evaluations $\boldsymbol{y}^{(H_t)} = (y_{i,j}^{(H_t)})_{j=1,\ldots,N}^{i=0,\ldots,\mu-1}$ for $t = 0, \ldots, s-1$, where $H_t = -sD - tG$ and $y_{i,j}^{(H_t)} = y_i^{(H_t)}(E_j) \in \mathbb{F}_q$.

Output: a matrix $\boldsymbol{M}_{s,\ell,\boldsymbol{r}} := \left[\begin{smallmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \bar{\boldsymbol{R}} & \boldsymbol{I} \end{smallmatrix}\right] \in \mathbb{F}_q[x]^{m \times m}$ as in Theorem 3.15: $\boldsymbol{M}_{s,\ell,\boldsymbol{r}}$ is a basis of $\mathcal{M}_{s,\ell,\boldsymbol{r}}$ seen as an $\mathbb{F}_q[x]$-submodule of $\bigoplus_{0 \leq t \leq \ell} z^t \mathcal{R}(-tG)$ and $\deg(\bar{\boldsymbol{R}})$ has degree in $\mathcal{O}(s(n+g)/\mu)$.

▷ *Compute matrices $\boldsymbol{D}_t$ and $\boldsymbol{E}_t$ in $\mathbb{F}_q[x]^{\mu \times \mu}$, see Definitions 3.4 and 3.7*
for $t = 0, \ldots, s-1$ **do**
  $\boldsymbol{D}_t \leftarrow$ BasisProducts$((s-t)D, G_t, E, (1, \ldots, 1), \boldsymbol{x}, \boldsymbol{y}^{(-tG)}, \boldsymbol{y}^{(G_t)})$
  $\boldsymbol{E}_t \leftarrow$ BasisProducts$(sD, H_t, E, (1, \ldots, 1), \boldsymbol{x}, \boldsymbol{y}^{(-tG)}, \boldsymbol{y}^{(H_t)})$
▷ *Compute matrices $\boldsymbol{R}_1, \ldots, \boldsymbol{R}_\ell$ in $\mathbb{F}_q[x]^{\mu \times \mu}$, see Definition 3.9*
$R \in \mathcal{R}(G) \leftarrow$ Interpolate$(\boldsymbol{r}, D, G, \boldsymbol{x}, \boldsymbol{y}^{(G)})$ ▷ *[2, Algorithm 2]*
$\hat{\boldsymbol{r}} \in \mathbb{F}_q^N \leftarrow$ Evaluate$(R, E, G, \boldsymbol{x}, \boldsymbol{y}^{(G)})$ ▷ *[2, Algorithm 1]*
for $t = 1, \ldots, \ell$ **do**
  $\boldsymbol{R}_t \leftarrow$ BasisProducts$(G, -tG, E, \hat{\boldsymbol{r}}, \boldsymbol{x}, \boldsymbol{y}^{(-(t-1)G)}, \boldsymbol{y}^{(-tG)})$
▷ *Compute matrix $\boldsymbol{D} \in \mathbb{F}_q[x]^{(\mu s) \times (\mu s)}$, see Definition 3.13*
$\boldsymbol{D} = [\boldsymbol{D}^{(t,j)}]_{0 \leq t < s, 0 \leq j < s} \leftarrow \operatorname{Diag}(\boldsymbol{D}_0, \ldots, \boldsymbol{D}_{s-1})$, where $\boldsymbol{D}^{(t,j)} \in \mathbb{F}_q[x]^{\mu \times \mu}$
for $t = 1, \ldots, s-1$ **do**
  for $j = t-1, \ldots, 0$ **do** $\boldsymbol{D}^{(t,j)} \leftarrow \boldsymbol{D}^{(t,j+1)} \boldsymbol{R}_{j+1}$
  for $j = t-1, \ldots, 0$ **do** $\boldsymbol{D}^{(t,j)} \leftarrow (-1)^{t-j} \binom{t}{j} \boldsymbol{D}^{(t,j)}$
▷ *Compute matrix $\bar{\boldsymbol{R}} \in \mathbb{F}_q[x]^{((\ell+1-s)\mu) \times (\mu s)}$, see Definition 3.13 and Theorem 3.17*
$\bar{\boldsymbol{R}} = [\bar{\boldsymbol{R}}^{(t,j)}]_{s \leq t \leq \ell, 0 \leq j < s} \leftarrow$ zero matrix with blocks $\bar{\boldsymbol{R}}^{(t,j)} \in \mathbb{F}_q[x]^{\mu \times \mu}$
for $j = 0, \ldots, s-1$ **do**
  $\bar{\boldsymbol{R}}^{(s,j)} \leftarrow$ PM-Rem$(\boldsymbol{R}_s \boldsymbol{R}_{s-1} \cdots \boldsymbol{R}_{j+1}, \boldsymbol{E}_j)$ ▷ *algorithm from Lemma 2.7*
  for $t = s+1, \ldots, \ell$ **do** $\bar{\boldsymbol{R}}^{(t,j)} \leftarrow$ PM-Rem$(\boldsymbol{R}_t \bar{\boldsymbol{R}}^{(t-1,j)}, \boldsymbol{E}_j)$
  for $t = s, \ldots, \ell$ **do** $\bar{\boldsymbol{R}}^{(t,j)} \leftarrow \gamma_{t,j} \bar{\boldsymbol{R}}^{(t,j)}$ ▷ $\gamma_{t,j}$ *defined in Equation (3.1)*
return $\left[\begin{smallmatrix} \boldsymbol{D} & \boldsymbol{0} \\ \bar{\boldsymbol{R}} & \boldsymbol{I} \end{smallmatrix}\right] \in \mathbb{F}_q[x]^{((\ell+1)\mu) \times ((\ell+1)\mu)}$

The interpolation at Line 6 costs $\tilde{\mathcal{O}}(\mu^{\omega-1}(N+g))$, by [2, Lemma V.12]. The evaluation at Line 7 costs $\tilde{\mathcal{O}}(\mu N + \delta_G(R) + \deg(G))$, by [2, Lemma V.2]; our assumption on $\deg(E)$ implies that this is in $\tilde{\mathcal{O}}(\mu N)$.

The costly part of the computation of $\boldsymbol{D}$ at Lines 10 to 14 is the matrix products at Line 13. For each $t = 1, \ldots, s-1$, we start from $\boldsymbol{D}_t$ which has degree in $\mathcal{O}(s(n+g)/\mu)$ (see Lemma 3.6), and then we multiply iteratively for $j = t-1, \ldots, 0$ by $\boldsymbol{R}_j$ whose degree is in $\mathcal{O}((n+g)/\mu)$ (see Lemma 3.10). Thus, altogether we perform about $\frac{s^2}{2}$ multiplications of two $\mu \times \mu$ matrices of degree in $\mathcal{O}(s(n+g)/\mu)$, for a total cost of $\tilde{\mathcal{O}}(s^3\mu^{\omega-1}(n+g))$.

The costly part of the computation of $\bar{\boldsymbol{R}}$ at Lines 15 to 20 is the matrix products and matrix remainders at both Lines 18 and 19. Consider a fixed iteration j, for some $j \in \{0, \ldots, s-1\}$. The above recalled bound on $\deg(\boldsymbol{R}_t)$ ensures that the product $\boldsymbol{R}_s\boldsymbol{R}_{s-1}\cdots\boldsymbol{R}_{j+1}$ at Line 18 can be computed in $\tilde{\mathcal{O}}(s^2\mu^{\omega-1}(n+g))$, and has degree in $\mathcal{O}(s(n+g)/\mu)$. Then, since $\deg(\boldsymbol{E}_j)$ is in $\mathcal{O}(s(n+g)/\mu)$ as well (see Lemma 3.8), the matrix division with remainder at the same line costs $\tilde{\mathcal{O}}(s\mu^{\omega-1}(n+g))$ and returns a matrix whose degree is in $\mathcal{O}(s(n+g)/\mu)$ (see Lemma 2.7). At Line 19 there are $\leq \ell$ iterations, and similarly to Line 18, each of them performs a matrix product and then a matrix division with remainder which both cost $\tilde{\mathcal{O}}(s\mu^{\omega-1}(n+g))$, for a total of $\tilde{\mathcal{O}}(s\ell\mu^{\omega-1}(n+g))$. Note that degrees remain controlled since each of these iterations produces a matrix remainder whose degree is less than $\deg(\boldsymbol{E}_j)$, which is in $\mathcal{O}(s(n+g)/\mu)$. Summing over the iterations for $j = 0, \ldots, s-1$, and using $s \leq \ell$, we get a cost bound of $\tilde{\mathcal{O}}(s^2\ell\mu^{\omega-1}(n+g))$ operations in $\mathbb{F}_q$ for Lines 15 to 20.

Finally, summing the costs of each analyzed part above yields the result. □

5 Decoder with better complexity

5.1 The decoding algorithm

The overall decoding algorithm is the one in [2, Algorithm 7] with the first three lines replaced by a call to InterpolantPolMatBasis, which provides $\boldsymbol{P}_{s,\ell,\boldsymbol{r}}$ in complexity $\tilde{\mathcal{O}}(s^2\ell\mu^{\omega-1}(n+g))$ according to Theorem 4.9; indeed one can take $N \in \mathcal{O}(sn+g+\mu) \subset \mathcal{O}(s(n+g))$. After that, two expensive computations remain. The first one asks to find the shifted Popov form of $\boldsymbol{P}_{s,\ell,\boldsymbol{r}}$ [2, Algorithm 7, Line 5], which costs $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g)+\ell^\omega\mu^\omega)$ operations in $\mathbb{F}_q$ according to Theorem 3.15. The second one is the root finding step [2, Algorithm 7, Line 10], whose complexity is in $\tilde{\mathcal{O}}(s\ell\mu^{\omega-1}(n+g))$ as detailed in Section 5.2. Hence the overall cost bound $\tilde{\mathcal{O}}(s^2\ell^{\omega-1}\mu^{\omega-1}(n+g)+\ell^\omega\mu^\omega)$ for the list decoder.

Due to the modification of the first steps, the precomputed data slightly differs from the one listed in [2, Section VI]. Here, we do not need to know the evaluations of $\mathcal{R}$-module generators for $\mathcal{R}(G_t)$, $t = 0, \ldots, \ell$, denoted by "$\boldsymbol{g}$" in the above reference. As a kind of replacement, we need the evaluations $\boldsymbol{y}^{(G_t)}$ and $\boldsymbol{y}^{(H_t)}$ for $t = 0, \ldots, s-1$ and $\boldsymbol{y}^{(-tG)}$ for $t = 0, \ldots, \ell$, as defined in the input of InterpolantPolMatBasis. Observe that this algorithm also requires $\boldsymbol{y}^{(-tG)}$ for $t = -1$; but $\boldsymbol{y}^{(G)}$ is already part of the precomputation in [2, Section VI]

(denoted by $\boldsymbol{y}$). Except for "$\boldsymbol{g}$", the rest of the precomputed data listed in [2, Section VI] is kept as such.

5.2 The root finding step

In [2], an algorithm is given that finds all roots of the found polynomial $Q(z) \in \mathcal{M}_{s,\ell,\boldsymbol{r}}$ in complexity $\tilde{\mathcal{O}}(\ell^2\mu^{\omega-1}(n+g))$. The term ℓ^2 is at odds with our target complexity. Fortunately, a slightly better complexity analysis shows that [2, Algorithm 6] actually has complexity $\tilde{\mathcal{O}}(s\ell\mu^{\omega-1}(n+g))$. More precisely, in the proof of [2, Proposition V.33], the ℓ^2 term comes from the estimates $\tilde{\mathcal{O}}(\mu\ell\beta) \subseteq \tilde{\mathcal{O}}(\ell^2\mu(n+g))$ and $\tilde{\mathcal{O}}(\beta \deg_z(\hat{Q})) \subseteq \tilde{\mathcal{O}}(\ell^2(n+g))$, where β is chosen such that $\beta \geq 2\ell \deg(G) + s(n-\tau)$ and where $\deg_z(\hat{Q}) = \ell$. In [2] the estimate $\deg(G) \in \mathcal{O}(n+g)$ is used to show the mentioned inclusions. A third part of the complexity analysis of [2, Algorithm 6] adds a term $\tilde{\mathcal{O}}(\ell\mu^{\omega-1}(n+g))$, yielding as total complexity the mentioned $\tilde{\mathcal{O}}(\ell^2\mu^{\omega-1}(n+g))$.

However, the root finding has as input a polynomial $Q \in \mathcal{M}_{s,\ell,\boldsymbol{r}}$ satisfying $\delta_G(Q) < s(n-\tau)$. In particular $\delta_{-\ell G}(Q_\ell) < s(n-\tau)$, which implies that $Q_\ell \in \mathcal{L}(-\ell G + sP_\infty)$. This implies that either $-\ell \deg(G) + sn \geq 0$, or $Q_\ell = 0$ in all cases. In the latter case one might as well have started the decoding algorithm for a smaller value of designed list size ℓ. We may conclude that without loss of generality one can assume $\ell \deg(G) \leq sn$. This implies that $\beta \in \mathcal{O}(sn)$ and therefore $\tilde{\mathcal{O}}(\mu\ell\beta) \subseteq \tilde{\mathcal{O}}(s\ell\mu n)$ and $\tilde{\mathcal{O}}(\beta \deg_z(\hat{Q})) \subseteq \tilde{\mathcal{O}}(s\ell n)$. Leaving the remaining part of the complexity analysis exactly the same as in the proof of [2, Proposition V.33], we see that the root finding part can be handled using [2, Algorithm 6] in complexity $\tilde{\mathcal{O}}(s\ell\mu^{\omega-1}(n+g))$.

Acknowledgments

The first author would like to acknowledge the support from The Danish Council for Independent Research (DFF-FNU) for the project *Correcting on a Curve*, Grant No. 8021-00030B. The second author would like to acknowledge the support from Sorbonne Université's Faculty of Science and Engineering through the project *Tremplin 2022: Fast reconstruction of multivariate algebraic relations*; from the Agence nationale de la recherche (ANR), grant agreement ANR-19-CE40-0018 De Rerum Natura; from the ANR&Austrian Science Fund FWF, grant agreements ANR-22-CE91-0007 EAGLES and ANR-19-CE48-0015 ECARP; and from the EOARD-AFOSR, grant agreement FA8665-20-1-7029.

References

[1] B. Beckermann, G. Labahn, and G. Villard. Normal forms for general polynomial matrices. *Journal of Symbolic Computation*, 41(6):708–737, June 2006.

[2] P. Beelen, J. Rosenkilde, and G. Solomatov. Fast decoding of AG codes. *IEEE Transactions on Information Theory*, 2022.

[3] E. Berardini, A. Couvreur, and G. Lecerf. A proof of the Brill-Noether method from scratch. Submitted, 2022.

[4] M. Chowdhury, C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Faster Algorithms for Multivariate Interpolation With Multiplicities and Simultaneous Polynomial Approximations. *IEEE Transactions on Information Theory*, 61(5):2370–2387, May 2015.

[5] P. Giorgi, C. Jeannerod, and G. Villard. On the Complexity of Polynomial Matrix Computations. In *International Symposium on Symbolic and Algebraic Computation*, pages 135–142, 2003.

[6] S. Gupta, S. Sarkar, A. Storjohann, and J. Valeriote. Triangular x-basis decompositions and derandomization of linear algebra algorithms over. *Journal of Symbolic Computation*, 47(4):422–453, Apr. 2012.

[7] V. Guruswami and M. Sudan. Improved Decoding of Reed–Solomon Codes and Algebraic-Geometric Codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[8] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[9] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. Computing minimal interpolation bases. *Journal of Symbolic Computation*, 83:272–314, Nov. 2017.

[10] T. Kailath. *Linear Systems*. Prentice-Hall, 1980.

[11] K. Lee. Base field extension of AG codes for decoding. *IEEE Transactions on Information Theory*, 68(6):3740–3743, 2022.

[12] K. Lee, M. Bras-Amoros, and M. O'Sullivan. Unique Decoding of General AG Codes. *IEEE Transactions on Information Theory*, 60(4):2038–2053, Apr. 2014.

[13] V. Neiger. *Bases of relations in one or several variables: fast algorithms and applications*. PhD Thesis, ENS Lyon, Nov. 2016.

[14] V. Neiger and T. X. Vu. Computing Canonical Bases of Modules of Univariate Relations. In *International Symposium on Symbolic and Algebraic Computation*, page 8, July 2017.

[15] J. Nielsen and P. Beelen. Sub-Quadratic Decoding of One-Point Hermitian Codes. *IEEE Transactions on Information Theory*, 61(6):3225–3240, June 2015.

[16] S. Sarkar and A. Storjohann. Normalization of Row Reduced Matrices. In *International Symposium on Symbolic and Algebraic Computation*, pages 297–304, New York, NY, USA, 2011. ACM.

[17] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer, 2nd edition, 2009.