Abstract

Index Terms: Algebraic geometry codes, Berlekamp-Massey algorithm, Sakata algorithm, majority voting.

The Berlekamp-Massey-Sakata algorithm is generalized to a broad class of rings which includes polynomial rings over a field and the rings used for one-point codes. The key concept for the generalization is the existence of an order function, a map from the ring to the nonnegative integers which determines a filtration of the ring with one-dimensional quotients. The Feng-Rao majority voting technique for computing unknown syndromes is incorporated into the algorithm. We also derive an improved bound for decoding based on the geometry of the error locations rather than the total number of errors.

A Generalization of the Berlekamp-Massey-Sakata Algorithm

Michael E. O'Sullivan

June 15, 2001

Introduction

The Berlekamp-Massey algorithm was invented roughly 30 years ago to be used for decoding BCH and Reed-Solomon codes. It is a computationally efficient algorithm that is well-suited to implementation in VLSI circuitry. The algorithm first computes an "error locator" polynomial and an "error evaluator" polynomial. Then the locations of the errors are the zeros of the locator polynomial and the error values may be computed using the evaluator polynomial and the derivative of the locator polynomial.

Sakata [13] generalized the error location part of the Berlekamp-Massey algorithm to polynomial rings in n variables over a field. Sakata's algorithm produces a set of error locators which are simply a Gröbner basis for the ideal of nonzero positions in the error vector being decoded. Since the ideal of a set of points is not principal if $n \neq 1$, there are several error locators. Sakata's algorithm has been used to decode one-point codes [6]. These are codes defined using the ring R of functions on a smooth curve X over a finite field k (with k algebraically closed in R) which have poles only at a rational point Q. That is $R = \cup L(mQ)$. Since this curve may be embedded in some projective space with the point Q being the sole point at infinity, R can be considered a quotient of a polynomial ring over k. Thus Sakata's algorithm can be used to calculate an ideal in R via the preimage of the ideal in the polynomial ring.

The original utilization of Sakata's algorithm to decode one-point codes was unable to decode up to half the minimum distance of the code. In [4], Feng and Rao introduced a new lower bound on the minimum distance of an algebraic geometry code which could be larger than the designed distance of the code (from the Riemann-Roch theorem). They developed a decoding algorithm which used "majority voting"for unknown syndromes that allowed the algorithm to correct up to half of their bound. In [14, 15, 8], Sakata's algorithm and the Feng-Rao majority voting technique are brought together in a single efficient algorithm.

Sakata's algorithm and the majority voting technique can be extended to any ordered domain. Ordered domains and the decoding algorithm are presented in [7] and examples of ordered domains are given in [10]. In this article we cover much of the same material as in [7], with a few new approaches. We also give a more precise formulation of the correction capability of the algorithm than has appeared previously. Section 1 defines an order function and gives basic properties, it is a slight revision of [10, §1]. Section 2 presents the syndrome map defined by a vector and develops the results needed to establish the decoding algorithm. Section 3 gives the iterative algorithm for computing a Gröbner basis for the error locator ideal from the syndrome map. Section 4 discusses majority voting and the error correction capabilities of the algorithm. Section 5 gives some examples of decoding beyond the minimum distance of a code.

I would like to acknowledge the help of Maria Bras Amoros in working out some of the examples. Her careful reading of the manuscript also led to significant improvements in the exposition.

1 Order Functions and Gröbner Bases

In this section we will generalize the notion of monomial orderings and Gröbner bases to a broader class of rings than polynomial rings. We do this by defining an order function on an integral domain over a field. Order functions can be defined much more generally (see Bourbaki [1, III §2]) but the following definition is simple and appropriate for our purposes.

We will use $\mathbb{N}$ for the positive integers, $\mathbb{N}_0$ for the nonnegative integers and $\mathbb{N}_{-1}$ for the integers greater than or equal to -1.

Definition 1.1. Let R be a ring over a field k. An order function on R is a map

$$o : R \longrightarrow \mathbb{N}_{-1}$$

which satisfies the following.

O1. The set $L_a = \{r \in R \text{ such that } o(r) \leq a\}$ is an $a+1$ dimensional vector space over k.

O2. If $f, g, z \in R$ and z is nonzero then $o(f) > o(g) \Longrightarrow o(zf) > o(zg)$

Clearly $L_{-1} = \{0\}$. It is also easy to see that $L_0 = k$. Suppose, on the contrary, that $o(1) > 0$, and let $o(f) = 0$. Then, by **O2**, $o(1) > o(f) > o(f^2) > o(f^3) > \cdots$. This would give an infinite number of values less than $o(1)$ for the order function, which is impossible.

Proposition 1.2. *Let R be a ring over a field k with order function o. Then*

1. *R is an integral domain.*
2. *The only units in R are the nonzero elements of k.*
3. *Given any $f, g \in R \setminus k$, there exists an integer n such that $o(f^n) > o(g)$.*

Proof: If $f \neq 0$ then $o(f) > o(0) = -1$. For any nonzero z we have $o(fz) > o(0)$ by **O2**. So $fz \neq 0$ and R must be an integral domain. If $f \in R \setminus k$ then $o(f) > o(1) = 0$. For any nonzero z we have $o(fz) > o(z) \geq 0$ by **O2**. So $fz \neq 1$ and R can have no units except the elements of k.

For the final item, we have $0 = o(1) < o(f)$ and multiplying by powers of f we get $1 < o(f) < o(f^2) < \cdots < o(f^n)$, so $o(f^n) \geq n$. Choose $n > o(g)$. □

We will say that the pair R, o is an ordered domain. Numerous examples of ordered domains are given in [10].

Example 1.2.1. The degree function on a polynomial ring $k[x]$ is an order function. Monomial orderings on a polynomial ring $k[x_1, \ldots, x_n]$ give rise to an order function, provided that no monomial is larger than all the powers of some x_i. A common ordering to use is the lexicographic total degree ordering. On $k[x, y]$ this is given by $o(x^i y^j) < o(x^m y^n)$ if $i + j < m + n$ or if $i + j = m + n$ and $j < n$. Thus the monomials are in the order $1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^4, \ldots$. The order function is $o(1) = 0, o(x) = 1, o(y) = 2, o(x^2) = 3, \ldots$. The order of any polynomial is given by the order of its leading term.

The other monomial orderings on $k[x, y]$ that give order functions are similar to the above, but with $o(x^i y^j) < o(x^m y^n)$ if $i + \tau j < m + \tau n$ or if $i + \tau j = m + \tau n$ and $j < n$ (or alternatively $i < n$) [12].

The following two propositions give some basic properties of the order function.

Proposition 1.3. *Let R be a ring over a field k. Suppose there is a function*

$$o : R \longrightarrow \mathbb{N}_{-1}$$

Then condition **O1** *in the definition of order function is equivalent to*

1. *o is surjective,*
2. *$o(a) = -1$ if and only if $a = 0$,*
3. *$o(\lambda f) = o(f)$ for all $\lambda \in k^\star$ and all $f \in R$,*
4. *$o(f + g) \leq \max(o(f), o(g))$ for all $f, g \in R$, and*
5. *If f and g are nonzero and $o(f) = o(g)$, then there exists a unique $\lambda \in k^\star$ such that $o(f + \lambda g) < o(g)$.*

Proof: Let $L_a = \{f \in R : o(f) \leq a\}$. It is clear that condition **O1** implies the first four items above because the L_a are vector spaces of strictly increasing dimension and the dimension is 0 when $a = -1$. If f and g both have order a, then, since L_a/L_{a-1} is one dimensional, we can find a unique $\lambda \in k^\star$ such that $f - \lambda g \in L_{a-1}$, which gives item 5) above.

For the converse, items 3) and 4) imply that L_a is a vector space and 1) and 5) imply that the codimension of L_{a-1} in L_a is one. Since $L_{-1} = \{0\}$ the dimension of L_a is $a+1$. $\square$

Remark 1.3.1. In [7], an order function is defined differently. They define $\rho : R \to \mathbb{N}_0 \cup \{\infty\}$ satisfying condition **O2** and items 2), 3), 4) and 5) of the proposition with the minor modification in 2) that $o(a) = -\infty \iff a = 0$. Their order function is not necessarily surjective. Given ρ satisfying their definition, there is a unique o satisfying the one here. Just define a function $g : \mathbb{N}_0 \cup \{-\infty\} \to \mathbb{N}_{-1}$ by $g(-\infty) = -1$ and $g(n) = \dim\{f \in R : o(f) \leq n\} - 1$. Then set $o(f) = g(\rho(f))$.

Proposition 1.4. *Let R, o be an ordered domain over a field k. Let $f, g, z \in R$.*

1. *If $f \notin k$ then $o(fz) > o(z)$.*

2. *If $o(f) > o(g)$ then $o(f+g) = o(f)$*

3. *If $o(fz) = o(gz)$ for some $z \in R$ then $o(fz) = o(gz)$ for all $z \in R$*

4. *If $o(fz) > o(gz)$ for some $z \in R$ then $o(fz) > o(gz)$ for all $z \in R$*

PROOF: The first item is just condition **O2** with $g = 1$, using the fact that $L_0 = k$. For the second, let $o(f) = s$. If $o(g) < s$, then f and $f + g$ are equivalent in L_s/L_{s-1}, so $o(f + g) = s$.

If $o(f) = o(g) = s$, the previous proposition says that there is a $\lambda \in k^\star$ such that $o(f) > o(f + \lambda g)$. Then, for an arbitrary nonzero $z \in R$, $o(fz) > o(fz + \lambda gz)$. Applying item 2), $o(gz) = o(fz - (fz + \lambda gz)) = o(fz)$. Similarly, one has by **O2** $o(f) < o(g)$ implies $o(fz) < o(gz)$. Thus the relation between $o(f)$ and $o(g)$, ($<$,$>$, or $=$) is the same as the relation between $o(fz)$ and $o(gz)$. This proves the final two items. $\square$

Using the order function we can define a Gröbner basis for an ideal. First we need to define a partial ordering and a binary operation on $\mathbb{N}_0$. By the proposition, if f and f' have the same order then $o(fg) = o(f'g)$ for all $g \in R$. Thus if $a, b \in \mathbb{N}_0$, there is a well defined $c \in \mathbb{N}_0$ such that $o(fg) = c$ whenever $o(f) = a$ and $o(g) = b$. Furthermore, if $o(fg) = o(fg')$ and $f \neq 0$ then $o(g) = o(g')$. Thus we can make the following definitions.

Definition 1.5. Let R, o be an ordered domain over a field k. We define a binary operation $\oplus$ on $\mathbb{N}_0 \times \mathbb{N}_0$ by

$$a \oplus b = c \text{ if } o(fg) = c \text{ when } o(f) = a \text{ and } o(g) = b$$

We also define a relation, $\preccurlyeq$ by

$$a \preccurlyeq c \text{ if } \exists b \in \mathbb{N}_0 \text{ such that } a \oplus b = c$$

If $b \neq 0$, we say $a \prec c$. If $a \preccurlyeq c$ there is exactly one b such that $a \oplus b = c$ by the remarks above. In this case we also define $c \ominus a = b$.

The following results are easy consequences of Proposition 1.4.

Proposition 1.6. *Let R, o be an ordered domain over a field k. Let $\prec$, $\oplus$, $\ominus$ be as described above. Let $a, b, c \in \mathbb{N}_0$.*

1. *$\oplus$ is commutative and associative and 0 is an identity.*

2. *If $a \oplus c \prec b \oplus c$ for some c then $a \oplus c \prec b \oplus c$ for all c.*

3. *If $c \ominus a \succ b$ then $c \ominus b \succ a$.*

4. *If $b \succcurlyeq c$ then $(a \oplus b) \ominus c = a \oplus (b \ominus c)$.*

5. *If $c \succcurlyeq a \oplus b$ then $c \ominus (a \oplus b) = (c \ominus a) \ominus b$.*

6. *If $a \prec b$ then $a < b$.*

7. *If $a < b$ then $a \oplus c < b \oplus c$.*

The first item simply says that $(\mathbb{N}_0, \oplus)$ is a commutative monoid. Our definition of $\ominus$ is based on the cancellation law applying in this monoid. the items 2)-5) are consequences of the cancellation law. Item 7) says that $(\mathbb{N}_0, \oplus)$ is totally ordered by $<$ and item 6) may be derived as a consequence (Set $b = a \oplus c$ with $0 < c$. Then add a and use 7)).

We remark that Pelikaan, Hoholdt, and van Lint call a monoid with the cancellation law a semigroup (perhaps after Bourbaki) though in many algebra texts a semigroup satisfies fewer axioms than a monoid—it may not have an identity element.

Definition 1.7. Let $A \subset \mathbb{N}_0$. We define the set of minimal elements in A with respect to $\prec$ to be

$$\min_{\prec} A = \{a \in A : \nexists a' \in A \text{ with } a' \prec a\}$$

Similarly, if A is finite, we define the maximal set with respect to $\prec$,

$$\max_{\prec} A = \{a \in A : \nexists a' \in A \text{ with } a \prec a'\}$$

Lemma 1.8. *Let $A \subset \mathbb{N}_0$. For every $b \in A$ there is some $a \in \min_{\prec} A$ such that $a \preccurlyeq b$. If A is finite then for every $b \in A$ there is some $a \in \max_{\prec} A$ such that $a \succcurlyeq b$.*

PROOF: For $b \in A$ consider the set $A_{\preccurlyeq b} = \{a \in A : a \preccurlyeq b\}$. It is contained in $\{0, 1, \ldots, b\}$, is therefore finite, and so it has a least element a relative to $\preccurlyeq$. Then $a \preccurlyeq b$ and I claim $a \in \min_{\prec} A$. Suppose on the contrary that $a' \prec a$ and $a' \in A$. Then $a' < a$, but on the other hand, $a' \in A_{\preccurlyeq b}$ so that $a' \geq a$, a contradiction.

If A is finite, then for any $b \in A$ the set $A_{\succcurlyeq b}$ is finite and therefore has a greatest element a (relative to $<$). Arguing as above we can show $a \in \max_{\prec} A$. □

Proposition 1.9. *Let R, o be an ordered domain over a field k. Let I be an ideal of R and let*

$$\Sigma = \{s \in \mathbb{N}_0 : \exists f \in I \textit{ with } o(f) = s\} \tag{1}$$

$$\sigma = \min_{\prec} \Sigma \tag{2}$$

$$\Delta = \mathbb{N}_0 \setminus \Sigma \tag{3}$$

Let $F : \sigma \longrightarrow I$ be such that $o(F(s)) = s$. Then

1. *If $a \in \mathbb{N}_0$, and $s \in \Sigma$, then $a \oplus s \in \Sigma$.*
2. *The set $\{F(s) : s \in \sigma\}$ generates I.*
3. *Any $g \in R$ is equivalent modulo I to some $g' \in R$ such that $o(g') \notin \Sigma$.*
4. *If R/I is finite dimensional over k then $\dim_k R/I = \#(\Delta)$*

PROOF: For the first statement, let $a \in \mathbb{N}_0$ and $s \in \Sigma$ and choose $z \in R$ and $f \in I$ with $o(z) = a$ and $o(f) = s$. Then since $fz \in I$, $a \oplus s \in \Sigma$.

Now let $g \in R$, we will show that g may be reduced modulo the ideal generated by $F(\sigma)$ to some $g' \in R$ with $o(g') \notin \Sigma$. If $o(g) \in \Sigma$, then by the Lemma, there are $s \in \sigma$ and $a \in \mathbb{N}_0$ be such that $s \oplus a = o(g)$. Let $z \in R$ have order a. Then $o(F(s)z) = o(g)$ so there is some $\lambda \in k^\star$ such that $g_1 = g - \lambda F(s)z$ satisfies $o(g_1) < o(g)$. Thus g is equivalent, modulo $F(\sigma)$, to an element of smaller order. After a finite number of similar steps, we reduce to some g_r such that $o(g_r) \notin \Sigma$. This proves item 3). If $g \in I$ then g_r is also, so it must be zero. Thus $F(\sigma)$ generates I. If R/I is finite dimensional then any set $\{g_i : o(g_i) = i \text{ and } i \in \mathbb{N}_0 \setminus \Sigma\}$ is a set of representatives for R/I, which gives item 4). □

Definition 1.10. The set of functions $F(\sigma)$ in the proposition is called a *Gröbner basis* for I.

Proposition 1.11. *Let R, o be an ordered domain over a field k. Let $\{z_i\}_{i=0}^{\infty}$ be a basis for R over k such that $o(z_i) = i$. Then, in the previous proposition, there is a unique mapping F such that $F(s) - z_s$ written as a linear combination of the z_i has only terms with $i \notin \Sigma$.*

PROOF: Uniqueness is immediate because if F and F' both satisfy the proposition then $F(s) - F'(s) \in I$ but $o(F(s) - F'(s)) \notin \Sigma$. Therefore $F(s) - F'(s) = 0$.

Let F satisfy the previous proposition; we will create F' satisfying this one. Let $f_s = F(s)$. We use finite induction to create a sequence of functions g_i for $i = s, s-1, \ldots, 0$, all of order s, such that the coefficient of z_j in $g_i - z_s$ is zero when $j \geq i$ and $j \in \Sigma$. Then $g_0 - z_s$ written as a linear combination of the z_i has only terms with $z_i \notin \Sigma$, so we define $F'(s) = g_0$. Applying this algorithm for each $s \in \sigma$ gives the result.

The inductive step is to let $g_i = g_{i+1} - h$ with h defined as follows. If $i \notin \Sigma$ then $h = 0$. If $i \in \Sigma$, let $s' \in \sigma$ and $c \in \mathbb{N}_0$ be such that $s' \oplus c = i$. Let α be the coefficient of z_i in g_{i+1}, and let $\lambda \in k$ be such that $o(\alpha z_i - \lambda z_c F(s')) < i$. Then $h = \lambda z_c F(s')$. □

Definition 1.12. The set of functions $F(\sigma)$ in Proposition 1.11 is called a *reduced Gröbner basis* for I with respect to $\{z_i\}$.

2 Codes and the Syndrome Map

Throughout the rest of this article, R, o is an order domain over a field k. Let $P_1, \ldots, P_n$ be rational points of the variety defined by R. Each P_i corresponds to a maximal ideal $\mathfrak{m}_i$ of R and $R/\mathfrak{m}_i \cong k$. Define the evaluation map

$$\begin{aligned} R &\xrightarrow{ev} k^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)) \end{aligned} \tag{4}$$

For each $m \in \mathbb{N}_{-1}$, we get a code by restricting the evaluation map to L_m. Let $C_m = ev(L_m)$ and let $C_m^{\perp}$ be the subspace of k^n orthogonal to C_m. We will use C_m as the decoding code and $C_m^{\perp}$ as the encoding code. We will only discuss decoding in this article.

Definition 2.1. Given a vector $\mathbf{e} = (e_1, \ldots, e_n) \in k^n$, let $D_{\mathbf{e}}$ be the set of points P_k such that $e_k \neq 0$, let $\operatorname{wt}\mathbf{e}$ be the number of nonzero components of $\mathbf{e}$, and let $I_{\mathbf{e}} \subset R$ be the ideal of functions vanishing on $D_{\mathbf{e}}$. Throughout the rest of the paper we will use the sets $\Sigma = \{o(f) : f \in I_{\mathbf{e}}\}$ and $\Delta = \mathbb{N}_0 \setminus \Sigma$ defined in Proposition 1.9 with the implicit understanding that they depend on the vector $\mathbf{e}$. Since $I_{\mathbf{e}}$ is the ideal of a finite set of points, $\dim R/I_{\mathbf{e}}$ is finite and by Proposition 1.9, $\#(\Delta) = \dim R/I_{\mathbf{e}} = \operatorname{wt} \mathbf{e}$. As in [5], we call Δ the *footprint* of $\mathbf{e}$.

The *syndrome map* defined by $\mathbf{e}$ is

$$\begin{aligned} S_{\mathbf{e}} : R &\longrightarrow k \\ f &\longmapsto e \cdot ev(f) = \sum_{k=1}^{n} e_k f(P_k) \end{aligned}$$

In the decoding algorithm, $\mathbf{e}$ will be the error vector, so we will also call $D_{\mathbf{e}}$ the *error set* and $I_{\mathbf{e}}$ the *error ideal.* An $f \in I_{\mathbf{e}}$ is called a *locator*, since it vanishes at all the error locations.

The decoding problem may be formulated as follows: Using the restriction of the map $S_{\mathbf{e}}$ to one of the spaces L_a, find the vector $\mathbf{e}$. In a practical situation, a vector $\mathbf{v} \in C_a^{\perp}$ is sent, an error vector $\mathbf{e}$ occurs in transmission, and the vector $\mathbf{v}+\mathbf{e}$ is received. The syndrome maps $S_{\mathbf{e}}$ and $S_{\mathbf{v}+\mathbf{e}}$ agree on L_a because for $\mathbf{v} \in C_a^{\perp}$ and $f \in L_a$,

$$\begin{aligned} (\mathbf{v} + \mathbf{e}) \cdot ev(f) &= \mathbf{v} \cdot ev(f) + \mathbf{e} \cdot ev(f) \\ &= \mathbf{e} \cdot ev(f) \end{aligned}$$

Therefore, knowing $\mathbf{v} + \mathbf{e}$, the receiver can compute $S_{\mathbf{e}}|_{L_a}$. This knowledge is used to reconstruct $\mathbf{e}$.

The decoding problem is usually split into two parts:

1. Find the error locations.

2. Find the error values.

In this article, we will only be concerned with finding the error locations. More precisely, the algorithm to be presented uses the map $S_{\mathbf{e}}$ to find a Gröbner basis for the error ideal, $I_{\mathbf{e}}$.

Proposition 2.2. *Let $I_{\mathbf{e}}$ be the error ideal. Then $f \in I_{\mathbf{e}}$ if and only if $S_{\mathbf{e}}(fg) = 0$ for all $g \in R$.*

PROOF: If $f \in I_{\mathbf{e}}$, then whenever $e_k \neq 0$, $f(P_k) = 0$. Thus, for any $g \in R$, $S_{\mathbf{e}}(fg) = \sum_{k=1}^{n} e_k f(P_k) g(P_k) = 0$.

To prove the converse we simply need to show that for any r such that $P_r \in D_{\mathbf{e}}$, there is a function g that vanishes on all P_k for $k \neq r$ and does not vanish on P_r. Then $S_{\mathbf{e}}(fg) = e_r f(P_r) g(P_r)$ so if $S_{\mathbf{e}}(fg) = 0$, $f(P_r)$ must be 0. The function g exists since $\bigcap_{k \neq r} \mathfrak{m}_k \not\subset \mathfrak{m}_r$. □

Definition 2.3. Let $f \in R \setminus I_{\mathbf{e}}$. We define

$$\begin{aligned} \operatorname{span} f &= \min\{c : S_{\mathbf{e}}(fg) \neq 0 \text{ for some } g \in L_c\} \\ \operatorname{fail} f &= o(f) \oplus \operatorname{span} f \end{aligned}$$

For $f \in I_{\mathbf{e}}$ we set $\operatorname{span} f = \operatorname{fail} f = \infty$. We will also use the notation $\operatorname{sp}(f)$ and $\operatorname{fl}(f)$.

Remark 2.3.1. If $f \notin I_{\mathbf{e}}$ with $\operatorname{span} f = c$, and $h \in L_{c-1}$, then $S_{\mathbf{e}}(fh) = 0$ directly from the definition. On the other hand, if $o(h) = c$, then we can show that $S_{\mathbf{e}}(fh) \neq 0$. By definition there is some $g \in L_c$ such that $S_{\mathbf{e}}(fg) \neq 0$. By Proposition 1.3 there is some $\lambda \in k^\star$ such that $h + \lambda g = g'$ is in L_{c-1}. Then $0 = S_{\mathbf{e}}(fg') = S_{\mathbf{e}}(fh) + \lambda S_{\mathbf{e}}(fg)$, so $S_{\mathbf{e}}(fh) = -\lambda S_{\mathbf{e}}(fg) \neq 0$.

The observations made in the remark give us the following lemmas.

Lemma 2.4. *Suppose that $f \in R$ and that $o(f) = s$ and $\operatorname{sp}(f) = c$. Then every g of order c has span at most s and fail at most $s \oplus c$.*

Proof: From the remark, for any g such that $o(g) = c$, $S_{\mathbf{e}}(fg) \neq 0$. Thus $\operatorname{span} g \leq s$ and $\operatorname{fail} g \leq s \oplus c$. □

Lemma 2.5. *Suppose that f and f' both have span equal to c. Then there exists a $\lambda \in k^\star$ such that $\operatorname{span}(f + \lambda f') > c$.*

Proof: Let g have order c and let $\alpha = S_{\mathbf{e}}(fg)$ and $\alpha' = S_{\mathbf{e}}(f'g)$. These must both be nonzero. Let $\lambda = -\alpha/\alpha'$. Then $\operatorname{span} f + \lambda f'$ is at least c and $S_{\mathbf{e}}((f + \lambda f')g) = 0$. The remark tells us that $\operatorname{span}(f + \lambda f') > c$. □

As a consequence of Lemma 2.4 we have

$$\{\operatorname{span} f : f \notin I_{\mathbf{e}}\} \subset \Delta$$

for if $c = \operatorname{span} f$ there can be no locator of order c. We will show in a moment that these two sets are equal.

Suppose that $s \in \Delta$. By definition there is no locator of order s. Consider $\{\operatorname{span} f : o(f) = s\}$. Since this is contained in Δ, which is a finite set, it has a maximal element. Therefore we can make the following definition.

Definition 2.6. For $s \in \Delta$ let

$$\begin{aligned} \operatorname{sp}(s) &= \max\{\operatorname{sp}(f) : o(f) = s\} \\ \operatorname{fl}(s) &= s \oplus \operatorname{sp}(s) \end{aligned}$$

Proposition 2.7. *The map $\operatorname{sp} : \Delta \to \Delta$ is injective.*

Proof: Suppose $s > s'$ are elements of Δ such that $\operatorname{sp}(s) = \operatorname{sp}(s') = c$. Let f, f' have orders s, s' respectively with both having span c. Then by Lemma 2.5 there exists a λ such that $\operatorname{sp}(f + \lambda f') > c$. But $o(f + \lambda f') = s$ so we have a contradiction to $\operatorname{sp}(s) = c$. Therefore it is not possible to have distinct elements of Δ with the same span. □

Proposition 2.8. *For all $s \in \Delta$, $\operatorname{sp}(\operatorname{sp}(s)) = s$.*

Proof: Since sp is injective, so is the composition $\operatorname{sp} \circ \operatorname{sp}$. By Lemma 2.4, $\operatorname{sp}(\operatorname{sp}(s)) \leq s$. Thus $\operatorname{sp} \circ \operatorname{sp}$ is an injective non-increasing function on a totally ordered (by $<$) finite set. It must therefore be the identity. This can be shown by induction.

Let a be the smallest element of Δ ($a = 0$ but we don't need this). Since $\operatorname{sp} \circ \operatorname{sp}$ is non-increasing, $\operatorname{sp} \circ \operatorname{sp}(a) = a$. Suppose now that $\operatorname{sp} \circ \operatorname{sp}$ is the identity for all $s' < s$. We have $\operatorname{sp} \circ \operatorname{sp}(s) \leq s$ but $\operatorname{sp} \circ \operatorname{sp}(s') = s'$ for all $s' < s$. By injectivity, $\operatorname{sp} \circ \operatorname{sp}(s) = s$. □

As an easy corollary we have that sp is surjective.

Corollary 2.9. *The map* $\mathrm{sp} : \Delta \to \Delta$ *is bijective. Thus,* $\Delta = \{\mathrm{sp}(f) : f \notin I_{\mathbf{e}}\}$. *For any* $s \in \Delta$, $\mathrm{fl}(\mathrm{sp}(s)) = \mathrm{fl}(s)$

PROOF: $\mathrm{fl}(\mathrm{sp}(s)) = \mathrm{sp}(s) \oplus \mathrm{sp}(\mathrm{sp}(s)) = \mathrm{sp}(s) \oplus s = \mathrm{fl}(s)$. □

Definition 2.10. Given an error vector $\mathbf{e}$, for each $m \in \mathbb{N}_{-1}$ we define

$$\begin{aligned} \Sigma_m &= \{s \in \mathbb{N}_0 : \exists f \in R \text{ with } o(f) = s \text{ and } \operatorname{fail} f > m\} \\ \sigma_m &= \min_{\prec} \Sigma_m \\ \Delta_m &= \mathbb{N}_0 \setminus \Sigma_m \\ \delta_m &= \max_{\prec} \Delta_m \end{aligned}$$

We remark that for all m, $\Sigma \subset \Sigma_m$ and for $m' < m$, $\Sigma_m \subset \Sigma_{m'}$. We also have $s \in \Sigma_m$ if and only if $\mathrm{fl}(s) > m$. By Corollary 2.9, this is equivalent to $\mathrm{fl}(\mathrm{sp}(s)) > m$. Thus $s \in \Sigma_m$ if and only if $\mathrm{sp}(s) \in \Sigma_m$.

The essential idea of the decoding algorithm is to converge on $I_{\mathbf{e}}$ using functions whose order is in σ_m and whose fail is larger than m. The initial step is when $m = -1$, in which case $\Sigma_{-1} = \mathbb{N}_0$ and $\Delta_{-1} = \emptyset$. The following results give some of the basic properties of Σ_m and show how the successive approximations Σ_m and Σ_{m-1} differ. First we show that if $s \in \sigma_m$ then $s \oplus a \in \Sigma_m$ for any $a \in \mathbb{N}_0$.

Proposition 2.11. *Let* $f \in R \setminus I_{\mathbf{e}}$ *and suppose that* $\operatorname{fail} f = m$. *Then* $\operatorname{fail} fz \geq m$ *for all* $z \in R$ *with equality if and only if* $o(fz) \prec m$. *Consequently,*

1. $\Sigma_m = \{t \in \mathbb{N}_0 : t \succcurlyeq s$ *for some* $s \in \sigma_m\}$
2. $\Delta_m = \{b \in \mathbb{N}_0 : b \preccurlyeq c$ *for some* $c \in \delta_m\}$

PROOF: Let $o(f) = s$ and $\operatorname{fail} f = m$. Let $z, g \in R$. By the definition of $\operatorname{fail} f$, if $s \oplus (o(z) \oplus o(g)) < m$, then $S_{\mathbf{e}}(fzg) = 0$, but if $s \oplus (o(z) \oplus o(g)) = m$, $S_{\mathbf{e}}(fzg) \neq 0$. Since $\oplus$ is associative, this says that $\operatorname{fail} fz \geq m$ with equality if and only if there exists a c such that $(s \oplus o(z)) \oplus c = m$.

By Lemma 1.8, we know that $\Sigma_m \subset \{t \in \mathbb{N}_0 : t \succcurlyeq s$ for some $s \in \sigma_m\}$ For the reverse inclusion, suppose that $o(f) = s \in \sigma_m$ and $\mathrm{fl}(f) > m$. Then for any $a \in \mathbb{N}_0$, and $z \in R$ of order a, $\mathrm{fl}(fz) > m$ so $z \oplus a \in \Sigma_m$. Thus we have item 1).

By Lemma 1.8, since Δ_m is finite, $\Delta_m \subset \{b \in \mathbb{N}_0 : b \preccurlyeq c$ for some $c \in \delta_m\}$. Now suppose that $b \prec c$ for some $c \in \delta_m$, but $b \in \Sigma_m$. There exists an $s \in \sigma_m$ such that $b \succcurlyeq s$. Then $c \succcurlyeq s$ and by item 1), $c \in \Sigma_m$, a contradiction. □

Proposition 2.12. *For each* $m \in \mathbb{N}_0$, *the set* $W_m = \Delta_m \setminus \Delta_{m-1}$ *satisfies the following.*

1. $s \in W_m$ *if and only if* $m \ominus s \in W_m$.
2. $\min_{\prec} W_m = \sigma_{m-1} \setminus \sigma_m$.
3. $\max_{\prec} W_m = \{m \ominus s : s \in \sigma_{m-1} \setminus \sigma_m\}$.

PROOF: If $s \in \Delta_m \setminus \Delta_{m-1}$ then $\mathrm{fl}(s) = m$ and $\mathrm{sp}(s) = m \ominus s$. By Corollary 2.9, $\mathrm{fl}(m \ominus s) = m$ so $m \ominus s \in W_m$.

For item 2), note that if $s \in W_m$ and there is some $s' \in \Sigma_{m-1}$ with $s' \preccurlyeq s$ then $s' \in \Delta_m$ by Proposition 2.11, so $s' \in W_m$. Thus if s is minimal in W_m, s must be minimal in Σ_{m-1}. This gives $\min_\prec W_m = \sigma_{m-1} \setminus \sigma_m$.

For any $s, s' \in \mathbb{N}_0$, $s \preccurlyeq s'$ if and only if $m \ominus s \succcurlyeq m \ominus s'$ by Proposition 1.6. Therefore s is minimal in W_m if and only if $m \ominus s$ is maximal in $\{m \ominus s : s \in W_m\}$. But the latter set is W_m by item 1), so item 3) is proved. $\square$

The following corollary is needed for the updating step of the algorithm.

Corollary 2.13. *Let $t \in \sigma_m \setminus \sigma_{m-1}$. Then either $t \not\preccurlyeq m$ or $m \ominus t \in \Delta_{m-1}$.*

PROOF: By assumption $t = s \oplus a$ for a a *positive* integer and $s \in \sigma_{m-1}$. In fact, since $s \notin \sigma_m$, s, and also $m \ominus s$ are in the W_m of the proposition.

Now suppose that $m \succcurlyeq t$. Then $m \ominus s \succ m \ominus t$ and since $m \ominus s \in \Delta_m$, we have $m \ominus t \in \Delta_m$. Since $t \notin W_m$, $m \ominus t \notin W_m$. Thus $m \ominus t \in \Delta_m \setminus W_m = \Delta_{m-1}$. $\square$

The sets Δ_m grow with increasing m. The next proposition determines when $\Delta = \Delta_m$.

Proposition 2.14. *Let $c_{\max}$ be the largest integer in δ and let $M = c_{\max} \oplus c_{\max}$. Then for $m \geq M$, $\Sigma_m = \Sigma$ and $\Delta_m = \Delta$.*

PROOF: It is enough to show that $\Delta \subset \Delta_m$ since the reverse containment is clear and Δ_m and Σ_m partition $\mathbb{N}_0$. We noted earlier that for any m, $\Sigma_m = \{s : \mathrm{fl}(s) > m\}$, so $\Delta_M = \{s : \mathrm{fl}(s) \leq M\}$. Now, for any $s \in \Delta$, $\mathrm{fl}(s) = s \oplus \mathrm{sp}(s) \leq c_{\max} \oplus c_{\max} = M$. Thus $\Delta \subset \Delta_M$. $\square$

3 Computation of $I_{\mathbf{e}}$ from $S_{\mathbf{e}}$

The following algorithm will compute a Gröbner basis for the error ideal $I_{\mathbf{e}}$ after a finite number of steps. In the description of the algorithm, Σ_m is as defined in Definition 2.10. The algorithm produces sets σ_m and δ_m which we will prove in Theorem 3.1 also satsify that definition, i.e. $\sigma_m = \min_\prec \Sigma_m$ and $\delta_m = \max_\prec(\mathbb{N}_0 \setminus \Sigma_m)$.

Assumptions

- R, o is an ordered domain over a field k.
- $\{z_i\}$ is a basis of R over k such that $o(z_i z_j - z_k) < o(z_k)$ whenever $o(z_i z_j) = o(z_k)$.
- $P_1, \ldots, P_n$ are distinct rational points of the variety defined by R
- $\mathbf{e} \in k^n$, $D_{\mathbf{e}}$ is the set of points P_k such that $e_k \neq 0$, and $I_{\mathbf{e}}$ is the ideal of functions in R vanishing on $D_{\mathbf{e}}$.
- $\Sigma_m = \{s \in \mathbb{N}_0 : \exists f \in R \text{ with } o(f) = s, \mathrm{fail}\, f > m\}$

Data Structures Compute for each m:

$$\sigma_m \subset \mathbb{N}_0 \qquad\qquad F_m : \sigma_m \to R$$
$$\delta_m \subset \mathbb{N}_0 \qquad\qquad G_m : \delta_m \to R$$

Temporary Structures

$$\beta : \sigma_m \to k$$
$$\delta' \subset \mathbb{N}_0$$

Initialization

$$\sigma_{-1} = 0 \qquad\qquad F_{-1}(0) = 1$$
$$\delta_{-1} = \emptyset$$

Basic Algorithm For $m = 0$ to ∞,

1. For each $s \in \sigma_{m-1}$:
   If $s \preccurlyeq m$ calculate $\beta(s) = S_{\mathbf{e}}(F_{m-1}(s) z_{m \ominus s})$.
   If $\beta(s) \neq 0$, put $m \ominus s$ in δ'
2. Compute σ_m and δ_m:
$$\delta_m = \max_{\prec}(\delta' \cup \delta_{m-1})$$
$$\sigma_m = \min_{\prec}\{t \in \mathbb{N}_0 : t \not\succcurlyeq c \text{ for all } c \in \delta_m\}$$
3. For each $c \in \delta_m$:
$$G_m(c) = \begin{cases} G_{m-1}(c) & \text{if } c \in \delta_{m-1} \\ (\beta(m \ominus c))^{-1} F_{m-1}(m \ominus c) & \text{otherwise} \end{cases}$$
4. For each $t \in \sigma_m$:
   Find $s \in \sigma_{m-1}$ and $a \in \mathbb{N}_0$ such that $s \oplus a = t$.
   If $\exists c \in \delta_{m-1}$ and $b \in \mathbb{N}_0$ such that $m \ominus t = c \ominus b$,
$$F_m(t) = F_{m-1}(s) z_a - \beta(s) G_{m-1}(c) z_b$$
   Else
$$F_m(t) = F_{m-1}(s) z_a$$

Theorem 3.1. *The algorithm above computes a Gröbner basis for the ideal $I_{\mathbf{e}}$. For each m*

1. $\sigma_m = \min_{\prec} \Sigma_m$.

2. $\delta_m = \max_{\prec}(\mathbb{N}_0 \setminus \Sigma_m)$.

3. $o(F_m(s)) = s$ *and* $\operatorname{fail} F_m(s) > m$ *for each* $s \in \sigma_m$.

4. $\operatorname{span} G_m(c) = c$, $\operatorname{fail} G_m(c) \leq m$, *and* $S_{\mathbf{e}}(G_m(c) z_c) = 1$ *for each* $c \in \delta_m$.

Suppose that σ is finite with $s_{\max}$ the largest integer in σ. Let $c_{\max}$ be the largest integer in δ and let $M = c_{\max} \oplus \max\{c_{\max}, s_{\max}\}$. Then the computation is complete after M iterations.

PROOF: Suppose for a moment that items 1)-5) are true for all m. From Proposition 2.14, $\sigma_m = \sigma$ for all $m \geq c_{\max} \oplus c_{\max}$. Let $s \in \sigma$. Then for $m > s \oplus c_{\max}$, $\operatorname{span} F_m(s) > m \ominus s \geq c_{\max}$. This is possible only if $\operatorname{span} F_m(s)$ is infinite, that is, $F_m(s) \in I_{\mathbf{e}}$. Thus the algorithm does produce a Gröbner basis for $I_{\mathbf{e}}$ since for each $s \in \sigma$ it eventually produces a locator. If σ is finite then for $M = c_{\max} \oplus \max\{s_{\max}, c_{\max}\}$ we have both $\sigma_M = \sigma$ and for each $s \in \sigma$, $F_M(s)$ must be a locator.

We will prove items 1)-5) by induction. The initial step $m = -1$ is immediate from the initialization.

By construction, the set δ' contains the maximal elements of the set W_m of Proposition 2.12. From that proposition we also have that $\max_{\prec} \Delta_m$ is the maximal elements of $\delta_{m-1} \cup \delta'$, so the δ_m calculated in the algorithm is indeed $\max_{\prec} \Delta_m$. Now from Proposition 2.11, $\Sigma_m = \{t \in \mathbb{N}_0 : t \not\preccurlyeq c \text{ for some } c \in \delta_m\}$. Thus σ_m in the algorithm is $\min_{\prec} \Sigma_m$. This establishes items 1) and 2).

In Step 3, the algorithm simply assigns the correct data to G_m. If $c \in \delta_{m-1}$ then $\operatorname{span} G_{m-1}(c) = c$ and $\operatorname{fail} G_{m-1}(c) \leq m-1$ by the induction hypothesis. If $c \in \delta'$, then $c = m \ominus s$ for some $s \in \sigma_{m-1}$ such that $S_{\mathbf{e}}(F_{m-1}(s) z_{m \ominus s}) = \beta(s) \neq 0$. Thus $s = m \ominus c$ and $\operatorname{span} F_{m-1}(s)$ is c. Multiplying by $\beta(s)^{-1}$ doesn't change the span but gives $S_{\mathbf{e}}(\beta(s)^{-1} F_{m-1}(s) z_c) = 1$. This establishes items 4) and 5).

In Step 4 we compute F_m. If $t \in \sigma_m$ then there exists some $s \in \sigma_{m-1}$ and $a \in \mathbb{N}_0$ such that $s \oplus a = t$. We have three cases to consider.

Suppose $t \not\preccurlyeq m$. Then by Proposition 2.11, $\operatorname{fail} F_{m-1}(s) z_a > m$, so we set $F_m(t) = F_{m-1}(s) z_a$. Notice that $o(F_{m-1}(s) z_a) = s \oplus a = t$.

Suppose now that $t \preccurlyeq m$ and $t \notin \sigma_{m-1}$. Then by Corollary 2.13, $m \ominus t \in \Delta_{m-1}$ so there exist c and b as stated in the algorithm. Let $f = F_{m-1}(s)$ and $g = G_{m-1}(c)$. By Proposition 2.11, $\operatorname{sp} f z_a = m \ominus t = c \ominus b$ and $\operatorname{sp} g z_b = c \ominus b$. Because of the assumption on the basis $\{z_i\}$ we have $S_{\mathbf{e}}(f z_a z_{c \ominus b}) = \beta(s)$ and $S_{\mathbf{e}}(g z_b z_{c \ominus b}) = \alpha_{m-1}(c)$. So the linear combination in the algorithm has span larger than $c \ominus b$ and fail larger than m. Finally, we show that $o(F_m(t)) = t$. We have $o(g) \oplus c = \operatorname{fl}(g) = m' < m$ by the induction hypothesis. So $o(g z_b) \oplus c \leq m' \oplus b < m \oplus b = t \oplus c = o(f z_a) \oplus c$. Consequently, $o(g z_b) < o(f z_a)$ and therefore $o(F_m(t)) = o(f z_a) = t$.

Finally, suppose that $t \preccurlyeq m$ and $t \in \sigma_{m-1}$, so $t = s$. If $m \ominus s \in \Delta_{m-1}$, then there exist b, c as in the algorithm and the discussion in the preceeding paragraph applies. If $m \ominus s \in \Sigma_{m-1}$ then we must have $\operatorname{fl}(F_{m-1}(s)) > m$ for otherwise $m \ominus s$ and s are in Δ_m by Proposition 2.12. Thus $\beta(s) = 0$ and we may take $F_m(s) = F_{m-1}(s)$. □

There exist ordered domains where σ may not be finite. An example with $R = k[x, y]$ is given in [10].

4 Majority Voting

We now turn to the practical decoding situation. We use the code $C_{m^\star} = ev(L_{m^\star})$ for decoding, so we know the value of $S_{\mathbf{e}}$ only on the space $L_{m^\star}$. In this section we will compute a bound d_o on the minimum distance of $C_{m^\star}^\perp$, the *order bound*, and show that the decoding algorithm can decode up to half that bound. The known syndrome values are not enough for the task; using the algorithm of the previous section and proceeding only up to $m^\star$ typically does not ensure the computation of a Gröbner basis. We must incorporate a majority voting scheme due to Feng and Rao to compute $S_{\mathbf{e}}(z_m)$ for $m > m^\star$ up to the value M in Theorem 3.1 that guarantees the Gröbner basis. In fact, we will give a weaker condition than $\operatorname{wt} \mathbf{e} < d_o/2$ that guarantees that majority voting can proceed. Then for all vectors satisfying this weaker condition, the decoding algorithm is successful.

First we derive the order bound (also called the Feng-Rao bound) on the minimum distance. Then we define sets V_m and W_m which are used to vote for the syndrome $S_{\mathbf{e}}(z_m)$. If $\#V_m > \#W_m$ then the vote is succesful, so the decoding algorithm proceeds correctly. We next give conditions ensuring that $\#V_m > \#W_m$. We then amend the algorithm of the previous section to include majority voting. Finally, we consider the case of error vectors whose support is an independent set of points.

Definition 4.1. For $c \in \mathbb{N}_0$ define

$$\Lambda_{\preccurlyeq m} = \{c \in \mathbb{N}_0 : c \preccurlyeq m\}$$
$$\lambda_m = \#\Lambda_{\preccurlyeq m}$$

Proposition 4.2. *Suppose* $\mathbf{v} \in C_{m-1}^\perp$ *and* $\mathbf{v} \notin C_m^\perp$ *then* $\operatorname{wt} \mathbf{v} \geq \lambda_m$.

Proof: If $\mathbf{v} \in C_{m-1}^\perp \setminus C_m^\perp$ then $S_{\mathbf{v}}(f) = 0$ for all $f \in L_{m-1}$, but there is some g with $o(g) = m$ such that $S_{\mathbf{v}}(g) \neq 0$. Defining span, Δ and Δ_m relative to $\mathbf{v}$ we have that the span of the constant function 1 is m, and $m \in \Delta_m \subset \Delta$. By Proposition 2.11, every $c \preccurlyeq m$ is also in Δ_m. Thus $\Lambda_{\preccurlyeq m} \subset \Delta$ and $\lambda_m \leq \#\Delta = \operatorname{wt} \mathbf{v}$. □

Corollary 4.3. *Assume* $C_m^\perp$ *is a nontrivial code and let* $d(m)$ *be its minimum distance. Then* $d(m) \geq \min\{\lambda_{m'} : m' > m\}$.

Proof: For $\mathbf{v} \in C_m^\perp$ and $\mathbf{v} \neq 0$, let $m' = \min\{r : \mathbf{v} \notin C_r^\perp\}$. Then $m' > m$ and $\operatorname{wt} \mathbf{v} \geq \lambda_{m'}$ by the proposition. □

Definition 4.4. The *order bound* (or *Feng-Rao bound*) for the minimum distance of the code $C_m^\perp$ is $d_o(m) = \min\{\lambda_{m'} : m' > m\}$.

Let $\Gamma_m = \{s \in \Sigma_{m-1} : m \ominus s \in \Sigma_{m-1}\}$. Proposition 2.9 showed that $W_m = \Delta_m \setminus \Delta_{m-1}$ is contained in Γ_m. Let $V_m = \Gamma_m \setminus W_m$; these are the elements of Γ_m which are also in Σ_m. The next result gives a condition under which V_m is larger than W_m.

Proposition 4.5. *Let* $\mathbf{e}$ *be an error vector and let* m *be such that* $\lambda(m) > 2 \operatorname{wt} \mathbf{e}$. *Then* $\#V_m > \#W_m$.

PROOF: Since Δ has $\mathrm{wt}\,\mathbf{e}$ elements and Δ_{m-1} and W_m are disjoint subsets of Δ

$$\mathrm{wt}\,\mathbf{e} \geq \#\Delta_{m-1} + \#W_m$$

On the other hand we have the following partition of $\Lambda_{\preccurlyeq m}$,

$$V_m, W_m, \{s \in \Sigma_{m-1} : m \ominus s \in \Delta_{m-1}\}$$

and

$$\{c \in \Delta_{m-1} : m \ominus c \in \Lambda_{\preccurlyeq m}\}$$

the latter two sets contain at most $\#\Delta_{m-1}$ elements and therefore, counting elements we get

$$\lambda_m \leq \#V_m + \#W_m + 2\#\Delta_{m-1}$$

Subtracting twice the first inequality, we get

$$\lambda_m - 2\,\mathrm{wt}\,\mathbf{e} \leq \#V_m - \#W_m$$

which gives the result. □

The next result gives a weaker condition that still guarantees that V_m is larger than W_m. It will be used to show that the decoding algorithm can often decode well beyond $d_o/2$.

Proposition 4.6. *Let* $\mathbf{e}$ *be an error vector with footprint* Δ *and let* $m \in \mathbb{N}_0$ *be such that*

$$\lambda_m > 2\,\#(\Lambda_{\preccurlyeq m} \cap \Delta) \tag{5}$$

Then $\#V_m > \#W_m$.

PROOF: We consider the following partition of $\Lambda_{\preccurlyeq m}$.

$$\begin{aligned} T_m &= \{c \in \Lambda_{\preccurlyeq m} : c \in \Sigma \text{ and } m \ominus c \in \Sigma\} \\ U_m &= \{c \in \Lambda_{\preccurlyeq m} : c \in \Sigma \text{ and } m \ominus c \in \Delta\} \\ X_m &= \{c \in \Lambda_{\preccurlyeq m} : c \in \Delta \text{ and } m \ominus c \in \Sigma\} \\ Y_m &= \{c \in \Lambda_{\preccurlyeq m} : c \in \Delta \text{ and } m \ominus c \in \Delta\} \end{aligned}$$

We have,

$$\begin{aligned} \Lambda_{\preccurlyeq m} \cap \Sigma &= T_m \cup U_m \\ \Lambda_{\preccurlyeq m} \cap \Delta &= X_m \cup Y_m \end{aligned}$$

Now, assumption (5) is equivalent to

$$\#T_m + \#U_m + \#X_m + \#Y_m > 2(\#X_m + \#Y_m)$$

Clearly, $c \in U_m$ if and only if $m \ominus c \in X_m$, so $\#U_m = \#X_m$. Simplifying, we get (5) is equivalent to

$$\#T_m > \#Y_m \tag{6}$$

Since $V_m \supset T_m$ and $Y_m \supset W_m$, we can conclude that $\#V_m > \#W_m$. □

We now amend the Basic Algorithm by adding a step 0 which is used for $m > m^\star$ to compute $S_{\mathbf{e}}(z_m)$.

Objective For $m > m^\star$, given
$$s_0, s_1, s_2, s_3 \ldots, s_{m-1}$$
with $s_i = S_{\mathbf{e}}(z_i)$. Compute $S_{\mathbf{e}}(z_m)$.

Voting Algorithm Let $\Gamma_m = \{s \in \Sigma_{m-1} : m \ominus s \in \Sigma_{m-1}\}$.

0. Compute s_m

   (a) For $s \in \sigma_{m-1} \cap \Gamma_m$
   Compute $\beta(s) = S_{\mathbf{e}}(F_{m-1}(s) z_{m \ominus s} - z_m)$
   Let $A = \{\beta(s) : s \in \sigma_{m-1} \cap \Gamma_m\}$

   (b) Create sets Ψ_α for each $\alpha \in A$.
   For each $t \in \Gamma_m$ choose an $s \in \sigma_{m-1}$ such that $s \preccurlyeq t$. Then put t in $\Psi_{\beta(s)}$.

   (c) If for some $\alpha \in A$, $\#\Psi_\alpha > (\#\Gamma_m)/2$, let
   $$s_m = -\alpha$$
   Else abort.

Notice that $\{\Psi_\alpha\}_{\alpha \in A}$ is a partition of Γ_m.

Proposition 4.7. *If the data from the $(m-1)$th iteration of the algorithm satisfies Theoremt:alg and if $\#V_m > \#W_m$ then the output, s_m, of step 0 is $S_{\mathbf{e}}(z_m)$.*

PROOF: We will show that $\Psi_{S_{\mathbf{e}}(z_m)} = V_m$. We know that V_m and W_m partition Γ_m, so if $\#V_m > \#W_m$ then $\#\Psi_{S_{\mathbf{e}}(z_m)} = \#V_m > \#\Gamma_m/2$. Thus the output of the algorithm is $S_{\mathbf{e}}(z_m)$.

Let $t \in \Gamma_m$ and let $s \in \sigma_{m-1}$ be as in Step (b), $t \succcurlyeq s$. We now show that $t \in W_m$ if and only if $s \in W_m$. From Propositions 2.11 and 2.12, if $t \in W_m$ then $t \in \Delta_m$ and consequently $s \in \Delta_m$. Thus $s \in \Delta_m \cap \Sigma_{m-1} = W_m$. Conversely, if $s \in W_m$ then $m \ominus s \in W_m$ and since $m \ominus s \succcurlyeq m \ominus t$ we have $m \ominus t \in W_m$. This implies that $t \in W_m$.

Now we have the equivalences
$$\begin{aligned} t \in V_m &\iff s \in V_m \\ &\iff S_{\mathbf{e}}(F_{m-1}(s) z_{m \ominus s}) = 0 \\ &\iff S_{\mathbf{e}}(F_{m-1}(s) z_{m \ominus s} - z_m) = -S_{\mathbf{e}}(z_m) \end{aligned}$$
Thus $\Psi_{S_{\mathbf{e}}(z_m)} = V_m$. □

If the condition of the proposition holds for all $m > m^\star$ then majority voting for unknown syndromes will always be successful and the decoding algorithm can continue until a Gröbner basis is computed.

Definition 4.8. We will say that decoding of a vector e is *guaranteed* by the code $C_{m^\star}$ if (5), or equivalently, (6) holds for all $m > m^\star$. Otherwise decoding is not guaranteed.

In particular, we can now show that decoding up to $d_o/2$ is guaranteed.

Corollary 4.9. *Suppose that* $2\,\mathrm{wt}\,\mathbf{e} < d_o(m^\star)$*. Then decoding of* $\mathbf{e}$ *is guaranteed by the code* $C_{m^\star}$*.*

PROOF: By the definition of the order bound on the minimum distance, for all $m > m^\star$, $\lambda_m \geq d_o(m^\star)$. Since $\#(\Lambda_{\preccurlyeq m} \cap \Delta) \leq \mathrm{wt}\,\mathbf{e}$, our hypothesis on $\mathrm{wt}\,\mathbf{e}$ gives $\lambda_m > 2\,\#(\Lambda_{\preccurlyeq m} \cap \Delta)$. Thus decoding is guaranteed. □

Finally, we consider error vectors where $D_{\mathbf{e}}$ is an independent set. It will be handy to use the notation

$$\Sigma \oplus \Sigma = \{s \oplus s' : s, s' \in \Sigma\}$$

Definition 4.10. A vector $\mathbf{e}$ of weight t is called *independent* its footprint satisfies $\Delta_{\mathbf{e}} = \{0, 1, \ldots, t-1\}$.

The condition of being independent is due to the error positions not the error values. The positions $D_{\mathbf{e}}$ impose independent conditions on the space L_{t-1}.

Proposition 4.11. *Let* $\mathbf{e}$ *be an independent vector of weight* t*. Let* $m^\star$ *be the largest integer which is not in* $\Sigma \oplus \Sigma$*. Then decoding of* $\mathbf{e}$ *is guaranteed by the code* $C_{m^\star}$*.*

PROOF: Recall the definitions of T_m and Y_m from the proof of Proposition 4.6. We will show that if $m \in \Sigma \oplus \Sigma$ then T_m is nonempty and Y_m is empty. Then for all $m > m^\star$, condition (6) holds so decoding is guaranteed by $C_{m^\star}$.

Clearly, T_m is nonempty if and only if there exist $s, s' \in \Sigma$ such that $s \oplus s' = m$. This is equivalent to $m \in \Sigma \oplus \Sigma$. Similarly Y_m is nonempty if and only if there exist $c, c' \in \Delta$ such that $c \oplus c' = m$. Since $\mathbf{e}$ is independent of weight t, any $c, c' \in \Delta$ satisfy $c, c' \leq t-1$ and therefore $c \oplus c' \leq (t-1) \oplus (t-1)$. Thus Y_m is empty if $m > (t-1) \oplus (t-1)$. By similar reasoning, for $s, s' \in \Sigma$, $s \oplus s' > (t-1) \oplus (t-1)$, so T_m is nonempty only if $m > (t-1) \oplus (t-1)$. Thus $m \in \Sigma \oplus \Sigma$ implies that T_m is nonempty and that in turn implies Y_m is empty. □

Remark 4.11.1. When $\mathbf{e}$ is independent, the value of M that guarantees that all generators of $I_{\mathbf{e}}$ have been computed by the decoding algorithm is $M = c_{\max} \oplus s_{\max}$. This follows from Theorem 3.1 and $c_{\max} < s_{\max}$.

5 Examples

In this section we consider three examples. We will compute, for $\Delta = \{0, 1, \ldots, t-1\}$, the value $m^\star = \max\{m : m \notin \Sigma \oplus \Sigma\}$ that guarantees the correction of t independent errors from Proposition 4.11 and the value $M = c_{\max} + s_{\max}$ that determines when the computation of the Gröbner basis is complete from Remark 4.11.1. In each case the monoid structure that we imposed on $\mathbb{N}_0$ from the properties of multiplication in the ring R will have a much more natural representation.

Codes from the plane

Let $R = k[x, y]$ for some field k. We will use the total degree lexicographic order on $k[x, y]$,

$$1 < x < y < x^2 < xy < y^2 < \cdots$$

Taking the monomials as a basis for $k[x,y]$ we get a filtration of $k[x,y]$ with one-dimensional quotients and therefore an order function on $k[x,y]$. We now give a more formal presentation of the induced order function and it's monoid structure.

Consider $\mathbb{N}_0 \times \mathbb{N}_0$ with vector addition and total ordering defined by

$$(i,j) < (u,v) \text{ if } \begin{cases} i+j < u+v \text{ or,} \\ i+j = u+v \text{ and } j < v \end{cases}$$

Then $\mathbb{N}_0 \times \mathbb{N}_0$ is a totally ordered monoid. Let

$$\begin{aligned} \rho : k[x,y] &\longrightarrow \mathbb{N}_0 \times \mathbb{N}_0 \\ x^i y^j &\longmapsto (i,j) \\ \sum a_{ij} x^i y^j &\longmapsto \max\{(i,j) : a_{ij} \neq 0\} \end{aligned}$$

Clearly ρ induces the total degree lex order on $k[x,y]$. Now let

$$\begin{aligned} \phi : \mathbb{N}_0 \times \mathbb{N}_0 &\longrightarrow \mathbb{N}_0 \\ (i,j) &\longmapsto \binom{i+j+1}{1} + j \end{aligned}$$

One can show inductively that ϕ is a bijection of totally ordered sets: $\phi(i,j) < \phi(u,v)$ if and only if $(i,j) < (u,v)$. Now $o = \phi \circ \rho$, illustrated at the right, is the order function we sought. The monoid structure $\oplus$ on $\mathbb{N}_0$ is inherited from vector addition on $\mathbb{N}_0 \times \mathbb{N}_0$. To analyze the conditions defining M and $m^\star$ in the previous sections we will find it easier to use the evident struture on $\mathbb{N}_0 \times \mathbb{N}_0$. So Σ and Δ will be subsets of $\mathbb{N}_0 \times \mathbb{N}_0$ and we will write $\phi^{-1}(m^\star) = \vec{m^\star}$ and $\phi^{-1}(M) = \vec{M}$.

Proposition 5.1. *Let $(a,b) = \phi^{-1}(t)$ and let $\Delta = \{(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 : (i,j) < (a,b)\}$. Then $m^\star$ and M are determined by*

$$\vec{m^\star} = \begin{cases} (0, 2b+1) \text{ if } a = 0 \\ (2a+b+1, b) \text{ if } a \neq 0 \end{cases} \tag{7}$$

$$\vec{(M)} = \begin{cases} (0, 2b+1) \text{ if } a = 0 \\ (2a+1, 2b) \text{ if } a \neq 0 \end{cases} \tag{8}$$

Proof: Suppose first that $a = 0$. Then the set of minimal elements of Σ is $\sigma = \{(i,j) : i+j = b+1\}$. Now $\Sigma \oplus \Sigma$ contains all (i,j) such that $i+j \geq 2a+2$. The largest element of $\mathbb{N}_0 \times \mathbb{N}_0$ not contained in $\Sigma \oplus \Sigma$ is $(0, 2b+1)$, so $\vec{m^\star} = (0, 2b+1)$. Since $s_{\max} = (0, b+1)$, $M = (0,b) + (0,b+1) = (0, 2b+1)$. In this case majority voting is not required to compute the Gröbner basis.

Suppose now that $a \neq 0$. Then the set of minimal elements of Σ is

$$\begin{aligned} \sigma = \{&(i,j) : i+j = a+b \text{ and } i \leq a-1\} \\ &\cup \{(i,j) : i+j = a+b+1 \text{ and } i \geq a+1\} \end{aligned}$$

Now $\Sigma + \Sigma$ contains

$$
\begin{aligned}
&\{(i,j) : i+j = 2a+2b \text{ and } i \leq 2a-2\} && (9)\\
&\{(i,j) : i+j = 2a+2b+1 \text{ and } i \leq 2a+b\}, && (10)\\
&\{(i,j) : i+j \geq 2a+2b+2\}, && (11)\\
& && (12)
\end{aligned}
$$

The smallest element of $\mathbb{N}_0 \times \mathbb{N}_0$ not in $\Sigma \oplus \Sigma$ is $(2a+b+1, b)$, so $m^\star = (2a+b+1, b)$. The largest element of σ is $(a, b+1)$ so $M = (a,b) + (a+1,b) = (2a+1, 2b)$. $\square$

Notice that the code $C^\perp_{m^\star}$ with parity check matrix determined by $m^\star = (0, 2b+1)$ has $r = \binom{2b+3}{2} = 2b^2 + 5b + 3$ check symbols. The order bound on the minimum distance of this code is $d_o = 2b+2$, yet the code corrects independent errors of weight $\binom{b+2}{2} = (b^2+3b+2)/2$.

Codes from r-dimensional Euclidean space

We now extend the previous discussion to arbitrary dimension. Let $\mathbb{N}_0^r$ have the total degree lexicographic order. Let $\vec{a} \preccurlyeq \vec{b}$ if $\vec{b} - \vec{a} \in \mathbb{N}_0^r$. Let $R = k[x_1, \ldots, x_r]$ and let $\rho : R \longrightarrow \mathbb{N}_0^r$ take $x_1^{a_1} x_2^{a_2}, \ldots, x_r^{a_r}$ to $(a_1, a_2, \ldots, a_r)$. Extend ρ to all of R by defining $\rho(f)$ to be the image of its term of highest order. Let $\phi : \mathbb{N}_0^r \longrightarrow \mathbb{N}_0$ be the ordering determined by the total degree lexicographic order on $\mathbb{N}_0^r$. For an r-vector $\vec{a}$ let $\deg \vec{a} = a_1 + a_2 + \cdots + a_r$.

Proposition 5.2.

$$\phi(A_1, A_2, \ldots, A_r) = \sum_{i=1}^{r} \binom{A_i + A_{i+1} + \cdots + A_r + r - i}{r-i+1} \tag{13}$$

Proof: We proceed by induction on r. We want to show that the number of $\vec{a} \prec \vec{A}$ is given by (13). The case $r=1$ is immediate. Let $D = \deg \vec{A}$. We partition $\{\vec{a} \in \mathbb{N}_0^r : \vec{a} \prec \vec{A}\}$ into $S = \{\vec{a} \in \mathbb{N}_0^r : \vec{a} \prec \vec{A} \text{ and } \deg \vec{a} = D\}$ and $S' = \{\vec{a} \in \mathbb{N}_0^r : \deg \vec{a} < D\}$.

The first term in the sum of (13) is $\#S' = \binom{D-1+r}{r}$. Let $\vec{B} = (A_2, \ldots, A_r)$ and let $T = \{\vec{b} \in \mathbb{N}_0^{r-1} : \vec{b} \prec \vec{B}\}$. By the induction hypothesis, the number of elements in T is

$$\sum_{j=1}^{r-1} \binom{B_j + B_{j+1} + \cdots + B_r + r - 1 - j}{r-j}$$

Setting $i = j+1$ this gives the remaining terms in the sum of (13). But $\#T = \#S$ since we have a bijection:

$$
\begin{gathered}
S \longrightarrow T\\
(a_1, a_2, \ldots, a_r) \hookrightarrow (a_2, \ldots, a_r)\\
(0 - \sum_{2}^{r-1} b_i, b_1, \ldots, b_{r-1} \hookleftarrow (b_1, \ldots, b_{r-1})
\end{gathered}
$$

Thus we have $\{\vec{a} \in \mathbb{N}_0^r : \vec{a} \prec \vec{A}\} = \#S + \#S'$ is given by (13). $\square$

We now consider correction of t errors at an independent set of points. As with the plane, we consider Δ, Σ, contained in $\mathbb{N}_0^r$ and we write $\vec{m^\star} = \phi^{-1}(m^\star)$ and $\vec{M} = \phi^{-1}(M)$. Let $\vec{A} = \phi^{-1}(t-1)$ and $\Delta = \{\vec{a} \in \mathbb{N}_0^r : \vec{a} \preccurlyeq \vec{A}\}$. Let $\Sigma = \mathbb{N}_0^r \setminus \Delta$, let $\sigma = \min_\prec \Sigma$ and let $\vec{s}_{\max}$ be the largest vector in Σ with respect to the total degree lexicographic ordering. Finally, let $\vec{e}_i$ be the ith basis vector and let $I = \min\{i : A_i \neq 0\}$.

Proposition 5.3. *$\vec{s}_{\max} = \vec{A} + \vec{e}_I$ so $\vec{M} = 2\vec{A} + \vec{e}_I$.*

Proof: Since $\deg(\vec{A} + \vec{e}_I) = D + 1$, $\vec{A} + \vec{e}_I \in \Sigma$. We need to show: 1) $\vec{A} + \vec{e}_I - \vec{e}_j \notin \Sigma$ for all $j \in \{1, \ldots, r\}$, and 2) for any $\vec{a} > \vec{A} + \vec{e}_I$, $\vec{a} - e_j \in \Sigma$ for some $j \in \{1, \ldots, r\}$, so $\vec{a} \notin \sigma$.

For the first item, if $j < I$ then $\vec{A} + \vec{e}_I - \vec{e}_j$ has a negative coordinate, so it is not in Σ. For $j \geq I$, $\vec{A} + \vec{e}_I - \vec{e}_j \preccurlyeq \vec{A}$, since $e_I \preccurlyeq e_j$. So $\vec{A} + \vec{e}_I - \vec{e}_j \notin \Sigma$.

For the second item, if $\deg \vec{a} > D+1$ then $\vec{a} \notin \Sigma$ since all vectors of weight $D+1$ are in Σ. If $\deg \vec{a} = D + 1$ let $J = \min\{i : a_i \neq 0\}$. Since $\vec{a} > \vec{A} + \vec{e}_I$, we must have $J \geq I$. Then $\vec{a} - \vec{e}_J$ has nonnegative coordinates and $\vec{a} - \vec{e}_J > \vec{A} + \vec{e}_I - \vec{e}_J \geq \vec{A}$, so $\vec{a} - \vec{e}_J \in \Sigma$.

Now $\vec{M} = \vec{A} + \vec{s}_{\max} = 2\vec{A} + \vec{e}_I$. $\square$

Proposition 5.4. *$\vec{m^\star} = \vec{A} + (D+1)\vec{e}_I$.*

Proof: Let $\vec{B} = \vec{A} + (D+1)\vec{e}_I$. We must show: 1) $\vec{B} \notin \Sigma + \Sigma$, and 2) if $\vec{b} > \vec{B}$ then $\vec{b} \in \Sigma + \Sigma$.

Suppose $\vec{B} = \vec{a} + \vec{c}$ with $\vec{a}, \vec{c} \in \Sigma$, and $\deg \vec{a} \leq \deg \vec{b}$. Since $\deg \vec{B} = 2D + 1$, we must have $\deg \vec{a} = D$ and $\deg \vec{b} = D + 1$. Since $\vec{a} > \vec{A}$, $a_1 = a_2 = \ldots a_{I-1} = 0$ and $a_I \leq A_I$. This implies that $c_I = D + 1 + A_I - a_I \geq D + 1$. Since $\deg \vec{c} = D + 1$, $\vec{c} = (D+1)\vec{e}_I$. Then $\vec{a} = \vec{A}$, a contradiction. Thus $\vec{B} \notin \Sigma + \Sigma$.

To prove item 2) we note that if $\deg \vec{b} \geq 2D + 2$ then $\vec{b} \in \Sigma + \Sigma$ since Σ contains all vectors of degree $D + 1$ or larger. Thus we may assume $\deg \vec{b} = 2D + 1$. Since $\vec{b} > \vec{B}$, $b_1 = b_2 = \cdots = b_{I-1} = 0$. If $b_I \geq D + 1$, then $\vec{b} - (D+1)e_I \in \Sigma$, since it has nonzero coordinates and $\vec{b} - (D+1)\vec{e}_I > \vec{A}$. So we reduce to the case where $b_I < D + 1$.

Define $\vec{a}$ by $a_1 = \cdots = a_{I-1} = 0$, $a_I = \min\{A_I - 1, b_I\}$ and $a_i = \min\{b_i, D - \sum_{j<i} a_j\}$ for $i > I$. For all i, $\sum_{j<i} a_j \leq D$. This is clear for $i = 0, \ldots, I$ since $A_I \leq D$ and for $i > I$ from $a_i \leq D - \sum_{j<i} a_j$. An immediate consequence is that $a_i \geq 0$ for all i so $\vec{a} \in \mathbb{N}_0^r$.

I claim that $\deg \vec{a} = D$. If this is true then $\vec{a} > \vec{A}$ so $\vec{a} \in \Sigma$. By construction $\vec{b} \succcurlyeq \vec{a}$ and since $\deg \vec{b} - \vec{a} = D + 1$, we have $\vec{b} - \vec{a} \in \Sigma$. Thus $\vec{b} \in \Sigma + \Sigma$ as was to be proved.

Suppose the claim is false, $\deg \vec{a} < D$. Then for each $i > I$, $a_i \neq D - \sum_{j<i} a_j$, for if we ever get equality that will give $\deg \vec{a} = D$. This means $a_i = b_i$ for all $i > I$, so

$$\deg \vec{a} = \min\{A_I - 1, b_I\} + \sum_{i>I} b_i$$

since $\deg \vec{b} = 2D + 1$,

$$\deg \vec{a} = \min\{A_I - 1, b_I\} + 2D + 1 - b_I$$

Since $A_I \geq 1$ and $b_I \leq D$, this is minimal when $A_I = 1$ and $b_I = D$. This gives $\deg \vec{a} \geq D + 1$, contradicting our assumption that $\deg \vec{a} < D$. $\square$

Notice that the code $C^{\perp}_{m^\star}$ with parity check matrix determined by $\vec{m^\star} = (2b+1)\vec{e}_r$ has $\binom{2b+1+r}{r}$ check symbols The order bound on the minimum distance of this code is $d_o = 2b + 2$, yet the code corrects independent errors of weight $\binom{b+r}{r}$.

Hermitian Codes

We will first show a result that applies to any one-point code. Whenever t is larger than g, the genus of the curve, the code guaranteeing correction of t independent errors actually corrects all errors of weight t. So Proposition 4.11 is only interesting when $t < g$. Let $\mathcal{C}$ be a smooth absolutely irreducible curve over a field k. Let $Q \in \mathcal{C}$ be a rational point of $\mathcal{C}$ and let $R = \cup L(mQ)$ be the space of rational functions with poles only at Q. The pole order function for Q, ρ, gives a map from R to $\mathbb{N}_0$ whose image we will call Λ, the set of *nongaps* at Q.

Let $\phi : \Lambda \to \mathbb{N}_0$ be defined by $\phi(m) = \dim L(mQ) - 1$. Then the composite $o = \phi \circ \rho$ is the order function on R. Since the monoid structure of Λ uses addition of integers, we will consider Δ, Σ, as contained in Λ. We enumerate the nongaps using ϕ, $\Lambda = \{\lambda_0, \lambda_1, \dots\}$. For an independent set of t errors, $\Delta = \{\lambda_0, \dots, \lambda_{t-1}\}$.

Proposition 5.5. *If $t \geq g$ then the value of $m^\star$ which guarantees the correction of t independent errors is $m^\star = 2t + g - 1$. The designed distance of $C^{\perp}_{m^\star}$ is $2t + 1$.*

PROOF: For $t = g$, $\lambda_{t-1} = 2g - 1$ or $2g - 2$, and for $t > g$, $\lambda_{t-1} = t + g - 1$. In either case, $\Sigma = \{\lambda \in \mathbb{N}_0 : \lambda \geq t + g\}$ so $\Sigma + \Sigma = \{\lambda \in \mathbb{N}_0 : \lambda \geq 2t + 2g\}$. The largest nongap not in $\Sigma + \Sigma$ is $\lambda_{m^\star} = 2t + 2g - 1$. Then $m^\star = 2t + g - 1$. Now the designed distance of $C^{\perp}_{m^\star}$ is $\lambda_{m^\star} - 2g + 2 = 2t + 1$. $\square$

We now focus on Hermitian codes defined in the plane by the equation $x^{r+1} - y^r - y = 0$ over the field $\mathbb{F}_{r^2}$. The pole order of x is r and of y is $r+1$, so $\Lambda = \{ir + j(r+1) : i, j \geq 0\}$.

Proposition 5.6. *Let $t < g - 1$ and let $\lambda_{t-1} = ar + b(r+1)$. Then the value of $m^\star$ guaranteeing correction of a generic vector of weight t is $C_{m^\star}$ where*

$$\lambda_{m^\star} = \begin{cases} 2\lambda_t + r + 1 & \text{if } a = 0 \text{ and } b < (r-1)/2 \\ 2\lambda_t + 2(r-b) - 1 & \text{if } a = 0 \text{ and } b \geq (r-1)/2 \\ 2\lambda_t + r - b & \text{if } a \neq 0 \text{ and } 2a + b < r \\ 2\lambda_t + 1 & \text{if } a \neq 0 \text{ and } 2a + b \geq r \end{cases} \tag{14}$$

The value of M that guarantees that the decoding algorithm has produced a generating set for the ideal of error locators is determined by

$$\lambda_M = \begin{cases} \lambda_{t-1} + r + 1 & \text{if } a = 0 \\ \lambda_{t-1} + r & \text{if } a \neq 0 \end{cases}$$

PROOF: Note first that since $t < g - 1$, $\lambda_t < 2g - 2 = r^2 - r - 2$. This forces $a + b < r - 2$.

Suppose first that $a = 0$. Then the set of minimal elements of Σ is $\sigma = \{ir + j(r+1) : i+j = b+1\}$. The largest element of σ is $(b+1)(r+1)$ so $M = (2b+1)(r+1) = 2\lambda_t + r + 1$. Now $\Sigma + \Sigma$ contains

$$\{ir + j(r+1) : i + j \geq 2b + 2)\} \tag{15}$$

If $b < (r-1)/2$ then $2b+2 < r+1$, and the largest nongap not in $\Sigma+\Sigma$ is $(2b+1)(r+1) = 2\lambda_t + r + 1$.

If $b \geq (r-1)/2$ then $(2b+2)r$, which is the smallest element of $\Sigma + \Sigma$, may also be written $(2b + 1 - r)r + r(r+1)$. All nongaps larger than this are also in $\Sigma + \Sigma$, so the largest nongap not in $\Sigma+\Sigma$ is $(2b+2-r)r+(r-1)(r+1) = 2br+2r-1 = 2\lambda_t+2(r-b)-1$.

Now suppose that $a \neq 0$. Then the set of minimal elements of Σ is

$$\begin{aligned}\sigma = \{&ir + j(r+1) : j \geq b+1 \text{ and } i+j = a+b\} \\ &\cup \{ir + j(r+1) : j \leq b \text{ and } i + j = a + b + 1\}\end{aligned}$$

The largest element of σ is $(a+1)r + b(r+1)$ so $M = (2a+1)r + 2b(r+1) = 2\lambda_t + r$.

Now $\Sigma + \Sigma$ contains

$$\{ir + j(r+1) : j \geq 2b + 2 \text{ and } i + j = 2a + 2b\}, \tag{16}$$

$$\{ir + j(r+1) : j \geq b + 1 \text{ and } i + j = 2a + 2b + 1\}, \tag{17}$$

$$\{ir + j(r+1) : i + j \geq 2a + 2b + 2\} \tag{18}$$

If $2a + b < r$ then all nongaps larger than $(2a + b)r + (b+1)(r+1)$ are in $\Sigma + \Sigma$ but $(2a + b + 1)r + b(r + 1)$ is not. Thus $m^\star = (2a + b + 1)r + b(r+1) = 2\lambda_t + r - b$.

If $2a+b \geq r$ then $(2a+b+1)r+b(r+1)$ may also be written $(2a+b-r)r+(b+r)(r+1)$. This is in $\Sigma + \Sigma$ since $b + r \geq 2b + 2$. Indeed, any $ir + j(r+1)$ with $i \geq 2a + 2b + 1$ and $i + j = 2a + 2b + 1$ may be written as $(i - r - 1)r + (j + r)(r + 1)$. The latter is in $\Sigma + \Sigma$ if and only if $j + r \geq 2b + 2$. So the largest nongap not in $\Sigma + \Sigma$ is $(2a - 1)r + (2b+1)(r+1) = 2\lambda_t + 1$. □

The following three tables list parameters for Hermitian codes over $\mathbb{F}_{16}$, $\mathbb{F}_{64}$ and $\mathbb{F}_{256}$. For each curve and for several values of $t < g$ the tables give the required check dimension $(m^\star + 1)$, the code parameters for $C_{m^\star}^{\perp}$ (assuming we use all r^3 points on $\mathcal{C}$), and the last iteration of the algorithm, M.

number errors	check dimension	code parameters [n,k,d]	last iteration
2	7	[64, 57, 4]	19
3	10	[64, 54, 5]	21
4	12	[64, 52, 8]	23

Table 1: Hermitian codes over $\mathbb{F}_{16}$.

References

[1] Bourbaki, "Commutative Algebra", Addison-Wesley, 1972.

[2] D. Cox, J. Little, D. O'Shea, "Ideals, Varieties and Algorithms", Undergraduate Texts in Matematics, Springer-Verlag, 1997.

[3] G. L. Feng and T. R. N. Rao, Decoding algebraic-geometry codes up to the designed minimum distance, *IEEE Trans. Inform. Theory*, **39**, no. 1, (Jan. 1993) 37-45.

[4] G. L. Feng and T. R. N. Rao, "Decoding algebraic-geometry codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, **39**, no. 1, (Jan. 1993) 37-45.

[5] O. Geil, T. Høholdt, Footprints or generalized Bezout's theorem, *IEEE Trans. Inform. Theory*, **46**, no. 2, (Mar. 2000) 635-641.

[6] J. Justesen, K. J. Larsen, H. E. Jensen, and T. Høholdt, Fast decoding of codes from algebraic plane curves, *IEEE Trans. Inform. Theory*, **38**, no. 1, Jan. 1992, pp. 111-119.

[7] T. Høholdt, R. Pellikaan, J.H. van Lint : Algebraic geometry codes, *in* "Handbook of Coding Theory" (W.C.Huffmann, V. Pless eds.) Elsevier, 1998.

[8] M. E. O'Sullivan, Decoding of codes defined by a single point on a curve, *IEEE Trans. Inform. Theory*, **41** no. 6, (Nov. 1995) 1709-1719.

[9] M. E. O'Sullivan, The key equation for one-point codes and efficient error evaluation, to appear *J. Pure Appl. Alg.*.

[10] M. E. O'Sullivan, New codes for the Berlekamp-Massey algorithm *Finite Fields Appl. 7, 293-317 (2001)*

[11] R. Pellikaan and C. Kirfel, The minimum distance of codes in an array coming from telescopic semigroups, *IEEE Trans. Inform. Theory*, **41** no. 6, (Nov. 1995) 1720-1732.

[12] L. Robbiano, On the theory of graded structures, *J. Symb. Comp.*, **2** no. 2, (1986), 139-170.

[13] S. Sakata, Extension of the Berlekamp-Massey algorithm to N dimensions, *Informat. Comput.* **84**, (Feb. 1990) 207-239.

[14] S. Sakata, J. Justesen, Y. Madelung, H. Elbrønd Jensen and T. Høholdt, Fast decoding of algebraic codes up to the designed minimum distance, *IEEE Trans. Inform. Theory*, **41** no. 6, (Nov. 1995) 1672-1677.

[15] S. Sakata, H. Elbrønd Jensen and T. Høholdt, Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-Rao bound, *IEEE Trans. Inform. Theory*, **41** no. 6, (Nov. 1995) 1762-1768.

number errors	check dimension	code parameters [n,k,d]	last iteration
2	7	[512, 505, 4]	71
3	10	[512, 502,5]	73
4	16	[512, 496, 6]	79
5	17	[512, 495, 6]	80
6	21	[512, 491, 7]	82
7	29	[512, 483, 8]	87
8	30	[512, 482,8]	88
9	31	[512, 481, 8]	89
10	36	[512, 476, 9]	91
11	38	[512, 474, 16]	95
12	46	[512, 466, 24]	96
13	47	[512, 465, 24]	97
14	48	[512, 464, 24]	98
15	52	[512, 460, 25]	100
16	54	[512, 458, 27]	103
17	56	[512, 456, 32]	104
18	58	[512, 454, 32]	105
19	64	[512, 448, 40]	106
20	65	[512, 447, 40]	107
21	68	[512, 444, 41]	109
22	70	[512, 442, 43]	111
23	72	[512, 440, 45]	112
24	74	[512, 438, 48]	113
25	76	[512, 436, 49]	114
26	78	[512, 434, 51]	115
27	82	[512, 430, 56]	116

Table 2: Hermitian codes over $\mathbb{F}_{64}$.

number errors	check dimension	code parameters [n,k,d]	last iteration
10	36	[4096,4060, 9]	307
14	49	[4096,4047, 10]	322
15	55	[4096,4041, 11]	324
20	71	[4096,4025, 12]	339
21	78	[4096,4018, 13]	341
27	97	[4096,3999, 14]	356
28	105	[4096,3991, 15]	358
35	127	[4096,3969, 16]	373
36	136	[4096,3960, 17]	375
37	138	[4096,3958, 32]	383
45	168	[4096,3928, 49]	392
46	170	[4096,3926, 51]	281
55	200	[4096,3896, 81]	289
56	202	[4096,3894, 83]	297
65	226	[4096,3870,112]	305
66	232	[4096,3864,113]	306
67	234	[4096,3862,115]	313
74	256	[4096,3840,144]	319
75	257	[4096,3839,144]	320

Table 3: Hermitian codes over $\mathbb{F}_{256}$.