AAECC (2006) 17: 315–335
DOI 10.1007/s00200-006-0015-8

Maria Bras-Amorós · Michael E. O'Sullivan

The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting

Received: 1 November 2004 / Published online: 11 May 2006

Abstract Sakata's generalization of the Berlekamp–Massey algorithm applies to a broad class of codes defined by an evaluation map on an order domain. In order to decode up to the minimum distance bound, Sakata's algorithm must be combined with the majority voting algorithm of Feng, Rao and Duursma. This combined algorithm can often decode far more than $(d_{\min} - 1)/2$ errors, provided the errors are in general position. We give a precise characterization of the error correction capability of the combined algorithm. We also extend the concept behind Feng and Rao's improved codes to decoding of errors in general position. The analysis leads to a new characterization of Arf numerical semigroups.

Keywords Algebraic geometry codes · Order domains · Decoding · Arf semigroups

1 Introduction

In this article we investigate the error correction capability of the Berlekamp–Massey–Sakata algorithm as it works in combination with the majority voting algorithm due to Duursma [8] and Feng and Rao [9]. The Berlekamp–Massey algorithm applies to a polynomial ring in one variable, while Sakata's algorithm

M. Bras-Amorós
Departament d'Enginyeria de la Informació i de les Comunicacions,
Universitat Autònoma de Barcelona, 08193 Bellaterra, Spain
E-mail: mbras@deic.uab.cat

M.E. O'Sullivan (✉)
Department of Mathematics and Statistics,
San Diego State University, San Diego, CA 92182-7720, USA
E-mail: mosulliv@sciences.sdsu.edu
Tel.: +1-619-5946697
Fax: +1-619-5946746

[22] is the generalization of Berlekamp–Massey to polynomial rings in several variables. It was shown in [13] that Sakata's algorithm works, with little alteration, in the more general setting of *order domains*. We call the algorithm on order domains the Berlekamp–Massey–Sakata algorithm (BMS).

Reed–Solomon codes, Reed–Muller codes and one-point geometric Goppa codes may all be seen as special cases of codes from order domains. A standard method for decoding Reed–Solomon codes is to apply the Berlekamp–Massey algorithm to the syndromes of the received vector to find the error-locator polynomial. Generalizing to order domains, one applies the BMS algorithm to syndromes of the received vector to find a Gröbner basis for the ideal of error locator polynomials. Unfortunately, the syndromes of the received vector are insufficient for decoding up to the designed distance bound, $(d-1)/2$. In order to achieve that bound, one must use an algorithm due to Feng, Rao and Duursma which uses majority voting to compute new syndromes beyond those available from the received vector.

We will show in this paper how the BMS algorithm and majority voting work in tandem to correct error vectors whose weight may be larger than $(d-1)/2$, provided the error locations are not in special position (in a sense to be defined precisely). In other words, an error vector of weight t whose error locations are in general position may be decoded using fewer check symbols than an error vector whose locations are in special position. We also incorporate the improvements initiated by Feng and Rao [10] in which unnecessary check symbols are eliminated while retaining a prescribed correction capability. While they use only check symbols that are necessary to correct t errors – thus increasing the dimension of the code – we use only check symbols necessary to correct t errors which are in general position.

In section 2, we define order-prescribed evaluation codes constructed from an order domain. Section 3 establishes the algebraic tools for decoding these codes while sections 4 and 5 present, respectively, the Berlekamp–Massey–Sakata algorithm and the majority voting algorithm. Many of the results of these sections are present in the Höholdt et al. chapter [13] which consolidates and extends previous work [9,16,22]. The presentation here analyzes the objects appearing in the algorithms independently of the algorithms. The discussion of the BMS algorithm and the majority voting algorithm is thereby simplified, and the intimate relationship between them is apparent. Furthermore, we characterize the conditions ensuring the success of majority voting (Proposition 15) with a stronger result than previously obtained. Section 6 applies the conditions for success of the decoding algorithm to designing codes for a prescribed error correction capability, in particular to decoding of generic errors. Section 7 concerns order domains for which no increase in code dimension results by designing codes to correct generic errors of weight t rather than all errors of weight t.

2 Evaluation codes from order domains

In this section we review the basic properties of order functions and define order-prescribed evaluation codes. Order functions may be defined much more generally (see [4, III Section 2]), but the restriction used here, where the ordering is given by the natural numbers, seems to be the appropriate context for generalizing Sakata's algorithm.

Order functions

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 *Let $\mathbb{F}$ be a field and let A be an $\mathbb{F}$-algebra. An order function on A is a map*

$$\rho : A \longrightarrow \mathbb{N}_{-1},$$

which satisfies the following.

O1. The set $L_m = \{f \in A \mid \rho(f) \leqslant m\}$ is an $m+1$ dimensional vector space over $\mathbb{F}$.
O2. If $f, g, z \in A$ and z is nonzero then $\rho(f) > \rho(g) \Longrightarrow \rho(zf) > \rho(zg)$.

The pair A, ρ is often called an order domain.

It is easy to show that A must be an integral domain and that the only units in A are the nonzero elements of $\mathbb{F}$. One can also see that ρ is surjective, and that:

C1 $\rho(\lambda f) = \rho(f)$ for all $\lambda \in \mathbb{F}^*$ and all $f \in A$.
C2 $\rho(f+g) \leqslant \max(\rho(f), \rho(g))$ for all $f, g \in A$, with equality if $\rho(f) \neq \rho(g)$.
C3 If f and g are nonzero and $\rho(f) = \rho(g)$, then there exists a unique $\lambda \in \mathbb{F}^*$ such that $\rho(f + \lambda g) < \rho(g)$.

Our definition is from [18] and differs from [13] only by the restriction that ρ be surjective. An operation $\oplus$ in $\mathbb{N}_0$ can be well defined by $i \oplus j = \rho(fg)$ where f and g are such that $\rho(f) = i$ and $\rho(g) = j$. In fact $\mathbb{N}_0, \oplus$ is a commutative semigroup. We can define a partial ordering $\preccurlyeq$ on $\mathbb{N}_0$ by $i \preccurlyeq j$ if and only if there exists $k \in \mathbb{N}_0$ such that $i \oplus k = j$. When this holds we may also write $j \ominus i = k$. One can verify that for $i \preccurlyeq j \preccurlyeq m$, $m \ominus j \preccurlyeq m \ominus i$.

One can also show that the natural ordering on $\mathbb{N}_0$ respects the operation $\oplus$: if $i \preccurlyeq j$ then $i \leqslant j$, and if $i < j$ then for arbitrary $k \in \mathbb{N}_0$, $i \oplus k < j \oplus k$.

For $m \in \mathbb{N}_0$ let $N_m = \{a \in \mathbb{N}_0 \mid a \preccurlyeq m\}$, and $\nu_m = |N_m|$.

Evaluation codes

Let $\mathbb{F}$ be a field. Throughout this article we will consider $\mathbb{F}^n$ as an $\mathbb{F}$-algebra with component-wise multiplication, $v * w$ is the vector with ith component $v_i w_i$. Let φ be a surjective morphism of $\mathbb{F}$-algebras $\varphi : A \longrightarrow \mathbb{F}^n$. We remark that for each $i = 1, \ldots, n$, $\{f \in A \mid \varphi(f)_i = 0\}$ is a maximal ideal $\mathfrak{m}_i$ of A such that $A/\mathfrak{m}_i \cong \mathbb{F}$. For any $L \subseteq \{1, \ldots, n\}$ we have $\{f \in A \mid \varphi(f)_i = 0 \text{ for all } i \in L\}$ is the ideal $\cap_{i \in L} \mathfrak{m}_i$.

Definition 2 *Given an $\mathbb{F}$-algebra A, an order function ρ on A, and a surjective morphism $\varphi : A \longrightarrow \mathbb{F}^n$, define the mth evaluation code related to A, ρ and φ as $E_m = \{\varphi(f) \mid \rho(f) \leqslant m\}$ and its dual as $C_m = \{c \in \mathbb{F}^n \mid c \cdot \varphi(f) = 0$ for all f with $\rho(f) \leqslant m\}$.*

Example 1 Reed–Solomon codes Let $\alpha_0, \alpha_1, \ldots, \alpha_{q-1}$ be all the elements in $\mathbb{F}_q$ and let $\mathbb{F}_q[x]_{\leqslant_s}$ be the subspace of $\mathbb{F}_q[x]$ of polynomials with degree $\leqslant_s$. For $k \leqslant q$ the *Reed–Solomon* code over $\mathbb{F}_q$ with dimension k, denoted $\mathrm{RS}_q(k)$, is defined as the image of the map

$$\begin{aligned} \mathbb{F}_q[x]_{\leqslant_{k-1}} &\xrightarrow{\varphi_k} {\mathbb{F}_q}^q \\ f &\longmapsto (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q-1})). \end{aligned}$$

Notice that $\rho(f) = \deg(f)$, where $\deg(0)$ is defined to be -1, is an order function on $\mathbb{F}_q[x]$. Hence, $\mathrm{RS}_q(k)$ is the $(k-1)$th evaluation code related to the algebra $A = \mathbb{F}_q[x]$, the order function $\rho = \deg$ and the morphism $\varphi : f \mapsto (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{q-1}))$. Notice that the Vandermonde matrix $V_k(\alpha_0, \ldots, \alpha_{q-1})$ is a generating matrix for $RS_q(k)$.

Example 2 Reed–Muller codes Let $n = q^m$ and call $P_1, \ldots, P_n$ the n points in ${\mathbb{F}_q}^m$. The *Reed-Muller code* $RM_q(s, m)$ is defined as the image of the map

$$\begin{aligned} \mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant_s} &\xrightarrow{\varphi_s} {\mathbb{F}_q}^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)), \end{aligned}$$

where $\mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant_s}$ is the subspace of $\mathbb{F}_q[x_1, \ldots, x_m]$ of polynomials with total degree $\leqslant_s$. Notice that Reed–Solomon codes are a particular case of Reed-Muller codes. Let $A = \mathbb{F}_q[x_1, \ldots, x_m]$ and let $\ll$ be the graded lexicographic order on monomials in A, with $x_1 < x_2 < \cdots < x_m$. Let z_i be the ith monomial with respect to $\ll$. It can be shown that $\ll$ induces an order function ρ on A such that $\rho(z_i) = i$ (see [13]). Let l be such that $z_l = x_m^s$, then $z_{l+1} = x_1^{s+1}$. Consequently, $\mathbb{F}_q[x_1, \ldots, x_m]_{\leqslant_s}$ is the space generated by $\{z_i \mid i \leqslant l\}$. Now, take $A = \mathbb{F}_q[x_1, \ldots, x_m]$, ρ the order function induced by $\ll$ and $\varphi : f \mapsto (f(P_1), \ldots, f(P_n))$, and obtain $E_l = \mathrm{RM}_q(s, m)$. By letting l vary in $\mathbb{N}_0$, we get many more codes, in addition to the usual Reed–Muller codes.

Example 3 One-point Goppa codes Another important example is given by the valuation of functions on a rational point P of a function field $F/\mathbb{F}$. Let A be the ring of functions in F which have poles only at P. Let v_P be the valuation of F associated with P and let $\Lambda = \{-v_P(f) \mid f \in A\}$. Enumerate the elements of Λ so that $\Lambda = \{-v_i \mid i \in \mathbb{N}_0\}$ with $-v_i < -v_{i+1}$. Define $\rho(f)$ to be -1 if $f = 0$ and i if $f \neq 0$ and $v_P(f) = v_i$. Then ρ is an order function on A.

Let $P_1, \ldots, P_n$ be pairwise distinct rational points of $F/\mathbb{F}$ which are different from P and let φ be the map $A \to \mathbb{F}^n$ such that $f \mapsto (f(P_1), \ldots, f(P_n))$. The mth evaluation code related to A, ρ and φ is $E_m = \{\varphi(f) \mid v_P(f) \leqslant v_m\}$.

Order-prescribed evaluation codes

We continue with A, an $\mathbb{F}$-algebra over a finite field, ρ, an order function on A and $\varphi : A \to \mathbb{F}^n$, a surjective morphism of $\mathbb{F}$-algebras. We also fix a subset $\{z_i, i \in \mathbb{N}_0\}$ of A such that $\rho(z_i) = i$ for all i. This set is an $\mathbb{F}$-basis of A, which we call a *ρ-good basis* of A.

Definition 3 *Given a subset W of $\mathbb{N}_0$, define the order-prescribed evaluation code related to W as the $\mathbb{F}$-subspace E_W generated by $\{\varphi(z_i) \mid i \in W\}$. Define C_W to be the dual code $C_W = \{c \in \mathbb{F}^n \mid c \cdot \varphi(z_i) = 0 \text{ for all } i \in W\}$.*

Evaluation codes are a particular case of order-prescribed evaluation codes. Indeed, the mth evaluation code C_m is the order-prescribed evaluation code C_W with W equal to $\{0, 1, \ldots, m\}$. Notice that the evaluation codes are independent of the choice of a ρ-good basis, but order-prescribed evaluation codes do depend on the choice.

The interest in order-prescribed evaluation codes is that, by choosing proper subsets, we can get codes that have better parameters than evaluation codes.

3 Algebraic tools for decoding

In this section, we define the structures used by the BMS algorithm and the majority voting algorithm. We give the key results underlying the validity of the algorithms.

Let $W \subset \mathbb{N}_0$, let $c \in C_W$ and let $e \in \mathbb{F}^n$ be an error vector.

The *error ideal* is defined by

$$I^e = \{f \in A \mid \varphi(f)_i = 0 \ \forall i \text{ such that } e_i \neq 0\}.$$

The remark preceding Definition 2 shows that $I^e = \cap_{i|e_i \neq 0} \mathfrak{m}_i$. For any j such that $e_j = 0$, the ideal $\cap_{i|e_i \neq 0} \mathfrak{m}_i$ is not contained in $\mathfrak{m}_j$, [2, Proposition 1.11]. Consequently, there is some $g \in I^e \setminus \mathfrak{m}_j$ such that $\varphi(g)_j \neq 0$. Thus the error ideal satisfies

$$\{i \mid \varphi(f)_i = 0 \ \forall f \in I^e\} = \{i \mid e_i \neq 0\}.$$

For any subset S of $\mathbb{N}_0$, we denote by $\min_{\preccurlyeq} S$ the set of minimal elements of S relative to the partial order $\preccurlyeq$ of section 2 (similarly for $\max_{\preccurlyeq} S$). We define the following subsets of $\mathbb{N}_0$:

$$\begin{aligned} \Sigma^e &= \rho(I^e \setminus \{0\}), \\ \sigma^e &= \min_{\preccurlyeq}(\Sigma^e), \\ \Delta^e &= \mathbb{N}_0 \setminus \Sigma^e, \\ \delta^e &= \max_{\preccurlyeq}(\Delta^e). \end{aligned}$$

The set Δ^e is called the *footprint* of e [12]. Its cardinality is the number of nonzero positions of the error word. Moreover, for each $a \in \mathbb{N}_0$ and $s \in \Sigma^e$, $a \oplus s \in \Sigma^e$. Consequently, if $a \in \Delta^e$ then $N_a \subseteq \Delta^e$. For these results see [13] and [18, 1.13]. The interest of these definitions is due to the next proposition.

Proposition 1 *For each $s \in \sigma^e$ let $f_s \in I^e$ satisfy $\rho(f_s) = s$. Then $\{f_s \mid s \in \sigma^e\}$ generates I^e.*

Proof See Ref. [18].

The set $\{f_s \mid s \in \sigma^e\}$ will be called a *Gröbner basis* for I^e. Now, for $v \in \mathbb{F}^n$ and $f \in A$, define the *v-syndrome* of f as

$$S^v(f) = v \cdot \varphi(f).$$

Note that $S^e(fg) = (e * \varphi(f)) \cdot \varphi(g)$. So we have $f \in I^e \iff e * \varphi(f) = 0 \iff (e * \varphi(f)) \cdot v = 0 \ \forall v \in \mathbb{F}^n$ and since φ is surjective, this is equivalent to $S^e(fg) = 0 \ \forall g \in A$. Hence, $f \in I^e$ if and only if all multiples f' of f satisfy $S^e(f') = 0$. This discussion motivates the following definition.

Definition 4 *For $f \in A \setminus I^e$ let*

$$\begin{aligned} \operatorname{span}(f) &= \min\{\rho(g) \mid S^e(fg) \neq 0\}, \\ fail(f) &= \rho(f) \oplus \operatorname{span} f \\ &= \min\{\rho(fg) \mid S^e(fg) \neq 0\}. \end{aligned}$$

For $f \in I^e$ set $\operatorname{span}(f) = \operatorname{fail}(f) = \infty$.

The three following lemmas are the basis for the updating step in the BMS algorithm.

Lemma 2 *Let $f \notin I^e$. Then $span(f) = b$ if and only if*

1. *$S^e(fg) = 0$ for all $g \in A$ with $\rho(g) < b$, and*
2. *$S^e(fg) \neq 0$ for all $g \in A$ with $\rho(g) = b$.*

Consequently, when $span(f) = b$, any $g \in A$ with $\rho(g) = b$ has $span(g) \leqslant \rho(f)$ and $fail(g) \leqslant fail(f)$.

Proof From the definition of span we see that the conditions (1) and (2) of the lemma imply $\operatorname{span}(f) = b$. Conversely, if $\operatorname{span}(f) = b$ then condition (1) is satisfied and there exists some g with $\rho(g) = b$ such that $S^e(fg) \neq 0$. Let h also satisfy $\rho(h) = b$. By C3, there is some $\lambda \in \mathbb{F}^*$ such that $h + \lambda g = g'$ has order less than b. Then $0 = S^e(fg') = S^e(fh) + \lambda S^e(fg)$, so $S^e(fh) = -\lambda S^e(fg) \neq 0$. Thus condition (2) is satisfied.

Lemma 3 *Suppose $\rho(f) = s$ and $fail(f) = m$. Then $\rho(fz_b) = s \oplus b$ and $fail(fz_b) \geqslant m$ with equality if and only if $m \succcurlyeq s \oplus b$.*

Proof For any j with $s \oplus b \oplus j < m$, we have $b \oplus j < m \ominus s$, so by the previous lemma, $S^e(fz_bz_j) = 0$. Thus $\operatorname{fail}(fz_b)$ is at least m. If $m \not\succcurlyeq s \oplus b$ then $\operatorname{fail}(fz_b)$ is larger than m. Otherwise, there is some j such that $m = s \oplus b \oplus j$. Then $S^e(fz_bz_j) \neq 0$ by the previous lemma, so $\operatorname{fail}(fz_b) = m$.

Lemma 4 *Suppose* $\operatorname{span}(f) = \operatorname{span}(f')$. *There exists an $\alpha \in \mathbb{F}^*$ such that* $\operatorname{span}(f + \alpha f') > \operatorname{span}(f)$.

Proof Let $b = \operatorname{spain}(f)$. By linearity of S^e, for any $\alpha \in \mathbb{F}$, and for all g with $\rho(g) < b$ we have $S^e((f + \alpha f')g) = 0$. Thus $\operatorname{span}(f + \alpha f') \geqslant b$. Let $\alpha = -S^e(fz_b)/S^e(f'z_b)$. By Lemma 2, α is well-defined and nonzero. Furthermore $S^e((f + \alpha f')z_b) = 0$. Thus Lemma 2 says that $\operatorname{span}(f + \alpha f')$ cannot be b. It must therefore be larger than b.

Definition 5 *If $m \in \mathbb{N}_{-1}$, define $I_m = \{f \in A \mid fail(f) > m\}$ and let*

$$\begin{aligned} \Sigma_m &= \{\rho(f) \mid f \in I_m\}, \\ \sigma_m &= \min_{\preccurlyeq} \Sigma_m, \\ \Delta_m &= \mathbb{N}_0 \setminus \Sigma_m, \\ \delta_m &= \max_{\preccurlyeq} \Delta_m. \end{aligned}$$

For any $f \in A$, $\text{fail}(f) \geqslant 0$ so $I_{-1} = A$. It is also clear that $I_{m+1} \subseteq I_m$ and that $I^e = \cap_{m\in\mathbb{N}} I_m$. Consequently $\Sigma_{m+1} \subseteq \Sigma_m$ and $\Sigma^e = \cap_{m\in\mathbb{N}} \Sigma_m$. In general, I_m is not an ideal, but the idea of the Gröbner basis for I^e can be extended to I_m. For each $s \in \sigma_m$ let f_s satisfy $\rho(f_s) = s$ and $f_s \in I_m$. We call $\{f_s \mid s \in \sigma_m\}$ a *Gröbner subset* of I_m. Our interest in the sets I_m is that for m large enough, a Gröbner subset of I_m is a Gröbner basis of I^e (Proposition 10).

Proposition 5 *With the notation above,*

1. *I_m is closed under multiplication by elements of A.*
2. *For any $s \in \Sigma_m$ and $a \in \mathbb{N}$, we have $s \oplus a \in \Sigma_m$.*
3. *For any $a \in \Delta_m$, $N_a \subseteq \Delta_m$.*

Proof Let $f \in I_m$, so $\text{fail}(f) > m$. By the definition of fail, $S^e(fh) = 0$ whenever $\rho(fh) \leqslant m$. Consequently, for any $g \in A$, $S^e(fgh) = 0$ whenever $\rho(fgh) \leqslant m$. Thus $\text{fail}(fg) > m$.

For any $s \in \Sigma_m$ and $a \in \mathbb{N}$, let $f \in I_m$ satisfy $\rho(f) = s$. Since $fz_a \in I_m$, $\rho(fz_a) = s \oplus a \in \Sigma_m$.

Let $a \in \Delta_m$ and let $b \preccurlyeq a$. If b were in Σ_m, then the previous paragraph would say that $a \in \Sigma_m$. Thus $b \in \Delta_m$.

The following key result gives an intrinsic characterization of Δ_m.

Proposition 6 *For each $m \in \mathbb{N}_0$, $\Delta_m = \{span(f) \mid f \notin I_m\}$. Furthermore $a \in \Delta_m \setminus \Delta_{m-1}$ if and only if $a \preccurlyeq m$ and $m \ominus a \in \Delta_m \setminus \Delta_{m-1}$.*

Proof Let Υ_m denote the set $\{\text{span}(f) \mid f \notin I_m\}$.

First, let us prove the inclusion $\Delta_m \supseteq \Upsilon_m$. Suppose $b \in \Upsilon_m$. Then there exists $f \in A$ with $\text{span}(f) = b$ and $\text{fail}(f) \leqslant m$. By Lemma 2, for all g such that $\rho(g) = b$, $S^e(fg) \neq 0$, and $\text{fail}(g) \leqslant \text{fail}(f) = m$. Therefore $b \in \Delta_m$.

We will use induction on m to prove the inclusion $\Delta_m \subseteq \Upsilon_m$. For $m = -1$ it is obvious, since $I_{-1} = A$ and therefore $\Delta_{-1} = \emptyset$.

Now suppose $m \geqslant 0$ and $a \in \Delta_m$. If $a \in \Delta_{m-1}$ then $\text{fail}(f) < m$ for all f with $\rho(f) = a$. By the induction hypothesis, there exists g such that $a = \text{span}(g)$ and $g \notin I_{m-1}$. Since $I_m \subseteq I_{m-1}$, $g \notin I_m$. Thus, $a \in \Upsilon_m$. If, on the other hand, $a \in \Delta_m \setminus \Delta_{m-1}$, there exists f with $\rho(f) = a$ and $\text{fail}(f) = m$, so $a \preccurlyeq m$. We will show that there exists g with $\rho(g) = m \ominus a$ and $\text{fail}(g) = m$. Then $a = \text{span}(g) \in \Upsilon_m$ as claimed. This also shows that $a \in \Delta_m \setminus \Delta_{m-1}$ if and only if $m \ominus a \in \Delta_m \setminus \Delta_{m-1}$.

By Lemma 2, any g with $\rho(g) = m \ominus a$, satisfies $\text{fail}(g) \leqslant m$. Suppose, contrary to the claim above, any such g actually satisfies $\text{fail}(g) < m$. Then $m \ominus a \in \Delta_{m-1}$, and by the induction hypothesis, there exists h such that $\text{span}(h) = m \ominus a$ and

$h \notin I_{m-1}$. Then $\rho(h) = \text{fail}(h) \ominus \text{span}(h) < m \ominus (m \ominus a)$ so $\rho(h) < \rho(f)$. By Lemma 4, there is a $\lambda \in \mathbb{F}^*$ such that $\text{span}(f + \lambda h) > m \ominus a$. Thus we have $\rho(f+\lambda h) = a$ and $\text{fail}(f+\lambda h) > m$. This contradicts $a \in \Delta_m$, so our assumption that there is no g with $\rho(g) = m \ominus a$ and $\text{fail}(g) = m$ was incorrect. This completes the proof.

This corollary will be useful in the decoding algorithm.

Corollary 7 *With respect to the partial order $\preccurlyeq$,*

1. *c is minimal in $\Delta_m \setminus \Delta_{m-1}$ if and only if $m \ominus c$ is maximal in $\Delta_m \setminus \Delta_{m-1}$.*
2. *If c is maximal in $\Delta_m \setminus \Delta_{m-1}$ then c is maximal in Δ_m.*
3. *$\delta_m = \max_{\preccurlyeq}(\delta_{m-1} \cup \{m \ominus s \mid s \in (\sigma_{m-1} \cap \Delta_m)\})$.*

Proof Item (1) follows immediately from $b \preccurlyeq c \preccurlyeq m$ implies $m \ominus c \preccurlyeq m \ominus b$. For (2), we need to show there is no $b \in \Delta_{m-1}$ with $b \succcurlyeq c$ and $b \neq c$. This follows from Proposition 6 item (2); since $c \in \Sigma_{m-1}$ and $b \succcurlyeq c$ implies $b \in \Sigma_{m-1}$. For (3), we note that $\{m \ominus s \mid s \in (\sigma_{m-1} \cap \Delta_m)\} = \max_{\preccurlyeq}(\Delta_m \setminus \Delta_{m-1})$. Thus item (3) says that $\max_{\preccurlyeq} \Delta_m = \max_{\preccurlyeq}(\max_{\preccurlyeq}(\Delta_{m-1}) \cup \max_{\preccurlyeq}(\Delta_m \setminus \Delta_{m-1}))$. This result holds for any partition of a partially ordered set.

From the remarks after Definition 5, it is clear that $\Delta^e = \cup_{m \in \mathbb{N}_0} \Delta_m$ and that $\Delta_m \subseteq \Delta_{m+1}$. Since Δ^e is a finite set, it is equal to Δ_m for m large enough. We now give an upper bound.

Proposition 8 *Let $c_{\max}$ be the largest integer in Δ^e. Then, for $m \geqslant c_{\max} \oplus c_{\max}$, $\Delta_m = \Delta^e$.*

Proof Let $M = c_{\max} \oplus c_{\max}$. We need only show that $\Delta_M \supseteq \Delta^e$. Suppose $a \in \Delta^e$. Then $a \in \Delta_k$ for some k and we may choose k minimal in this regard. By Proposition 6, $k \ominus a \in \Delta_k$ also. Since a and $k \ominus a$ are both less than $c_{\max}$, $k = a \oplus (k \ominus a) < c_{\max} \oplus c_{\max}$. Thus $a \in \Delta_M$.

Corollary 9 $\Delta^e = \{\text{span}(f) \mid f \notin I^e\}$.

Proof By Lemma 2, $\{\text{span}(f) \mid f \notin I^e\} \subseteq \Delta^e$. On the other hand, by Propositions 6 and 8, for $M = c_{\max} \oplus c_{\max}$, $\Delta^e = \Delta_M = \{\text{span}(f) \mid f \notin I_M\} \supseteq \{\text{span}(f) \mid f \notin I^e\}$.

The final result of this section identifies when the computation of the Gröbner basis for the error locator ideal is complete.

Proposition 10 *Let $s_{\max}$ be the largest integer in σ^e and let $M = c_{\max} \oplus \max\{c_{\max}, s_{\max}\}$. For any $m \geqslant M$, if F_m is a Gröbner subset of I_m, then F_m is a Gröbner basis of I^e.*

Proof By Proposition 8, $\Sigma_m = \Sigma^e$ and obviously, $\sigma_m = \sigma^e$. A Gröbner subset of I_m contains, for each $s \in \sigma^e$ one $f_s \in I_m$ with $\rho(f_s) = s$. Suppose $f_s \notin I^e$. By Corollary 9, $\text{span}(f_s) \in \Delta^e$ and $\text{fail}(f_s) = \text{span}(f_s) \oplus \rho(f_s) \leqslant c_{\max} \oplus s \leqslant c_{\max} \oplus s_{\max} \leqslant m$. So, $f_s \notin I_m$, a contradiction.

4 Localization of errors

We have defined a Gröbner subset of I_m to be a collection of elements in I_m containing, for each $s \in \sigma_m$, a unique element with order s. For each $c \in \delta_m$, Proposition 6 asserts that there is a $g_c \in A \setminus I_m$ such that $\mathrm{span}(g_c) = c$ and $\mathrm{fail}(g_c) \leqslant m$. We call a set of such g_c a *Gröbner complementary subset* for I_m.

The data structures computed in the BMS algorithm are σ_m, δ_m, F_m – a Gröbner subset of I_m – and G_m – a Gröbner complementary subset for I_m. In this section we show how to compute the data σ_m, δ_m, F_m and G_m from the data σ_{m-1}, δ_{m-1}, F_{m-1} and G_{m-1}. By Proposition 10, repeating this procedure yields, for m large enough, a Gröbner basis for I^e. If $s \in \sigma_m$ we will denote by $F_m(s)$ the element in F_m with order equal to s and if $c \in \delta_m$, we will denote by $G_m(c)$ the element in G_m with span equal to c.

From Propositions 5 and 6, we have the following. Suppose $s \in \sigma_{m-1}$ and $m \ominus s \in \Sigma_{m-1}$. Then $\mathrm{fail}(F_{m-1}(s)) = m$ if and only if $s, m \ominus s \in \Delta_m$. When this holds, $m \ominus s$ is maximal in Δ_m. The other maximal elements of Δ_m must be maximal in Δ_{m-1}. Thus we have the following result.

Proposition 11 *The computation of δ_m and G_m from the data for $m-1$ is as follows. Let*

$$\delta' = \{m \ominus s \mid s \in \sigma_{m-1},\ fail(F_{m-1}(s)) = m, \text{ and } m \ominus s \notin \Delta_{m-1}\}.$$

Then

$$\delta_m = \max_{\preccurlyeq}(\delta_{m-1} \cup \delta'),$$

$$G_m(c) = \begin{cases} G_{m-1}(c) & \text{if } c \in \delta_{m-1}, \\ F_{m-1}(m \ominus c) & \text{else.} \end{cases}$$

From δ_m, Δ_m is easily computed, and then σ_m is the set of minimal elements of $\mathbb{N} \setminus \Delta_m$. So, our interest is now in finding, for any $s \in \sigma_m$, an $f \in A$ with $\rho(f) = s$ and $\mathrm{fail}(f) > m$.

Proposition 12 *Let F_{m-1} be a Gröbner subset and let G_{m-1} be a Gröbner complementary subset for I_{m-1}. Let $t \in \sigma_m$, and let $s \in \sigma_{m-1}$ and $a \in \mathbb{N}_0$ be such that $t = s \oplus a$.*

1. *If $t \not\preccurlyeq m$ or $m \ominus t \in \Sigma_{m-1}$ then*

$$\rho(F_{m-1}(s)z_a) = t,$$
$$fail(F_{m-1}(s)z_a) > m.$$

2. *If $m \ominus t \in \Delta_{m-1}$, let $c \in \delta_{m-1}$ and $b \in \mathbb{N}_0$ be such that $m \ominus t = c \ominus b$. Then*

$$\rho(F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b) = t,$$
$$fail(F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b) > m.$$

where $\mu = S^e(F_{m-1}(s)z_a z_{c\ominus b})/S^e(G_{m-1}(c)z_b z_{c\ominus b})$.

Proof First we establish the claim about the order. Note that $\rho(F_{m-1}(s)z_a) = s \oplus a = t$. In the case where $m \ominus t = c \ominus b$,

$$\rho(G_{m-1}(c)) = \text{fail}(G_{m-1}(c)) \ominus \text{span}(G_{m-1}(c)) < m \ominus c.$$

Thus $\rho(G_{m-1}(c)z_b) < (m \ominus c) \oplus b = t$. Consequently, by C2, $\rho(F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b) = t$.

For the claims about fail, suppose first that $t \not\preccurlyeq m$. Then by Lemma 3, $\text{fail}(F_{m-1}(s)z_a) > m$. Next suppose $m \ominus t \in \Sigma_{m-1}$. We claim $\text{fail}(F_{m-1}(s)) > m$, so in fact $t = s$ and $a = 0$. Using $m \ominus s \geqslant m \ominus t$ and Propositions 3 and 4 we have the following:

$$\begin{aligned} \text{fail}(F_{m-1}(s)) = m &\Longrightarrow m \ominus s \in \Delta_m \setminus \Delta_{m-1} \\ &\Longrightarrow m \ominus t \in \Delta_m \setminus \Delta_{m-1} \\ &\Longrightarrow t \in \Delta_m \setminus \Delta_{m-1}. \end{aligned}$$

This is a contradiction to $t \in \Sigma_m$.

Finally, consider $t \preccurlyeq m$ and $m \ominus t \in \Delta_{m-1}$. Let $c \in \delta_{m-1}$ and $b \in \mathbb{N}_0$ be such that $m \ominus t = c \ominus b$. By Lemma 3,

$$\begin{aligned} \text{span}(G_{m-1}(c)z_b) &= c \ominus b, \\ \text{span}(F_{m-1}(s)z_a) &= m \ominus t. \end{aligned}$$

Since these are equal, Lemma 4 and its proof show that with μ as given in the statement of the proposition, $F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b$ has span strictly larger than $m \ominus t$. Since $\rho(F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b) = t$ we get $\text{fail}(F_{m-1}(s)z_a - \mu G_{m-1}(c)z_b) > m$.

Combining the last two results we have an algorithm for computing a Gröbner basis for I^e. Since $I_{-1} = A$ we initialize $\sigma^{-1} = \{0\}$, $\delta^{-1} = \emptyset$, $F^{-1}(0) = 1$ and $G^{-1} = \emptyset$. Then for m from 0 to $c_{\max} \oplus \max\{c_{\max}, s_{\max}\}$ do the following:

Input: $\sigma_{m-1}, \delta_{m-1}, F_{m-1}, G_{m-1}$ and syndromes with order up to m.
Step 1: Compute $\delta' = \{m \ominus s \mid S^e(F_{m-1}(s)z_{m\ominus s}) \neq 0\}$.
Step 2: Compute $\delta_m = \max_{\preccurlyeq}(\delta_{m-1} \cup \delta')$.
Step 3: Compute $\sigma_m = \min_{\preccurlyeq}(\mathbb{N}_0 \setminus \{a \mid a \preccurlyeq c \text{ for some } c \in \delta_m\})$.
Step 4: For each $t \in \sigma_m$ compute $F_m(t)$ according to Proposition 12.
Output: $\sigma_m, \delta_m, F_m, G_m$.

5 Majority voting for syndromes

In this section we will show how to compute $S^e(z_m)$ from $S^e(z_i)$ for $0 \leqslant i < m$ and from the data F_{m-1}. The algorithm is based on a voting function v defined on a subset Γ_m of N_m – to be defined in a moment – and taking values in $\mathbb{F}$. If a majority of the votes agree then we take $S^e(z_m)$ to be the value on which they agree. If there is no majority agreement then the algorithm fails. We will derive a simple condition for success of the algorithm, which depends only on the footprint of e and the set N_m. The condition is $\nu_m > 2|N_m \cap \Delta^e|$ where $\nu_m = |N_m|$.

Definition 6 *let* $\Gamma_m = \{s \in \Sigma_{m-1} \mid s \preccurlyeq m, \text{and } m \ominus s \in \Sigma_{m-1}\}$.

We make several observations about the set Γ_m. First, $\Sigma_m \cap \Gamma_m$ and $\Delta_m \cap \Gamma_m$ partition Γ_m. Second, $\Delta_m \cap \Gamma_m = \Delta_m \setminus \Delta_{m-1}$. The containment $\Delta_m \cap \Gamma_m \subseteq \Delta_m \setminus \Delta_{m-1}$ is immediate. The reverse containment follows from Proposition 6 which says that if $a \in \Delta_m \setminus \Delta_{m-1}$ then $a \preccurlyeq m$ and $m \ominus a \in \Delta_m \setminus \Delta_{m-1}$. A third

observation is that each set of the partition of Γ_m is fixed when subtracted from m. That is $a \in \Delta_m \cap \Gamma_m$ if and only if $m \ominus a \in \Delta_m \cap \Gamma_m$ and similarly – it is just the contrapositive – $a \in \Sigma_m \cap \Gamma_m$ if and only if $m \ominus a \in \Sigma_m \cap \Gamma_m$. This also follows from Proposition 6 and the observation that $\Delta_m \cap \Gamma_m = \Delta_m \setminus \Delta_{m-1}$.

For each $m \in \mathbb{N}_0$ we define a voting function v on the set Γ_m as the composition of the two maps v_1 and v_2 described below.

Let $a \in \Gamma_m$. Since $\Gamma_m \subseteq \Sigma_{m-1}$ it is possible to choose some $s \in \sigma_{m-1}$ with $s \preccurlyeq a$. Since $a \preccurlyeq m$ we get $s \preccurlyeq m$ so $s \in \sigma_{m-1} \cap \Gamma_m$. Thus we can define $v_1 : \Gamma_m \to \sigma_{m-1} \cap \Gamma_m$ such that $v_1(a) \preccurlyeq a$. Note that v_1 is not uniquely defined.

Now let $s \in \sigma_{m-1} \cap \Gamma_m$. Note that $m \ominus s$ is well defined since $s \in \Gamma_m$. Let α be the unique element of $\mathbb{F}^*$ such that $\rho(z_m + \alpha F_{m-1}(s) z_{m \ominus s}) < m$. Define $v_2 : \sigma_{m-1} \cap \Gamma_m \to \mathbb{F}$ by $v_2(s) = S^e(z_m + \alpha F_{m-1}(s) z_{m \ominus s})$. The map v_2 may be computed from $S^e(z_i)$ for $i < m$ since $\rho(z_m + \alpha F_{m-1}(s) z_{m \ominus s}) < m$.

Let v be the composition $\Gamma_m \xrightarrow{v_1} \sigma_{m-1} \cap \Gamma_m \xrightarrow{v_2} \mathbb{F}$.

Proposition 13 *Let $a \in \Gamma_m$. Then $a \in \Sigma_m$ if and only if $v_2 \circ v_1(a) = S^e(z_m)$.*

Proof The proof has two parts. First we show that $a \in \Sigma_m$ if and only if $v_1(a) \in \Sigma_m$. Second, we show that for $s \in \sigma_{m-1} \cap \Gamma_m$, $s \in \Sigma_m$ if and only if $v_2(s) = S^e(z_m)$. This gives the result.

Suppose $a \in \Gamma_m$ and $s \in \sigma_{m-1}$ with $s \preccurlyeq a$. Then $m \ominus a \preccurlyeq m \ominus s$. We use Proposition 5 and the observation that $\Sigma_m \cap \Gamma_m$ is closed under subtraction from m in the following

$$\begin{aligned} s \in \Sigma_m &\implies a \in \Sigma_m \\ &\implies m \ominus a \in \Sigma_m \\ &\implies m \ominus s \in \Sigma_m \\ &\implies s \in \Sigma_m. \end{aligned}$$

The chain of implications must be a chain of equivalences, so $s \in \Sigma_m \iff a \in \Sigma_m$.

Now let $s \in \sigma_{m-1} \cap \Gamma_m$. By assumption, $F_{m-1}(s)$ has fail at least m. Now for any $\alpha \in \mathbb{F}^*$,

$$\begin{aligned} \mathrm{fail}(F_{m-1}(s)) > m &\iff S^e(F_{m-1}(s) z_{m \ominus s}) = 0 \\ &\iff S^e(z_m + \alpha F_{m-1}(s) z_{m \ominus s}) = S^e(z_m). \end{aligned}$$

So $s \in \Sigma_m$ if and only if $v_2(s) = S^e(z_m)$ as claimed.

The following corollary is immediate from the proposition.

Corollary 14 *A majority of Γ_m votes for $S^e(z_m)$ if and only if $|\Sigma_m \cap \Gamma_m| > |\Delta_m \cap \Gamma_m|$.*

Now we have the algorithm.

Input: σ_{m-1}, F_{m-1} and the syndromes of order up to $m-1$.
Step 1: Compute Γ_m.
Step 2: Compute $\sigma_{m-1} \cap \Gamma_m$.
Step 3: Compute v_1. For each $a \in \Gamma_m$, find $s \in \sigma_m$ with $s \preccurlyeq a$. Set $v_1(a) = s$.
Step 4: Compute v_2:
- ▷ For each $s \in \sigma_m \cap \Gamma_m$ find α such that $\rho(z_m + \alpha F_{m-1}(s) z_{m \ominus s}) < m$.
- ▷ Set $v_2(s) = S^e(z_m + \xi f^{s_a} z_{m \ominus s_a})$.

Output: If a majority of the elements of Γ_m have the same image under $v_2 \circ v_1$ output that image. Else abort.

The following theorem gives a condition for voting to be successful at $m \in \mathbb{N}_0$, based only on the footprint of e and the set $N_m = \{a \in \mathbb{N}_0 \mid a \preccurlyeq m\}$. The theorem may be used to design a code. Let W be the subset of $\mathbb{N}_0$ for which the condition is satisfied. For the code C_W, the combination of the BMS algorithm and majority voting will correct all vectors with the same footprint as e.

Proposition 15 *Let e be an error vector with footprint Δ^e and let $m \in \mathbb{N}_0$ be such that*

$$\nu_m > 2\,|N_m \cap \Delta^e|. \tag{1}$$

Then $|\Sigma_m \cap \Gamma_m| > |\Delta_m \cap \Gamma_m|$. Therefore the voting algorithm for $S^e(z_m)$ will be successful.

Proof We consider the following partition of N_m.

$$\begin{aligned} T_m &= \{c \in N_m \mid c \in \Sigma^e \text{ and } m \ominus c \in \Sigma^e\},\\ U_m &= \{c \in N_m \mid c \in \Sigma^e \text{ and } m \ominus c \in \Delta^e\},\\ X_m &= \{c \in N_m \mid c \in \Delta^e \text{ and } m \ominus c \in \Sigma^e\},\\ Y_m &= \{c \in N_m \mid c \in \Delta^e \text{ and } m \ominus c \in \Delta^e\}. \end{aligned}$$

We have,

$$\begin{aligned} N_m \cap \Sigma^e &= T_m \cup U_m,\\ N_m \cap \Delta^e &= X_m \cup Y_m. \end{aligned}$$

Now, assumption (1) 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 (1) is equivalent to

$$|T_m| > |Y_m|. \tag{2}$$

Since $\Sigma_m \cap \Gamma_m \supseteq T_m$ and $Y_m \supseteq \Delta_m \cap \Gamma_m$, we can conclude that (1) implies $|\Sigma_m \cap \Gamma_m| > |\Delta_m \cap \Gamma_m|$. That is, voting is successful for m.

Since $|\Delta^e| = \mathrm{wt}(e)$ we have the following.

Corollary 16 *If $wt(e) = t$ and $\nu_m > 2t$ then the voting algorithm is successful.*

6 Designing codes for prescribed correction capability

Our aim in this section is to take advantage of two improvements to standard evaluation codes. As before A is an $\mathbb{F}$ algebra with order function ρ and ρ-good basis $\{z_i, i \in \mathbb{N}_0\}$; $\varphi : A \longrightarrow \mathbb{F}^n$ is a surjective morphism of $\mathbb{F}$-algebras. We will choose subsets $W \subset \mathbb{N}_0$ and consider the correction capability under the BMS algorithm with majority voting of the codes $C_W = \{c \in \mathbb{F}^n \mid c \cdot \varphi(z_i) = 0 \text{ for all } i \in W\}$.

Definition 7 (Standard evaluation codes) *To design a standard evaluation code (using Definition 2) which will correct t errors, let* $m(t) = \max\{r \in \mathbb{N}_0 \mid \nu_r < 2t+1\}$. *Let* $R(t) = \{r \in \mathbb{N}_0 \mid r \leqslant m(t)\}$ *and* $r(t) = |R(t)|$.

The code $C_{R(t)}$ *has minimum distance at least* $2t+1$.

Definition 8 (Feng–Rao improved codes) *To design an order-prescribed evaluation code correcting t errors, we take* $\widetilde{R}(t) = \{r \in \mathbb{N}_0 \mid \nu_r < 2t+1\}$ *and use the code* $C_{\widetilde{R}(t)}$.

Feng and Rao [10] discovered that their majority voting algorithm could be used to correct t errors for these improved codes. We can see this result from Corollary 16. The set $\widetilde{R}(t)$ is crafted exactly to ensure that for $m \notin \widetilde{R}(t)$ the condition of the corollary is satisfied, so majority voting is successful. Let $\widetilde{r}(t) = |\widetilde{R}(t)|$. The Feng–Rao improved code correcting t errors requires $r(t) - \widetilde{r}(t)$ fewer check symbols than the standard code correcting t errors.

The approach suggested in [17] is to aim to correct only the most likely errors of weight less than t.

Definition 9 *An error word e of weight t is said to be generic if* $\Delta^e = \{0, 1, \ldots, t-1\}$, *or equivalently, if* $\Sigma^e = \{a \in \mathbb{N}_0 \mid a \geqslant t\}$.

Generic errors were also called independent errors in [14,19].

Example 4 Dual Reed–Solomon codes For Reed–Solomon codes, a polynomial of degree less than t cannot vanish at t points. So every error vector is generic.

Example 5 Dual Reed–Muller codes As in Example 2, let $n = q^m$ and call $P_1, \ldots, P_n$ the n points in $\mathbb{F}_q^m$. Let the set of error positions be $I = \{i_1, \ldots, i_t\}$. From the definition, it is clear that a vector e with support I is not generic if and only if there is some nonzero polynomial $\sum_{i=0}^{t-1} \alpha_i z_i$ which vanishes on $P_{i_1}, \ldots, P_{i_t}$. So, the condition of not being generic corresponds to a certain geometric distribution of the points corresponding to error positions.

For instance, suppose $m = 2$, i.e., $A = \mathbb{F}_q[x_1, x_2] = \mathbb{F}_q[x, y]$. For $t = 1$, any error vector is generic; for $t = 2$, e is not generic if and only if P_{i_1}, P_{i_2} lie in a vertical line; for $t = 3$, e is not generic if and only if $P_{i_1}, P_{i_2}, P_{i_3}$ are collinear; for $t = 4$, e is not generic if and only if $P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}$ lie on a vertical parabola or the union of two vertical lines; for $t = 5$, e is not generic if and only if $P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}, P_{i_5}$ lie on a parabola a hyperbola with vertical asymptote or the union of a vertical line and a horizontal line; for $t = 6$, e is not generic if and only if $P_{i_1}, P_{i_2}, P_{i_3}, P_{i_4}, P_{i_5}, P_{i_6}$ are in any conic.

From the previous example it seems reasonable to expect that the probability of a generic error is much higher than the probability of a nongeneric error of the same weight. Experimental results in [17] showed that for a Hermitian code over $\mathbb{F}_{q^2}$, and for weights t less than the genus of the curve, nongeneric errors occurred with proportion roughly $1/q^2$. This motivates the investigation of majority voting for generic errors.

Proposition 17 *For a generic error vector e of weight t, the voting algorithm for* $S^e(z_m)$ *is successful provided* $m \in \{a \oplus b \mid a, b \geqslant t\}$.

Proof Referring back to Proposition 15 and its proof, we see that majority voting is successful when $\nu_m > 2|N_m \cap \Delta^e|$ and that this condition is equivalent to $|T_m| > |Y_m|$ where

$$T_m = \{c \in N_m \mid c \in \Sigma^e \text{ and } m \ominus c \in \Sigma^e\},$$
$$Y_m = \{c \in N_m \mid c \in \Delta^e \text{ and } m \ominus c \in \Delta^e\}.$$

We remark that T_m is nonempty if and only if there are $s, s' \in \Sigma^e$ such that $m = s \oplus s'$. Similarly Y_m is nonempty if and only if there exist $s, s' \in \Delta^e$ such that $s \oplus s' = m$.

For a generic error vector of weight t, the requirement of the proposition, $m \in \{a \oplus b \mid a, b \geqslant t\}$ is saying exactly that T_m is non-empty. In particular, if $m = s \oplus s'$ with $s, s' \geqslant t$ then $m \geqslant t \oplus t$. On the other hand if Y_m is non-empty then there are $c, c' < t$ such that $m = c \oplus c'$. But then $m = c \oplus c' < t \oplus t$. Thus if T_m is nonempty then Y_m is empty.

We conclude that if $m \in \{a \oplus b \mid a, b \geqslant t\}$ then there will be correct votes for $S^e(z_m)$ and there will be no incorrect votes.

Definition 10 (Standard generic evaluation codes) *To design a standard evaluation code (using Definition 2) that will correct all generic errors of weight at most t, let $m^*(t) = \max(\mathbb{N}_0 \setminus \{a \oplus b \mid a, b \geqslant t\})$ and let $R^*(t) = \{r \in \mathbb{N}_0 \mid r \leqslant m^*(t)\}$. The number of check symbols for the code $C_{R^*(t)}$ is $r^*(t) = |R^*(t)|$.*

Definition 11 (Improved generic evaluation codes) *To design an order-prescribed evaluation code correcting t generic errors, we use the code $C_{\widetilde{R}^*(t)}$ where $\widetilde{R}^*(t)$ is $\mathbb{N}_0 \setminus \{a \oplus b \mid a, b \geqslant t\}$. Let $\widetilde{r}^*(t) = |\widetilde{R}^*(t)|$. Clearly $\widetilde{r}^*(t) \leqslant r^*(t)$.*

Example 6 Reed–Muller type codes Recall the Reed–Muller codes from Example 2. In this case, for every $t \in \mathbb{N}_0$,

- $r(t) = \binom{2t-1+m}{m}$,
- $\tilde{r}(t) = \left|\left\{a \in {\mathbb{N}_0}^m \mid \prod_{j=1}^{m}(a_j+1) < 2t+1\right\}\right|$.

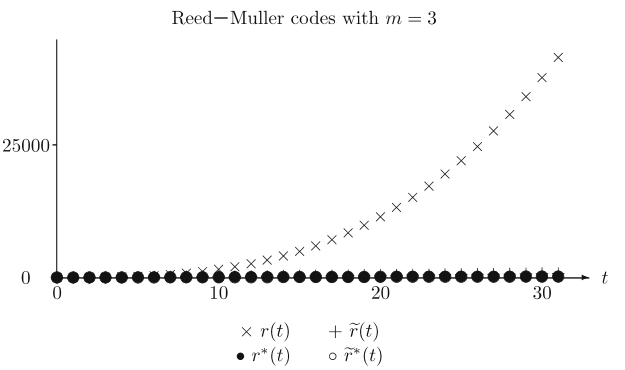
Let $z_t = x_1^{a_1} \cdots x_m^{a_m}$ and let $d = \deg(z_t) = \sum_{i=1}^m a_i$.

1. If $a_1 = a_2 = \cdots = a_{m-1} = 0$, then
   $r^*(t) = \binom{2d-1+m}{m}$,
   $\tilde{r}^*(t) = r^*(t)$.
2. Otherwise,
   - $r^*(t) = \binom{2d+1+m}{m} - \sum_{k=1}^{m} \binom{2d-\sum_{j=1}^{k} a_j+m-k}{m-k}$,
   - $\tilde{r}^*(t) = r^*(t) - 1 - \sum_{k=1}^{m-1}\sum_{j=k}^{m-1} \binom{2d-2-\sum_{i=1}^{j} a_i-\sum_{i=1}^{k} a_i+m-j}{m-j} - \left|\left\{k \mid d - \sum_{i=1}^{k} a_i > 0\right\}\right|$.

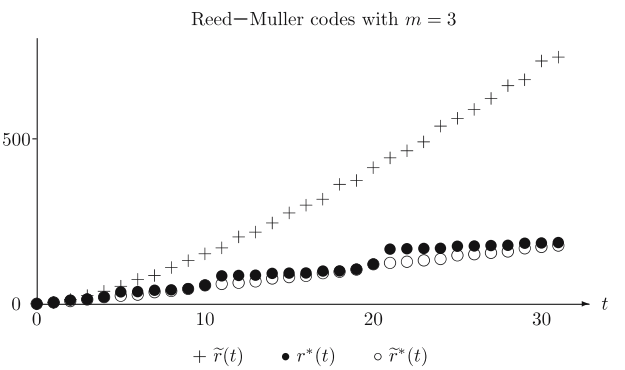
The proof of these results is very technical and therefore omitted for the sake of brevity. One can find it in [5].

Notice that for $m \ll t$, $r(t)$ is $o(t^m)$, while $r^*(t)$ and $\tilde{r}^*(t)$ are $o(t)$. Indeed, $\binom{a+b}{b} = \frac{a\cdot(a-1)\cdots(a-b+1)}{b!}$ is $o(a^b)$ if $a \gg b$. Now, for $m \ll t$, $r(t)$ is $o(t^m)$ while $r^*(t)$ and $\tilde{r}^*(t)$ are $o((\deg(z_t))^m)$. On the other hand, $\deg(z_t)$ is $o(t^{1/m})$, since all polynomials of degree k have order from $\binom{m+k-1}{m}$ to $\binom{m+k}{m} - 1$.

Let $m = 3$. In the following figure we plot $r(t)$, $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$ as a function of t for the first values of t.



Notice that for all t, $r(t)$ is $o(t^3)$ while $r^*(t)$ and $\tilde{r}^*(t)$ are $o(t)$. The function $\tilde{r}(t)$ seems to be also $o(t)$. Since $r(t)$ is much larger than the other three functions, we cannot appreciate the differences between $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$. If we only plot $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$, then the relative behavior of these functions becomes apparent.



Notice that the redundancy for codes correcting generic errors is significantly lower. We also remark that $\tilde{r}^*(t)$ is like a smooth version of $r^*(t)$.

Example 7 Hermitian codes Let q be a prime power. The Hermitian curve over $\mathbb{F}_{q^2}$ may be defined by the affine equation $x^{q+1} = y^q + y$, which has a single rational

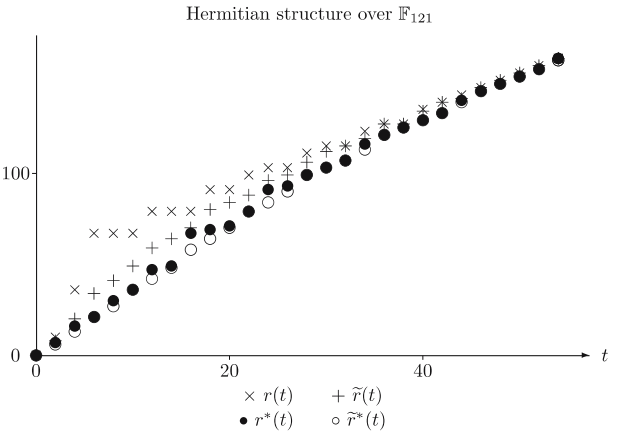
point at infinity. The Weierstrass semigroup at the rational point at infinity is generated by q and $q+1$ (for further details see [13,23]). Now, if the tth nonzero element of the semigroup λ_t is larger than or equal to $q(q-1)$ then $r^*(t) = \tilde{r}^*(t) = \lambda_t + t$. Otherwise, one can prove that it can be written as $Qq + r$ for some unique Q and r with $0 \leqslant r \leqslant Q < q-1$. In this case,

$$r^*(t) = \begin{cases} 2Q^2 + Q & \text{if } 2Q < q,\ r = 0, \\ 2Q^2 + 3Q + r + 1 & \text{if } 2Q < q,\ r > 0, \\ 2Qq + r - \frac{q^2-3q}{2} & \text{if } 2Q \geqslant q,\ r > 2Q - q + 1, \\ 2Qq + 2r - \frac{q^2-q}{2} & \text{if } 2Q \geqslant q,\ r \leqslant 2Q - q + 1, \end{cases}$$

$$\tilde{r}^*(t) = \begin{cases} 2Q^2 + Q + 3r & \text{if } 2Q < q, \\ 2Qq + 3r - 2Q - \frac{q^2-3q}{2} - 1 & \text{if } 2Q \geqslant q,\ r > 2Q - q + 1, \\ 2Qq + 2r - \frac{q^2-q}{2} & \text{if } 2Q \geqslant q,\ r \leqslant 2Q - q + 1. \end{cases}$$

Again, the proof is very technical and is therefore omitted.

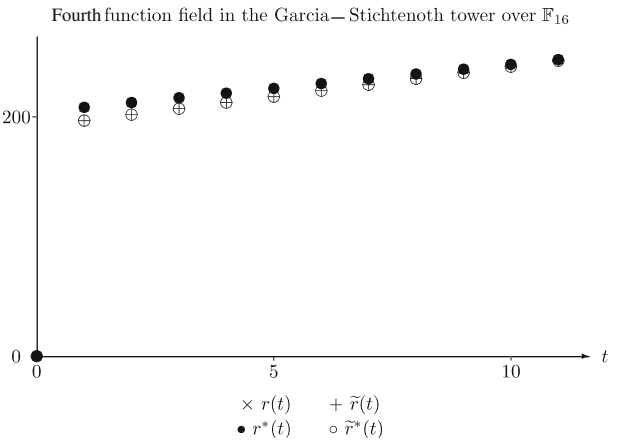
Let us see the behavior of $r(t)$, $\tilde{r}(t)$, $r^*(t)$ and $\tilde{r}^*(t)$ for an example of a Hermitian curve. Notice that in general $r(t) > \tilde{r}(t) > r^*(t) > \tilde{r}^*(t)$ and that the differences are largest for small values of t. As with the example of Reed–Muller codes, $\tilde{r}^*(t)$ is a smoother version of the others.



Example 8 A Garcia–Stichtenoth tower Pellikaan et al. proved in [20] that the numerical semigroups for the codes over $\mathbb{F}_{q^2}$ associated to the tower of Garcia–Stichtenoth presented in [11] attaining the Drinfeld–Vlăduţ bound are given recursively by $\Lambda_1 = \mathbb{N}_0$ and, for $m > 0$,

$$\Lambda_m = q \cdot \Lambda_{m-1} \cup \{i \in \mathbb{N}_0 \mid i \geqslant q^m - q^{\lfloor (m+1)/2 \rfloor}\}.$$

They are examples of Arf numerical semigroups. In the next section we show that for Arf numerical semigroups there is no improvement to code dimension by restricting to generic errors. The next figure shows the graph of $r(t) = r^*(t)$ and $\tilde{r}(t) = \tilde{r}^*(t)$ for all t. Evidently, there is also little gain from the Feng–Rao improvements.



7 Analysis of the improvement

In [1], Arf studied certain curve singularities and associated semigroups. The notion of an Arf numerical semigroup, Definition 14, evolved from that article and subsequent work by Lipman [15]. Recent work includes [3,21]. In this section we introduce Arf order functions, which generalize the Arf property to the semigroup structure on $\mathbb{N}_0$ induced by the order function. We then show that when the order function is Arf the code correcting t generic errors will in fact correct any error vector of weight t. Thus, one cannot do better than the Feng–Rao improved codes. We then consider the special case of weight functions, those order functions for which $(\mathbb{N}_0, \oplus)$ is isomorphic to a numerical semigroup. In this case we give an explicit formula for $\widetilde{r}^*(t)$.

Arf order functions

Definition 12 *We say that an order function ρ is Arf when for all $i, j, k \in \mathbb{N}_0$,*

$$i \preccurlyeq j \oplus k \quad \textit{for all } i \leqslant j \leqslant k.$$

Lemma 18 *An order function ρ is Arf if and only if, for all t, $\{a \oplus b \mid a, b \geqslant t\} = \{a \oplus t \mid a \in \mathbb{N}_0\}$.*

Proof For any order function, $\{a \oplus t \mid a \in \mathbb{N}_0\} \subseteq \{a \oplus b \mid a, b \geqslant t\}$. Suppose the two sets are equal and let $t \leqslant i \leqslant j$. Then $i \oplus j = a \oplus t$ for some $a \in \mathbb{N}_0$ and consequently $j \oplus k \succcurlyeq t$. Thus ρ is Arf. Conversely, if ρ is Arf, and $a, b \geqslant t$ then $a \oplus b \succcurlyeq t$ so $a \oplus b = c \oplus t$ for some $c \in \mathbb{N}_0$. This proves the equality of the two sets.

Proposition 19 *Let $m = a \oplus b$ with $a \leqslant b$ and $b - a$ minimal. Then*

$$\nu_m \leqslant \begin{cases} 2a+1 & \text{if } a = b, \\ 2a+2 & \text{otherwise.} \end{cases}$$

Equality holds if and only if we have $i \in N_m$ for all $i \leqslant \lfloor \frac{\nu_m - 1}{2} \rfloor$. Equality holds for all m if and only if ρ is Arf.

Proof Let $m \in \mathbb{N}_0$ and let $a_1, \ldots, a_{\nu_m}$ be the distinct elements of N_m with $0 = a_1 < a_2 < \cdots < a_{\nu_m} = m$. Since $m \ominus a_k \in N_m$ and $m \ominus a_k > m \ominus a_{k+1}$, we conclude that $m \ominus a_k = a_{\nu_m - k + 1}$. If ν_m is even, say $\nu_m = 2t$, then $m \ominus a_t = a_{t+1}$. If ν_m is odd, say $\nu_m = 2t - 1$, then $m \ominus a_t = a_t$. This gives the decomposition of m stated in the hypothesis of the proposition, $a = a_t$ and $b = a_t$ or $b = a_{t+1}$. The a_k are strictly increasing so $a_t \geqslant t - 1$. Thus we have $\nu_m \leqslant 2a_t + 2$, when ν_m is even, and $\nu_m \leqslant 2a_t + 1$, when ν_m is odd. We may consolidate the two cases as $\lfloor \frac{\nu_m - 1}{2} \rfloor \leqslant a_t$.

Equality holds in this last equation if and only if $a_t = t - 1$. Furthermore, $a_t = t - 1$ if and only if $i \in N_m$ for all $i \leqslant t - 1$.

Suppose now that ρ is Arf. Let m be given and write $m = a \oplus b$ with $a \leqslant b$ and $b - a$ minimal. For any $i \leqslant a$, the Arf property shows that $i \preccurlyeq m$, so $i \in N_m$. Thus ν_m is either $2a + 1$, if $a = b$, or $2a + 2$, if $a < b$.

Suppose that for any m the formula of the lemma is actually an equality. We have shown this is equivalent to $i \in N_m$ for all $i \leqslant \lfloor \frac{\nu_m - 1}{2} \rfloor$. Let $i \leqslant j \leqslant k$ be given and let $m = j \oplus k$. Write $m = a \oplus b$ with $a \leqslant b$ and $b - a$ minimal. Clearly $j \leqslant a$, so by assumption $i \in N_m$. Thus we have shown $i \preccurlyeq j \oplus k$. This establishes the Arf property.

It is clear from the proof of the proposition that there is a unique way to write $m \in \mathbb{N}_0$ as a sum $m = a \oplus b$ with $a \leqslant b$ and $b - a$ minimal. We will call this the *standard form* for m. The following proposition shows that there is no benefit to designing a code for generic error correction when the order function is Arf.

Proposition 20 *For all t, $\widetilde{R}^*(t) \subseteq \widetilde{R}(t)$. Equality holds for all t if and only if ρ is Arf. In this case $R^*(t) = R(t)$ also.*

Proof It is immediate from the definitions that if $\widetilde{R}^*(t) = \widetilde{R}(t)$ then also $R^*(t) = R(t)$.

Recall that $m \in \widetilde{R}(t)$ when $\nu_m \leqslant 2t$ and that $\widetilde{R}^*(t) = \mathbb{N}_0 \setminus \{i \oplus j \mid i, j \geqslant t\}$. Let m be arbitrary and write $m = a \oplus b$ in standard form. We observe that $m \in \widetilde{R}^*(t)$ if and only if $a \leqslant t - 1$. Therefore the previous proposition shows that when $m \in \widetilde{R}^*(t)$ we have $\nu_m \leqslant 2a + 2 \leqslant 2t$. This shows $m \in \widetilde{R}(t)$.

Suppose ρ is Arf. Let t be arbitrary. Suppose $m \in \widetilde{R}(t)$ – so $\nu_m \leqslant 2t$ – and write $m = a \oplus b$ in standard form. From the proposition, $t > \lfloor \frac{\nu_m - 1}{2} \rfloor = a$. Thus $a \leqslant t - 1$ and consequently $m \in \widetilde{R}^*(t)$. Thus we have shown for an arbitrary t that $\widetilde{R}^*(t) = \widetilde{R}(t)$.

Conversely, suppose $\widetilde{R}(t) = \widetilde{R}^*(t)$ for all t. Given an arbitrary m, write $m = a \oplus b$ in standard form and let $t = \lfloor \frac{\nu_m + 1}{2} \rfloor$. Then $\nu_m = 2t$ or $\nu_m = 2t - 1$, so $m \in \widetilde{R}(t)$. Since $\widetilde{R}(t) = \widetilde{R}^*(t)$, $a \leqslant t - 1$. By the proposition, $t - 1 = \lfloor \frac{\nu_m - 1}{2} \rfloor \leqslant a$, so we have equality. Since m was arbitrary, the previous proposition says that ρ is Arf.

Numerical semigroups and weight functions

Definition 13 *A numerical semigroup is a subset* Λ *of* $\mathbb{N}_0$ *containing* 0*, closed under summation and with finite complement in* $\mathbb{N}_0$*. For a numerical semigroup* Λ *we define the genus of* Λ *as the number* $g = |\mathbb{N}_0 \setminus \Lambda|$*. The enumeration of* Λ *is the unique increasing bijective map* $\lambda : \mathbb{N}_0 \longrightarrow \Lambda$*. We will use* λ_i *for* $\lambda(i)$*.*

Definition 14 *A numerical semigroup* Λ *is called Arf when for every* $\alpha, \beta, \gamma \in \Lambda$ *with* $\alpha \leqslant \beta \leqslant \gamma$*, we have* $\gamma + \beta - \alpha \in \Lambda$*.*

The codes in the second tower of Garcia–Stichtenoth attaining the Drinfeld-Vlăduţ bound (Example 8) are Arf numerical semigroups.

Definition 15 *Let* A *be an* $\mathbb{F}$*-algebra and let* ρ *be an order function on* A*. We will say that it is a weight function if there exists a numerical semigroup* Λ *with enumeration* λ *such that* $(\lambda \circ \rho)(fg) = (\lambda \circ \rho)(f) + (\lambda \circ \rho)(g)$ *for all* $f, g \neq 0$*.*

Note that the condition in Definition 15 is equivalent to $\lambda_{i \oplus j} = \lambda_i + \lambda_j$ for all $i, j \in \mathbb{N}_0$. It implies moreover that $i \preccurlyeq j$ if and only if $\lambda_j - \lambda_i = \lambda_k$ for some $k \in \mathbb{N}_0$. It can be proven (see [5]) that if ρ is a weight function there exists only one numerical semigroup Λ such that its enumeration λ satisfies the condition in Definition 15. If ρ is a weight function, we will say the *numerical semigroup* of ρ, and the *genus* of ρ to refer to the unique numerical semigroup whose enumeration satisfies the condition in Definition 15, and its genus.

As one would expect, if a weight function is Arf then the corresponding numerical semigroup is also. From Proposition 20 one can derive that for one-point codes, $\widetilde{R}^*(t) = \widetilde{R}(t)$ for all t if and only if the associated Weierstrass semigroup is Arf. An analogous result is presented in [6] for the Feng–Rao improved codes. The result proved there is that $\widetilde{R}(t) = R(t)$ for all t if and only if the associated semigroup is ordinary.

Suppose that ρ is a weight function. There exists a unique integer c with $c-1 \notin \Lambda$ and $c + \mathbb{N}_0 \subseteq \Lambda$. It is exactly the integer right after the largest gap. Notice that if $c = \lambda_i$ then $i = c - g$. It is easy to show that for $i \geqslant g$, $\lambda_i = i + g$. Furthermore, any fixed t satisfies that for all $m > c + \lambda_t - g$, $m \succcurlyeq t$.

In Lemma 18 we showed that for any $t \in \mathbb{N}_0$,

$$\{a \oplus t \mid a \in \mathbb{N}_0\} \subseteq \{a \oplus b \mid a, b \geqslant t\},$$

and that the two sets are equal for all t when ρ is Arf. Let

$$\alpha(t) = |\{a \oplus b \mid a, b \geqslant t\} \setminus \{a \oplus t \mid a \in \mathbb{N}_0\}|.$$

Clearly ρ is Arf if and only if $\alpha(t) = 0$ for all t. We now give an explicit formula, involving $\alpha(t)$, for $\widetilde{r}^*(t)$ when ρ is a weight function.

Proposition 21 *Let* ρ *be a weight function with numerical semigroup* Λ *and enumeration* λ*. Then, for all* $t \in \mathbb{N}_0$*,* $\tilde{r}^*(t) = \lambda_t + t - \alpha(t)$*.*

Proof Let g be the genus of Λ and let h be such that $h > \max(g, t)$ and such that for all $m > t \oplus h$, $m \succcurlyeq t$. Since $h \geqslant g$,

$$\begin{aligned} \lambda_t &= \lambda_{t \oplus h} - \lambda_h \\ &= t \oplus h - g - (h - g) \\ &= t \oplus h - h. \end{aligned}$$

Therefore $\lambda_t + h = t \oplus h$.

For an integer m there are three possibilities:

- $m \in \widetilde{R}^*(t) = \mathbb{N}_0 \setminus \{a \oplus b \mid a, b \geqslant t\}$,
- $m \in \{a \oplus b \mid a, b \geqslant t\}$ but $m \not\succ t$, or
- $m \in \{a \oplus b \mid a, b \geqslant t\}$ and $m \succ t$.

In the last case, $m = t \oplus a$ for some $a \geqslant t$. Those m satisfying the first two conditions are all at most $t \oplus h$, by our choice of h. Thus we have a partition of $\{0, \ldots, t \oplus h\}$ into three sets, $\widetilde{R}^*(t)$, $\{a \oplus b \mid a, b \geqslant t\} \cap \{m \in \mathbb{N}_0 \mid m \not\succ t\}$ and $\{t \oplus a \mid a \in \{t, \ldots, h\}\}$. Counting elements we have

$$t \oplus h + 1 = \widetilde{r}^*(t) + \alpha(t) + h - t + 1.$$

Substituting $t \oplus h = \lambda_t + h$ gives the result.

Corollary 22 *Let ρ be a weight function with numerical semigroup Λ and enumeration λ. Then, for all $t \in \mathbb{N}_0$, $\tilde{r}^*(t) \leqslant \lambda_t + t$. Equality holds for all t if and only if Λ is Arf.*

In [7] there is a similar characterization of Arf numerical semigroups. A numerical semigroup is Arf if and only if $\widetilde{r}(t) = \lambda_t + t$ for any integer t.

Acknowledgements The first author was supported in part by the Spanish CICYT under Grant TIC2003-08604-C04-01 and FEDER, Catalan DURSI under SGR2005-00319.

References

1. Arf, C.: Une interprétation algébrique de la suite des ordres de multiplicité d'une branche algébrique. Proc Lond Math Soc **50**(2), 256–287 (1948)
2. Atiyah, M.F., Macdonald, I.G.: Introduction to commutative algebra. Reading, MA: Addison-Wesley 1969
3. Barucci, V., Dobbs, D.E., Fontana, M.: Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains. Mem Am Math Soc **125**(598), x+78 (1997)
4. Bourbaki, N.: Commutative algebra. Reading, MA: Addison-Wesley, 1972
5. Bras-Amorós, M.: Improving evaluation codes. PhD Thesis, Universitat Politècnica de Catalunya, Barcelona 2003
6. Bras-Amorós, M.: Acute semigroups, the order bound on the minimum distance, and the Feng–Rao improvements. IEEE Trans Inform Theory **50**(6), 1282–1289 (2004)
7. Campillo, A., Farrán, J.I., Munuera, C.: On the parameters of algebraic–geometry codes related to Arf semigroups. IEEE Trans Inform Theory **46**(7), 2634–2638 (2000)
8. Duursma, I.M.: Majority coset decoding. IEEE Trans Inform Theory **39**(3), 1067–1070 (1993)
9. Feng, G.L., Rao, T.R.N.: Decoding algebraic-geometric codes up to the designed minimum distance. IEEE Trans Inform Theory **39**(1), 37–45 (1993)
10. Feng, G.-L., Rao, T.R.N.: Improved geometric Goppa codes. I. Basic theory. IEEE Trans Inform Theory **41**(6, part 1), 1678–1693 (1995) (Special issue on algebraic geometry codes)
11. Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. J Number Theory **61**(2), 248–273 (1996)
12. Geil, O., Høholdt, T.: Footprints or generalized Bezout's theorem. IEEE Trans Inform Theory **46**(2), 635–641 (2000)
13. Høholdt, T., van Lint, J.H., Pellikaan, R.: Algebraic geometry codes. pp 871–961. Amsterdam: North-Holland 1998

14. Jensen, H.E., Nielsen, R.R., Høholdt, T.: Performance analysis of a decoding algorithm for algebraic-geometry codes. IEEE Trans Inform Theory **45**(5), 1712–1717 (1999)
15. Lipman, J.: Stable ideals and Arf rings. Am J Math **93**, 649–685 (1971)
16. O'Sullivan, M.E.: Decoding of codes defined by a single point on a curve. IEEE Trans Inform Theory **41**(6, part 1), 1709–1719 (1995) (Special issue on algebraic geometry codes)
17. O'Sullivan, M.E.: Decoding of Hermitian codes beyond $(d_{\min} - 1)/2$. In: Proceedings of the 1997 IEEE international symposium on information theory, pp 384. Germany: Ulm 1997
18. O'Sullivan, M.E.: New codes for the Berlekamp–Massey–Sakata algorithm. Finite Fields Appl **7**(2), 293–317 (2001)
19. Pellikaan, R.: On decoding by error location and dependent sets of error positions. Discrete Math **106/107**, 369–381 (1992) (A collection of contributions in honour of Jack van Lint)
20. Pellikaan, R., Stichtenoth, H., Torres, F.: Weierstrass semigroups in an asymptotically good tower of function fields. Finite Fields Appl **4**(4), 381–392 (1998)
21. Rosales, J.C., García-Sánchez, P.A., García-García, J.I., Branco, M.B.: Arf numerical semigroups. J Algebra **276**(1), 3–12 (2004)
22. Sakata, S.: Extension of the Berlekamp–Massey algorithm to N dimensions. Inform Comput **84**(2), 207–239 (1990)
23. Stichtenoth, H.: A note on Hermitian codes over GF(q^2). IEEE Trans Inform Theory **34**(5, part 2), 1345–1348 (1988) (Coding techniques and coding theory)