

## The key equation for codes from order domains

John B. Little

*Department of Mathematics and Computer Science,  
College of the Holy Cross,  
Worcester, MA 01610, USA  
E-mail: little@mathcs.holycross.edu*

We study a sort of analog of the *key equation* for decoding Reed-Solomon and BCH codes and identify a key equation for all codes from order domains which have finitely-generated value semigroups (the field of fractions of the order domain may have arbitrary transcendence degree, however). We provide a natural interpretation of the construction using the theory of Macaulay's *inverse systems* and duality. O'Sullivan's generalized Berlekamp-Massey-Sakata (BMS) decoding algorithm applies to the duals of suitable evaluation codes from these order domains. When the BMS algorithm does apply, we will show how it can be understood as a process for constructing a collection of solutions of our key equation.

*Keywords:* order domain, key equation, Berlekamp-Massey-Sakata algorithm

### 1. Introduction

The theory of error control codes constructed using ideas from algebraic geometry (including the geometric Goppa and related codes) has undergone a remarkable extension and simplification with the introduction of codes constructed from *order domains*. This development has been largely motivated by the structures utilized in the Berlekamp-Massey-Sakata decoding algorithm with Feng-Rao-Duursma majority voting for unknown syndromes.

The order domains, see [1–4], form a class of rings having many of the same properties as the rings  $R = \cup_{m=0}^{\infty} L(mQ)$  underlying the one-point geometric Goppa codes constructed from curves. The general theory gives a common framework for these codes,  $n$ -dimensional cyclic codes, as well as many other Goppa-type codes constructed from varieties of dimension  $> 1$ . Moreover, O'Sullivan has shown in [5] that the Berlekamp-Massey-Sakata decoding algorithm (abbreviated as the BMS algorithm in the following) and the Feng-Rao procedure extend in a natural way to a suitable class of

codes in this much more general setting.

For the Reed-Solomon codes, the Berlekamp-Massey decoding algorithm can be phrased as a method for solving a *key equation*. For a Reed-Solomon code with minimum distance  $d = 2t + 1$ , the key equation has the form

$$fS \equiv g \pmod{\langle X^{2t} \rangle}. \quad (1)$$

Here  $S$  is a known univariate polynomial in  $X$  constructed from the error syndromes, and  $f, g$  are unknown polynomials in  $X$ . If the error vector  $e$  satisfies  $wt(e) \leq t$ , there is a unique solution  $(f, g)$  with  $\deg(f) \leq t$ , and  $\deg(g) < \deg(f)$  (up to a constant multiple). The polynomial  $f$  is known as the *error locator* because its roots give the *inverses* of the error locations; the polynomial  $g$  is known as the *error evaluator* because the error values can be determined from values of  $g$  at the roots of  $f$ , via the Forney formula.

O'Sullivan has introduced a generalization of this key equation for one-point geometric Goppa codes from curves in [6] and shown that the BMS algorithm can be modified to compute the analogs of the error-evaluator polynomial together with error locators.

Our main goal in this article is to identify an analog of the key equation Eq. (1) for codes from general order domains, and to give a natural interpretation of these ideas in the context of Macaulay's *inverse systems* for ideals in a polynomial ring (see [7–10]) and the theory of duality. We will only consider order domains whose value semigroups are finitely generated. In these cases, the ring  $R$  can be presented as an affine algebra  $R \cong \mathbb{F}[X_1, \dots, X_s]/I$ , where the ideal  $I$  has a Gröbner basis of a very particular form (see [3]). Although O'Sullivan has shown how more general order domains arise naturally from valuations on function fields, it is not clear to us how our approach applies to those examples. On the positive side, by basing all constructions on algebra in polynomial rings, all codes from these order domains can be treated in a uniform way. Second, we also propose to study the relation between the BMS algorithm and the process of solving this key equation in the cases where BMS is applicable.

Our key equation generalizes the key equation for  $n$ -dimensional cyclic codes studied by Chabanne and Norton in [12]. Results on the algebraic background for their construction appear in [13]. See also [14] for connections with the more general problem of finding shortest linear recurrences, and [15] for a generalization giving a key equation for codes over commutative rings.

The present article is organized as follows. In Section 2 we will briefly review the definition of an order domain, evaluation codes and dual evalu-

ation codes. Section 3 contains a quick summary of the basics of Macaulay inverse systems and duality. In Section 4 we introduce the key equation and relate the BMS algorithm to the process of solving this equation.

## 2. Codes from Order Domains

In this section we will briefly recall the definition of order domains and explain how they can be used to construct error control codes. We will use the following formulation.

**Definition 2.1.** Let  $R$  be a  $\mathbb{F}_q$ -algebra and let  $(\Gamma, +, \succ)$  be a well-ordered semigroup. We assume the ordering is compatible with the semigroup operation in the sense that if  $a \succ b$  and  $c$  is arbitrary in  $\Gamma$ , then  $a + c \succ b + c$ . An *order function* on  $R$  is a surjective mapping  $\rho : R \rightarrow \{-\infty\} \cup \Gamma$  satisfying:

- (1)  $\rho(f) = -\infty \Leftrightarrow f = 0$ ,
- (2)  $\rho(cf) = \rho(f)$  for all  $f \in R$ , all  $c \neq 0$  in  $\mathbb{F}_q$ ,
- (3)  $\rho(f + g) \preceq \max_{\succ} \{\rho(f), \rho(g)\}$ ,
- (4) if  $\rho(f) = \rho(g) \neq -\infty$ , then there exists  $c \neq 0$  in  $\mathbb{F}_q$  such that  $\rho(f) \prec \rho(f - cg)$ ,
- (5)  $\rho(fg) = \rho(f) + \rho(g)$ .

We call  $\Gamma$  the *value semigroup* of  $\rho$ .

Axioms 1 and 5 in this definition imply that  $R$  must be an integral domain. In the cases where the transcendence degree of  $R$  over  $\mathbb{F}_q$  is at least 2, a ring  $R$  with one order function will have many others too. For this reason an *order domain* is formally defined as a pair  $(R, \rho)$  where  $R$  is an  $\mathbb{F}_q$ -algebra and  $\rho$  is an order function on  $R$ . However, from now on, we will only use one particular order function on  $R$  at any one time. Hence we will often omit it in referring to the order domain, and we will refer to  $\Gamma$  as the value semigroup of  $R$ . Several constructions of order domains are discussed in [3] and [4].

The most direct way to construct codes from an order domain given by a particular presentation  $R \cong \mathbb{F}_q[X_1, \dots, X_s]/I$  is to generalize Goppa's construction in the case of curves.

Let  $X_R$  be the variety  $V(I) \subset \mathbb{A}^s$  and let

$$X_R(\mathbb{F}_q) = \{P_1, \dots, P_n\}$$

be the set of  $\mathbb{F}_q$ -rational points on  $X_R$ . Define an evaluation mapping

$$\begin{aligned} ev : R &\rightarrow \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \dots, f(P_n)) \end{aligned}$$

Let  $V \subset R$  be any finite-dimensional vector subspace. Then the image  $ev(V) \subseteq \mathbb{F}_q^n$  will be a linear code in  $\mathbb{F}_q^n$ . One can also consider the dual code  $ev(V)^\perp$ .

Of particular interest here are the codes constructed as follows (see [5]). Let  $R$  be an order domain whose value semigroup  $\Gamma$  can be put into order-preserving one-to-one correspondence with  $\mathbb{Z}_{\geq 0}$ . We refer to such  $\Gamma$  as *Archimedean* value semigroups because it follows that for all nonconstant  $f \in R$  and all  $g \in R$  there is some  $n \geq 1$  such that  $\rho(f^n) \succ \rho(g)$ . This property is equivalent to saying that the corresponding valuation of  $K = QF(R)$  has *rank 1*. O'Sullivan gives a necessary and sufficient condition for this property when  $\succ$  is given by a monomial order on  $\mathbb{Z}_{\geq 0}^r$  in [2], Example 1.3. Let  $\Delta$  be the ordered basis of  $R$  with ordering by  $\rho$ -value. Let  $\ell \in \mathbb{N}$  and let  $V_\ell$  be the span of the first  $\ell$  elements of  $\Delta$ . In this way, we obtain evaluation codes  $Ev_\ell = ev(V_\ell)$  and dual codes  $C_\ell = Ev_\ell^\perp$  for all  $\ell$ .

O'Sullivan's generalized BMS algorithm is specifically tailored for this last class of codes from order domains with  $\Gamma$  Archimedean. If the  $C_\ell$  codes are used to encode messages, then the  $Ev_\ell$  codes describe the parity checks and the syndromes used in the decoding algorithm.

### 3. Preliminaries on Inverse Systems

A natural setting for our formulation of a key equation for codes from order domains is the theory of inverse systems of polynomial ideals originally introduced by Macaulay. There are several different versions of this theory. For modern versions using the language of differentiation operators, see [9, 10]. Here, we will summarize a number of more or less well-known results, using an alternate formulation of the definitions that works in any characteristic. A reference for this approach is [8].

Let  $k$  be a field, let  $S = k[X_1, \dots, X_s]$  and let  $T$  be the formal power series ring  $k[[X_1^{-1}, \dots, X_s^{-1}]]$  in the inverse variables.  $T$  is an  $S$ -module under a mapping

$$\begin{aligned} c : S \times T &\rightarrow T \\ (f, g) &\mapsto f \cdot g, \end{aligned}$$

sometimes called *contraction*, defined as follows. First, given monomials  $X^\alpha$  in  $S$  and  $X^{-\beta}$  in  $T$ ,  $X^\alpha \cdot X^{-\beta}$  is defined to be  $X^{\alpha-\beta}$  if this is in  $T$ , and 0 otherwise. We then extend by linearity to define  $c : S \times T \rightarrow T$ .

Let  $Hom_k(S, k)$  be the usual linear dual vector space. It is a standard

fact that the mapping

$$\begin{aligned} \phi : \text{Hom}_k(S, k) &\rightarrow T \\ \Lambda &\mapsto \sum_{\beta \in \mathbb{Z}_{\geq 0}^s} \Lambda(X^\beta) X^{-\beta} \end{aligned}$$

is an isomorphism of  $S$ -modules, if we make  $\text{Hom}_k(S, k)$  into an  $S$ -module in the usual way by defining  $(q\Lambda)(p) = \Lambda(qp)$  for all polynomials  $p, q$  in  $S$ . In explicit terms, the  $k$ -linear form on  $S$  obtained from an element  $g \in T$  is a mapping  $\Lambda_g$  defined as follows. For all  $f \in S$ ,

$$\Lambda_g(f) = (f \cdot g)_0,$$

where  $(t)_0$  denotes the constant term in  $t \in T$ . In the following we will identify elements of  $T$  with their corresponding linear forms on  $S$ .

The theory of inverse systems sets up a correspondence between ideals in  $S$  and submodules of  $T$ . All such ideals and submodules are finitely generated and we will use the standard notation  $\langle f_1, \dots, f_t \rangle$  for the ideal generated by a collection of polynomials  $f_i \in S$ .

For each ideal  $I \subseteq S$ , we can define the annihilator, or *inverse system*, of  $I$  in  $T$  as

$$I^\perp = \{\Lambda \in T : \Lambda(p) = 0, \forall p \in I\}.$$

It is easy to check that  $I^\perp$  is an  $S$ -submodule of  $T$  under the module structure defined above. Similarly, given an  $S$ -submodule  $H \subseteq T$ , we can define

$$H^\perp = \{p \in S : \Lambda(p) = 0, \forall \Lambda \in H\},$$

and  $H^\perp$  is an ideal in  $S$ . The key point in this theory is the following duality statement.

**Theorem 3.1.** *The ideals of  $S$  and the  $S$ -submodules of  $T$  are in inclusion-reversing bijective correspondence via the constructions above, and for all  $I, H$  we have:*

$$(I^\perp)^\perp = I, \quad (H^\perp)^\perp = H.$$

See [8] for a proof.

We will be interested in applying Theorem 3.1 when  $I$  is the ideal of some finite set of points in the  $n$ -dimensional affine space over  $k$  (e.g. when  $k = \mathbb{F}_q$  and  $I$  is an error-locator ideal arising in decoding – see Section 4 below). In the following, we will use the notation  $m_P$  for the maximal ideal of  $S$  corresponding to the point  $P \in k^s$ .

**Theorem 3.2.** Let  $P_1, \dots, P_t$  be points in  $k^s$  and let

$$I = m_{P_1} \cap \dots \cap m_{P_t}.$$

The submodule of  $T$  corresponding to  $I$  has the form

$$H = I^\perp = (m_{P_1})^\perp \oplus \dots \oplus (m_{P_t})^\perp.$$

**Proof.** In Proposition 2.6 of [11], Geramita shows that  $(I \cap J)^\perp = I^\perp + J^\perp$  for any pair of ideals. The idea is that  $I^\perp$  and  $J^\perp$  can be constructed degree by degree, so the corresponding statement from the linear algebra of finite-dimensional vector spaces applies. The equality  $(I + J)^\perp = I^\perp \cap J^\perp$  also holds from linear algebra (and no finite-dimensionality is needed). The sum in the statement of the Lemma is a direct sum since  $m_{P_i} + \bigcap_{j \neq i} m_{P_j} = S$ , hence  $(m_{P_i})^\perp \cap \bigcap_{j \neq i} (m_{P_j})^\perp = \{0\}$ .  $\square$

We can also give a concrete description of the elements of  $(m_P)^\perp$ .

**Theorem 3.3.** Let  $P = (a_1, \dots, a_s) \in \mathbb{A}^s$  over  $k$ , and let  $L_i$  be the coordinate hyperplane  $X_i = a_i$  containing  $P$ .

(1)  $(m_P)^\perp$  is the cyclic  $S$ -submodule of  $T$  generated by

$$h_P = \sum_{u \in \mathbb{Z}_{\geq 0}^s} P^u X^{-u},$$

where if  $u = (u_1, \dots, u_s)$ ,  $P^u$  denotes the product  $a_1^{u_1} \dots a_s^{u_s}$  ( $X^u$  evaluated at  $P$ ).

(2)  $f \cdot h_P = f(P)h_P$  for all  $f \in S$ , and the submodule  $(m_P)^\perp$  is a one-dimensional vector space over  $k$ .

(3) Let  $I_{L_i}$  be the ideal  $\langle X_i - a_i \rangle$  in  $S$  (the ideal of  $L_i$ ). Then  $(I_{L_i})^\perp$  is the submodule of  $T$  generated by  $h_{L_i} = \sum_{j=0}^{\infty} a_i^j X_i^{-j}$ .

(4) In  $T$ , we have  $h_P = \prod_{i=1}^s h_{L_i}$ .

**Proof.** (1) First, if  $f \in m_P$ , and  $g \in S$  is arbitrary then

$$\Lambda_{g \cdot h_P}(f) = (f \cdot (g \cdot h_P))_0 = ((fg) \cdot h_P)_0 = f(P)g(P) = 0.$$

Hence the  $S$ -submodule  $\langle h_P \rangle$  is contained in  $(m_P)^\perp$ . Conversely, if  $h \in (m_P)^\perp$ , then for all  $f \in m_P$ ,

$$0 = \Lambda_h(f) = (f \cdot h)_0.$$

An easy calculation using all  $f$  of the form  $f = x^\beta - a^\beta \in m_P$  shows that  $h = ch_P$  for some constant  $c$ . Hence  $(m_P)^\perp = \langle h_P \rangle$ .

(2) The second claim follows by a direct computation of the contraction product  $f \cdot h_P$ .

(3) Let  $f \in I_{L_i}$  (so  $f$  vanishes at all points of the hyperplane  $L_i$ ), and let  $g \in S$  be arbitrary. Then

$$\begin{aligned}\Lambda_{g \cdot h_{L_i}}(f) &= (f \cdot (g \cdot h_{L_i}))_0 = ((fg) \cdot h_{L_i})_0 \\ &= f(0, \dots, 0, a_i, 0, \dots, 0)g(0, \dots, 0, a_i, 0, \dots, 0) = 0,\end{aligned}$$

since the only nonzero terms in the product  $((fg) \cdot h_{L_i})$  come from monomials in  $fg$  containing only the variable  $X_i$ . Hence  $\langle h_{L_i} \rangle \subset T$  is contained in  $I_{L_i}^\perp$ . Then we show the other inclusion as in the proof of (1).

(4) We have  $m_P = I_{L_1} + \dots + I_{L_s}$ . Hence  $(m_P)^\perp = (I_{L_1})^\perp \cap \dots \cap (I_{L_s})^\perp$ , and the claim follows. We note that a more explicit form of this equation can be derived by the formal geometric series summation formula:

$$h_P = \sum_{u \in \mathbb{Z}_{\geq 0}^s} P^u X^{-u} = \prod_{i=1}^s \frac{1}{1 - a_i/X_i} = \prod_{i=1}^s h_{L_i}. \quad \square$$

Both the polynomial ring  $S$  and the formal power series ring  $T$  can be viewed as subrings of the field of formal Laurent series in the inverse variables,

$$K = k((X_1^{-1}, \dots, X_s^{-1})),$$

which is the field of fractions of  $T$ . Hence the (full) product  $fg$  for  $f \in S$  and  $g \in T$  is an element of  $K$ . The contraction product  $f \cdot g$  is a projection of  $fg$  into  $T \subset K$ . We can also consider the projection of  $fg$  into  $S_+ = \langle X_1, \dots, X_s \rangle \subset S \subset K$  under the linear projection with kernel spanned by all monomials not in  $S_+$ . We will denote this by  $(fg)_+$ .

#### 4. The Key Equation and its Relation to the BMS

##### Algorithm

Let  $C$  be one of the codes  $C = ev(V)$  or  $ev(V)^\perp$  constructed from an order domain  $R \cong \mathbb{F}_q[X_1, \dots, X_s]/I$ . Consider an error vector  $e \in \mathbb{F}_q^n$  (where entries are indexed by the elements of the set  $X_R(\mathbb{F}_q)$ ). In the usual terminology, the *error-locator ideal* corresponding to  $e$  is the ideal  $I_e \subset \mathbb{F}_q[X_1, \dots, X_s]$  defining the set of error locations:

$$I_e = \{f \in \mathbb{F}_q[X_1, \dots, X_s] : f(P) = 0, \forall P \text{ s.t. } e_P \neq 0\}.$$

We will use a slightly different notation and terminology in the following because we want to make a systematic use of the observation that this ideal

depends only on the support of  $e$ , not on the error values. Indeed, many different error vectors yield the same ideal defining the error locations. For this reason we will introduce  $\mathcal{E} = \{P : e_P \neq 0\}$ , and refer to the error-locator ideal for any  $e$  with  $\text{supp}(e) = \mathcal{E}$  as  $I_{\mathcal{E}}$ .

For each monomial  $X^u \in \mathbb{F}_q[X_1, \dots, X_s]$ , we let

$$E_u = \langle e, ev(X^u) \rangle = \sum_{P \in X_R(\mathbb{F}_q)} e_P P^u \tag{2}$$

be the corresponding syndrome of the error vector. (As in Theorem 3.3,  $P^u$  is shorthand notation for the evaluation of the monomial  $X^u$  at  $P$ .)

In the practical decoding situation, of course, for a code  $C = ev(V)^\perp$  where  $V$  is a subspace of  $R$  spanned by some set of monomials, only the  $E_u$  for the  $X^u$  in a basis of  $V$  are initially known from the received word.

In addition, the elements of the ideal  $I + \langle X_1^q - X_1, \dots, X_s^q - X_s \rangle$  defining the set  $X_R(\mathbb{F}_q)$  give relations between the  $E_u$ . Indeed, the  $E_u$  for  $u$  in the ordered basis  $\Delta$  for  $R$  with all components  $\leq q - 1$  determine all the others, and these syndromes still satisfy additional relations. Thus the  $E_u$  are, in a sense, highly redundant.

To package the syndromes into a single algebraic object, following [12], we define the *syndrome series*

$$\mathcal{S}_e = \sum_{u \in \mathbb{Z}_{\geq 0}^s} E_u X^{-u}$$

in the formal power series ring  $T = \mathbb{F}_q[[X_1^{-1}, \dots, X_s^{-1}]]$ . (This depends both on the set of error locations  $\mathcal{E}$  and on the error values.) As in Section 3, we have a natural interpretation for  $\mathcal{S}_e$  as an element of the dual space of the ring  $S = \mathbb{F}_q[X_1, \dots, X_s]$ .

The following expression for the syndrome series  $\mathcal{S}_e$  will be fundamental. We substitute from Eq. (2) for the syndrome  $E_u$  and change the order of summation to obtain:

$$\begin{aligned} \mathcal{S}_e &= \sum_{u \in \mathbb{Z}_{\geq 0}^s} E_u X^{-u} = \sum_{u \in \mathbb{Z}_{\geq 0}^s} \sum_{P \in X_R(\mathbb{F}_q)} e_P P^u X^{-u} \\ &= \sum_{P \in X_R(\mathbb{F}_q)} e_P \sum_{u \in \mathbb{Z}_{\geq 0}^s} P^u X^{-u} = \sum_{P \in X_R(\mathbb{F}_q)} e_P h_P, \end{aligned}$$

where  $h_P$  is the generator of  $(m_P)^\perp$  from Theorem 3.3. The sum here taking the terms with  $e_P \neq 0$ , gives the decomposition of  $\mathcal{S}_e$  in the direct sum expression for  $I_{\mathcal{E}}^\perp$  as in Theorem 3.2.

The first statement in the following Theorem is well-known; it is a translation of the standard fact that error-locators give linear recurrences on the

syndromes. But to our knowledge, this fact has not been considered from exactly our point of view in this generality (see [16] for a special case).

**Theorem 4.1.** *With all notation as above,*

- (1)  $f \in I_{\mathcal{E}}$  if and only if  $f \cdot \mathcal{S}_e = 0$  for all error vectors  $e$  with  $\text{supp}(e) = \mathcal{E}$ .
- (2) For each  $e$  with  $\text{supp}(e) = \mathcal{E}$ ,  $I_{\mathcal{E}} = \langle \mathcal{S}_e \rangle^{\perp}$  in the duality from Theorem 3.1.
- (3) If  $e, e'$  are two error vectors with the same support, then  $\langle \mathcal{S}_e \rangle = \langle \mathcal{S}_{e'} \rangle$  as submodules of  $T$ .

**Proof.** For (1), we start from the expression for  $\mathcal{S}_e$  from Eq. (3). Then by Theorem 3.3, we have

$$f \cdot \mathcal{S}_e = \sum_{P \in \mathcal{E}} e_P (f \cdot h_P) = \sum_{P \in \mathcal{E}} e_P f(P) h_P.$$

If  $f \in I_{\mathcal{E}}$ , then clearly  $f \cdot \mathcal{S}_e = 0$  for all choices of error values  $e_P$ . Conversely, if  $f \cdot \mathcal{S}_e = 0$  for all  $e$  with  $\text{supp}(e) = \mathcal{E}$ , then  $f(P) = 0$  for all  $P \in \mathcal{E}$ , so  $f \in I_{\mathcal{E}}$ .

Claim (2) follows from (1).

The perhaps surprising claim (3) is a consequence of (2). Another way to prove (3) is to note that there exist  $g \in R$  such that  $g(P)e_P = e'_P$  for all  $P \in \mathcal{E}$ . We have

$$g \cdot \mathcal{S}_e = \sum_{P \in \mathcal{E}} e_P (g \cdot h_P) = \sum_{P \in \mathcal{E}} e_P g(P) h_P = \sum_{P \in \mathcal{E}} e'_P h_P = \mathcal{S}_{e'}.$$

Hence  $\langle \mathcal{S}_{e'} \rangle \subseteq \langle \mathcal{S}_e \rangle$ . Reversing the roles of  $e$  and  $e'$ , we get the other inclusion as well, and (3) follows.  $\square$

The following explicit expression for the terms in  $f \cdot \mathcal{S}_e$  is also useful. Let  $f = \sum_m f_m X^m \in S$ . Then

$$f \cdot \mathcal{S}_e = \left( \sum_m f_m X^m \right) \cdot \left( \sum_{u \in \mathbb{Z}_{\geq 0}^s} E_u X^{-u} \right) = \sum_{r \in \mathbb{Z}_{\geq 0}^s} \left( \sum_m f_m E_{m+r} \right) X^{-r}.$$

Hence  $f \cdot \mathcal{S}_e = 0 \Leftrightarrow \sum_m f_m E_{m+r} = 0$  for all  $r \geq 0$ .

The equation  $f \cdot \mathcal{S} = 0$  from (1) in Theorem 4.1 is the prototype, so to speak, for our generalizations of the key equation to codes from order domains, and we will refer to it as the *key equation* in the following. It also naturally generalizes all the various key equations that have been developed in special cases, as we will demonstrate shortly. Before proceeding with that, however, we wish to make several comments about the form of this equation.

Comparing the equation  $f \cdot \mathcal{S}_e = 0$  with the familiar form Eq. (1), several differences may be apparent. First, note that the syndrome series  $\mathcal{S}_e$  will not be entirely known from the received word in the decoding situation. The same is true in the Reed-Solomon case, of course. The polynomial  $S$  in the congruence in Eq. (1) involves only the known syndromes, and Eq. (1) is derived by accounting for the other terms in the full syndrome series. With a truncation of  $\mathcal{S}_e$  in our situation we would obtain a similar type of congruence (see the discussion following Eq. (8) below, for instance). It is apparently somewhat rare, however, that the portion of  $\mathcal{S}_e$  known from the received word suffices for decoding up to half the minimum distance of the code.

Another difference is that there is no apparent analog of the error-evaluator polynomial  $g$  from Eq. (1) in the equation  $f \cdot \mathcal{S}_e = 0$ . The way to obtain error evaluators in this situation is to consider the “purely positive parts”  $(f\mathcal{S}_e)_+$  for certain solutions of our key equation.

We now turn to several examples that show how our key equation relates to several special cases that have appeared in the literature.

**Example 4.1.** We begin by providing more detail on the precise relation between Theorem 4.1, part (1) in the case of a Reed-Solomon code and the usual key equation from Eq. (1). These codes are constructed from the order domain  $R = \mathbb{F}_q[X]$  (where  $\Gamma = \mathbb{Z}_{\geq 0}$  and  $\rho$  is the degree mapping). The key equation Eq. (1) applies to the code  $Ev_\ell = ev(V_\ell)$ , where  $V_\ell = \text{Span}\{1, X, X^2, \dots, X^{\ell-1}\}$ , and the evaluation takes place at all  $\mathbb{F}_q$ -rational points on the affine line, omitting 0.

Our key equation in this case is closely related to, but not precisely the same, as Eq. (1). The reason for the difference is that Theorem 4.1 is applied to the dual code  $C_\ell = Ev_\ell^\perp$  rather than  $Ev_\ell$ . Starting from Eq. (3) and using the formal geometric series summation formula as in Theorem 3.3 part (4), we can write:

$$\mathcal{S}_e = \sum_{P \in \mathcal{E}} e_P \sum_{u \geq 0} P^u X^{-u} = X \frac{\sum_{P \in \mathcal{E}} e_P \prod_{Q \in \mathcal{E}, Q \neq P} (X - Q)}{\prod_{P \in \mathcal{E}} (X - P)}.$$

Hence, in this formulation,  $\mathcal{S}_e = Xq/p$ , where  $p$  is the generator of the actual error locator ideal (not the ideal of the inverses of the error locations). Moreover if we take  $f = p$  in Theorem 4.1, then

$$(p\mathcal{S}_e)_+ = Xq \tag{3}$$

gives an analog of the error evaluator. There are no “mixed terms” in the products  $f\mathcal{S}_e$  in this one-variable situation.

**Example 4.2.** The key equation for  $s$ -dimensional cyclic codes introduced by Chabanne and Norton in [12] has the form

$$\sigma \mathcal{S}_e = \left( \prod_{i=1}^s X_i \right) g, \quad (4)$$

where  $\sigma = \prod_{i=1}^s \sigma_i(X_i)$ , and  $\sigma_i$  is the univariate generator of the elimination ideal  $I_{\mathcal{E}} \cap \mathbb{F}_q[X_i]$ . Our version of the Reed-Solomon key equation from Eq. (3) is a special case of Eq. (4). Moreover, Eq. (4) is clearly the special case of Theorem 4.1, part (1) for these codes where  $f = \sigma$  is the particular error locator polynomial  $\prod_{i=1}^s \sigma_i(X_i) \in I_{\mathcal{E}}$ . For this special choice of error locator,  $\sigma \cdot \mathcal{S}_e = 0$ , and  $(\sigma \mathcal{S}_e)_+ = (\prod_{i=1}^s X_i) g$  for some polynomial  $g$ . We see that  $\mathcal{S}_e$  can be written as

$$\mathcal{S}_e = \sum_P e_P h_P = \left( \prod_{i=1}^s X_i \right) \sum_P e_P \frac{1}{\prod_{i=1}^s (X_i - X_i(P))},$$

and the product  $\sigma \mathcal{S}_e = (\sigma \mathcal{S}_e)_+$  reduces to a polynomial (again, there are no “mixed terms”).

**Example 4.3.** We now turn to the key equation for one-point geometric Goppa codes introduced by O’Sullivan in [6]. Let  $\mathcal{X}$  be a smooth curve over  $\mathbb{F}_q$  of genus  $g$ , and consider one-point codes constructed from  $R = \cup_{m=0}^{\infty} L(mQ)$  for some point  $Q \in \mathcal{X}(\mathbb{F}_q)$ , O’Sullivan’s key equation has the form:

$$f \omega_e = \phi. \quad (5)$$

Here  $\omega_e$  is the syndrome differential, which can be expressed as

$$\omega_e = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} e_P \omega_{P,Q},$$

where  $\omega_{P,Q}$  is the differential of the third kind on  $Y$  with simple poles at  $P$  and  $Q$ , no other poles, and residues  $\text{res}_P(\omega_{P,Q}) = 1, \text{res}_Q(\omega_{P,Q}) = -1$ . For any  $f \in R$ , we have

$$\text{res}_Q(f \omega_e) = \sum_P e_P f(P),$$

the syndrome of  $e$  corresponding to  $f$ . (We only defined syndromes for monomials above; taking a presentation  $R = \mathbb{F}_q[X_1, \dots, X_s]/I$ , however, any  $f \in R$  can be expressed as a linear combination of monomials and the syndrome of  $f$  is defined accordingly.) The right-hand side of Eq. (5) is also a differential. In this situation, Eq. (5) furnishes a key equation in the

following sense:  $f$  is an error locator (i.e.  $f$  is in the ideal of  $R$  corresponding to  $I_{\mathcal{E}}$ ) if and only if  $\phi$  has poles only at  $Q$ . In the special case that  $(2g - 2)Q$  is a canonical divisor (the divisor of zeroes of some differential of the first kind  $\omega_0$  on  $\mathcal{X}$ ), Eq. (5) can be replaced by the equivalent equation  $f o_e = g$ , where  $o_e = \omega_e/\omega_0$  and  $g = \phi/\omega_0$  are rational functions on  $\mathcal{X}$ . Since  $\omega_0$  is zero only at  $Q$ , the key equation is now that  $f$  is an error locator if and only if Eq. (5) is satisfied for some  $g \in R$ .

For instance, when  $\mathcal{X}$  is a smooth plane curve  $V(F)$  over  $\mathbb{F}_q$  defined by  $F \in \mathbb{F}_q[X, Y]$ , with a single smooth point  $Q$  at infinity, then it is true that  $(2g - 2)Q$  is canonical. O’Sullivan shows in Example 4.2 of [6] (using a slightly different notation) that

$$o_e = \sum_{P \in \mathcal{X}(\mathbb{F}_q)} e_P H_P, \tag{6}$$

where if  $P = (a, b)$ , then  $H_P = \frac{F(a, Y)}{(X - a)(Y - b)}$ . This is a function with a pole of order 1 at  $P$ , a pole of order  $2g - 1$  at  $Q$ , and no other poles.

To relate this to our approach, note that we may assume from the start that  $Q = (0 : 1 : 0)$  and that  $F$  is taken in the form

$$F(X, Y) = X^\beta - cY^\alpha + G(X, Y)$$

for some relatively prime  $\alpha < \beta$  generating the value semigroup at  $Q$ . Every term in  $G$  has  $(\alpha, \beta)$ -weight less than  $\alpha\beta$ . First we rearrange to obtain

$$H_P = \frac{F(a, Y)}{(X - a)(Y - b)} = \frac{(a^\beta - X^\beta) + F(X, Y) + (G(a, Y) - G(X, Y))}{(X - a)(Y - b)}$$

The  $F(X, Y)$  term in the numerator does not depend on  $P$ . We can collect those terms in the sum Eq. (6) and factor out the  $F(X, Y)$ . We will see shortly that those terms can in fact be ignored. The  $G(a, Y) - G(X, Y)$  in the numerator furnish terms that go into the error evaluator  $g$  here. The remaining portion is

$$\frac{-(X^\beta - a^\beta)}{(X - a)(Y - b)} = -\frac{X^{\beta-1}}{Y} \sum_{i=0}^{\beta-1} \sum_{j=0}^{\infty} \frac{a^i b^j}{X^i Y^j}.$$

The sum here looks very much like that defining our  $h_P$  from Theorem 3.3, except that it only extends over the monomials in complement of  $\langle LT(F) \rangle$ . Call this last sum  $h'_P$ . As noted before the full series  $h_P$  (and consequently  $S$ ) are redundant. For example, every ideal contained in  $m_P$  (for instance the ideal  $I = \langle F \rangle$  defining the curve), produces relations between the coefficients. From the duality theorem, Theorem 3.1, we have that  $I \subset m_P$  implies  $(m_P)^\perp \subset I^\perp$ , so  $F \cdot h_P = 0$ .

The relation  $F \cdot h_P = 0$  says in particular that the terms in  $h'_P$  are sufficient to determine the whole series  $h_P$ . Indeed, we have

$$h_P = \sum_{i=0}^{\infty} \left( \frac{(cY^\alpha - G)}{X^\beta} \right)^i h'_P = \left( \frac{X^\beta}{F} \right) h'_P.$$

It follows that O'Sullivan's key equation and ours are equivalent.

We now turn to the precise relation between solutions of our key equation and the polynomials generated by the BMS decoding algorithm applied to the  $C_\ell = Ev_\ell^\perp$  codes from order domains  $R$ . We will see that the BMS algorithm systematically produces successively better approximations to solutions of  $f \cdot \mathcal{S}_e = 0$ , so that in effect, *the BMS algorithm is a method for solving the key equation for these codes.*

For our purposes, it will suffice to consider the "Basic Algorithm" from §3 of [5], in which all needed syndromes are assumed known and no sharp stopping criteria are identified. The *syndrome mapping* corresponding to the error vector  $e$  is

$$\begin{aligned} \text{Syn}_e : R &\rightarrow \mathbb{F}_q \\ f &\mapsto \sum_{P \in \mathcal{E}} e_P f(P), \end{aligned}$$

where as above  $\mathcal{E}$  is the set of error locations. The same reasoning used in the proof of our Theorem 4.1 shows

$$f \in I_{\mathcal{E}} \Leftrightarrow \text{Syn}_e(fg) = 0, \forall g \in R. \quad (7)$$

From Definition 2.1 and Geil and Pelikaan's presentation theorem, we have an ordered monomial basis of  $R$ :

$$\Delta = \{X^{\alpha(j)} : j \in \mathbb{N}\},$$

whose elements have distinct  $\rho$ -values. As in the construction of the  $Ev_\ell$  codes, we write  $V_\ell = \text{Span}\{1 = X^{\alpha(1)}, \dots, X^{\alpha(\ell)}\}$ . The  $V_\ell$  exhaust  $R$ , so for  $f \neq 0 \in R$ , we may define

$$o(f) = \min\{\ell : f \in V_\ell\},$$

and (for instance)  $o(0) = -1$ . In particular the semigroup  $\Gamma$  in our presentation carries over to a (nonstandard) semigroup structure on  $\mathbb{N}$  defined by the addition operation

$$i \oplus j = k \Leftrightarrow o(X^{\alpha(i)} X^{\alpha(j)}) = k.$$

Given  $f \in R$ , one defines

$$\begin{aligned} \text{span}(f) &= \min\{\ell : \exists g \in V_\ell \text{ s.t. } \text{Syn}_e(fg) \neq 0\} \\ \text{fail}(f) &= o(f) \oplus \text{span}(f). \end{aligned}$$

When  $f \in I_\mathcal{E}$ ,  $\text{span}(f) = \text{fail}(f) = \infty$ .

The BMS algorithm, then, is an iterative process which produces a Gröbner basis for  $I_\mathcal{E}$  with respect to a certain monomial order  $>$ . The strategy is to maintain data structures for all  $m \geq 1$  as follows. The  $\Delta_m$  are an increasing sequence of sets of monomials, converging to the monomial basis for  $I_\mathcal{E}$  as  $m \rightarrow \infty$ , and  $\delta_m$  is the set of maximal elements of  $\Delta_m$  with respect to  $>$  (the “interior corners of the footprint”). Similarly, we consider the complement  $\Sigma_m$  of  $\Delta_m$ , and  $\sigma_m$ , the set of minimal elements of  $\Sigma_m$  (the “exterior corners”). For sufficiently large  $m$ , the elements of  $\sigma_m$  will be the leading terms of the elements of the Gröbner basis of  $I_\mathcal{E}$ , and  $\Sigma_m$  will be the set of monomials in  $LT_>(I_\mathcal{E})$ .

For each  $m$ , the algorithm also produces collections of polynomials  $F_m = \{f_m(s) : s \in \sigma_m\}$  and  $G_m = \{g_m(c) : c \in \delta_m\}$  satisfying:

$$\begin{aligned} o(f_m(s)) &= s, & \text{fail}(f_m(s)) &> m \\ \text{span}(g_m(c)) &= c, & \text{fail}(g_m(c)) &\leq m. \end{aligned}$$

In the limit as  $m \rightarrow \infty$ , by Eq. (7), the  $F_m$  yield the Gröbner basis for  $I_\mathcal{E}$ .

We record the following simple observation.

**Theorem 4.2.** *With all notation as above, suppose  $f \in R$  satisfies  $o(f) = s$ ,  $\text{fail}(f) > m$ . Then*

$$f \cdot \mathcal{S}_e \equiv 0 \pmod{W_{s,m}},$$

where  $W_{s,m}$  is the  $\mathbb{F}_q$ -vector subspace of the formal power series ring  $T$  spanned by the  $X^{-\alpha(j)}$  such that  $s \oplus j > m$ .

**Proof.** By the definition,  $\text{fail}(f) > m$  means that  $\text{Syn}_e(fX^{\alpha(k)}) = 0$  for all  $k$  with  $o(f) \oplus k \leq m$ . By the definitions of  $\mathcal{S}_e$  and the contraction product,  $\text{Syn}_e(fX^{\alpha(k)})$  is exactly the coefficient of  $X^{-\alpha(k)}$  in  $f \cdot \mathcal{S}_e$ .  $\square$

The subspace  $W_{s,m}$  in Theorem 4.2 depends on  $s = o(f)$ . In our situation, though, note that if  $s' = \max\{o(f) : f \in F_m\}$ , then Theorem 4.2 implies

$$f \cdot \mathcal{S}_e \equiv 0 \pmod{W_{s',m}} \tag{8}$$

for all  $f = f_m(s)$  in  $F_m$ . Moreover, only finitely many terms from  $\mathcal{S}_e$  enter into any one of these congruences, so Eq. (8) is, in effect, a sort of general analog of Eq. (1).

The  $f_m(s)$  from  $F_m$  can be understood as approximate solutions of key equation (where the goodness of the approximation is determined by the subspaces  $W_{s',m}$ , a decreasing chain, tending to  $\{0\}$  in  $T$ , as  $m \rightarrow \infty$ ). The BMS algorithm thus systematically constructs better and better approximations to solutions of the key equation. O'Sullivan's stopping criteria (see [5]) show when further steps of the algorithm make no changes. The Feng-Rao theorem shows that any additional syndromes needed for this can be determined by the majority-voting process when  $wt(e) \leq \lfloor \frac{d_{FR}(C_\ell)-1}{2} \rfloor$ .

We conclude by noting that O'Sullivan has also shown in [6] that, for codes from curves, the BMS algorithm can be slightly modified to compute error locators and error evaluators simultaneously in the situation studied in Example 4.3. The same is almost certainly true in our general setting, although we have not worked out all the details.

## Acknowledgements

Thanks go to Mike O'Sullivan and Graham Norton for comments on an earlier version prepared while the author was a visitor at MSRI. Research at MSRI is supported in part by NSF grant DMS-9810361.

## References

- [1] T. Høholdt, R. Pellikaan, and J. van Lint, Algebraic Geometry Codes, in: *Handbook of Coding Theory*, W. Huffman and V. Pless, eds. (Elsevier, Amsterdam, 1998), 871-962.
- [2] M. O'Sullivan, New Codes for the Berlekamp-Massey-Sakata Algorithm, *Finite Fields Appl.* **7** (2001), 293-317.
- [3] O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields Appl.* **8** (2002), 369-396.
- [4] J. Little, The Ubiquity of Order Domains for the Construction of Error Control Codes, *Advances in Mathematics of Communications* **1** (2007), 151-171.
- [5] M. O'Sullivan, A Generalization of the Berlekamp-Massey-Sakata Algorithm, preprint, 2001.
- [6] M. O'Sullivan, The key equation for one-point codes and efficient error evaluation, *J. Pure Appl. Algebra* **169** (2002), 295-320.
- [7] F.S. Macaulay, *Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics, v. 19, (Cambridge University Press, Cambridge, UK, 1916).

- [8] D.G. Northcott, Injective envelopes and inverse polynomials, *J. London Math. Soc. (2)* **8** (1974), 290-296.
- [9] J. Emsalem and A. Iarrobino, Inverse System of a Symbolic Power, I, *J. Algebra* **174** (1995), 1080-1090.
- [10] B. Mourrain, Isolated points, duality, and residues *J. Pure Appl. Algebra* **117/118** (1997), 469-493.
- [11] A. Geramita, Inverse systems of fat points, Waring's problem, secant varieties of Veronese varieties and parameter spaces for Gorenstein ideals, *The Curves Seminar at Queen's (Kingston, ON)* **X** (1995), 2-114.
- [12] H. Chabanne and G. Norton, The  $n$ -dimensional key equation and a decoding application, *IEEE Trans. Inform Theory* **40** (1994), 200-203.
- [13] G.H. Norton, On  $n$ -dimensional Sequences. I, II, *J. Symbolic Comput.* **20** (1995), 71-92, 769-770.
- [14] G.H. Norton, On Shortest Linear Recurrences, *J. Symbolic Comput.* **27** (1999), 323-347.
- [15] G.H. Norton and A. Salagean, On the key equation over a commutative ring, *Designs, Codes and Cryptography* **20** (2000), 125-141.
- [16] J. Althaler and A. Dür, Finite linear recurring sequences and homogeneous ideals, *Appl. Algebra. Engrg. Comm. Comput.* **7** (1996), 377-390.