On a key equation and error evaluation 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

March 31, 2007

The Berlekamp-Massey decoding algorithm for a Reed-Solomon code can be phrased as a method for solving the *key equation*

$$fS \equiv g \bmod \langle X^{2t} \rangle. \tag{1}$$

Here S is the known univariate syndrome polynomial in X, and the error locator f and error evaluator g are unknown polynomials in X.

We identify an algebraic context for related key equations in the theory of Macaulay's *inverse systems*, [7, 8], and develop an analog of (1) for codes from order domains ([4, 10, 3, 6]). We also relate O'Sullivan's general version of the Berlkamp-Massey-Sakata (BMS) algorithm from [11] to the process of solving this equation. The key equation for n-dimensional cyclic codes studied by Chabanne and Norton, [2, 9], is a special case. Althaler and Dür, [1], consider a form of (1) from our point of view. This note is a summary of the results of [5] to which we refer for proofs.

Codes from order domains

A fundamental theorem of Geil and Pellikaan, [3], shows that order domains all have presentations as affine algebras $R \cong \mathbb{F}_q[x_1, \ldots, x_s]/I$ where I is an ideal generated by a Gröbner basis with a very specific form. We write

$X_R = \mathcal{V}(I)$ for the corresponding algebraic variety. The value semigroup Γ and the weight function $\rho : R \to \Gamma$ are defined using a suitable monomial order. In this note, we will assume that Γ can be put into order-preserving one-to-one correspondence with $\mathbb{Z}_{\geq 0}$. Such Γ are said to be *Archimedean* because it follows that for all nonconstant $f \in R$ and all $g \in R$ there is some $n \geq 1$ such that $\rho(f^n) \succ \rho(g)$. Let Δ be the ordered "footprint" basis of R with ordering by ρ-value. Let $\ell \in \mathbb{N}$ and let V_ℓ be the span of the first ℓ elements of Δ. In this way, we obtain evaluation codes $Ev_\ell = ev(V_\ell)$ defined on $X_R(\mathbb{F}_q)$ and dual codes $C_\ell = Ev_\ell^\perp$ for all ℓ.

Inverse systems

Let k be a field, let $S = k[X_1, \ldots, X_s]$ and let T be the formal power series ring $k[[X_1^{-1}, \ldots, X_s^{-1}]]$ in the inverse variables. T is an S-module under the *contraction* mapping $c : (f, g) \mapsto f \cdot g$ defined as follows. First, given monomials X^α 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 $c : S \times T \to T$.

Let $Hom_k(S, k)$ be the dual vector space, which is an S-module under $q\Lambda(p) = \Lambda(qp)$ for $p, q \in S$. $Hom_k(S, k)$ and T are isomorphic as S-modules via $\Lambda \leftrightarrow \sum_{\beta \in \mathbb{Z}^s_{\geq 0}} \Lambda(X^\beta) X^{-\beta}$; see [8] for more details.

For each ideal $I \subseteq S$, the annihilator, or *inverse system*, of I is

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

an S-submodule of T. Similarly, given an S-submodule $H \subseteq T$,

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

an ideal in S. The ideals of S and the S-submodules of T are in inclusion-reversing bijective correspondence, and for all I, H we have $(I^\perp)^\perp = I$ and $(H^\perp)^\perp = H$.

Theorem 1 *If m_P is the maximal ideal of a point in affine space, then $(m_P)^\perp$ is generated by $h_P = \sum_{u \in \mathbb{Z}^s_{\geq 0}} P^u X^{-u}$. For all $f \in S$, $f \cdot h_P = f(P) h_P$, and the submodule $(m_P)^\perp$ is a one-dimensional vector space over k. If $I = m_{P_1} \cap \cdots \cap m_{P_\ell}$, then $I^\perp = \oplus (m_{P_i})^\perp$ is generated by $\sum_i h_{P_i}$.*

Both S and T are subrings of $K = k((X_1^{-1}, \ldots, X_s^{-1}))$, the field of fractions of T. 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 $S_+ = \langle X_1, \ldots, X_s \rangle \subset S \subset K$. We will denote this by $(fg)_+$.

The key equation and the BMS algorithm

Let C_ℓ be a dual evaluation code from an order domain R. Consider an error vector $e \in \mathbb{F}_q^n$. If $\mathcal{E}$ is the support of the error, then we define

$$I_{\mathcal{E}} = \{f \in \mathbb{F}_q[X_1, \ldots, X_s] : f(P) = 0, \ \forall P \in \mathcal{E}\}.$$

For each monomial $X^u \in \mathbb{F}_q[X_1, \ldots, X_s]$, the error syndrome is

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

Generalizing [2], we define the *syndrome series*

$$\mathcal{S}_e = \sum_{u \in \mathbb{Z}^s_{\geq 0}} E_u X^{-u} \in T = \mathbb{F}_q[[X_1^{-1}, \ldots, X_s^{-1}]] \cong Hom_{\mathbb{F}_q}(S, \mathbb{F}_q).$$

We substitute from (2) for the syndrome E_u and change the order of summation to obtain:

$$\mathcal{S}_e = \sum_{u \in \mathbb{Z}^n_{\geq 0}} E_u X^{-u} = \sum_{P \in X_R(\mathbb{F}_q)} e_P \sum_{u \in \mathbb{Z}^n_{\geq 0}} P^u X^{-u} = \sum_{P \in X_R(\mathbb{F}_q)} e_P h_P, \tag{3}$$

where h_P is the generator of $(m_P)^\perp$ from Theorem 1.

Theorem 2 *For each e with $supp(e) = \mathcal{E}$, $I_{\mathcal{E}} = \langle \mathcal{S}_e \rangle^\perp$.*

In other words, $f \in I_{\mathcal{E}}$ if and only if $f \cdot \mathcal{S}_e = 0$ for all error vectors e with $supp(e) = \mathcal{E}$. This result is a restatement of the standard fact that the error locators give recurrences on the syndromes. Let $f = \sum_m f_m X^m \in S$. Then

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

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

The equation $f \cdot \mathcal{S}_e = 0$ for $f \in I_{\mathcal{E}}$ will be called the general *key equation*. In [5] it is shown how this relates to known key equations for various classes of codes. Truncating $\mathcal{S}_e$, we could obtain a congruence similar to (1) involving only known syndromes (see the discussion following (4) below). The way to obtain error evaluators in this situation is to consider the "purely positive parts" $(f\mathcal{S}_e)_+$ for certain solutions f of our key equation.

To relate solutions of our key equation and the BMS algorithm, we refer to the *"Basic Algorithm"* from §3 of [11], in which all needed syndromes are assumed known and no stopping criteria are specified. The *syndrome mapping* is defined by $Syn_e(f) = \sum_{P \in \mathcal{E}} e_P f(P)$ where $f \in R$. The proof of our Theorem 2 also shows $f \in I_{\mathcal{E}} \Leftrightarrow Syn_e(fg) = 0, \forall g \in R$.

From Geil and Pellikaan's presentation theorem, we have the ordered monomial basis $\Delta = \{X^{\alpha(j)} : j \in \mathbb{N}\}$ of R. The $V_\ell = \text{Span}\{X^{\alpha(j)} : j \leq \ell\}$ exhaust R, so for $f \neq 0 \in R$, we may define $o(f) = \min\{\ell : f \in V_\ell\}$. This induces a (nonstandard) semigroup operation on $\mathbb{N}$ defined by $i \oplus j = k \Leftrightarrow o(X^{\alpha(i)}X^{\alpha(j)}) = k$. Given $f \in R$, one defines

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

so $f \in I_{\mathcal{E}} \Leftrightarrow span(f) = fail(f) = \infty$.

The mth iteration of the BMS algorithm produces a collection of polynomials F_m satisfying $fail(f) > m$.

Theorem 3 *With all notation as above, suppose $f \in R$ satisfies $o(f) = s$, $fail(f) > m$. Then*

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

where $W_{s,m} = \text{Span}\{X^{-\alpha(j)} : s \oplus j > m\} \subset T$.

The subspace $W_{s,m}$ depends on $s = o(f)$. In our situation, though, note that if $s' = \max\{o(f) : f \in F_m\}$, then Theorem 3 implies

$$f \cdot \mathcal{S}_e \equiv 0 \bmod W_{s',m} \tag{4}$$

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 (4) is, in effect, a sort of general analog of (1). Moreover, as is well-known, BMS produces a Gröbner basis for $I_{\mathcal{E}}$.

In [5] it is shown that univariate error locators and evaluators can be produced as in [2]. Moreover, O'Sullivan has shown in [12] that, for codes

from curves, the BMS algorithm can be slightly modified to compute more useful error locators and error evaluators simultaneously. We conjecture that the same is true in our general setting.

References

[1] J. Althaler and A. Dür, Finite linear recurring sequences and homogeneous ideals, *Appl. Algebra. Engrg. Comm. Comput.* **7** (1996), 377-390.

[2] H. Chabanne and G. Norton, The n-dimensional key equation and a decoding application, *IEEE Trans. Inform Theory* **40** (1994), 200-203.

[3] O. Geil and R. Pellikaan, On the Structure of Order Domains, *Finite Fields Appl.* **8** (2002), 369-396.

[4] 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.

[5] J. Little, A key equation and the computation of error values for codes from order domains, *preprint*, ArXiv: math.AC/0303299.

[6] J. Little, The Ubiquity of Order Domains for the Construction of Error Control Codes, *Advances in Mathematics of Communications* **1** (2007), 151-171.

[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] G.H. Norton, On n-dimensional Sequences. I, II, *J. Symbolic Comput.* **20** (1995), 71-92, 769-770.

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

[11] M. O'Sullivan, A Generalization of the Berlekamp-Massey-Sakata Algorithm, preprint, 2001.

[12] M. O'Sullivan, The key equation for one-point codes and efficient error evaluation, *J. Pure Appl. Algebra* **169** (2002), 295-320.