Journal of Statistical Planning and Inference 94 (2001) 371–380

journal of
statistical planning
and inference

www.elsevier.com/locate/jspi

Analytic approach to coset–leader decoding leads to extension of the Welch–Berlekamp theorem ☆

Dingjia Xin

Fudan University, Shanghai 200433, People's Republic of China

(In honor of the tenth anniversary of the Welch–Berlekamp algorithm)

Abstract

This paper provides a complete proof of the Welch–Berlekamp theorem on which the Welch–Berlekamp algorithm was founded. By introducing an analytic approach to coset–leader decoders for Reed–Solomon codes, the Welch–Berlekamp key-equation of error corrections is enlarged and a complete proof of the Welch–Berlekamp theorem is derived in a natural way, and the theorem is extended such that the BCH-bound constraint is moved. © 2001 Published by Elsevier Science B.V.

Keywords: Coset–leader decoding; Cyclic codes; Reed–Solomon codes; Welch–Berlekamp algorithm

1. Basic feature of the research

As the Welch–Berlekamp (W–B) algorithm of decoding Reed–Solomon codes has evident superiority to that of the classic Berlekamp–Massey's, and in view of the fact that the W–B theorem on which the W–B algorithm is founded has not been proved yet while the algorithm was published as US patent in 1986, this paper aims at a complete proof of the W–B Theorem. It also aims at extension of the W–B theorem so that the restriction from the BCH bound can be removed and validity of the W–B algorithm enables us to enlarge as far as a universal algorithm of decoding cyclic codes beyond the BCH bound.

In the paper, we recall the coset–leader decoder (Section 2) for decoding cyclic codes so that the BCH bound as well as other bounds will not be taken into consideration. Especially, under participation of proper analytic approach to coset–decoder for Reed–Solomon codes, extension of the W–B theorem as well as the strengthened W–B algorithm is obtained. The fundamental frame of the approach is analysis of solutions

☆ Supported by National Natural Science Foundation of China under Contract No. 69252005.

E-mail address: djxin@solaris.fudan.sh.cn (D. Xin).

PII: S0378-3758(00)00267-6

of co-adjunctive systems of minimum homogeneous interpolation problems (MHIP) we settled specially (Section 3). By introducing the concept of *character pair of* elements in cosets induced by received word, an associated co-adjunctive system of MHIP is introduced (Section 4), it is shown that the character pairs of elements in cosets can be regarded as a weak solution of the associated MHIP systems, and the W–B theorem is derived in a natural way and is extended in the following fashion:

1. When coset–leader of coset induced by a received word is weighted within the BCH bound of codes, its characteristic pair is just a solution of MHIP-I in the associated systems of the coset. It is a variation of the W–B theorem;
2. In case the weight is greater than the BCH bound, the character pair is a polynomial combination of solutions of the associated co-adjunctive systems. It is an extension of the W–B theorem in which error locators beyond the BCH bound are involved.

Based on the extension, a strengthened W–B algorithm for decoding cyclic codes beyond the BCH bound is scheduled with numeric example for illustrations (Section 5).

2. Generalized coset–leader decoding for linear codes

The kernel problem in decoding cyclic codes beyond the BCH bound is how to predict the error locators when weight exceeds the bound. In an earlier stage, many resourceful designed algorithms aimed at meeting the diverse bounds: HT bound, Roos bound, LW bound, etc., by and by, complete decoding for errors of weight beyond the t_{true} was considered. During the research, no general formula was produced to predict error locator polynomials; it is open till today. However, a classical but universal decoding strategy called the coset–leader decoding (CL decoding, briefly) should be accepted as the universal way to meet the requisition if we have an efficient method to describe analytically elements in cosets; it is the starting point in our consideration.

Suppose $\sum_q = \{(c_0, c_1, \ldots, c_{n-1})\}$ is a linear code over F_q. Let c$'$ be a received word, with coset $\{c'\} = \{c' + \sum_q\}$ being induced by the c$'$. Denote the coset–leaders (elements of least weight in the coset) by $e_1, e_2, \ldots, e_s$, thus for $c^{(i)} = c' - e_i \in \sum_q$, it holds (coset–leader decoder): $d(c', c^{(1)}) = d(c', c^{(2)}) = \cdots = d(c', c^{(s)}) < d(c', c)$, $c \in \sum_q \backslash \{c^{(i)}\}_{i=1}^{s}$. When $s = 1$, it decodes c$'$ to a unique codeword $c = c' - e_1$ in the sense of minimum distance decoding, and when $s > 1$, it embodies complete decoding for c$'$. When the CL-decoder is employed to decode cyclic codes in general, it no longer takes into consideration the states of bounds even when they are important in theoretical study.

Finding coset–leaders for coset is not easy if it is treated rigidly by definition, this is the reason why CL decoding is not popular in practice. In the paper, an analytic manipulation of finding coset–leader in case of cyclic codes is presented based on analysis of co-adjunctive system of minimal homogeneous interpolation problems associated with a given codeword.

3. Minimum interpolation systems and weak solutions

Let F be a field, t_i, $a_i, b_i \in F$, $(a_i, b_i) \neq (0,0)$, $t_i \neq t_j$, $i \neq j$; $i,j = 1,2,\dots n$, and $d(x)$ be a polynomial over F. The task of finding a pair of polynomials $(g(x), f(x))$ over F subject to interpolative constraints:

$$\begin{aligned}
&L_j(g,f) = a_j g(t_j) - b_j f(t_j) = 0, \quad j = 1,2,\dots,n,\\
&\deg(g(x)) < \deg(f(x)),\\
&\text{Minimize}(\deg(f(x))), \qquad (1)
\end{aligned}$$

is called the I-category of minimum homogeneous interpolation problem *(MHIP-I) over field F. The pair $(g(x), f(x))$ is called the solution of the problem, in which the polynomial $f(x)$ is called the principal solution. Besides, the degree of $(g(x), f(x))$ is defined by $\deg(f(x))$. Correspondingly, the task of finding a pair of polynomials $(h(x), k(x))$, $(h(x), k(x)) \neq (0,0)$, over an F subject to constraints:

$$\begin{aligned}
&L_j(h,k) = a_j h(t_j) - b_j k(t_j) = 0, \quad j = 1,2,\dots,n,\\
&\deg(k(x)) \leqslant \deg(h(x)),\\
&\text{Minimize}(\deg(h(x))), \qquad (2)
\end{aligned}$$

is called the II-category of MHIP (MHIP-II), the pair $(h(x), k(x))$ is called solution of the MHIP-II, and polynomial $h(x)$ is called the principal solution. Besides, the degree of $(h(x), k(x))$ is defined by $\deg(h(x))$. Finally, systems of MHIP-I (1) and MHIP-II (2) are called co-adjunctive MHIP systems (Xin, 1994).

Solving systems (1) will lead to solving system (2); it can be accomplished by *Point–Point Extension*, precisely, after getting two pairs $(g^{(i)}(x), f^{(i)}(x))$ and $(h^{(i)}(x), k^{(i)}(x))$ for (1) and (2) up to $i = j$, the solving strategy focuses on the pairs so that the modified pairs $(g^{(i+1)}(x), g^{(i+1)}(x))$ and $(h^{(i+1)}(x), k^{(i+1)}(x))$ satisfy (1) and (2) up to $i = j+1$. An iterative manipulation named the Pull–Push iteration is available (Welch and Berlekamp, 1986; Xin, 1994).

Initiation

$$\begin{aligned}
(g^{(1)}(x), f^{(1)}(x)) &= (0, (x - t_1)), & b_1 &\neq 0,\\
&=(0,1), & b_1 &= 0,\\
(h^{(1)}(x), k^{(1)}(x)) &= (b_1, a_1), & b_1 &\neq 0,\\
&= ((x - t_1), 0), & b_1 &= 0.
\end{aligned}$$

Step A: For $(g^{(i)}(x), f^{(i)}(x))$, $(h^{(i)}(x), k^{(i)}(x))$, compute deviation for the next point t_{i+1} : $l_{i+1} = L_{i+1}(g^{(i)}(x), f^{(i)}(x))$, $m_{i+1} = L_{i+1}(h^{(i)}(x), k^{(i)}(x))$, go to Step B;

Step B: $\deg(l_{i+1} h^{(i)}(x)) < \deg(m_{i+1} f^{(i)}(x))$? if yes, set

$$(g^{(i+1)}(x), g^{(i+1)}(x)) = (m_{i+1} g^{(i)}(x) - l_{i+1} h^{(i)}(x), m_{i+1} f^{(i)}(x) - l_{i+1} k^{(i)}(x)),$$

$$(h^{(i+1)}(x), k^{(i+1)}(x)) = ((x - t_{i+1}) h^{(i)}(x), (x - t_{i+1}) k^{(i)}(x)),$$

go to step C; otherwise, set

$$(g^{(i+1)}(x), g^{(i+1)}(x)) = ((x - t_{i+1})g^{(i)}(x), (x - t_{i+1})f^{(i)}(x)),$$

$$(h^{(i+1)}(x), k^{(i+1)}(x)) = (m_{i+1}h^{(i)}(x) - l_{i+1}g^{(i)}(x), m_{i+1}k^{(i)}(x) - l_{i+1}f^{(i)}(x)),$$

go to Step C,

Step C: $i+1 < n$? if yes, $i \leftarrow i+1$, go back to Step B; otherwise, $(g^{(n)}(x), f^{(n)}(x))$ and $(g^{(n)}(x), f^{(n)}(x))$ are solutions of the co-adjunctive systems (1) and (2).

Some theorems guarantee the correctness of the iteration (see Xin, 1994); here we introduce a few of them.

Theorem 2.1. *The ith interim result* $(g^{(i)}(x), f^{(i)}(x))$, $(h^{(i)}(x), k^{(i)}(x))$ *of systems* (1) *and* (2) *cannot be simultaneously the* $(i+1)$*th interim result of the systems.*

The theorem removes the possibility of simultaneous occurrence of $l_{i+1} = 0$ and $m_{i+1} = 0$; it guarantees that the inequality criterion in Step B has deterministic meaning, and leads to the following fundamental property of principal solutions of co-adjunctive systems (1) and (2):

Theorem 2.2. *For solutions* $(g(x), f(x))$ *and* $(h(x), k(x))$ *of the co-adjunctive systems* (1) *and* (2), *it holds for principals*: $\deg(f(x)) + \deg(h(x)) = n$.

Definition. Suppose $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$ are two pairs of polynomials over F with $\deg(a_1(x)) < \deg(b_1(x))$ and $\deg(a_2(x)) < \deg(b_2(x))$. We call $(a'(x), b'(x))$ the remainder pair after division between the given pairs, in which, $b'(x)$ is the remainder between $b_1(x)$ and $b_2(x)$ (divisor is assigned to be the one of lower degree; in the case of equi-degree, it is assigned arbitrarily), and $a'(x)$ is formed by a coordinated operation acts on $a_1(x)$ and $a_2(x)$ (e.g. if $b'(x) = \lambda(x)b_1(x) + \mu(x)b_2(x)$, then $a'(x)$ is appointed as $\lambda(x)a_1(x) + \mu(x)a_2(x)$). The process is denoted symbolically as

$$((a_1(x), b_1(x)), a_2(x), b_2(x)) \to (a'(x), b'(x)).$$

Analogously, for two non-zero pairs $(c_1(x), d_1(x))$, and $(c_2(x), d_2(x))$ over F with $\deg(c_1(x)) \geqslant \deg(d_1(x))$, $\deg(c_2(x)) \geqslant \deg(d_2(x))$, we call the pair of polynomials $(c'(x), d'(x))$ the remainder pair after division between the given pairs, in which $c'(x)$ is the remainder after division between $c_1(x)$ and $c_2(x)$, and $d'(x)$ is formed coordinatedly as $d_1(x)$ and $d_2(x)$. The process is denoted symbolically as

$$((c_1(x), d_1(x)), c_2(x), d_2(x)) \to (c'(x), d'(x)).$$

Lemma 2.1. *The remainder between weak solutions and solution of system MHIP-I* (*MHIP-II*) *is a weak solution of its adjunctive system MHIP-II* (*MHIP-I*) *if the remainder is a non-zero pair* $(0, 0)$.

Theorem 2.3 (Decomposition of weak solutions). *Let* $(g(x), f(x))$ *and* $(h(x), k(x))$ *be solutions of co-adjunctive systems MHIP-I* (1) *and MHIP-II* (2), *respectively.*

Suppose $(\bar{g}(x), \bar{f}(x))$ *is a weak solution of the system* MHIP-I, *then polynomials* $a(x)$, $b(x)$ *exist uniquely*, *such that*

$$\begin{aligned}
&(\bar{g}(x), \bar{f}(x)) = a(x)(g(x), f(x)) + b(x)(h(x), k(x)),\\
&\deg(a(x)) = \deg(\bar{f}(x)) - \deg(f(x)),\\
&\deg(b(x)) \leqslant \deg(\bar{f}(x)) - \deg(h(x)) - 1.
\end{aligned} \tag{3}$$

Proof. Inequalities $\deg(g(x)) < \deg(f(x))$ and $\deg(k(x)) \leqslant \deg(h(x))$ lead to uniqueness of the composition. Now, consider a remainder $(h'(x), k'(x))$ between $(\bar{g}(x), f(x))$ and $(g(x), f(x))$. If $(h'(x), k'(x)) = (0, 0)$, the theorem holds; otherwise, $(h'(x), k'(x))$ is a weak solution of MHIP-II (2); thus division on pairs $(h'(x), k'(x))$ and $(h(x), k(x))$ will result in $(g'(x), f'(x))$. $(g'(x), f'(x))$ must be (0,0), otherwise, $(g'(x), f'(x))$ is a weak solution of MHIP-I (1) with $\deg(f'(x)) \leqslant \deg(h'(x)) < \deg(f(x))$, it is impossible. Expanding $(0, 0) = (g'(x), f'(x))$ in terms of $(h'(x), k'(x))$ and $(h(x), k(x))$, and substituting $(h'(x), k'(x))$ in terms of $(g(x), f(x))$ and $(\bar{g}(x), \bar{f}(x))$, the assertion of decomposition theorem holds. □

4. Extension of Welch–Berlekamp theorem

The classic Shortest Shifting Register Algorithm created by Berlekamp and Massey provided a less computationally complex way to meet the error locator in decoding cyclic codes within the BCH bound. Since then, establishing error-locator prediction beyond the BCH bound enjoys popular confidence in decoding cyclic codes. Welch and Berlekamp (1986) provided a new strategy to predict structure of error locators; validity is, however, still limited in the BCH bound. Here we present a new approach to establish a general prediction formula for error locators whatever the weight is. The new approach is based on structure analysis of elements in coset induced by received word while the code is employed for data transmission.

Let Ω_q be a q-ary cyclic code embedded in a Reed–Solomon code Ω_{q^r} generated by $G(x) = \prod_{i=1}^{2t}(x - \alpha^{m+i})$ with m being an integer. We assume that Ω_{q^r} admits a systematic structure with $R = \{\alpha^0, \alpha^1, \ldots, \alpha^{2t-1}\}$, and $I = \{\alpha^{2t}, \alpha^{2t+1}, \ldots, \alpha^{q^r-2}\}$ for redundant location and message location, respectively.

Introduce auxiliary functions $\gamma(x)$ and $v(x)$ (Xin, 1994):

$$\gamma(x) = G(x)/(x - \alpha^{m+1}) = \sum_{i=0}^{2t-1} \gamma_i x^i, \quad v(x) = x^{-(m+1)} \sum_{k=0}^{2t-1} (\gamma_k \alpha^{(m+1)k}/(\alpha^k - x)).$$

Suppose $c'(x)$ is a received word:

$$c'(x) = c_{\mathrm{R}}(x) + c_I(x) = \sum_{j=1}^{e_1} Z_j x^{m_j} + \sum_{j=1}^{e_2} Y_j x^{l_j}$$

and $r(x)=c'(x)(\bmod G(x))=\sum_{i=0}^{e_1} r_i x^i$, we have

$$r_i=\sum_{j=1}^{e_1} Z_j\delta_{i,mj}+\alpha^i\gamma_i\left(\sum_{j=1}^{e_2} Y_j/(v(\alpha^{l_j})(\alpha^i-\alpha^{l_j}))\right).$$

Set $n(x),m(x),\tau(x)$ and $\sigma(x)$ as $n(x)/m(x)=\sum_{j=1}^{e_2}(Y_j/v(\alpha^{l_j})(x-\alpha^{l_j}))$, $\tau(x)=\prod_{j=1}^{e_1}(x-\alpha^{m_j})n(x)$, and $\sigma(x)=\prod_{j=1}^{e_1}(x-\alpha^{m_j})m(x)$, $(GCD(n(x),m(x))=1)$. The polynomial $\sigma(x)$ thus defined is just the locator of $e(x)$. Since the non-zero components $\{Y_j\}_{j=1}^{e_2}$ of $c'(x)$ can be expressed as $Y_j=(v(x)\tau(x)/(\mathrm{d}\sigma(x)/\mathrm{d}x))|_{x=\alpha^{l_j}}$ (Welch and Berlekamp, 1986; Xin, 1994) $c'(x)$ can be converted as

$$c'(x)=r(x)-\sum_{j=1}^{e_2} Y_j x^{l_j}(\bmod G(x))-\sum_{j=1}^{e_2} Y_j x^{l_j},$$

The pair $(\tau(x)(x),\sigma(x))$ is logically called the characteristic of $c'(x)$; evidently, $\alpha^i\gamma_i\tau(\alpha^i)-r_i\sigma(\alpha^i)=0,\ \alpha^i\in R,\ \deg(\tau(x))<\deg(\sigma(X))$.

Consider a coset $\{c'(x)\}$ induced by $c'(x),\{c'(x)\}=\{c'(x)\}+\Omega_q$, the above process of establishing character pair is available to all elements in the coset $c'(x)$. In view of finding elements of least weight (coset–leader) in the $c'(x)$ which embodies minimum distance decoding for the received $c'(x)$, solving the following system is meaningful:

$$\begin{aligned}&\alpha^i\gamma_i g(\alpha^i)-r_i f(\alpha^i)=0,\quad \alpha^i\in R,\\&\deg(g(x))<\deg(f(x)),\\&\text{minimize}(\deg(f(x))).\end{aligned}$$

It is just the Welch–Berlekamp key-equation of decoding cyclic codes. However, we consider the following co-adjunctive systems rather than the above single one:

Definition (*Co-adjunctive systems*).

$$\begin{aligned}&\alpha^i\gamma_i g(\alpha^i)-r_i f(\alpha^i)=0,\quad \alpha\in R,\\&\deg(g(x))<\deg(f(x)),\\&\text{minimize}(\deg(f(x))),\end{aligned}\tag{4}$$

$$\begin{aligned}&\alpha^i\gamma_i h(\alpha^i)-r_i k(\alpha^i)=0,\quad \alpha^i R,\\&\deg(k(x))\leqslant\deg(h(x)),\ (h(x),k(x))\neq(0,0),\\&\text{minimize}(\deg(h(x)))\end{aligned}\tag{5}$$

are called the associated systems of the coset $\{c'(x)\}$ induced by received $c'(x)$.

Since character pair of $\{c'(x)\}$ is a weak solution of system (4) over F_{q^r}, it holds from Theorem (2.3):

Theorem 3.1. *Character pair $(\tau(x),\sigma(x))$ of $\{c'(x)\}$ is a combination of solution $(g(x),f(x))$ of* (4) *and solution $(h(x),k(x))$ of* (5) *in polynomials $a(x)$ and $b(x)$*

over F_{q^r}:

$$(\tau(x),\sigma(x)) = a(x)(g(x),f(x)) + b(x)(h(x),k(x)).$$

We now consider the relation between character $(\tau(x),\sigma(x))$ of the least-weight elements $e(x)$ and solutions $(g(x),f(x))$ and $(h(x),k(x))$ of the associated systems (4) and (5).

Lemma 3.1. *For character* $(\tau(x),\sigma(x))$ *of an element in coset* $\{c'(x)\}$, *the equality* $(\tau(x),\sigma(x)) = \lambda(x)(g(x),f(x))$ *leads to* $\lambda(x)=\lambda$, $\lambda \in F_{q^r}$, *where* $\lambda(x)$ *is assumed as a polynomial over* F_{q^r}.

Proof. It can be verified straightforwardly by viewing the structure of character pair $(\tau(x),\sigma(x))$ of the element $e(x)$ as defined above. If $e(x)$ has no components in the location R, the lemma is valid due to $\gcd(n(x),m(x)) = 1$. Now turn to the other case, i.e. the element takes non-zero components at positions $\{\alpha^{m_j}\}$, $j = 1,2,\ldots,e_1$, in location R, and $\deg(\lambda(x)) > 0$, $\lambda(x)$ must be a product $\prod_{j=1}^{e_1}(x-\alpha^{m_j})$, $(g(x),f(x))$ will no longer be a solution of (4), a contradiction! So $\lambda(x)$ must be an element in F_{q^r}. □

Theorem 3.2 (Extension of the Welch–Berlekamp theorem). *Suppose* $e(x)$ *is an element of* $\{c'(x)\}$, *let* $(\tau(x),\sigma(x))$ *be its character pair, it holds that*

I. *If* $wt(e(x)) \leqslant t$, *then* $(\tau(x),\sigma(x)) = \lambda(g(x),f(x))$, $\lambda \in F_{q^n}$;

II. *If* $wt(e(x)) = t+\delta$, $\delta > 0$, *then* $\deg(f(x)) > t-\delta$ *and polynomials* $a(x)$, $b(x)$ *exist such that*

$$(\tau(x),\sigma(x)) = a(x)(g(x),f(x)) + b(x)(h(x),k(x)),$$
$$\deg(a(x)) = \deg(\sigma(x)) - \deg(f(x)),$$
$$\deg(b(x)) + \deg(h(x)) \leqslant \deg(\sigma(x)) - 1.$$

Proof. For assertion I, since $(\tau(x),\sigma(x))$ is a weak solution of MHIP (4), two polynomials $a(x)$ and $b(x)$ exist such that $(\tau(x),\sigma(x)) = a(x)(g(x),f(x)) + b(x)(h(x),k(x))$. On the other hand, for Assertion II $\deg(f(x)) \leqslant \deg(\sigma(x)) \leqslant t$, hence from Theorem 2.2, $\deg(h(x)) \geqslant t$, $b(x) = 0$; thereby, from Lemma 3.1, $a(x) = \lambda \in F_{q^r}$. If on the contrary, $\deg(f(x)) \leqslant t-\delta$, then $\deg(h(x)) \geqslant t+\delta = \deg(\sigma(x))$ follows and therefore $(\tau(x),\sigma(x)) = a(x)(g(x),f(x))$, so $a(x) = c \in F_{q^r}$; however, $\deg(\sigma(x)) \neq \deg(f(x))$, a contradiction! So we have to assume that $\deg(f(x)) > t-\delta$, and polynomials $a(x)$, $b(x)$ exist such that $(\tau(x),\sigma(x)) = a(x)(g(x),f(x)) + b(x)$, $\deg(a(x)) = \deg(\sigma(x)) - \deg(f(x))$, $\deg(b(x)) \leqslant \deg(\sigma(x)) - \deg(h(x)) - 1$. □

The requisition "$Wt(e(x)) \leqslant t$" in case I of Theorem 3.1 is equivalent to the statement "$c'(x) = c(x) + e(x)$", $wt(e(x)) \leqslant 1$, it is just the Welch–Berlekamp algorithm published as a US patent (Welch and Berlekamp, 1986; see also Xin, 1994) and Theorem 3.1 extends the Welch–Berlekamp theorem as described in Case II. In practical use, we have the following prediction which is equivalent to Theorem 3.2.

Theorem 3.3 (Extension of the W–B prediction). *Let $(g(x), f(x))$ and $(h(x), k(x))$ be solutions of co-adjunctive systems* (4) *and* (5), *respectively, with respect to received word $c'(x)$. Suppose $(\tau(x), \sigma(x))$ is character pair of coset–leader $e(x)$ of $\{c'(x)\}$, then it holds that*

1. *If* $\deg(f(x)) = t+\delta,\ \delta > 0$, *then* $\deg(\sigma(x)) \geqslant t+\delta$, *and polynomials $a(x),\ b(x)$ exist*:
$$(\tau(x), \sigma(x)) = a(x)(g(x), f(x)) + b(x)(h(x), k(x)),$$
$$\deg(a(x)) = \deg(\sigma(x)) - \deg(f(x)),$$
$$\deg(b(x)) + \deg(h(x)) \leqslant \deg(\sigma(x)) - 1,$$
$$\text{minimize}(\deg(\sigma(x))),$$
2. *If* $\deg(f(x)) = t - \delta,\ \delta \geqslant 0$, *then either the Welch–Berlekamp prediction*:
$$\deg(\sigma(x)) = t - \delta,$$
$$(\tau(x), \sigma(x)) = c(g(x), f(x)), \quad c \in F_{q^r},$$
or $\deg(\sigma(x)) > t$, *with*
$$(\tau(x), \sigma(x)) = a(x)(g(x), f(x)) + b(x)(h(x), k(x)),$$
$$\deg(\sigma(x)) = \deg(a(x)) + \deg(f(x)),$$
$$\deg(b(x)) \leqslant \deg(\sigma(x)) - \deg(h(x)) - 1,$$
$$\text{minimize}(\deg(\sigma(x))),$$
holds.

Proof. It is needed only to prove Assertion 2.2. If, on the contrary, $t - \delta < \deg(\sigma(x)) \leqslant t + \delta$, then by assumption of $\deg(f(x))$, we have $\deg(h(x)) = t + \delta$, so $(\tau(x), \sigma(x)) = a(x)(g(x), f(x))$ and $\deg(a(x)) = 0$, and it leads to $\deg(\sigma(x)) = \deg(f(x))$, a contradiction! It means $\deg(\sigma(x)) > t + \delta$. □

Once $(\tau(x), \sigma(x))$ is obtained by means of the extended W–B prediction, erroneous Y_i at α^{l_i} can be determined as (Welch and Berlekamp, 1986)
$$Y_i = (v(x)\tau(x)/\mathrm{d}(\sigma(x)/\mathrm{d}x))|_{x=\alpha^{l_i}},$$
where α^{l_i} are roots of $\sigma(x) = 0$ in message location I.

The above theorems and corollary constitute a strategy of coset–leader prediction via solving co-adjunctive systems of MHIP (4), (5). It is quite different from the Welch–Berlekamp prediction, as it no longer depends on a single solution of (4) but on a pair of solutions of (4) and (5) while the weight of the coset–leader to beyond the BCH bound. We call the associated systems (4) and (5) the key-equation of decoding Ω_q, and call solutions of the system the base of coset $\{c'(x)\}$ induced by received $c'(x)$. The problem of finding error locator of error patterns in the sense of minimum distance decoding turns now to determining projection $a(x)$ and $b(x)$ on the base. With use of the Pull–Push algorithm, it constitutes extension of the Welch–Berlekamp algorithm.

Remark. Theorems 3.2 and 3.3 are also valid in the case of both primitive and non-primitive cyclic codes embedded in Reed–Solomon code Ω_{q^r} generated by $G(x)=\prod_{i=1}^{2t}(x-\alpha^{m+i})$. Furthermore, the treatment above is also available for the case when the embedded Reed–Solomon is encoded in a non-systematic structure (Berlekamp, 1989; Xin, 1995).

5. Numeric illustration

Let Ω_2 be a binary cyclic code determined by $\{\alpha^1,\alpha^2,\ldots,\alpha^6\}$ embedded in RS code Ω_{2^4} generated by $\prod_{i=1}^{6}(x-\alpha^i)$. Suppose received $c'(x)=x^1+x^{10}+x^{13}+x^{14}$ is a received word, find sending word $c(x)$.

Solution: The embedded Reed–Solomon (RS) code Ω_{2^4} has generator $G(x)=\prod_{i=1}^{6}(x-\alpha^i)=x^6+\alpha^{10}x^5+\alpha^{14}x^4+\alpha^4x^3+\alpha^6x^2+\alpha^9x+\alpha^6$, $\alpha^4+\alpha^1+\alpha^0=0$, and

$$\gamma(x)=G(x)/(x-\alpha^1)=\alpha^5+\alpha^{10}x+\alpha^8x^2+\alpha^4x^3+\alpha^3x^4+\alpha^5x^5,$$

$$r(x)=c'(x)(\operatorname{mod}G(x))=\alpha^6+\alpha^9x^1+\alpha^8x^2+\alpha^1x^3+\alpha^3x^4+\alpha^5x^5,$$

$$S(x)=\{r(\alpha^i)\}_{i=1}^{6}=\{s_1,s_2,\ldots,s_6\}=(1,1,\alpha^6,1,1,\alpha^{12}).$$

Step 1: Solving key-equation (4), (5) leads to solutions:

$$(g(x),f(x))=(\ldots,x^3+x^2+x^1+\alpha^6),$$

$$(h(x),k(x))=(\ldots,x^3+\alpha^7x^2+\alpha^7x^1+\alpha^{10}).$$

Go to Step 2.

Step 2: Since $\deg(f(x))=3$, the W–B strategy predicts error locator as $\sigma(x)=f(x)$. However, $f(x)$ being irreducible in $GF(2^4)$, W–B prediction fails. After extended WB prediction, predict $\sigma(x)=4$ first, and set:

$$\begin{aligned}\sigma(x)&=a(x)f(x)+b(x)k(x)\\&=(x+a)(x^3+x^2+x^1+\alpha^6)+b(x^3+\alpha^7x^2+\alpha^7x^1+\alpha^{10})\\&=x^4+\sigma_1x^3+\sigma_2x^2+\sigma_3x^1+\sigma^4.\end{aligned}$$

Identities $s_1=\sigma_1$, $s_3=\sigma_1s_2+\sigma_2s_1+\sigma_3$, and s_7,s_8,s_9 in terms of $s_1,s_2,\ldots,s_6$; $\sigma_1,\ldots,\sigma_4$ lead to $a=b$, $a^2+a\alpha^6+\alpha^{12}=0$; two solutions of a are thus obtained: $a_1=b_1=\alpha^{11}$, $a_2=b_2=\alpha^1$, hence

$$\sigma_1(x)=x^4+x^3+\alpha^{10}x^2+\alpha^3x^1+\alpha^3=(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6),$$

$$\sigma_2(x)=x^4+x^3+\alpha^5x^2+\alpha^7x^1+\alpha^3=(x-\alpha^1)(x-\alpha^{10})(x-\alpha^{13})(x-\alpha^{14}),$$

two coset–leaders are determined as

$$e_1 = (0,0,0,1,1,1,1,0,0,0,0,0,0,0,0),$$

$$e_2 = (0,1,0,0,0,0,0,0,0,0,1,0,0,1,1)$$

and the sending words are $c^{(1)}(x)=0$, and $c^{(2)}(x)=x^1+x^4+x^5+x^+x^7+x^{10}+x^{13}+x^{14}$.

Since the Ω_2 admits $d_{\text{true}} = d_{\text{BCH}} = 7$, the example shows a complete decoding procedure by using the extended Welch–Berlekamp prediction.

6. Uncited Reference

Jennings, 1995; Van Lint and Wilson, 1986; Wan, 1976.

References

Berlekamp, E.R., 1989. Soft-decision Reed–Solomon decoders. US Patent 4821268.

Jennings, S.M., 1995. Grobner basis view of Welch–Berlekamp algorithm for Reed–Solomon codes. IEE Proceedings (Communications) Vol. 142, No. 6, December.

Van Lint, J.L., Wilson, R.M., 1986. IEEE IT-32, January.

Wan, Z.X., 1976. Algebra and Coding. Academy Press, New York (in Chinese).

Welch, R.L., Berlekamp, E.R., 1986. Error Correction for Algebraic Block Codes. US Patent 4633470.

Xin, D., 1995. Decoding goppa codes in extended Welch–Berlekamp frame. 18th Symposium on Communications, Kingston, Canada, June.

Xin, D., 1994. Homogeneous minimum interpolation problems and key-equation of decoding Reed–Solomon codes. Sci. China 37 (11), 1387–1398.