Solving The Welch-Berlekamp Key Equation Over A Galois Ring

MARC A. ARMAND
Department of Electrical & Computer Engineering
National University of Singapore, 10 Kent Ridge Crescent,
SINGAPORE 119260.
eleama@nus.edu.sg   http://www.ece.nus.edu.sg

Abstract: – The Welch-Berlekamp (WB) key equation arises in the decoding of Reed-Solomon (RS) codes over finite fields where the decoding problem is viewed as a rational interpolation problem. The significance of this decoding approach lies in the fact that it does not require the prior evaluation of power sum symmetric functions, i.e. the so-called syndrome vector corresponding to a received word. It has recently been shown that RS codes over $\mathbb{Z}_q$, q a prime power, can also be decoded in the same way as their field counterparts. The purpose of this paper is therefore to present a generalization of a WB-type algorithm for solving the key equation over a Galois ring.

Key-Words: – Rational interpolation, Reed-Solomon codes, Welch-Berlekamp key equation, Galois rings.

1 Introduction

In [7], a new key equation based on rational interpolation for algebraically decoding Reed-Solomon (RS) codes over finite fields was given. This decoding strategy dispenses with the need of having to compute syndromes and hence boasts a significant computational advantage over conventional syndrome-based decoding procedures in this respect, particularly for long codes and when the number of correctable errors in a received word is large. Motivated by this computational advantage, we extend in [2], the approach of [7] to decode RS codes over $\mathbb{Z}_q$ where q is a prime power. In particular, we gave a characterization of the set of minimal solutions to the key equation over $\mathbb{Z}_q[[X]]$ as well as a modified Welch-Berlekamp (WB) algorithm for solving it. This algorithm is only valid when the cardinality of the prescribed set of interpolating points is four, which in the decoding context, implies that it is only applicable to double-error correction. Here, we present a different WB-type algorithm for solving the key equation without any restriction on the order of the data set. With it, the extended decoding approach of [2] can now be applied to RS codes over $\mathbb{Z}_q$ of arbitrary minimum distance.

As the underlying algebraic structure that we will be working with is a Galois ring, we begin with a brief review of some basic facts about it.

2 Galois rings

The Galois extension ring $R = \mathrm{GR}(q, a)$ is the quotient ring given by $\mathbb{Z}_q[y]/\Phi$ where p is prime, $l \geq 1$, $q = p^l$ and $a \geq 1$. The polynomial $\Phi \in \mathbb{Z}_q[y]$ is a basic irreducible polynomial of degree a, i.e. it is irreducible both over $\mathbb{Z}_q$ and $\mathrm{GF}(p)$. Further, R is a commutative ring with identity consisting of all the polynomials of degree at most $a-1$ over $\mathbb{Z}_q$. Addition and multiplication is modulo Φ.

Let ψ_p denote the induced (polynomial) reduction mapping, i.e. $\psi_p : \mathbb{Z}_q[y]/\Phi \mapsto \mathbb{Z}_p[y]/\overline{\Phi}$ where $\overline{\Phi}$ is the image of Φ over $\mathrm{GF}(p)$, and let $\mathcal{K} = \ker \psi_p$. Then $\psi_p : R/\mathcal{K} \cong \mathbb{Z}_p[y]/\overline{\Phi} = \mathrm{GF}(p^a)$, and $\mathcal{K}$ is a maximal ideal of R and is generated by p.

Any element of $R \setminus \{0\}$ is either a unit or a zero divisor. By [6, Theorem V.1], $\mathcal{K}$ is the set of zero divisors in R, which implies that the zero divisors in R are those elements divisible by p. Any element $r \in R \setminus \{0\}$ can be written as $r = u \cdot p^t$ where u is a unit in R, and t $(0 \leq t \leq l-1)$ is the unique power of p, [8, p. 308]. Thus, for $r, r' \in R$, $r'|r$ if and only if $\log_p r' \leq \log_p r$.

From [6, Theorem XVI.9], the group of units in R can be expressed as a direct product of cyclic groups. One of these groups has order $p^a - 1 = n$, say, and $\gcd(n, q) = \gcd(n, p) = 1$. Let γ be primitive in this cyclic group. Thus this group consists of all the roots of $X^n - 1$ in R, i.e. $\{1, \gamma, \ldots, \gamma^{n-1}\}$.

3 The Welch-Berlekamp key equation

Assume all polynomials are in $R[X]$ and all symbols in R. By δf and λf, we denote the degree, respectively, the leading coefficient of the polynomial f.

The decoding technique of RS codes over $\mathbb{Z}_q$ of [2] concerns determining the pair $(P, Q) \in R[X]^2$ satisfying the key equation

$$s_i Q(x_i) = P(x_i), \qquad i = 0, 1, \ldots, L-1 \qquad (1)$$

with $\delta P < \delta Q \leq \lfloor L/2 \rfloor$, δQ minimal, λQ a unit in R. Throughout, we shall take the x_i to be contained in distinct cosets of γ^i, i.e. $x_i \in \gamma^{j_i} + \mathcal{K}$ such that $j_i \neq j_k$ if $i \neq k$.

Let $S \in R[X]$, $\delta S < L - 1$ satisfy $S(x_i) = 0$ for $i = 0, 1, \ldots, L-1$ and let $H = \prod_{i=0}^{L-1}(X - x_i)$. Observe that such an S is well-defined as $x_i - x_j$ is a unit and hence invertible for $i \neq j$. So (1) can be recast as

$$QS - P \equiv 0 \bmod H. \qquad (2)$$

4 An iterative solution

In this section, we give an iterative method for solving (2). Throughout, for $(P, Q), (P', Q') \in R[X]^2$ and $f, g \in R[X]$, we take $f(P, Q) + g(P', Q')$ to mean $(fP, fQ) + (gP', gQ')$.

Let $H^{(i)} = \prod_{k=0}^{i-1}(X - x_k)$ and let the $R[X]$-submodule $M^{(i)}$ of $R[X]^2$ contain all solutions to the key equation modulo $H^{(i)}$, i.e.

$$M^{(i)} = \left\{ (P, Q) : QS - P \equiv 0 \bmod H^{(i)} \right\}.$$

We obtain the following sequence of modules

$$M^{(L)} \subset M^{(L-1)} \subset \ldots \subset M^{(0)} = R[X]^2$$

which is strictly increasing, since $(0, H^{(i)}) \in M^{(i)} \setminus M^{(i+1)}$.

Suppose $(P, Q) \in M^{(i)}$. The *discrepancy* d of (P, Q) is the obstruction to (P, Q) from also being contained in $M^{(i+1)}$ and is given by the quantity $s_i Q(x_i) - P(x_i)$. Thus, if $d = 0$, then (P, Q) is also an element of $M^{(i+1)}$. On the other hand, if $(P, Q) \notin M^{(i+1)}$ so that $d \neq 0$, then by commutativity, it can be verified that

$$(P, Q) - \frac{d}{d'}(P', Q')$$

is an element of $M^{(i+1)}$ where $(P', Q') \in M^{(i)}$ such that its discrepancy d' divides d. Trivially,

$$(P, Q)(X - x_{i-1})$$

is also contained in $M^{(i+1)}$.

Adopting the terminology of [3], the *rank* of $(P, Q) \in R[X]^2$ is the quantity $\max\{2\delta P + 1, 2\delta Q\}$, written $\mathrm{Rank}(P, Q)$. We state a useful result.

Theorem 1 *Let* (P, Q) *and* (P', Q') *be such that* $\mathrm{Rank}(P, Q) > \mathrm{Rank}(P', Q')$. *Then for any* $r \in R$,

(i) $\mathrm{Rank}((P, Q) + r(P', Q')) = \mathrm{Rank}(P, Q)$,

(ii) if $\mathrm{Rank}(P, Q)$ *is even, then* $\lambda(Q - rQ') = \lambda Q$; *otherwise,* $\lambda(P - rP') = \lambda P$.

Proof. (i) Suppose $\mathrm{Rank}(P, Q)$ is odd and $\mathrm{Rank}(P', Q')$ is even. Then $2\delta P' + 1 < \mathrm{Rank}(P', Q') = 2\delta Q' < \mathrm{Rank}(P, Q) = 2\delta P + 1$ and so $\delta(rP') \leq \delta P' < \delta P$ and in turn $\delta(P + rP') = \delta P$. Further, $\mathrm{Rank}(P, Q) > 2\delta Q$ and so $\max\{2\delta(rQ') \leq 2\delta Q', 2\delta Q\} < \mathrm{Rank}(P, Q)$. Thus,

$$\begin{aligned} & \mathrm{Rank}((P, Q) + r(P', Q')) \\ = \; & \max\{2\delta(P + rP') + 1 = 2\delta P + 1, \\ & \quad 2\delta(Q + rQ') \leq \max\{2\delta(rQ'), 2\delta Q\}\} \\ = \; & \mathrm{Rank}(P, Q) \end{aligned}$$

as required. If however, $\mathrm{Rank}(P', Q')$ is odd. Then $\mathrm{Rank}(P, Q) = 2\delta Q > \mathrm{Rank}(P', Q') = 2\delta Q'$ and so $\mathrm{Rank}((P, Q) + r(P', Q')) = 2\delta(Q + rQ') = 2\delta Q = \mathrm{Rank}(P, Q)$, as required. The proof for the case when $\mathrm{Rank}(P, Q)$ is even is similar. (ii) is a simple consequence of (i). ‡

Extending the definition of complementary interpolants of [1] to R, we say that (P, Q), $(P', Q') \in M^{(i)}$ are *complementary* if $\mathrm{Rank}(P, Q) + \mathrm{Rank}(P', Q') = 2i + 1$ and $P'Q - PQ' = up^{l-1}\prod_{k=0}^{i-1}(X - x_k - z_k)$ where u is some unit in R and $z_i \in \mathcal{K}$. One checks that the following l pairs

$$(0, p^{j-1}),\ (p^{l-j}, 0), \qquad j = 1, 2, \ldots l$$

are complementary interpolants in $M^{(0)}$. We shall use these $2l$ elements of $M^{(0)}$ to initialize our iterative procedure and thus fix $(P^{(0,j)}, Q^{(0,j)}) = (0, p^{j-1})$ and $(P^{(0,j+l)}, Q^{(0,j+l)}) = (p^{j-1}, 0)$ for $j = 1, 2, \ldots, l$. The reason for this will be clear in the following section.

At the i-th iteration, the idea is then to compute $2l$ elements $(P^{(i+1,1)}, Q^{(i+1,1)}), \ldots, (P^{(i+1,2l)}, Q^{(i+1,2l)})$ of $M^{(i+1)}$ from $2l$ elements $(P^{(i,1)}, Q^{(i,1)}), \ldots, (P^{(i,2l)}, Q^{(i,2l)})$ of $M^{(i)}$ obtained from the previous iteration. Denoting the discrepancy of $(P^{(i,j)}, Q^{(i,j)}) \in M^{(i)}$ as d_j, we update $(P^{(i,j)}, Q^{(i,j)})$ as follows:

Suppose $d_j \neq 0$. If there exists a k such that $d_k | d_j$ and $\mathrm{Rank}(P^{(i,k)}, Q^{(i,k)}) < \mathrm{Rank}(P^{(i,j)}, Q^{(i,j)})$, then set $(P^{(i+1,j)}, Q^{(i+1,j)}) = (P^{(i,j)}, Q^{(i,j)}) - \frac{d_j}{d_k}(P^{(i,k)}, Q^{(i,k)})$. If no such k exists, then set $(P^{(i+1,j)}, Q^{(i+1,j)}) = (P^{(i,j)}, Q^{(i,j)})(X - x_i)$. On the other hand, if $d_j = 0$, then we simply set $(P^{(i+1,j)}, Q^{(i+1,j)}) = (P^{(i,j)}, Q^{(i,j)})$. In both cases, $(P^{(i+1,j)}, Q^{(i+1,j)}) \in M^{(i+1)}$.

These statements give rise to an iterative procedure which we formally state in Algorithm 1 below.

Algorithm 1 *(Rational interpolation over a Galois ring)*

```
for $j := 1$ to $l$ do
  $(P^{(0,j)}, Q^{(0,j)}) := (0, p^{j-1})$;
  $(P^{(0,j+l)}, Q^{(0,j+l)}) := (p^{j-1}, 0)$;

for $i := 0$ to $L-1$ do
  for $j := 1$ to $2l$ do
    $d_j := s_i Q^{(i,j)}(x_i) - P^{(i,j)}(x_i)$;
  for $j := 1$ to $2l$ do
    if $d_j = 0$ then
      $(P^{(i+1,j)}, Q^{(i+1,j)}) := (P^{(i,j)}, Q^{(i,j)})$;
    else
      if $\exists\, k$ such that $d_k | d_j$ and $\mathrm{Rank}(P^{(i,k)}, Q^{(i,k)})$
        $< \mathrm{Rank}(P^{(i,j)}, Q^{(i,j)})$ then
        $(P^{(i+1,j)}, Q^{(i+1,j)}) := (P^{(i,j)}, Q^{(i,j)}) -$
                        $\frac{d_j}{d_k}(P^{(i,k)}, Q^{(i,k)})$;
      else
        $(P^{(i+1,j)}, Q^{(i+1,j)}) := (P^{(i,j)}, Q^{(i,j)})(X - x_i)$;

Return the $(P^{(L,j)}, Q^{(L,j)})$ for which $\lambda Q^{(L,j)}$ is a
unit and its rank is as small as possible.
```

Remark 1 *When $l = 1$ so that R is a field, Algorithm 1 reduces to what is essentially the WB algorithm of [5].*

At this point, we have only showed that the algorithm computes $2l$ elements of $M^{(i+1)}$ in the i-th iteration. We proceed with a detailed example on Algorithm 1, deferring the remaining justification to the next section.

Example 1 *Consider $R = \mathbb{Z}_{49}$, $H = \prod_{i=0}^{3}(X - 5^i)$, $s_0 = 8$, $s_1 = 34$, $s_2 = 19$ and $s_3 = 18$. In the initialization phase, we have $(P^{(0,1)}, Q^{(0,1)}) = (0, 1)$, $(P^{(0,2)}, Q^{(0,2)}) = (0, 7)$, $(P^{(0,3)}, Q^{(0,3)}) = (1, 0)$ and $(P^{(0,4)}, Q^{(0,4)}) = (7, 0)$.*

In the first iteration, the discrepancies of the $(P^{(0,j)}, Q^{(0,j)})$ are as follows: $d_1 = 8$, $d_2 = 7$, $d_3 = 48$ and $d_4 = 42$. Accordingly, the $(P^{(0,j)}, Q^{(0,j)})$ are updated as follows:

$$\begin{aligned}
(P^{(1,1)}, Q^{(1,1)}) &= (0,1)(X-1) = (0, X-1) \\
(P^{(1,2)}, Q^{(1,2)}) &= (0,7)(X-1) = (0, 7X-7) \\
(P^{(1,3)}, Q^{(1,3)}) &= (1,0) - \frac{48}{8}(0,1) = (1, 43) \\
(P^{(1,4)}, Q^{(1,4)}) &= (7,0) - \frac{42}{7}(0,7) = (7,7).
\end{aligned}$$

In the second iteration, we have $d_1 = 38$, $d_2 = 21$, $d_3 = 40$ and $d_4 = 35$. Accordingly,

$$\begin{aligned}
(P^{(2,1)}, Q^{(2,1)}) &= (0, X-1) - \frac{38}{40}(1, 43) \\
&= (26, X+39) \\
(P^{(2,2)}, Q^{(2,2)}) &= (0, 7X-7) - \frac{21}{35}(7,7) \\
&= (35, 7X+28) \\
(P^{(2,3)}, Q^{(2,3)}) &= (1,43)(X-5) \\
&= (X+44, 43X+30) \\
(P^{(2,4)}, Q^{(2,4)}) &= (7,7)(X-7) \\
&= (7X+14, 7X+14).
\end{aligned}$$

In the third iteration, we have $d_1 = 14$, $d_2 = 0$, $d_3 = 3$ and $d_4 = 21$. Accordingly,

$$\begin{aligned}
(P^{(3,1)}, Q^{(3,1)}) &= (26, X+39)(X-25) \\
&= (26X+36, X^2+14X+5) \\
(P^{(3,2)}, Q^{(3,2)}) &= (35, 7X+28) \\
(P^{(3,3)}, Q^{(3,3)}) &= (X+44, 43X+30)(X-25) \\
&= (X^2+19X+27, 43X^2+33X
\end{aligned}$$

$$\begin{aligned}
&\quad +34)\\
(P^{(3,4)},Q^{(3,4)}) &= (7X+14,7X+14) - \frac{21}{14}(26,\\
&\quad X+39)\\
&= (7X+24,30X+29).
\end{aligned}$$

In the final iteration, we have $d_1 = 21$*,* $d_2 = 0$*,* $d_3 = 6$ *and* $d_4 = 42$*. Accordingly,*

$$\begin{aligned}
(P^{(4,1)},Q^{(4,1)}) &= (26X+36,X^2+14X+5) -\\
&\quad \frac{21}{42}(7X+24,30X+29)\\
&= (47X+24,X^2+48X+15)\\
(P^{(4,2)},Q^{(4,2)}) &= (35,7X+28)\\
(P^{(4,3)},Q^{(4,3)}) &= (X^2+19X+27,43X^2+33X\\
&\quad +34)(X-27)\\
&= (X^3+41X^2+4X+6,43X^3\\
&\quad +48X^2+25X+13)\\
(P^{(4,4)},Q^{(4,4)}) &= (7X+24,30X+29)(X-27)\\
&= (7X^2+31X+38,30X^2+3X\\
&\quad +1).
\end{aligned}$$

5 Connection to Gröbner basis of $M^{(i)}$

Now, $\mathrm{Rank}(0,X^i) < \mathrm{Rank}(0,X^j)$ and $\mathrm{Rank}(X^i,0) < \mathrm{Rank}(X^j,0)$ for $i < j$, and $\mathrm{Rank}(X^j,0) < \mathrm{Rank}(0,X^i)$ for $j+1 \leq i$. Thus, by ordering with respect to their ranks, the terms whose linear combination over R gives a prescribed element $(P,Q) \in R[X]^2$, we may define the *leading monomial* $\mathrm{lm}(P,Q)$ of (P,Q) in the usual way. That is,

$$\mathrm{lm}(P,Q) = \begin{cases} (\lambda P \cdot X^{\delta P},\, 0) & : \ \mathrm{Rank}(P,Q) \text{ even} \\ (0,\, \lambda Q \cdot X^{\delta Q}) & : \ \text{otherwise.} \end{cases}$$

By Theorem 1(ii), for $i = 0,1,\ldots,L$, the $2l$ elements $(P^{(i,1)},Q^{(i,1)}),\ldots,(P^{(i,2l)},Q^{(i,2l)})$ of $M^{(i)}$ computed by Algorithm 1 satisfy $\mathrm{lm}(P^{(i,j)},Q^{(i,j)}) = (0,\, p^{j-1}X^{\delta Q^{(i,j)}})$ and $\mathrm{lm}(P^{(i,j+l)},Q^{(i,j+l)}) = (p^{j-1}X^{\delta P^{(i,j+l)}},\, 0)$ for $j = 1,2,\ldots,l$.

Let A be an $R[X]$-submodule of $R[X]^2$. A set $\mathcal{G} = \{g_1,\ldots,g_n\} \subseteq A$ of nonzero elements is a *Gröbner basis* of A if for each $a \in A$, there exists an $i \in \{1,\ldots,n\}$ such that $\mathrm{lm}(a)$ is divisible by $\mathrm{lm}(g_i)$. An arbitrary subset $\mathcal{G}$ of $R[X]^2$ is called a Gröbner basis if it is a Gröbner basis of the ideal $\langle\mathcal{G}\rangle$ generated by $\mathcal{G}$.

By [4, Theorem V.3], since $(H^{(i)},0)$ and $(0,H^{(i)})$ are elements of $M^{(i)}$ for $i = 1,2,\ldots,L$, $M^{(i)}$ is an $R[X]$-submodule of $R[X]^2$ having ordered Gröbner basis of the form

$$\{(a^{(i,1)},b^{(i,1)}),(a^{(i,2)},b^{(i,2)}),\ldots,(a^{(i,2l)},b^{(i,2l)})\}$$

where $\mathrm{lm}(a^{(i,j)},b^{(i,j)}) = (0,\, p^{j-1}X^{\delta b^{(i,j)}})$ and $\mathrm{lm}(a^{(i,j+l)},b^{(i,j+l)}) = (p^{j-1}X^{\delta a^{(i,j+l)}},\, 0)$ for $j = 1,2,\ldots,l$. By the same theorem, we have that the ranks of these $2l$ interpolants are uniquely determined by $M^{(i)}$ and so we may associate with it, the vector

$$(r^{(i,1)},r^{(i,2)},\ldots,r^{(i,2l)})$$

where $r^{(i,j)}$ denotes the unique rank of $(a^{(i,j)},b^{(i,j)})$.

We now state two key results.

Lemma 1 *For* $j = 1,2,\ldots,2l$*, either* $r^{(i+1,j)} = r^{(i,j)}$ *or* $r^{(i+1,j)} = r^{(i,j)} + 2$*.*

Theorem 2 *For* $k = i, i+1$*, let* $M^{(k)}$ *have Gröbner basis*

$$\{(a^{(k,1)},b^{(k,1)}),(a^{(k,2)},b^{(k,2)}),\ldots,(a^{(k,2l)},b^{(k,2l)})\}$$

where $\mathrm{lm}(a^{(k,j)},b^{(k,j)}) = (0,\, p^{j-1}X^{\delta b^{(k,j)}})$ *and* $\mathrm{lm}(a^{(k,j+l)},b^{(k,j+l)}) = (p^{j-1}X^{\delta a^{(k,j+l)}},\, 0)$ *for* $j = 1,2,\ldots,l$*. Further, for* $j = 1,2,\ldots,2l$*, let* $\alpha_j = s_i b^{(i,j)}(x_i) - a^{(i,j)}(x_i)$*. Then for each* j*, there exist* j' *such that* $\alpha_{j'}|\alpha_j$ *and* $\mathrm{Rank}(a^{(i,j')},b^{(i,j')}) < \mathrm{Rank}(a^{(i,j)},b^{(i,j)})$ *if and only if* $r^{(i,j)} = r^{(i+1,j)}$*.*

The proofs of Lemma 1 and Theorem 2 are similar to that of Lemma VI.1 and Theorem VI.3 in [4], respectively. Term ordering is with respect to their ranks.

Returning to Algorithm 1, evidently the initial set $\{(P^{(0,1)},Q^{(0,1)}),\ldots,(P^{(0,2l)},Q^{(0,2l)})\}$ is a Gröbner basis of $M^{(0)}$. Next, suppose that for $i \geq 0$, $\{(P^{(i,1)},Q^{(i,1)}),\ldots,(P^{(i,2l)},Q^{(i,2l)})\}$ is a Gröbner basis of $M^{(i)}$. Then if $(P^{(i,j)},Q^{(i,j)})$ is updated as

$$\begin{aligned}
(P^{(i+1,j)},Q^{(i+1,j)}) &= (P^{(i,j)},Q^{(i,j)}) - \frac{d_j}{d_k}(P^{(i,k)},\\
&\quad Q^{(i,k)}),
\end{aligned}$$

by Theorem 1(i) we have that $\mathrm{Rank}(P^{(i+1,j)},Q^{(i+1,j)}) = \mathrm{Rank}(P^{(i,j)},Q^{(i,j)}) = r^{(i,j)}$. From Theorem 2, it follows that $(P^{(i+1,j)},Q^{(i+1,j)})$ is contained in a

Gröbner basis of $M^{(i+1)}$. On the other hand, suppose $(P^{(i,j)}, Q^{(i,j)})$ is updated as

$$(P^{(i+1,j)}, Q^{(i+1,j)}) = (P^{(i,j)}, Q^{(i,j)})(X - x_i)$$

so that $\mathrm{Rank}(P^{(i+1,j)}, Q^{(i+1,j)}) = \mathrm{Rank}(P^{(i,j)}, Q^{(i,j)})$ $+2 = r^{(i,j)} + 2$. From Lemma 1 and Theorem 2, $(P^{(i+1,j)}, Q^{(i+1,j)})$ is again contained in a Gröbner basis of $M^{(i+1)}$ and so we have

Theorem 3 *The set*

$$\{(P^{(i,1)}, Q^{(i,1)}), \ldots, (P^{(i,2l)}, Q^{(i,2l)})\}$$

that Algorithm 1 computes is a Gröbner basis of $M^{(i+1)}$ for $i = 1, 2, \ldots, L$.

Finally, from Section 3, the desired solution to the key equation is an element (P, Q) of $M^{(L)}$ and in turn a Gröbner basis of $M^{(L)}$ such that λQ is a unit in R and $\mathrm{Rank}(P, Q)$ is minimal. With this, the justification for Algorithm 1 is complete.

Example 2 *In Example 1, Algorithm 1 will return $(47X + 24, X^2 + 48X + 15)$ which is the minimal regular element in the computed Gröbner basis for $M^{(4)}$.*

6 Concluding remarks

We have given a generalization of the WB algorithm for solving the WB key equation over a Galois ring. In the aforementioned decoding application, this algorithm represents a significant improvement over that given in [2] since we are no longer restricted to double-error correction.

Finally, we recall that in the field case, the WB algorithm computes a pair of complementary interpolants in each iteration – see [1, 3]. It is likely that the Gröbner basis that Algorithm 1 computes in each iteration can in fact be divided into l pairs of complementary interpolants, namely, $(P^{(i,j)}, Q^{(i,j)})$ and $(P^{(i,2l-j+1)}, Q^{(i,2l-j+1)})$ for $j = 1, 2, \ldots, l$.

References:

[1] Armand, M.A., Complementary interpolants and a Welch-Berlekamp-style algorithm, *Sequences and their Applications, Discrete Mathematics and Theoretical Computer Science series, Springer-Verlag*, 1999, pg. 131–145.

[2] Armand, M.A., Efficient decoding of Reed-Solomon codes over $\mathbb{Z}_q$ based on remainder polynomials.” *WSEAS Trans. Comms.*, Vol. 1, No. 1, pg. 116–121.

[3] Berlekamp, E., Bounded distance +1 soft-decision Reed-Solomon decoding, *IEEE Trans. Inform. Theory*, Vol. 42, No. 3, 1996, pg. 704–720.

[4] Byrne, E., Fitzpatrick, P., Hamming metric decoding of alternant codes over Galois rings, *IEEE Trans. Inform. Theory*, Vol. 48, No. 3, 2002, pg. 683–694.

[5] Chambers, W.G., Peile, R.E., Tsie, K.Y., Zein, N., Algorithm for solving the Welch-Berlekamp key-equation, with a simplified proof. *Electronic Letters*, Vol. 29, No. 18, 1993, pg. 1620–1621.

[6] MacDonald, B.R., Finite rings with identity, *Marcel Dekker Inc*, 1974.

[7] Welch, L., Berlekamp, E.R., Error correction for algebraic block codes, *US Patent*, 4 633 470, 1983.