Contemporary Engineering Sciences, Vol. 2, 2009, no. 5, 239 - 248

A p-Adic View of the Algebraic Decoding of Lifted Golay Codes[1]

Michele Elia

Politecnico di Torino, Italy
eliamike@tin.it

Abstract

The perfect Golay codes lifted over the finite rings $\mathbb{Z}_{2^m}$ and $\mathbb{Z}_{3^m}$, or over their infinite counterparts, namely the 2-adic and 3-adic rings, are considered, and their algebraic decoding is obtained as a non-trivial extension of the algebraic decoding of the perfect Golay codes.

Mathematics Subject Classification: 94B15, 94B35, 11D88, 14G50

Keywords: p-adic fields, Golay codes, algebraic decoding

1 - Introduction

Sloane and Calderbank have described the structure of cyclic codes of length n over rings of integers modulo p^m and over the integer ring of a p-adic field $\mathbb{Q}_p$, denoted $\mathbb{Z}_{p^\infty}$, where p is a prime not dividing n [5]. Linear codes over $\mathbb{Z}_{p^\infty}$ are global codes, and an advantage of this notion is that it establishes a framework for dealing with every lifted code over some prime power residue ring $\mathbb{Z}_{p^m}$. Any code lifted from a code over $\mathbb{Z}_p$ may be seen as a residual code modulo p^m of a convenient p-adic code.
The same article [5] analyzes the 2-adic and 3-adic Golay codes and their extended versions of length 24 and 12, respectively, but does not consider any algebraic decoding. Here we describe an algebraic decoding of every lifted Golay code that may be seen as being lifted from the algebraic decoding of the perfect Golay codes over $\mathbb{Z}_2$ or $\mathbb{Z}_3$ [7, 8]. The algebraic decoding algorithms for the corresponding extended Golay codes, $(24, 12, 8)$ and $(12, 6, 6)$ can be derived from those of these Golay codes, as shown in [15].

[1] A preliminary version was presented at MTNS 2008, July 28-August 1, 2008, Blacksburg, Virginia.

2 - Lifting Golay Codes

The binary Golay code is a perfect cyclic code $(23, 12, 7)$ over the Galois field $\mathbb{F}_2$ with generator polynomial $g_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$, an 11-degree irreducible factor of $x^{23} - 1$.
The 2-adic Golay code is a cyclic code over the ring $\mathbb{Z}_{2^\infty}$ of 2-adic integers with generator polynomial of the form

$$\begin{aligned} g_{2\infty}(x) &= x^{11} + \nu x^{10} + (\nu - 3)x^9 - 4x^8 - (\nu + 3)x^7 - (2\nu + 1)x^6 - \\ &\quad (2\nu - 3)x^5 - (v - 4)x^4 + 4x^3 + (\nu + 2)x^2 + (\nu - 1)x - 1 \end{aligned}$$

where ν is a 2-adic number satisfying the equation $\nu^2 - \nu + 6 = 0$ [5, p.31]. A few initial terms of its 2-adic expansion are

$$\begin{aligned} g_{2\infty}(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 + 2(x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + 1) \\ + 4(x^9 + x^8 + x^5 + x^3 + x^2 + 1) + 8(x^{10} + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1) \cdots \quad . \end{aligned}$$

Letting ζ denote a root of $g_2(x)$, which is irreducible over $\mathbb{Q}_2$, a few initial terms of the 2-adic expansion of a root Ξ of $g_{2\infty}(x)$ are

$$\Xi = \zeta + 2(\zeta^{10} + \zeta^6 + \zeta^4 + \zeta^3 + \zeta^2) + 4(\zeta^9 + \zeta^8 + \zeta^6) + 8\zeta^6 + \cdots \quad .$$

When $g_{2\infty}(x)$ is taken modulo 2^m, we get the generator polynomial $g_{2m}(x)$ of the Golay code over $\mathbb{Z}_{2^m}$. Clearly, the cyclotomic coset
$\mathcal{C}_1^{(2)} = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$ of $g_2(x)$ is also the cyclotomic coset of any lifted polynomial.

The ternary Golay code is a perfect cyclic code $(11, 6, 5)$ over the Galois field $\mathbb{F}_3$ with generator polynomial $g_3(x) = x^5 - x^3 + x^2 - x - 1$, a 5-degree irreducible factor of $x^{11} - 1$.
The 3-adic Golay code is a cyclic code over the ring $\mathbb{Z}_{3^\infty}$ of 3-adic integers with generator polynomial of the form

$$g_{3\infty}(x) = x^5 + \theta x^4 - x^3 + x^2 + (\theta - 1)x - 1 \quad ,$$

where θ is a 3-adic number satisfying the equation $\theta^2 - \theta + 3 = 0$ [5, p.31]. A few initial terms of its 3-adic expansion are

$$g_{3\infty}(x) = x^5 + x^4 + 2x^3 + x^2 + 2 - 3(x^4 + x^3 + x + 1) + 9(x^4 + 2x^3 + x + 2) - 27(x^3 + 1) + \cdots \quad .$$

Letting η denote a root of $g_3(x)$, which is irreducible over $\mathbb{Q}_3$, a few initial terms of a 3-adic expansion of a root Θ of $g_{3\infty}(x)$ are

$$\Theta = \eta + 3(\eta^2 + \eta^3 + \eta^4) + 9(1 + 2\eta + \eta^2 + \eta^3 + 2\eta^4) + 27(\eta^4 + 2\eta^3 + 2\eta^2 + 2) + \cdots \quad .$$

When $g_{3\infty}(x)$ is taken modulo 3^m, we get the generator polynomial $g_{3m}(x)$ of a Golay code over $\mathbb{Z}_{3^m}$. Clearly, the cyclotomic coset $\mathcal{C}_1^{(3)} = \{1, 3, 9, 5, 4\}$ of $g_3(x)$ is also the cyclotomic coset of any lifted polynomial.

Remark. The generator polynomials $g_{2\infty}(x)$ and $g_{3\infty}(x)$ of the 2-adic and 3-adic codes may be obtained by applying Hensel lifting up to infinity to the generator polynomials $g_2(x)$ and $g_3(x)$ of the codes over finite fields. However, these polynomials admit "closed" forms, i.e.: $g_{2\infty}(x) = g_2(x)+\nu c_2(x)$ and $g_{3\infty}(x) = g_3(x) + \theta c_3(x)$, where ν is a root of $x^2 - x + 6$ and θ is a root of $x^2 - x + 3$, which define quadratic extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$ respectively. A natural question arises whether the roots Ξ and Θ have closed forms in terms of the roots ζ of $g_2(x)$ and η of $g_3(x)$, using ν and θ, respectively. The negative answer is due to the fact that $g_{2\infty}(x)$ and $g_2(x)$ have different Galois groups over $\mathbb{Q}_2(\nu)$, and analogously that $g_{3\infty}(x)$ and $g_3(x)$ have different Galois groups over $\mathbb{Q}_3(\theta)$. For instance, in the ternary case (the argument in the binary case is exactly the same) assuming that we may write

$$\Theta = (a_0 + \theta b_0) + (a_1 + \theta b_1)\eta + (a_2 + \theta b_2)\eta^2 + (a_3 + \theta b_3)\eta^3 + (a_4 + \theta b_4)\eta^4$$

where a_i, b_i are rational integers, then this relation between η and Θ implies the existence of a Tschirnhaus transformation of $g_3(x)$ into $g_{3\infty}(x)$ with coefficients in the field $\mathbb{Q}_3(\theta)$. This transformation is possible if and only if the two polynomials have the same Galois groups over $\mathbb{Q}_3(\theta)$ [1, p.45-46]. However, the Galois group of $g_{3\infty}(x)$ over $\mathbb{Q}_3(\theta)$ is cyclic of order 5, while the Galois group of $g_3(x)$ over $\mathbb{Q}_3(\theta)$ is the symmetric group S_5. Note that the Galois group of $g_3(x)$ over $GF(3)$ is cyclic of order 5, while its Galois group over $\mathbb{Q}$, $\mathbb{Q}_p$, or $\mathbb{Q}_3(\theta)$ is the symmetric group.

2.1 Syndrome decoding

The syndrome decoding procedures are described assuming that $r(x) = c(x) + e(x)$ is a received word, where $c(x) = g(x)f(x)$ is a transmitted code word, $g(x)$ is the generator polynomial, and $e(x)$ is the error pattern. The output is a code word $\hat{c}(x) = r(x) - \hat{e}(x)$, where $\hat{e}(x)$ is the estimated error pattern if the number of errors is not greater than the code's error-correcting capability. When more errors are detected, some decision strategy must be adopted, for instance the bounded decoding strategy sets the estimated error pattern equal to 0, i.e. $\hat{e}(x) = 0$.
The algorithm is in two steps. At the first step, the error positions are computed from the roots of the error locator polynomial, obtained considering convenient projections of the syndromes on the base prime field. At the second step, the error magnitudes are easily computed solving a linear system of equations. Note that the Gorenstein-Peterson-Zierler method for finding the error locator polynomial is not applicable, and the procedures described in [7, 8] for locating the errors require some modifications when the error magnitudes are in strictly different zero divisor subrings of $\mathbb{Z}_{p^m}$, $p = 2, 3$.

3 - Decoding lifted codes over $\mathbb{Z}_{2^m}$

Let $\hat{e}(x) = E_1 x^{j_1} + E_2 x^{j_2} + E_3 x^{j_3}$ be the error pattern to be estimated, where E_1, E_2 and E_3 are error magnitudes, and j_1, j_2 and j_3 are error positions. The decoding algorithm is a procedure that finds the error pattern $\hat{e}(x)$, or detects more than three errors; however this event is not handled to give optimal complete decoding. Letting Ξ_m to denote a root of $g_{2m}(x)$, a description of the algorithm makes use of a set of six syndromes

$$S_j = r(\Xi_m^j) = E_1 \Xi_m^{j_1 j} + E_2 \Xi_m^{j_2 j} + E_3 \Xi_m^{j_3 j} \quad j \in \{1,2,3,4,6,9\} \subset \mathcal{C}_1^{(2)} \quad ,$$

and is based on the following Theorems.
Let us assume that S_1 is not zero, and set $T_1 = \frac{S_1}{2^{t_o}}$, $T_3 = \frac{S_3}{2^{t_o}}$, and $T_9 = \frac{S_9}{2^{t_o}}$, where t_o is defined as the minimum integer such that at least one among T_1, T_3, or T_9 taken modulo 2 is not zero.

Theorem 1. *With the above hypotheses and notations:*
i) if at least one among T_1, T_3, or T_9 taken modulo 2 is 0, then more than three errors are detected.
ii) if $T_1 \neq 0$, $T_3 \neq 0$, and $T_9 \neq 0$ taken mod2*, then the error locator polynomial*

$$\sigma(z) = z^3 - \sigma_1 z^2 + \sigma_2 z + \sigma_3$$

is computed, and the error positions j_1, j_2, and j_3 are recovered when the roots of $\sigma(z)$ are in $\mathbb{F}_{2^{11}}$; otherwise more than three errors are detected. If three errors are located, their magnitudes E_1, E_2, and E_3 are obtained by solving the linear system

$$\begin{cases} E_1 \Xi_m^{j_1} + E_2 \Xi_m^{j_2} + E_3 \Xi_m^{j_3} &= S_1 \\ E_1 \Xi_m^{2j_1} + E_2 \Xi_m^{2j_2} + E_3 \Xi_m^{2j_3} &= S_2 \\ E_1 \Xi_m^{3j_1} + E_2 \Xi_m^{3j_2} + E_3 \Xi_m^{3j_3} &= S_3 \end{cases} \tag{1}$$

Proof. Statement i) is a trivial consequence of the fact that the syndromes modulo 2 are powers one of another, thus, if some syndrome is zero, necessarily more than three errors are detected.
To prove statement ii), observe that the error positions are not changed by working modulo 2, thus if every error magnitude is not a zero divisor, $\sigma(z)$ may be computed by the method described in [7], defining

$$D = (T_3 + T_1^3)^2 + \frac{T_9 + T_1^9}{T_3 + T_1^3} \bmod 2 \quad , \quad D^{1/3} = D^{1365} \bmod 2$$

and obtaining $\sigma_1 = T_1 \bmod 2$, $\sigma_2 = T_1^2 + D^{1/3} \bmod 2$, and $\sigma_3 = T_3 + T_1 D^{1/3} \bmod 2$.
If $T_3 + T_1 D^{1/3} \neq 0 \bmod 2$, and the roots of $\sigma(z)$ are in $\mathbb{F}_{2^{11}}$, the error magnitudes

are given by solving (1) modulo 2^m; otherwise more than three errors are detected.
If $T_3 + T_1 D^{1/3} = 0 \bmod 2$, two errors are detected and located in positions j_1 and j_2 by solving the equation

$$\sigma(z) = z^2 - \sigma_1 z^2 + \sigma_2 = 0 \quad .$$

Therefore, to compute the further error position and the three error magnitudes, it is necessary to consider system (1) with the equation $E_1 \Xi_m^{4j_1} + E_2 \Xi_m^{4j_2} + E_3 \Xi_m^{4j_3} = S_4$. This system of four equations can easily be solved by defining the expression

$$\Delta = \frac{S_4 - [(\Xi_m^{j_1})^2 + \Xi_m^{j_1}\Xi_m^{j_2} + (\Xi_m^{j_2})^2)S_2 + \Xi_m^{j_1}\Xi_m^{j_2}(\Xi_m^{j_1} + \Xi_m^{j_2})S_1}{S_3 - (\Xi_m^{j_1} + \Xi_m^{j_2})S_2 + \Xi_m^{j_1}\Xi_m^{j_2} S_1} - \Xi_m^{j_1} - \Xi_m^{j_2} \quad .$$

If $\Delta = 0$ then only two errors are detected and their magnitudes are easily obtained from (1).
If $\Delta \neq 0$, then the error location j_3 is computed from the equation $\Xi_m^{j_3} = \Delta$, thus three error magnitudes are obtained solving (1) modulo 2^m.
If the denominator of $\Delta \bmod 2^m$ is still a multiple of 2, then more than three errors are detected. □

Theorem 2. *With the above hypotheses and notations, if* $T_1^3 = T_3 \bmod 2$*, a single error is detected, and the magnitudes of the remaining errors may be zero divisors. The error position* j_1 *is obtained from the error locator polynomial* $\sigma(z) = z - T_1 \bmod 2$*; the remaining error positions are obtained from the error locator polynomial* $\sigma(z) = z^2 - \bar{\sigma}_1 z + \bar{\sigma}_2$ *where* $\bar{\sigma}_1 = \tau_1 \bmod 2$*, and* $\bar{\sigma}_2 = \tau_2 \bmod 2$ *with*

$$\tau_2 = \frac{T_3 - T_4 + \tau_1(T_3 - T_2)}{T_2 - T_1} \bmod 2^m \quad , \tag{2}$$

and τ_1 *a root of the equation*

$$x^2 + x + \frac{T_6(T_1 - T_2) + T_4^2 - T_4(T_1 + T_3) + T_2 T_3}{T_4(T_2 - T_1) - T_2^2 - T_3^2 + T_3(T_2 + T_1)} = 0 \bmod 2^m \quad . \tag{3}$$

If τ_1 *is divisible by* 2*, then more than three errors are detected.*

Proof. The error position j_1 is computed from the zero of $z - T_1 \bmod 2$, thus we only need five equations to compute the remaining five unknowns. It is convenient to define the variables $\bar{X}_2 = \Xi_m^{-j_0}\Xi_m^{j_2}$ and $\bar{X}_3 = \Xi_m^{-j_1}\Xi_m^{j_3}$, associated to the error positions; then, performing this substitution into the five equations

$$E_1 \Xi_m^{\ell j_0} + E_2 \Xi_m^{\ell j_2} + E_3 \Xi_m^{\ell j_3} = S_\ell, \quad \ell = 1, 2, 3, 4, 6 \quad ,$$

we get the five equations

$$E_1 + E_2\bar{X}_2^{\ell} + E_3\bar{X}_3^{\ell} = \bar{S}_{\ell}, \quad \ell = 1, 2, 3, 4, 6 \ ,$$

where the bar syndromes are defined as $\bar{S}_{\ell} = \Xi_m^{-\ell j_0} S_{\ell}$. Finally, we obtain four syndrome equations for the four unknowns E_1, $\bar{S}_5$, $\bar{\sigma}_1$, and $\bar{\sigma}_2$

$$\begin{cases} \bar{S}_3 - \bar{\sigma}_1\bar{S}_2 + \bar{\sigma}_2\bar{S}_1 = E_1(1 - \bar{\sigma}_1 + \bar{\sigma}_2) \\ \bar{S}_4 - \bar{\sigma}_1\bar{S}_3 + \bar{\sigma}_2\bar{S}_2 = E_1(1 - \bar{\sigma}_1 + \bar{\sigma}_2) \\ \bar{S}_5 - \bar{\sigma}_1\bar{S}_4 + \bar{\sigma}_2\bar{S}_3 = E_1(1 - \bar{\sigma}_1 + \bar{\sigma}_2) \\ \bar{S}_6 - \bar{\sigma}_1\bar{S}_5 + \bar{\sigma}_2\bar{S}_4 = E_1(1 - \bar{\sigma}_1 + \bar{\sigma}_2) \end{cases}$$

Solving for $\bar{\sigma}_1$ and $\bar{\sigma}_2$ we get the claimed expressions. If τ_1 is divisible by 2, then $\bar{\sigma}_1$ cannot be computed, which means that more than three errors are detected. □

4 - Decoding lifted codes over $\mathbb{Z}_{3^m}$

We assume that the error pattern to be estimated is $\hat{e}(x) = E_1 x^{j_1} + E_2 x^{j_2}$, where E_1 and E_2 are the error magnitudes, and j_1 and j_2 are the error positions. If the number of errors is greater than 2, then we set $\hat{e}(x) = 0$.
Letting Θ_m to denote a root of $g_{3m}(x)$, a simple description of the algorithm makes use of a set of four syndromes

$$S_j = r(\Theta_m^j) = E_1\Theta_m^{j_1 j} + E_2\Theta_m^{j_2 j} \quad j \in \{1, 3, 4, 5\} \ .$$

The procedure always finds j_1 and j_2, and computes the error magnitudes by solving a system of two equations, for example

$$E_1\Theta_m^{j_1} + E_2\Theta_m^{j_2} = S_1 \ , \ E_1\Theta_m^{5j_1} + E_2\Theta_m^{5j_2} = S_5 \ .$$

More than two errors are detected if at least one of the computed errors E_1 or E_2 does not lie in $\mathbb{Z}_{3^m}$. The following theorem is key to the algorithm motivation. Let us assume that S_1 is not zero, and set $T_1 = \frac{S_1}{3^{j_o}}$, $T_5 = \frac{S_5}{3^{j_o}}$, where j_o is defined as the minimum integer such that at least one among T_1 or T_5 taken mod3 is not zero.

Theorem 3. *With the above hypotheses and notations:*

i) If only T_1 or only T_5 taken modulo 3 is zero, then more than two errors are detected.

ii) If $T_1^5 = T_5 \neq 0 \bmod 3$, an error is located in position j_1 from the root in $\mathbb{F}_{3^5}$ of $\sigma(z) = z - (\frac{T_5}{T_1})^{1/4}$. Moreover, if $S_5 - \Theta_m^{j_1} S_4 \neq 0 \bmod 3^m$, the second error position j_2 is computed from the root $\Theta_m^{j_2}$ of

$$z - \frac{S_5 - \Theta_m^{j_1} S_4}{S_4 - \Theta_m^{j_1} S_3} = 0 \bmod 3^m \ .$$

iii) If $T_1^5 \neq T_5 \neq 0 \bmod 3$*, the error locator polynomial* $\sigma(z) = z^2 - T_1 z + \sigma_2$ *is computed, where* σ_2 *is the root of* $\sigma_2^2 - T_1^2\sigma_2 + \frac{T_5 - T_1^5}{T_1} = 0$ *such that* $\sigma_2^{22} = 1$*, then*

1. *If the roots* z_1, z_2 *of* $\sigma(z) = 0$ *are in* $GF(3^5)$*, then two errors are located in positions* j_1 *and* j_2*, and the error magnitudes are computed from the system*

$$\begin{cases} E_1\Xi_m^{j_1} + E_2\Xi_m^{j_2} &= S_1 \\ E_1\Xi_m^{5j_1} + E_2\Xi_m^{5j_2} &= S_5 \end{cases} \tag{4}$$

2. *If the roots of* $\sigma(z) = 0$ *are not in* $GF(3^5)$*, then more than two errors are detected.*

Proof. Statement i) is a trivial consequence of the fact that the syndromes modulo 3 are powers of each other, thus, if some syndrome is zero, necessarily more than three errors are detected.
The first part of statement ii) is an immediate consequence of the fact that, in $\mathbb{F}_3$, a single error occurs if $T_1 = E_1\theta^j$ and $T_5 = E_1\theta^{5j}$, thus considering the ratio $\frac{T_5}{T_1} = \theta^{4j_1}$ we get j_1 from the claimed equation. To compute E_1, E_2, and the error position j_2, we consider a system of three equations for three unknowns which can be written knowing S_3, S_4 and S_5

$$\begin{cases} S_3 = E_1\Theta_m^{3j_1} + E_2\Theta_m^{3j_2} \\ S_4 = E_1\Theta_m^{4j_1} + E_2\Theta_m^{4j_2} \\ S_5 = E_1\Theta_m^{5j_1} + E_2\Theta_m^{5j_2} \end{cases} .$$

From this system two equations are obtained by eliminating E_1, that is $S_4 - \Theta_m^{j_1}S_3 = E_2\Theta_m^{3j_2}(\Theta_m^{j_2} - \Theta_m^{j_1})$ and $S_5 - \Theta_m^{j_1}S_4 = E_2\Theta_m^{4j_2}(\Theta_m^{j_2} - \Theta_m^{j_1})$ whose ratio yields the claimed result. The proof of item iii) is essentially the same as that given in [8] for the perfect ternary Golay code. □

5 - Decoding lifted codes over 2-adic and 3-adic rings

The 3-adic Golay code is an MDS code, thus it has minimum distance 6, although it may correct only 2 errors; thus the same algorithm working over the finite rings may be applied to decode this code.
The situation is totally different for the 2-adic Golay code, which is an MDS code with minimum distance 12 [5]; thus it can correct 5 errors, and the decoding algorithm for the perfect Golay code can no longer be lifted. Furthermore, it is questionable whether a decoding algorithm for the 2-adic Golay code will

ever be of any use. However, for purely theoretical purposes, a decoding algorithm of moderate complexity may be the following.
Let $r(x) = c(x) + e(x)$ be a received word, where the error pattern is assumed to be

$$e(x) = E_1 x^{j_1} + E_2 x^{j_2} + E_3 x^{j_3} + E_4 x^{j_4} + E_5 x^{j_5} \quad ,$$

and let $\sigma(z) = z^5 - \sigma_1 z^4 + \sigma_2 z^3 - \sigma_3 z^2 + \sigma_4 z - \sigma_5$ be the error locator polynomial. To compute the 5 elementary symmetric functions, it is necessary to compute the 11 syndromes $S_j = r(\Xi_m^j)$, $j \in \mathcal{C}^{(2)}$, which allow us to write a syndrome system of 13 equations in 12 unknowns, namely the 5 elementary symmetric functions and 7 syndromes that cannot be computed from $r(x)$:

$$S_j = \sigma_1 S_{j-1} - \sigma_2 S_{j-2} + \sigma_3 S_{j-3} - \sigma_4 S_{j-4} + \sigma_5 S_{j-5} \qquad j = 6, \ldots, 18 \quad .$$

A direct approach to this system entails solving an algebraic equation of degree 8192. This complexity may be significantly reduced for computational purposes, by considering a set of three elementary symmetric functions $\{\bar{\sigma}_1, \bar{\sigma}_2, \bar{\sigma}_3\}$ in X_1, X_2, X_3 and writing

$$\begin{cases} \sigma_1 = \bar{\sigma}_1 + X_4 + X_5 \\ \sigma_2 = \bar{\sigma}_2 + (X_4 + X_5)\bar{\sigma}_1 + X_4 X_5 \\ \sigma_3 = \bar{\sigma}_3 + (X_4 + X_5)\bar{\sigma}_2 + X_4 X_5 \bar{\sigma}_1 \\ \sigma_4 = (X_4 + X_5)\bar{\sigma}_3 + X_4 X_5 \bar{\sigma}_2 \\ \sigma_5 = X_4 X_5 \bar{\sigma}_3 \end{cases}$$

Substituting into the above system we get

$$S_j - (X_4 + X_5)S_{j-1} + X_4 X_5 S_{j-2} = \bar{\sigma}_1(S_{j-1} - (X_4 + X_5)S_{j-2} + X_4 X_5 S_{j-3}) -$$

$$\bar{\sigma}_2(S_{j-2} - (X_4 + X_5)S_{j-3} + X_4 X_5 S_{j-4}) + \bar{\sigma}_3(S_{j-3} - (X_4 + X_5)S_{j-4} + X_4 X_5 S_{j-5})$$

for $j = 6, \ldots, 18$. The pair of variables X_4, X_5 may take 253 values, thus we may consider 253 systems, and for each system derive the cubic error locator polynomial for the remaining three errors. Following this approach, we need only 7 syndrome equations, since for each system we have only three unknown elementary symmetric functions, and four unknown syndromes, namely S_5, S_7, S_{10}, and S_{11}. Moreover, using an additional syndrome equation, the three elementary symmetric functions may be obtained from linear equations. The burden is the reduction process, which may be fast when all variables assumed to be known have specific numerical values.

6 Conclusions

Algebraic decoding algorithms for binary and ternary Golay codes lifted over the corresponding power rings are described in full. The same algorithm also

works for the 3-adic Golay code, while the situation is totally different for the 2-adic $(23, 12, 12)$ Golay code which is MDS; for this code, an algebraic decoding algorithm of moderate complexity to correct 5 errors is outlined.

References

[1] E. Artin, *Galois Theory*, Notre Dame, Indiana, 1959.

[2] E.F. Assmus, H.F. Mattson, New 5-designs, *J. Combinatorial Theory* 6, 1969, p. 122-151.

[3] I. F. Blake, Codes over integer residue rings, *Inform. Contr.*, vol. 29, pp.295-300, 1975.

[4] A. R. Calderbank and N. J. A. Sloane, The ternary Golay code, the integers mod 9, and the Coxeter-Todd lattice, *IEEE Trans. Inform. Theory*, vol. 42, pp.636-637, Mar. 1996.

[5] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, *Des., Codes Cryptogr.*, vol. 6, 1995, pp.21-35.

[6] J. H. Conway and N. J. A. Sloane, Self-dual codes over integers modulo 4, *J. Comb. Theory*, vol. A-62, pp.30-45, 1993.

[7] M. Elia, Algebraic decoding of the binary $(23, 12, 7)$ Golay code, *IEEE Trans. Inform. Theory*, vol. IT-33, pp.150-151, Oct. 1987.

[8] M. Elia and E. Viterbo, Algebraic decoding of the Ternary $(11, 6, 5)$ Golay code, *Electron. Lett.*, vol. 28, no. 21, pp.2021-2022, Oct. 1992.

[9] M. Greferath, Cyclic codes over finite rings, *Discr. Math.*, vol.177, pp.273-277, 1997.

[10] M. Greferath and U. Vellbinger, Efficient decoding of p-linear codes, *IEEE Trans. Inform. Theory*, vol. 44, pp. 1288-1291, 1998.

[11] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, The 4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory*, vol. 40, pp.301-319, 1994.

[12] K. Hensel, *Theorie der Algebraischen Zahlen*, Leipzig, Teubner, 1908.

[13] N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Springer, New York, 1984.

[14] F.J. MacWilliams and N.A.J. Sloane, *The Theory of Error Correcting Codes,* North Holland, Amsterdam, 1977.

[15] I.S. Reed, X. Yin, T.K. Truong, J.K. Holmes, Decoding the $(24, 12, 8)$ code, *Computers and Digital Techniques, IEE Proceedings*, vol.137, Issue 3, pp.202-206, 1990.

[16] E. Spiegel, Codes over $\mathbb{Z}_m$, *Inform. Contr.*, vol. 35, pp.48-51, 1977.

Received: November, 2008