On Algebraic Decoding of the Z_4-Linear Goethals-like Codes

Kalle Ranto

Turku Centre for Computer Science TUCS
FIN-20520 Turku, Finland
e-mail: kara@utu.fi

Turku Centre for Computer Science
TUCS Technical Report No 301
September 1999
ISBN 952-12-0517-2
ISSN 1239-1891

Abstract

The quaternary Goethals-like code is a Z_4-linear code of length 2^m which has $2^{2^{m+1}-3m-2}$ codewords and minimum Lee distance 8 for any odd integer $m \geq 3$. The Gray map of this code is known to be a nonlinear binary code with the same parameters as the Goethals code. We present an algebraic decoding algorithm for all Z_4-linear Goethals-like codes introduced by Helleseth et al. which corrects all errors with Lee weight ≤ 3.

Keywords: Decoding, Z_4-linear codes, Goethals code, Dickson polynomials

TUCS Research Group
Coding Theory Group

1 Introduction

Let m be an odd integer and let $\mathbb{Z}_4$ denote the ring of integers modulo 4. Let also $R = \mathrm{GR}(4, m)$ be a Galois ring of characteristic 4 with 4^m elements. The multiplicative group of units in R contains a unique cyclic subgroup of order $2^m - 1$. Let β be a generator of this subgroup and let

$$\mathcal{T} = \{0, 1, \beta, \ldots, \beta^{2^m-2}\}.$$

Every element of R can be expressed uniquely in the form $A + 2B$ where $A, B \in \mathcal{T}$. Let $\mu : \mathbb{Z}_4 \to \mathbb{Z}_2$ denote the modulo 2 reduction map. We can extend μ to R in a natural way and it can be shown that $\mu(\mathcal{T}) = \mathbb{F}$ where $\mathbb{F}$ is a finite field of order 2^m.

The Gray map ϕ is defined by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$ and $\phi(3) = 10$. Let $\mathcal{C}_1$ be the quaternary code with parity-check matrix given by

$$H_1 = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^3 & 2\beta^6 & \ldots & 2\beta^{3(2^m-2)} \end{bmatrix}.$$

Hammons et al. [4] showed that $\mathcal{C}_1$ has minimum Lee distance 8 which is equal to the minimum Hamming distance of $\phi(\mathcal{C}_1)$. They also showed that the quaternary code $\mathcal{P}$ with parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \end{bmatrix}$$

has minimum Lee distance equal to 6 and presented a decoding algorithm for this code.

The binary codes $\phi(\mathcal{C}_1)$ and $\phi(\mathcal{P})$ are nonlinear codes with parameters $(2^{m+1}, 2^{2^{m+1}-3m-2}, 8)$ and $(2^{m+1}, 2^{2^{m+1}-2m-2}, 6)$, respectively. These parameters are identical to those of the Goethals and Preparata codes. The Preparata code is known to be optimal and the Goethals code has four times as many codewords as the comparable extended triple error-correcting primitive BCH code.

Helleseth, Kumar and Shanbhag [6] observed that the quaternary codes $\mathcal{C}_k$ with parity-check matrices

$$H_k = \begin{bmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \beta & \beta^2 & \ldots & \beta^{2^m-2} \\ 0 & 2 & 2\beta^{2^k+1} & 2\beta^{(2^k+1)2} & \ldots & 2\beta^{(2^k+1)(2^m-2)} \end{bmatrix}$$

have the same weight distribution as the "Goethals" code $\mathcal{C}_1$ whenever $\gcd(k, m) = 1$. Helleseth and Kumar [5] presented a complete decoding algorithm for the code $\mathcal{C}_1$. In this paper we give an algebraic decoding algorithm for all codes $\mathcal{C}_k$ up to the error-correcting capability.

In Table 1 we see different values of parameter k which can be used. If $2^k + 1$ and $2^{k'} + 1$ are in the same 2-cyclotomic coset modulo $q - 1$, then the codes $\mathcal{C}_k$ and $\mathcal{C}_{k'}$ are equal.

Table 1: Different choices for k with different codelengths.

m	Codelength	k	$2^k + 1$
3	8	1	3
5	32	1,2	3,5
7	128	1,2,3	3,5,9
9	512	1,2, ,4	3,5, ,17
11	2048	1,2,3,4,5	3,5,9,17,33
13	8192	1,2,3,4,5,6	3,5,9,17,33,65
15	32768	1,2, ,4, , ,7	3,5, ,17, , ,129
17	131072	1,2,3,4,5,6,7,8	3,5,9,17,33,65,129,257
19	524288	1,2,3,4,5,6,7,8,9	3,5,9,17,33,65,129,257,513
21	2097152	1,2, ,4,5, , ,8, ,10	3,5, ,17,33, , ,257, ,1025

2 Preliminaries

Let $\mathrm{Tr}(x)$ denote the trace function from $\mathbb{F}$ to $\mathbb{Z}_2$. The following lemma is well known. For even m see for example [1].

Lemma 2.1. *The quadratic equation $x^2 + x + \delta = 0$ with $\delta \in \mathbb{F}$ has two roots $\theta = \sum_{j=0}^{\frac{m-1}{2}} \delta^{4^j}$ and $\theta + 1$ in $\mathbb{F}$ if $\mathrm{Tr}(\delta) = 0$ and no roots in $\mathbb{F}$ if $\mathrm{Tr}(\delta) = 1$. In the latter case the two roots $\theta + \gamma$ and $\theta + \gamma + 1$ are in the quadratic extension of $\mathbb{F}$ where $\gamma^2 + \gamma + 1 = 0$.*

Equation $x^2 + \gamma x + \delta = 0$ where $\gamma \neq 0$ can be transformed to $(\frac{x}{\gamma})^2 + \frac{x}{\gamma} + \frac{\delta}{\gamma^2} = 0$ and the condition in the previous lemma changes to $\mathrm{Tr}(\frac{\delta}{\gamma^2}) = 0$.

In order to transform the syndrome equations over the Galois ring to equations over the finite field the next lemma is useful.

Lemma 2.2 (Helleseth and Kumar [5]). *Let $\mathrm{e} = (e_X)_{X \in \mathcal{T}} \in \mathbb{Z}_4^{2^m}$ and $E_j = \{x = \mu(X) \mid e_X = j\}$ for $j = 0, 1, 2, 3$. The equation*

$$\sum_{X \in \mathcal{T}} e_X X = A + 2B, \qquad A, B \in \mathcal{T}$$

is equivalent to the two equations over the finite field $\mathbb{F}$ *:*

$$a = \sum_{x \in E_1 \cup E_2} x$$
$$b^2 = \sum_{x \in E_2 \cup E_3} x^2 + \sum_{\substack{x,y \in E_1 \cup E_3 \\ x<y}} xy$$

where $a = \mu(A)$*,* $b = \mu(B)$ *and* $<$ *is any ordering of the finite field.*

3 Dickson polynomials

In the decoding procedure of the next section we have to find the roots of an equation

$$D_n(x, u) = v$$

where $D_n(x, u)$ is a Dickson polynomial defined by

$$D_n(x, u) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-u)^i x^{n-2i}.$$

To that end we need to state a few basic properties of these polynomials. Most of the results in this section can be found in the survey [7] by Lidl, Mullen and Türnwald.

Dickson polynomials arise from Waring's formula in the following manner

$$\gamma^n + \delta^n = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-\gamma\delta)^i (\gamma+\delta)^{n-2i} = D_n(\gamma+\delta, \gamma\delta).$$

If we let $u = \gamma\delta$ and $x = \gamma + \frac{u}{\gamma}$, then we obtain a useful functional equation

$$D_n(\gamma + \frac{u}{\gamma}, u) = \gamma^n + \left(\frac{u}{\gamma}\right)^n. \quad (1)$$

This functional equation yields a number of properties of Dickson polynomials. From now on we study Dickson polynomials over the field $\mathbb{F}$.

Lemma 3.1. *The Dickson polynomials* $D_n(x, u)$ *satisfy the following*

(i) $D_{n+2}(x, u) = x\, D_{n+1}(x, u) + u\, D_n(x, u)$ *for* $n \geq 0$ *with initial values* $D_0(x, u) = 0$ *and* $D_1(x, u) = x$*.*

(ii) $D_{nl}(x,u) = D_n(D_l(x,u), u^l)$.

(iii) $D_{2^k}(x,u) = x^{2^k}$ *for every* $k \geq 0$.

(iv) $D_{2^k+1}(x, u+v) = D_{2^k+1}(x,u) + D_{2^k+1}(x,v) + x^{2^k+1}$ *for every* $k \geq 0$.

(v) $D_{2^k+1}(x, x^2) = x^{2^k+1}$ *if* k *is even and 0 if* k *is odd.*

The last two facts are consequences of the relation

$$D_{2^k+1}(x,u) = x^{2^k+1} + ux^{2^k-1} + u^2x^{2^k-3} + u^4x^{2^k-7} + \cdots + u^{2^{k-1}}x \qquad (2)$$

which can be verified by Lucas theorem for binomial coefficients.

The next result was originally proved in [2] by Chou et al. Let $s = \gcd(n, 2^m - 1)$ and $t = \gcd(n, 2^m + 1)$.

Theorem 3.2. *Let* $x \in \mathbb{F}$ *and let* $D_n^{-1}(D_n(x,u^2))$ *be the preimage of* $D_n(x,u^2)$ *with* $u \in \mathbb{F}^*$. *Then* $|D_n^{-1}(D_n(x,u^2))|$

$$= \begin{cases} s & \textit{if } D_n(x,u^2) \neq 0 \textit{ and } \operatorname{Tr}\left(\frac{u}{x}\right) = 0 \\ t & \textit{if } D_n(x,u^2) \neq 0 \textit{ and } \operatorname{Tr}\left(\frac{u}{x}\right) = 1 \\ \frac{s+t}{2} & \textit{if } D_n(x,u^2) = 0. \end{cases}$$

In this paper we have always $s = 1$ and in this case we can easily deduce the following lemma.

Lemma 3.3. *Let* $s = 1$ *and* $D_n(x,u^2) \neq 0$. *Then*

$$\operatorname{Tr}\left(\frac{u}{x}\right) = \operatorname{Tr}\left(\frac{u^n}{D_n(x,u^2)}\right).$$

Proof. Clearly $x \neq 0$ since $D_n(x,u^2) \neq 0$. Assume $\operatorname{Tr}(\frac{u}{x}) = 0$. By Lemma 2.1 this means that we can express x in the form $\gamma + \frac{u^2}{\gamma}$ where γ is in the field $\mathbb{F}$. Then also γ^n and $\frac{u^{2n}}{\gamma^n}$ are in the field $\mathbb{F}$. By the functional equation (1) they are the roots of the equation $T^2 + D_n(x,u^2)T + u^{2n} = 0$ and hence $\operatorname{Tr}(\frac{u^n}{D_n(x,u^2)}) = 0$.

Assume now that $\operatorname{Tr}(\frac{u^n}{D_n(x,u^2)}) = 0$. This implies that the roots γ and $\frac{u^{2n}}{\gamma}$ of the equation $T^2 + D_n(x,u^2)T + u^{2n} = 0$ are now in the field $\mathbb{F}$. We have assumed that $s = 1$ and therefore γ has a unique nth root $\sqrt[n]{\gamma}$ in $\mathbb{F}$. So by the functional equation $x = \sqrt[n]{\gamma} + \frac{u^2}{\sqrt[n]{\gamma}}$ and therefore $\operatorname{Tr}(\frac{u}{x}) = 0$. □

Cardan's method for solving a cubic equation can be used to calculate roots of equations involving Dickson polynomials as can be seen in the previous proof. This was known already to Dickson, see e.g. [3].

Proposition 3.4. *Let $s = 1$ and $v \neq 0$. Then we have an effective procedure for solving all the roots x of the equation*

$$D_n(x, u^2) = v.$$

Proof. (i) When $\mathrm{Tr}(\frac{u^n}{v}) = \mathrm{Tr}(\frac{u}{x}) = 0$ we can find one root x as in the proof of Lemma 3.3 and according to Theorem 3.2 it is the only root in $\mathbb{F}$. In calculations we have to solve one quadratic equation and this can be done by Lemma 2.1.

(ii) When $\mathrm{Tr}(\frac{u^n}{v}) = \mathrm{Tr}(\frac{u}{x}) = 1$ we can find the roots γ and $\frac{u^{2n}}{\gamma}$ of the equation $T^2 + D_n(x, u^2)T + u^{2n} = 0$ in the quadratic extension of $\mathbb{F}$ by Lemma 2.1. If there does not exist an nth root of γ in this quadratic extension, the equation has no roots in $\mathbb{F}$. If there is one nth root of γ, there are t of them and every such root gives a different solution to the equation. According to Theorem 3.2 these are then all the solutions. Although $x = \sqrt[n]{\gamma} + \frac{a^2}{\sqrt[n]{\gamma}}$ and $\sqrt[n]{\gamma}$ are no longer in $\mathbb{F}$, the roots x are still in $\mathbb{F}$. $\square$

The interested reader is referred to [2] or [7] for further details.

4 Decoding of the Goethals-like codes $\mathcal{C}_k$

Let X, Y, Z, A, B, C denote elements in $\mathcal{T}$ and x, y, z, a, b, c their respective projections under μ-mapping in $\mathbb{F}$. Let $\mathbf{r} \in \mathbb{Z}_4^{2^m}$ be the received vector and let $\mathbf{e} \in \mathbb{Z}_4^{2^m}$ be the error vector. The syndrome of the received vector is

$$\mathbf{S} = \mathbf{r}H_k^T = \mathbf{e}H_k^T = (t, A + 2B, 2C)$$

where H_k^T denotes the transpose of H_k and

$$\begin{aligned} \sum_{X \in \mathcal{T}} e_X &= t, & t &\in \mathbb{Z}_4 \\ \sum_{X \in \mathcal{T}} e_X X &= A + 2B, & A, B &\in \mathcal{T} \\ 2 \sum_{X \in \mathcal{T}} e_X X^{2^k+1} &= 2C, & C &\in \mathcal{T}. \end{aligned}$$

By Lemma 2.2, the last two equations are equivalent to the following system of three binary equations:

$$\begin{aligned} a &= \sum_{x \in E_1 \cup E_3} x \\ b^2 &= \sum_{x \in E_2 \cup E_3} x^2 + \sum_{\substack{x,y \in E_1 \cup E_3 \\ x<y}} xy \\ c &= \sum_{x \in E_1 \cup E_3} x^{2^k+1}. \end{aligned}$$

Observing that syndrome

$$-\mathbf{S} = (-t, -(A+2B), -2C) = (-t, A+2(A+B), 2C)$$

corresponds to the error vector $-\mathbf{e}$ we can reduce the number of different error patterns that need to be considered.

We will divide the discussion into four cases depending on the value of t. As examples we have expanded the resulting polynomial conditions in the case $k = 2$.

4.1 The case of $t = 0$

Theorem 4.1. *Let* $\mathbf{S} = (0, A+2B, 2C)$ *denote the syndrome of a coset.*

(i) If $a = b = c = 0$*, then* $\mathbf{0}$ *is the coset leader.*

(ii) If $a \neq 0$ *and* $c = (\frac{b^2}{a} + a)^{2^k+1} + (\frac{b^2}{a})^{2^k+1}$*, then the coset leader has Lee weight 2 and is uniquely determined by* $x = \frac{b^2}{a} + a$*,* $e_X = 1$*,* $y = \frac{b^2}{a}$*, and* $e_Y = 3$*. In particular in the case* $k = 2$*, the latter condition can be rewritten in the form* $a^8 + a^6 b^2 + b^8 + a^3 c = 0$*.*

(iii) If (i) and (ii) do not hold, then any coset leader has Lee weight ≥ 4*.*

Proof. (i) Clear.

(ii) Suppose we have an error of Lee weight 2 where $e_X = 1$, $e_Y = 3$ and $X \neq Y$. This leads to the syndrome equations

$$\begin{aligned} a &= x + y \\ b^2 &= y^2 + xy \\ c &= x^{2^k+1} + y^{2^k+1}. \end{aligned}$$

Since $X \neq Y$ it follows that $a = x + y \neq 0$. The first two equations have the unique solution

$$x = \frac{b^2}{a} + a \qquad y = \frac{b^2}{a}$$

which obeys the third equation if and only if

$$c = (\frac{b^2}{a} + a)^{2^k+1} + (\frac{b^2}{a})^{2^k+1}.$$

(iii) If cases (i) and (ii) do not hold, we detect an error of Lee weight ≥ 4, since the conditions in (i) and (ii) describe all cosets of Lee weight 0 and 2, respectively, where $t = 0$. □

4.2 The case of $t = 1$

Theorem 4.2. *Let* $\mathbf{S} = (1, A + 2B, 2C)$ *denote the syndrome of a coset.*

(i) If $b = 0$ and $c = a^{2^k+1}$, then the coset leader has Lee weight 1 and is uniquely determined by $x = a$ and $e_X = 1$.

(ii) If $b \neq 0$ and $c = a^{2^k+1}$, then the coset leader has Lee weight 3 and is uniquely determined by $x = a + b$, $e_X = 2$, $y = a$, and $e_Y = 3$.

(iii) If $b \neq 0$, $c \neq a^{2^k+1}$ and $\mathrm{Tr}(\frac{b^{2^k+1}}{a^{2^k+1}+c}) = 0$, then the coset leader has Lee weight 3. The coset leader is uniquely determined by $e_X = e_Y = 1$, $e_Z = 3$, $D_{2^k-1}(z + a, b^2) = \frac{a^{2^k+1}+c}{b^2}$ and x and y are the zeros of $T^2 + (z + a)T + b^2 + az = 0$. In particular in the case $k = 2$ the variable z should satisfy $(z + a)^3 + b^2(z + a) = \frac{a^5+c}{b^2}$.

(iv) If $b \neq 0$, $c \neq a^{2^k+1}$ and $p(T) = T^3 + aT^2 + (a^2 + b^2)T + \sigma_3$ has three distinct zeros in $\mathbb{F}$ where σ_3 satisfies $D_n(\sigma_3 + a^3 + ab^2, b^6) = \frac{a^{2^k+1}+c}{d}$ and

$$\begin{cases} n = \frac{2^k+1}{3} \text{ and } d = 1 & \text{if } 2 \nmid k \\ n = \frac{2^k-1}{3} \text{ and } d = b^2 & \text{if } 2 \mid k, \end{cases}$$

then a coset leader has Lee weight 3 and is uniquely determined such that x, y, z are the three distinct zeros of $p(T)$ in $\mathbb{F}$ and $e_X = e_Y = e_Z = 3$. Especially, when $k = 2$ the condition for σ_3 can be stated as $\sigma_3 = \frac{c+a^5+a^3b^2+ab^4}{b^2}$.

(v) If none of (i)–(iv) hold, then any coset leader has Lee weight ≥ 5.

Proof. (i) Consider a single error in the location X with $e_X = 1$. Then $a = x$, $b = 0$ and $c = x^{2^k+1} = a^{2^k+1}$ and the coset leader with this syndrome is therefore uniquely determined by $x = a$ and $e_X = 1$.

(ii) In the case of an error of Lee weight 3 where $e_X = 2$, $e_Y = 3$ and $X \neq Y$, we obtain the syndrome equations

$$\begin{aligned} a &= y \\ b^2 &= x^2 + y^2 \\ c &= y^{2^k+1}. \end{aligned}$$

Since $X \neq Y$ we have $b = x + y \neq 0$. The above system of equations has a solution if and only if $c = a^{2^k+1}$ and in this case the solution gives the coset leader uniquely determined by

$$x = a + b \quad \text{and} \quad y = a$$

where $e_X = 2$ and $e_Y = 3$.

(iii) Suppose we have an error of Lee weight 3 where $e_X = e_Y = 1$ and $e_Z = 3$ such that X, Y and Z are pairwisely distinct. We get the syndrome equations

$$\begin{aligned} a &= x + y + z \\ b^2 &= z^2 + xy + xz + yz \\ c &= x^{2^k+1} + y^{2^k+1} + z^{2^k+1}. \end{aligned}$$

If $B = 0$, we would have a codeword of Lee weight 4 in $\mathcal{P}$ with $e_X = e_Y = 1$ and $e_Z = e_A = 3$. So $b \neq 0$. From the first two equations we see that $xy = az + b^2$ and using the functional equation (1) and Lemma 3.1 we derive

$$\begin{aligned} c &= D_{2^k+1}(x + y, xy) + z^{2^k+1} \\ &= D_{2^k+1}(z + a, az + b^2) + z^{2^k+1} \\ &= D_{2^k+1}(z + a, az) + D_{2^k+1}(z + a, b^2) + (z + a)^{2^k+1} + z^{2^k+1} \\ &= a^{2^k+1} + (z + a)D_{2^k}(z + a, b^2) + b^2 D_{2^k-1}(z + a, b^2) + (z + a)^{2^k+1} \\ &= a^{2^k+1} + b^2 D_{2^k-1}(z + a, b^2). \end{aligned}$$

All in all we have

$$D_{2^k-1}(z + a, b^2) = \frac{a^{2^k+1} + c}{b^2}. \tag{3}$$

Now we have $s = \gcd(2^k - 1, 2^m - 1) = 2^{\gcd(k,m)} - 1 = 1$.

Assume we could solve z from the previous equation. Then we could find x and y as roots of the equation

$$T^2 + (z + a)T + b^2 + az = 0.$$

This has two roots in $\mathbb{F}$ if and only if

$$\mathrm{Tr}\left(\frac{b^2 + az}{(z + a)^2}\right) = \mathrm{Tr}\left(\frac{b^2}{(z + a)^2}\right) = \mathrm{Tr}\left(\frac{b}{z + a}\right) = \mathrm{Tr}\left(\frac{b^{2^k+1}}{a^{2^k+1} + c}\right) = 0$$

by Lemma 3.3. So when we have this error pattern the above condition must hold and therefore we can also calculate the unique root of equation (3) by Proposition 3.4.

(iv) Consider the error of Lee weight 3 with distinct error locations X, Y and Z where $e_X = e_Y = e_Z = 3$. This leads to the syndrome equations

$$\begin{aligned} a &= x + y + z \\ b^2 &= x^2 + y^2 + z^2 + xy + xz + yz \\ c &= x^{2^k+1} + y^{2^k+1} + z^{2^k+1}. \end{aligned}$$

If B would be 0, we would have a codeword of Lee weight 4 with $e_X = e_Y = e_Z = e_A = 3$ in $\mathcal{P}$. So we have $b \neq 0$. We know that x, y and z are the zeros of the polynomial

$$p(T) = T^3 + aT^2 + (a^2 + b^2)T + \sigma_3$$

where $\sigma_3 = xyz$. If we can find σ_3, then we can calculate the zeros. We need the following simple fact

$$p(U + a) = D_3(U, b^2) + \sigma_3 + a^3 + ab^2. \tag{4}$$

Now we solve σ_3 from the syndrome equations. From the first two equations we get $xy = z^2 + a^2 + az + b^2$ and by the functional equation (1) and Lemma 3.1

$$\begin{aligned} c &= D_{2^k+1}(x + y, xy) + z^{2^k+1} \\ &= D_{2^k+1}(z + a, z^2 + a^2) + D_{2^k+1}(z + a, az) + D_{2^k+1}(z + a, b^2) + z^{2^k+1} \\ &= (k + 1)(z + a)^{2^k+1} + a^{2^k+1} + D_{2^k+1}(z + a, b^2). \end{aligned}$$

If $2 \nmid k$, then $3 \mid 2^k + 1$ and

$$c = a^{2^k+1} + D_{\frac{2^k+1}{3}}(D_3(z + a, b^2), b^6).$$

If $2 \mid k$, then $3 \mid 2^k - 1$ and

$$
\begin{aligned}
c &= (z+a)^{2^k+1} + a^{2^k+1} + (z+a)D_{2^k}(z+a,b^2) + b^2 D_{2^k-1}(z+a,b^2) \\
&= a^{2^k+1} + b^2 D_{\frac{2^k-1}{3}}(D_3(z+a,b^2), b^6)
\end{aligned}
$$

By the equation (4)

$$p(z) = D_3(z+a,b^2) + \sigma_3 + a^3 + ab^2 = 0$$

and we conclude that

$$D_n(\sigma_3 + a^3 + ab^2, b^6) = \frac{a^{2^k+1} + c}{d} \tag{5}$$

where

$$\begin{cases} n = \frac{2^k+1}{3} \text{ and } d = 1 & \text{if } 2 \nmid k \\ n = \frac{2^k-1}{3} \text{ and } d = b^2 & \text{if } 2 \mid k. \end{cases}$$

It is straightforward to see that $s = \gcd(n, 2^m - 1) = 1$ and

$$t = \gcd(n, 2^m + 1) = \begin{cases} 1 & \text{if } 3 \nmid k \\ 3 & \text{if } 3 \mid k. \end{cases}$$

By Theorem 3.2 and the equation (4) the polynomial $p(T)$ can have three zeros in $\mathbb{F}$ only if $\sigma_3 + a^3 + ab^2 \neq 0$ and

$$\mathrm{Tr}\left(\frac{b}{U}\right) = \mathrm{Tr}\left(\frac{b^3}{\sigma_3 + a^3 + ab^2}\right) = 1.$$

By Lemma 3.3 and the equation (5) this condition is equivalent to the condition

$$\mathrm{Tr}\left(\frac{b^{3n}}{D_n(\sigma_3 + a^3 + ab^2, b^6)}\right) = \mathrm{Tr}\left(\frac{b^{2^k+1}}{a^{2^k+1} + c}\right) = 1,$$

but this is always true as otherwise we would be in the case (iii). This means that when σ_3 satisfies equation (5), then $p(T) = 0$ has either 0 or 3 roots.

When $3 \nmid k$ we can find the unique root of (5) by Proposition 3.4 and then get the zeros x, y and z of $p(T)$.

When $3 \mid k$ the equation (5) has three different roots and the calculation can be done by Proposition 3.4. We thus get 3 candidate values for σ_3. For two of the resulting candidates polynomial $p(T)$ has no zeros, and for the correct candidate σ_3 the polynomial has three zeros, which are then x, y and z.

(v) In all other cases, when $t = 1$ we detect an error of Lee weight ≥ 5. □

Of all the cases (iv) is computationally the most demanding. Syndrome with the coset leader of Lee weight 5 and $t = 1$ gives in the worst case 3 different σ_3's and for none of them $p(T)$ has three zeros.

Time consumption can be reduced by using more look-up tables. One table could have "true" in index δ iff $x^3 + x = \delta$ has three roots. With the aid of such a table one can quickly check when $p(T)$ has three zeros. Another table could list all $(2^m + 1)$th roots of unity in the quadratic extension of $\mathbb{F}$. This can be used to speed up the computation of nth roots in this bigger field.

4.3 The case of $t = 2$

Theorem 4.3. *Let* $\mathrm{S} = (2, A + 2B, 2C)$ *denote the syndrome of a coset.*

(i) If $a = c = 0$, then the coset leader has Lee weight 2 and is uniquely determined by $x = b$ and $e_X = 2$.

(ii) If $a \neq 0$ and $c = D_{2^k+1}(a, b^2)$ and $\mathrm{Tr}(\frac{b}{a}) = 0$, then the coset leader has Lee weight 2 and is uniquely determined such that x and y are zeros of $T^2 + aT + b^2 = 0$ and $e_X = e_Y = 1$. Especially, if $k = 2$, then c should be $a^5 + a^3b^2 + ab^4$.

(iii) If $a \neq 0$ and $c = D_{2^k+1}(a, a^2 + b^2)$ and $\mathrm{Tr}(\frac{b}{a}) = 1$, then the coset leader has Lee weight 2 and is uniquely determined such that x and y are zeros of $T^2 + aT + a^2 + b^2 = 0$ and $e_X = e_Y = 3$. In particular if $k = 2$, then c should be $a^5 + a^3b^2 + ab^4$.

(iv) If (i)–(iii) do not hold, then any coset leader has Lee weight ≥ 4.

Proof. (i) Consider a single error in the location X with $e_X = 2$. Then $a = c = 0$ and $x = b$.

(ii) In the case of an error of Lee weight 2 where $e_X = e_Y = 1$ and $X \neq Y$ we obtain the syndrome equations

$$\begin{aligned} a &= x + y \\ b^2 &= xy \\ c &= x^{2^k+1} + y^{2^k+1}. \end{aligned}$$

The first two equations show that x and y are the solutions of

$$p(T) = T^2 + aT + b^2 = 0.$$

Since $X \neq Y$ we have $a \neq 0$. By Lemma 2.1 the previous equation has two solutions in $\mathbb{F}$ if and only if

$$\mathrm{Tr}(\frac{b^2}{a^2}) = \mathrm{Tr}(\frac{b}{a}) = 0.$$

The solutions x and y obey the third equation if and only if $c = D_{2^k+1}(x+y, xy) = D_{2^k+1}(a, b^2)$ which is given explicitly in the equation (2). If the conditions of the theorem are satisfied, then we find the error positions as the zeros of $p(T)$ and $e_X = e_Y = 1$.

(iii) Assume error of Lee weight 2 where $e_X = e_Y = 3$ and $X \neq Y$. As mentioned in the beginning of this section we can now consider error $-\mathbf{e}$ as in the case (ii) with one difference: we replace b^2 by $(a+b)^2 = a^2+b^2$. So $x+y = a \neq 0$, $xy = a^2 + b^2$ and the equation

$$T^2 + aT + a^2 + b^2 = 0$$

should have two roots in $\mathbb{F}$. This condition is equivalent to

$$\mathrm{Tr}(\frac{a^2 + b^2}{a^2}) = \mathrm{Tr}(\frac{b}{a}) + 1 = 0.$$

(iv) In all other cases with $t = 2$ than (i)-(iii) an error of Lee weight ≥ 4 is detected. $\square$

By Lemma 3.1 we get that

$$D_{2^k+1}(a, a^2 + b^2) = D_{2^k+1}(a, b^2) + \begin{cases} 0 & \text{if } 2 \mid k \\ a^{2^k+1} & \text{if } 2 \nmid k. \end{cases}$$

In the case $2 \mid k$ we could implement this algorithm in a slightly different order: if $c = D_{2^k+1}(a, b^2)$, then we may branch into the cases (ii) and (iii) according to the value of $\mathrm{Tr}(\frac{b}{a})$.

4.4 The case of $t = 3$

As noted above if we have a syndrome $\mathbf{S} = (3, A + 2B, 2C)$ we can decode with syndrome $-\mathbf{S} = (1, A + 2(A + B), 2C)$ and get an error vector $\mathbf{e}$. Then the real error vector is $-\mathbf{e}$.

5 Conclusions and further research

We have given a decoding algorithm for all codes $\mathcal{C}_k$ which corrects all errors of Lee weight ≤ 3. Interestingly, when we study solutions to the syndrome equations this problem changes in some cases to a problem of finding the roots of certain Dickson polynomials.

Helleseth and Kumar [5] also presented a complete decoding algorithm for $\mathcal{C}_1$. Except in the two hard cases this complete decoding can be similarly generalized for $\mathcal{C}_k$. How about these two cases?

Another interesting question is: Are some codes $\mathcal{C}_k$ and C_l equivalent? In other words: Do we get the parity-check matrix of $\mathcal{C}_k$ by permuting and multiplying by ± 1 the columns of the parity-check matrix of $\mathcal{C}_l$? By a computer search we were able to verify that $\mathcal{C}_1$ and $\mathcal{C}_2$ of length 32 are inequivalent.

Acknowledgment

The author wishes to thank Jyrki Lahtonen for several useful discussions and also for suggesting this problem.

References

[1] Chin-Long Chen, *Formulas for the Solutions of Quadratic Equations over* $GF(2^m)$, IEEE Trans. Inform. Theory **28** (1982), no. 5, 792–794.

[2] W.-S. Chou, J. Gomez-Calderon, and G. L. Mullen, *Value sets of Dickson polynomials over finite fields*, J. Number Theory **30** (1988), 334–344.

[3] Leonard Eugene Dickson, *Linear Groups with an exposition of the Galois field theory*, Dover Publications, Inc., New York, 1958.

[4] A. Roger Hammons Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and Patrick Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and Related Codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319.

[5] Tor Helleseth and P. Vijay Kumar, *The Algebraic Decoding of the* Z_4*-Linear Goethals Code*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 2040–2048.

[6] Tor Helleseth, P. Vijay Kumar, and A. Shanbhag, *Codes with the Same Weight Distributions as the Goethals Codes and the Delsarte-Goethals Codes*, Designs, Codes and Cryptography **9** (1996), no. 3, 257–266.

[7] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65, Longman Scientific & Technical, Harlow, 1993.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**