Improving the minimum distance bound of Trace Goppa codes

Isabel Byrne[1†], Natalie Dodson[2†], Ryan Lynch[3†], Eric Pabón–Cancel[4†] and Fernando Piñero González[5*†]

[1]Department of Mathematics, Virginia Tech, 925 Prices Fork Road, Blacksburg, 24060, VA, USA.
[2]Department of Mathematics, Middlebury College, 75 Shannon Street,Middlebury, 05753, VT, USA.
[3]Department of Mathematics, Notre Dame University, 255 Hurley Bldg,Notre Dame, 46556, IN, USA.
[4]Department of Mathematics, University of Puerto Rico – Mayagüez Campus, 259 Blvd. Alfonso Valdés Cobián, Mayagüez, 00682, Puerto Rico, USA.
[5*]Department of Mathematics, University of Puerto Rico in Ponce, 2151 Ave. Santiago de los Caballeros, Ponce, 00716, PR, USA.

*Corresponding author(s). E-mail(s): isabeltb@vt.edu; ndodson@middlebury.edu; rlynch6@nd.edu; eric.pabon1@upr.edu; fernando.pinero1@upr.edu;
†These authors contributed equally to this work.

Abstract

In this paper we prove that the class of Goppa codes whose Goppa polynomial is of the form $\boldsymbol{g(x) = \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}$ where $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ is a trace polynomial from a field extension of degree $\boldsymbol{m \geq 3}$ has a better minimum distance than what the Goppa bound $\boldsymbol{d \geq 2\deg(g(x)) + 1}$ implies. This result is a significant improvement compared to the minimum distance of Trace Goppa codes over quadratic field extensions (the case $\boldsymbol{m = 2}$). We present two different techniques to improve the minimum distance bound. For general $\boldsymbol{p}$ we prove that the Goppa code $\boldsymbol{C(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q})}$ is equivalent to another Goppa code $\boldsymbol{C(M, h)}$ where $\boldsymbol{\deg(h) > \deg(\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q})}$. For $\boldsymbol{p = 2}$ we use the fact that

the values of $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ are fixed under q–powers to find several new parity check equations which increase the known distance bounds.

Keywords: Binary Goppa Codes, Trace Goppa codes, Minimum Distance

1 Introduction

Binary Goppa codes are one of the fundamental linear code constructions in Coding Theory. Binary Goppa codes have been extensively studied since their introduction by V.D. Goppa in [1]. Their rich algebraic structure and good decoding capabilities make binary Goppa codes suitable for cryptography applications. There are also Best Known Linear Codes constructions realized by binary Goppa codes.

Throughout this article we assume:

- q is a prime power
- $q = p^s$ for some natural number s
- $m \geq 3$

We focus on binary Goppa codes where the defining polynomial $g(x)$ is of the form $g(x) = \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$, that is

$$g(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}.$$

Definition 1 [1] Suppose $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$. Let $g(x)$ be a univariate polynomial of degree t such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. The *p–ary Goppa code* is defined as

$$C(L, g) := \{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_p^n : \sum_{i=1}^{n} \frac{c_i}{x - \alpha_i} \equiv 0 \mod g(x)\}.$$

Goppa codes satisfy the following:

Proposition 1 *[1] Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$. Let $g(x)$ be a polynomial of degree t such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. Then the dimension of $C(L, g)$ is at least $n - smt$ and the minimum distance of $C(L, g)$ is at least $t + 1$.*

We have stated the Goppa code dimension bound, $\dim C(L, g) \geq n - mst$, slightly differently from the classical dimension bound $\dim C(L, g) \geq n - mt$. This difference is because the set L is traditionally defined over $\mathbb{F}_q$ where $q = p^m$ but in our case $q^m = p^{ms}$.

The image of $g(x) = \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ is restricted to the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^m}$. Thus, there are two subfields to consider: the subfield containing $Im(g(x))$ and the subfield $\mathbb{F}_p$ over which $C(L, g)$ is defined. The set $Im(g(x)) \subseteq \mathbb{F}_q$ and $C(L, g)$

will be defined in $\mathbb{F}_p$. While Goppa codes can be defined over any subfield of $\mathbb{F}_{q^m}$, Goppa codes over the prime subfield $\mathbb{F}_p$ (and particularly in $\mathbb{F}_2$) remain the most interesting. Although our results hold for any subfield $\mathbb{F}_{q_0} \subseteq \mathbb{F}_{q^m}$, in this article we restrict ourselves to Goppa codes over the prime field $\mathbb{F}_p$.

One of the first improvements on the bounds of binary Goppa codes was given by Goppa in [1]. Goppa established that two different Goppa polynomials define the same binary Goppa codes, so one polynomial bounds the dimension of the code and the other polynomial bounds the minimum distance.

Proposition 2 *[1] Let $q = 2^s$. Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_{q^m}$. Let $g(x)$ be a squarefree polynomial of degree t such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. Then the binary Goppa codes satisfy:*

$$C(L, g) = C(L, g^2).$$

This proposition improves the distance bound from $t + 1$ to $2t + 1$. The distance bound on the Goppa code $C(L, g)$ follows from the fact that the codewords of $C(L, g)$ satisfy certain special parity check equations. Sugiyama et al. generalize this equivalence between Goppa codes over arbitrary fields $\mathbb{F}_{q_0}$.

Proposition 3 *[10] Let q^m be a prime power. Let $\mathbb{F}_{q_0}$ be a subfield of $\mathbb{F}_{q^m}$. Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subset of $\mathbb{F}_{q^m}$. Let $g(x)$ be a squarefree polynomial of degree t such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. Then Goppa codes defined over $\mathbb{F}_{q_0}$ satisfy:*

$$C(L, g^{q_0 - 1}) = C(L, g^{q_0}).$$

Definition 2 Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_{q^m}$ where $\#L = n$. Let $f(x) \in \mathbb{F}_{q^m}[X]$ be a polynomial. We define the evaluation map ev as

$$ev_L : \mathbb{F}_{q^m}[X] \to \mathbb{F}_{q^m}^n, ev_L(f) = (f(\alpha_1), f(\alpha_2) \ldots, f(\alpha_n)).$$

The map ev is a linear map from the polynomial ring $\mathbb{F}_{q^m}[X]$ to the vector space $\mathbb{F}_{q^m}^n$. Its kernel is $ker(ev) = \langle \prod_{\alpha \in L} (X - \alpha) \rangle$. We found $f(x) \in \mathbb{F}_{q^m}[X]$ very helpful for understanding the parity check equations of $C(L, g)$ and their linear relations. From the definition of Goppa codes it follows that the parity check equations for $C(L, g)$ may also be written as evaluation maps $ev_L(f)$. We describe these parity check equations as follows.

Proposition 4 *[1] Let q be a prime power. Let $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq \mathbb{F}_q$. Let $g(x)$ be a polynomial of degree t such that $g(\alpha_i) \neq 0$, for $\alpha_i \in L$. Then any codeword $c = (c_1, c_2, \ldots, c_n) \in C(L, g)$ satisfies*

$$c \cdot ev_L\left(\frac{X^j}{g(X)}\right) = 0 \text{ where } 0 \leq j \leq t - 1$$

Proposition 4 follows from the fact that $\frac{\alpha_i^j}{g(\alpha_i)}$ is the evaluation of $\frac{X^j}{g(X)}$ at α_i and the definition of Goppa codes. Goppa codes belong to a class of codes known as Alternant Codes, which are subfield subcodes of Generalized Reed–Solomon codes. Goppa codes are Alternant codes where $a_i = \frac{g(\alpha_i)}{\prod_{j \neq i}(\alpha_j - \alpha_i)}$). One important property of Alternant codes is that a decent bound on its minimum distance can be determined as follows:

Proposition 5 *Let $q = p^s$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct elements in $\mathbb{F}_{q^m}$. Let $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ be nonzero elements in $\mathbb{F}_{q^m}$. Let δ be a positive integer. Let C be a code of length n over $\mathbb{F}_p$. If $\sum_{i=1}^{n} c_i a_i \alpha_i^j = 0$ for $0 \leq j \leq \delta - 2$ for any $(c_1, c_2, \cdots, c_n) \in C$, then the minimum distance of C is at least δ.*

Proposition 5 is a restatement of the well known BCH bound which is the Goppa bound on the minimum distance of Goppa codes. The classical Goppa distance bound comes from the consecutive powers from $j = 0$ to $j = \deg(g) - 1$. We improved the distance bound by finding more consecutive powers which are parity check equations for $C(L, \mathbf{Tr}_{\mathbb{F}_{q^m} \setminus \mathbb{F}_q})$.

Goppa codes are linear codes defined over a small field, $\mathbb{F}_p$. However, the parity check equations describing the Goppa codes are defined over the larger field, $\mathbb{F}_{q^m}$. For $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ denote

$$x^{(p^i)} = (x_1^{p^i}, x_2^{p^i}, \ldots, x_n^{p^i}) \in \mathbb{F}_{q^m}^n.$$

Note that if $c \in C(L, g)$ and $c \cdot ev_L\left(\frac{X^j}{g(X)}\right) = 0$ then $c^{(p^i)} \cdot ev_L\left(\frac{X^j}{g(X)}\right)^{(p^i)} = 0$. Since $c \in \mathbb{F}_p$ it follows that $c^{(p^i)} = c$. Thus, for each p–power, we obtain additional parity check equations $c \cdot ev_L\left(\left(\frac{X^j}{g(X)}\right)^{p^i}\right) = 0$ as linear combinations of the defining parity check equations of the Goppa code. As $q^m = p^{ms}$ and there are ms different p–powers, the dimension bound $\dim(C(L, g)) \geq n - mst$ is obtained. Recall that the trace function $\mathbf{Tr}_{\mathbb{F}_{q^m} \setminus \mathbb{F}_q}(\alpha)$ takes values in the subfield $\mathbb{F}_q$ for any $\alpha \in \mathbb{F}_{q^m}$, implying that $\mathbf{Tr}_{\mathbb{F}_{q^m} \setminus \mathbb{F}_q}(\alpha)^q = \mathbf{Tr}_{\mathbb{F}_{q^m} \setminus \mathbb{F}_q}(\alpha)$ and that $ev_L\left(\frac{X^i}{g(X)^q}\right) = ev_L\left(\frac{X^i}{g(X)}\right)$. This fact will be important later when we prove that certain p–powers of evaluation vectors $ev_L\left(\frac{X^i}{g(X)^q}\right)$ and $ev_M\left(\frac{Y^j}{h(Y)^q}\right)$ are in the dual codes of another Goppa code with larger degree.

2 Improving the Minimum Distance of Trace Goppa Codes

P. Véron has improved bounds on the dimension and distance of Trace Goppa codes. Those bounds are sharp for $m = 2$. S. Bezzatev and N.

Shekhunova in [9] proved that the classical Goppa distance bound is sharp for $m = 2$. In this manuscript we improve the minimum distance for trace Goppa codes when $m \geq 3$. Véron's improvements are for a more general class of Trace Goppa codes, namely those where $g(x) = a(x)\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(b(x))$ where a and b are polynomials. Since the trace polynomial has a very high degree $\deg(\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}) = q^{m-1}$, then any Goppa code with Goppa polynomial $g(x) = a(x)\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(b(x))$ would have a lot of parity check equations and low dimension. In fact, $\dim C(L, \mathbf{Tr}_{\mathbb{F}_{2^m}\setminus\mathbb{F}_2}) = 0$ and $\dim C(L, \mathbf{Tr}_{\mathbb{F}_{4^m}\setminus\mathbb{F}_4}) = 1$. In many cases, the degree of $g(x) = a(x)\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(b(x))$ is too high and leads to trivial binary Goppa codes. For example, in the binary trace case (i.e. $q = 2$) the degree of the trace polynomial is the same as the length of the code and the resulting binary Goppa code has dimension 0. In the quaternary trace case, (i.e. $q = 4$) direct computations show that the resulting binary Goppa code is a repetition code.

We restrict ourselves to the class of trace Goppa codes where $a(x) = 1$ and $b(x) = x$. Although the trace polynomial may have a relatively high degree and therefore poor dimension, this class of trace Goppa codes includes codes with highly interesting parameters. For example, the trace Goppa code $C(L, x^{16} + x^2)$ is a best possible $[56, 16, 20]$ binary code. In [9] the authors established that the Goppa code $C(L, \mathbf{Tr}_{\mathbb{F}_{256}\setminus\mathbb{F}_{16}})$ is a best known $[240, 123, 36]$ binary code [11]. The binary code $C(L, \mathbf{Tr}^6_{\mathbb{F}_{256}\setminus\mathbb{F}_{16}})$ is also a best known $[240, 21, 104]$ binary code ([11]). Strangely enough, the Goppa code $C(L, \mathbf{Tr}^4_{\mathbb{F}_{256}\setminus\mathbb{F}_{16}})$ is not the best known code for its dimension. In this case the best known code is a binary $[240, 39, 79]$ code obtained from a BCH code.

We improve the minimum distance bound of Trace Goppa codes with $g(x) = \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ by finding additional parity check equations.

Lemma 6 *Suppose* $0 \leq i \leq q^m - 2$. *Assume the* q*–ary expansion of* $i = \sum_{s=0}^{m-1} i_r q^r$ *where* $0 \leq i_r \leq q - 1$. *Then* $qi \mod q^m - 1 = \sum_{r=0}^{m-1} i_{r-1} q^s$.

The parity check equations for $C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$ are $ev_L\left(\frac{X^i}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ for $0 \leq i \leq q^{m-1} - 1$ and their p–powers. Since $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(\alpha)^q = \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(\alpha)$ for any $\alpha \in \mathbb{F}_{q^m}$, $ev_L\left(\frac{X^i}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ for $q^{m-1} \leq i \leq q^{m-1} + q^{m-2} + \cdots + q$ may be obtained from a q–power of some $ev_L\left(\frac{X^j}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}(X)}\right)$ where $0 \leq j \leq q^{m-1} - 1$.

Lemma 7 *Let* $q^{m-1} \leq i \leq q^{m-1} + q^{m-2} + \cdots + q$. *Then*

$$ev_L\left(\frac{X^i}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(q)} \in C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}.$$

Proof Suppose $q^{m-1} \leq i \leq q^{m-1}+q^{m-2}+\cdots+q$. The q-ary expansion of i is of the form $i = \sum_{r=0}^{m-1} i_r q^r$ where at least one of the entries $i_r = 0$. Otherwise if each $i_r \geq 1$ then $i > q^{m-1}+q^{m-2}+\cdot+q$. If $i_r = 0$, then $i' = q^{m-1-r}i \mod q^m - 1 < q^{m-1}$. Therefore, $ev_L\left(\frac{X^i}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(q^{m-1-r})} = ev_L\left(\frac{X^{i'}}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$.

□

Corollary 8 *The minimum distance of* $C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$ *is at least* $q^{m-1}+q^{m-2}+\cdots+q+2$.

Proof Since $ev_L\left(\frac{X^i}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$ for $0 \leq i \leq q^{m-1}+q^{m-2}+\cdots+q$, Proposition 5 implies

$$d(\left(C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)\right) \geq q^{m-1}+q^{m-2}+\cdots+q+2.$$

□

3 Further improvements on the minimum distance

For the remainder of the article we shall assume q is even and that the trace Goppa code $C(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q})$ is a binary code. Since $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ is a squarefree polynomial additional parity check equations can be of the form $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ can be found for the binary case. The definition of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$ implies that the evaluation vectors $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ for $0 \leq i < 2q^{m-1}$ span $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$. If q is a power of 2, we can generalize Lemma 7 to improve the minimum distance bound for $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$. Our improvement lies in finding additional consecutive powers $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ in the span of $C(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q})^{\perp}$. In the next Lemma we state a sufficient condition to determine when a function of the form $ev_L(X^i) \in C(L,g)^{\perp}$.

Lemma 9 *Let* g *be a monic polynomial of degree* t. *Let* $i \geq t$. *Suppose that* $ev_L\left(\frac{X^{i'}}{g(X)}\right) \in C(L,g)^{\perp}$ *for all* $0 \leq i' < i+t$. *Then*

$$ev_L\left(\frac{X^{i+t}}{g(X)}\right) \in C(L,g)^{\perp} \text{ if and only if } ev_L(X^i) \in C(L,g)^{\perp}.$$

Proof Suppose that $ev_L\left(\frac{X^{i'}}{g(X)}\right) \in C(L,g)^{\perp}$ for all $0 \leq i' < i+t$.

Note that

$$ev_L\left(X^i\right) - ev_L\left(\frac{X^{i+t}}{g(X)}\right) = ev_L\left(X^i - \frac{X^{i+t}}{g(X)}\right) = ev_L\left(\frac{X^i g(X) - g_t X^{i+t}}{g(X)}\right).$$

As g is a polynomial of degree t, all terms of $X^i g(X) - X^{i+t}$ have degree less than $i+t$. By the hypothesis of this Lemma, $ev_L\left(\frac{X^i g(X) - X^{i+t}}{g(X)}\right) \in C(L,g)^{\perp}$. As the difference

$$ev_L\left(X^i\right) - ev_L\left(\frac{X^{i+t}}{g(X)}\right) \in C(L,g)^{\perp}$$

it follows that $ev_L\left(\frac{X^{i+t}}{g(X)}\right) \in C(L,g)^{\perp}$ if and only if $ev_L(X^i) \in C(L,g)^{\perp}$. □

Since the code $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$ is closed under 2–powers, working with $ev_L(X^{i'})$ allows for a direct use of BCH techniques to increase the distance bound. It allows us to automatically assume all even powers are in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$. It also allows us to prove $ev_L(X^{\frac{q}{2}i'}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$ which can be easier to prove than $ev_L(X^{i'}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$

Lemma 10 *Let* $i = \sum_{r=0}^{m-1} i_r q^r$ *where* $0 \leq i_r \leq q-1$. *If*

$$2q^{m-1} \leq i < 2(q^{m-1} + q^{m-2} + \cdots + q + 1)$$

then $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$.

Proof By the bound on i, there is one coefficient i_r which is less than 2. By Lemma 6 there is some index r' such that the remainder $q^{r'} i \mod q^m - 1 < 2q^{m-1}$.

Therefore

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(q^{r'})} = ev_L\left(\frac{X^{iq^{r'}}}{\mathbf{Tr}^{2q^{r'}}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$$

$$= ev_L\left(\frac{X^{iq^{r'}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) = ev_L\left(\frac{X^{iq^{r'} \mod q^m - 1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right).$$

Since $iq^{r'} \mod q^m - 1$ is less than $2q^{m-1}$, it follows that $ev_L\left(\frac{X^{iq^{r'} \mod q^m - 1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$. Since $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$ is closed under 2–powers, it follows that $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^{\perp}$. □

We discover more parity check equations to improve the minimum distance bound by taking $\frac{q}{2}$ powers. The key insight is that if i is not too large then $i\frac{q}{2} \mod q^m-1$ is small and $ev_L\left(\frac{X^{i\frac{q}{2} \mod q^m-1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$.

Lemma 11 *If* $i = 2q^{m-1} + 2q^{m-2} + \cdots + 2q + 2$ *then*

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp.$$

Proof Note that $i\frac{q}{2} \mod q^m - 1 = q^{m-1} + q^{m-2} + \cdots + q + 1$.

Therefore

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(\frac{q}{2})} = ev_L\left(\frac{X^{i\frac{q}{2}}}{\mathbf{Tr}^q_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) = ev_L\left(\frac{X^{i\frac{q}{2}} \mod q^m-1}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right).$$

Since $ev_L\left(\frac{X^{i\frac{q}{2}} \mod q^m-1}{\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) = ev_L\left(\frac{X^{q^{m-1}+q^{m-2}+\cdots+q+1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ and all terms of $X^{q^{m-1}+q^{m-2}+\cdots+q+1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ have degree less than i, then $ev_L\left(\frac{X^{q^{m-1}+q^{m-2}+\cdots+q+1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$ which implies $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(\frac{q}{2})}$ and $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ are in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$.

□

Lemma 11 proves that the first $2(q^{m-1} + q^{m-2} + \cdots + q + 1)$ consecutive powers are in the span of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$. Our aim is to use these additional powers to prove that if i is small enough, then $i\frac{q}{2} + q^{m-1} \mod q^m - 1$ is also small enough such to imply $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$. If $2q^{m-1} \leq i < 2q^{m-1} + 3q^{m-2}$ then when writing i in its q basis expansion the first coefficient $i_{m-1} = 2$ and the second coefficient $0 \leq i_{m-2} \leq 2$. In this lemma we shall use the identity $q^{a-1} + q^{a-2} + \cdots + q + 1 = \frac{q^a-1}{q-1}$ to simplify notation.

Lemma 12 *Let* $2\frac{q^m-1}{q-1} < i \leq 2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1}$. *Then*

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp.$$

Proof Let i be as in the hypothesis of the theorem. Then $\frac{q}{2}i \leq q\frac{q^m-1}{q-1} + q\frac{q^{m-2}-1}{q-1}$. Taking the remainder of both sides modulo $q^m - 1$ we obtain $\frac{q}{2}i - q^m + 1 \leq \frac{q^m-1}{q-1} +$

$q\frac{q^{m-2}-1}{q-1}$. Adding q^{m-1} on both sides we obtain $\frac{q}{2}i - q^m + 1 + q^{m-1} \leq \frac{q^m-1}{q-1} + q\frac{q^{m-1}-1}{q-1}$. Note that $\frac{q^m-1}{q-1} + q\frac{q^{m-1}-1}{q-1} < 2\frac{q^m-1}{q-1}$.

Now that we have proven key bounds on $\frac{q}{2}i \mod q^m - 1$ we can prove the statement of the lemma.

Recall that

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(\frac{q}{2})} = ev_L\left(\frac{X^{\frac{q}{2}i \mod q^m-1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right).$$

The bounds on $\frac{q}{2}i \mod q^m - 1$ imply that all terms of $X^{\frac{q}{2}i \mod q^m-1}\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ have degree $< 2\frac{q^m-1}{q-1}$. Therefore $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{(\frac{q}{2})}$ and $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$ are in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$.

□

We use the additional parity check equations to state an improved distance bound for $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$.

Corollary 13 *Let q be an even prime power. The minimum distance of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$ is at least*

$$2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1} + 2$$

Proof Recall that $C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right) = C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)$. Lemmas 11 and 12 imply that

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$$

for $0 \leq i \leq 2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1}$. As there are $2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1} + 1$ consecutive parity check equations, we obtain $d\left(C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)\right) \geq 2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1} + 2$. □

4 Further improvements for $m = 3$

The technique presented in the previous section can be further extended for particular values of m and p. More consecutive powers in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$ implies more $\frac{q}{2}$ powers can be taken, which then implies more consecutive powers in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)^\perp$. For example, if we apply Lemma 12 again bounding $\frac{q}{2}i - q^m + 1 + q^{m-1}$ by $2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1}$ then the bound on i is increased by $4\frac{q^{m-3}-1}{q-1}$. This is a meaningful increase only if $m \geq 3$.

So far, we have improved the bound on $d\left(C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)\right)$ finding additional parity check equations leading to

$$d\left(C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}\right)\right) \geq 2\frac{q^m-1}{q-1} + 2\frac{q^{m-2}-1}{q-1} + 2.$$

Next, we improve the minimum distance for $m = 3$.

We prove that $ev_L\left(\frac{X^{2q^2+2q+5}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$. If true, then $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$ would contain $2q^2+2q+7$ consecutive powers, which implies the $d\left(C\left(L, \mathbf{Tr}_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)\right) \geq 2q^2+2q+8$. As in the previous section we assume that q is an even prime power such that $q \geq 8$ as the trace Goppa codes for $q = 2$ and $q = 4$ are trivial.

Corollary 14

$$ev_L\left(\frac{X^{2q^2+2q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)} \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$$

Proof This corollary is follows from Lemma 11 and Lemma 12. □

Lemma 15 *Let $q = 2^s$ where $s \geq 3$.*

$$ev_L\left(X^{2q+5}\right)^{\left(\frac{q}{2}\right)} \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$$

Proof We shall write $ev_L\left(X^{2q+5}\right)^{\left(\frac{q}{2}\right)}$ as a linear combination of 2–powers of $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$ where $0 \leq i < 2q^2$. Since each of the following powers satisfy $0 \leq i < 2q^2$ and $q \geq 8$ the following evaluation vectors are elements of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$:

$$c_1 = ev_L\left(\frac{X^{6q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)}, c_2 = ev_L\left(\frac{X^{q^2+(\frac{q}{2}+1)q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)^{(q^2)},$$

$$c_3 = ev_L\left(\frac{X^{q^2+\frac{q}{2}q+4}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)^{(q^2)}$$

$$c_4 = ev_L\left(\frac{X^{q^2+2q+\frac{q}{2}+2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_5 = ev_L\left(\frac{X^{q^2+4q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$$

Taking the 2–powers inside of the evaluation, we obtain:

$$c_1 = ev_L\left(\frac{X^{3q^2+q+\frac{q}{2}}}{\mathbf{Tr}_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_2 = ev_L\left(\frac{X^{3q^2+q+\frac{q}{2}+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right),$$

$$c_3 = ev_L\left(\frac{X^{4q^2+q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$$

$$c_4 = ev_L\left(\frac{X^{q^2+2q+\frac{q}{2}+2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_5 = ev_L\left(\frac{X^{q^2+4q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$$

Now we rewrite c_1 as the evaluation of a rational function with $\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}$ in the denominator by multiplying both sides by $\mathbf{Tr}_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}$.

$$c_1 = ev_L\left(\frac{X^{3q^2+q+\frac{q}{2}}(X+X^q+X^{q^2})}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_2 = ev_L\left(\frac{X^{3q^2+q+\frac{q}{2}+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$$

$$c_3 = ev_L\left(\frac{X^{4q^2+q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_4 = ev_L\left(\frac{X^{q^2+2q+\frac{q}{2}+2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right), c_5 = ev_L\left(\frac{X^{q^2+4q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right)$$

We expand c_1 as

$$c_1 = ev_L\left(\frac{X^{3q^2+q+\frac{q}{2}+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + ev_L\left(\frac{X^{3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + ev_L\left(\frac{X^{4q^2+q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right).$$

Therefore,

$$c_1 = c_2 + ev_L\left(\frac{X^{3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + c_3$$

Note that the sum $c_1+c_2+c_3+c_4+c_5$ equals

$$c_1+c_2+c_3+c_4+c_5 = c_2 + ev_L\left(\frac{X^{3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + c_3 + c_2 + c_3 + c_4 + c_5$$

$$= ev_L\left(\frac{X^{3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + c_4 + c_5$$

$$= ev_L\left(\frac{X^{3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + ev_L\left(\frac{X^{q^2+2q+\frac{q}{2}+2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) + ev_L\left(\frac{X^{q^2+4q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right).$$

$$= ev_L\left(\frac{X^{q^2+2q+\frac{q}{2}}(X^2+X^{2q}+X^{2q^2})}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) = ev_L\left(X^{q^2+2q+\frac{q}{2}}\right)$$

However $X^{q^2+2q+\frac{q}{2}} = (X^{2q+5})^{\frac{q}{2}}$. Therefore

$$c_1+c_2+c_3+c_4+c_5 = ev_L\left(X^{2q+5}\right)^{\left(\frac{q}{2}\right)}.$$

As we have decomposed $ev_L\left(X^{2q+5}\right)^{\left(\frac{q}{2}\right)}$ as the sum of elements of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$, it follows that $ev_L(X^{2q+5}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$. □

As a consequence we obtain the the following improvement on the minimum distance of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)$.

Theorem 16 *The minimum distance of* $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)$ *is at least* $2q^2+2q+8$.

Proof By the definition of the Goppa code

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}, 0 \leq i \leq 2q^2-1.$$

Lemma 11 and Lemma 12 imply that

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}, 0 \leq i \leq 2q^2+2q+4.$$

Corollary 14 implies

$$ev_L(X^{2q+3}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$$

and Lemma 15 suggests

$$ev_L(X^{2q+5}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}.$$

Because $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$ is closed under 2–powers, then

$$ev_L(X^{2q+2}), ev_L(X^{2q+4}), ev_L(X^{2q+6}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}.$$

Lemma 9 implies that

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}, 0 \leq i \leq 2q^2+2q+6.$$

There are $2q^2+2q+7$ consecutive powers in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}\right)^{\perp}$ which signifies

$$d(C(L, \mathbf{Tr}^2_{\mathbb{F}_{q^3}\setminus\mathbb{F}_q}) \geq 2q^2+2q+8.$$

□

5 Further improvements for $m = 4$

We apply a similar technique for the case $m = 4$ to increase the bound for $d\left(C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)\right)$.

Lemma 17 *Let* $q = 2^s$ *where* $s \geq 3$.

$$ev_L\left(X^{2q^2+4q+i}\right)^{\left(\frac{q}{2}\right)} \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$$

for $0 \leq i \leq q-1$.

Proof Lemma 11 implies $ev_L\left(X^{2q^2+4q+i}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ for $0 \leq i \leq 4$. Since $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ is closed under 2–powers, we may assume the theorem holds when i is even. We proceed by induction on i. Suppose $i = 2i_0 + 1$ is odd.

We shall write the vector $ev_L\left(X^{2q^2+4q+2i_0+1}\right)^{\left(\frac{q}{2}\right)}$ as a combination of 2–powers of evaluations of $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ where $0 \leq i < 2q^2$.

Note

$$ev_L\left(X^{2q^2+4q+2i_0+1}\right)^{\left(\frac{q}{2}\right)} = ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right).$$

The parity check equations $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^2}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$, $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^{2q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ and $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^{2q^2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ are in the code $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ because the power of X in the numerator is less than $2q^3$. Therefore $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^2}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$, $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^{2q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ and $ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^{2q^2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$

Therefore $ev_L(X^{2q^2+4q+2i_0+1}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ if and only if $ev_L\left(\frac{X^{3q^3+2q^2+i_0q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$. We need to determine if

$$ev_L\left(\frac{X^{q^3+2q^2+i_0q+\frac{q}{2}}X^{2q^3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) = ev_L\left(\frac{X^{3q^3+2q^2+i_0q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}.$$

Note that

$$ev_L\left(\frac{X^{6q^2+2q+2i_0+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)} = ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}}{\mathbf{Tr}_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$$

$$= ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}\mathbf{Tr}_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right).$$

Note that $ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}X^{q^3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$,$ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}X^{q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ and $ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}X}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ are in $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$.

Since $ev_L\left(\frac{X^{6q^2+2q+2i_0+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$, then both $ev_L\left(\frac{X^{3q^3+q^2+i_0q+\frac{q}{2}}X^{q^2}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$, $ev_L\left(X^{2q^2+4q+2i_0+1}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$.

Therefore $ev_L(X^{2q^2+4q+2i_0+1}) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ □

Now we extend the proof to powers of the form $ev_L(X^{2q^2+5q+i})$.

Lemma 18 *Let $q = 2^s$ where $s \geq 3$.*

$$ev_L\left(X^{2q^2+5q+i}\right)^{\left(\frac{q}{2}\right)} \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp} \text{ where } 0 \leq i \leq q-1.$$

Proof The proof is almost identical to the proof of Lemma 17. The key differences are as follows. Assuming i is odd, because the coefficient of q of the power of X is 5 instead of 4, we obtain $ev_L\left(X^{2q^2+5q+i}\right)^{\left(\frac{q}{2}\right)} = ev_L\left(X^{q^3+2q^2+(i_0+\frac{q}{2})q+\frac{q}{2}}\right)$ instead. Note $i_0 + \frac{q}{2} < q$. After considering $ev_L\left(X^{2q^2+5q+i}\right)^{\left(\frac{q}{2}\right)}$ every logical step of Lemma 17 also holds for $i_0 + \frac{q}{2}$ instead of i_0. We also take $ev_L\left(\frac{X^{6q^2+3q+2i_0+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)}$ instead of $ev_L\left(\frac{X^{6q^2+2q+2i_0+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)}$. □

We finish this section finding additional consecutive powers and improving the bound on $d(C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)$.

Corollary 19 *The minimum distance of $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)$ is at least $2q^3+2q^2+6q+8$.*

Proof Lemma 9, Lemma 17 and Lemma 18 imply that

$$ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp} \text{ for } 0 \leq i \leq 2q^3+2q^2+5q+q-1.$$

Because of Lemma 9 and because $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ is closed under 2–powers we only need to establish that $ev_L\left(\frac{X^{2q^3+2q^2+6q+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$,$ev_L\left(\frac{X^{2q^3+2q^2+6q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ and $ev_L\left(\frac{X^{2q^3+2q^2+6q+5}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ are in the code $C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$.

The parity check equation $ev_L\left(\frac{X^{2q^3+2q^2+6q+1}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ because the constant coefficient is 1 and $q^3(2q^3+2q^2+6q+1) \mod q^4-1 < 2q^3$.

The parity check equation $ev_L\left(\frac{X^{2q^3+2q^2+6q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L, \mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ because $ev_L(X^{2q^2+6q+3})^{\frac{q}{2}} = ev_L(X^{q^3+3q^2+q+\frac{q}{2}})$. Since the exponent $q^3+3q^2+q+\frac{q}{2}$ has

two coefficients equal to one, the terms of $ev_L\left(\frac{X^{q^3+3q^2+q+\frac{q}{2}}\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right)$ are all in $C\left(L,\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$. Using the same technique as in Lemma 17 the parity check equation $ev_L\left(\frac{X^{2q^3+2q^2+6q+5}}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L,\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)^{\perp}$ because

$$ev_L\left(X^{2q^2+6q+5}\right)^{\frac{q}{2}} = ev_L\left(X^{q^3+3q^2+2q+\frac{q}{2}}\right)$$

and

$$ev_L\left(\frac{X^{3q^3+3q^2+2q+\frac{q}{2}}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right) =$$

$$ev_L\left(\frac{X^{6q^2+6q+3}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)^{\left(\frac{q}{2}\right)} + \sum_{r\in\{0,1,3\}} ev_L\left(\frac{X^{3q^3+3q^2+q+\frac{q}{2}}X^{q^r}}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$$

are both in $C\left(L,\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)$. Since $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}}\right) \in C\left(L,\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)$ for $0 \le i \le 2q^3+2q^2+6q+7$ it follows that

$$d\left(C\left(L,\mathbf{Tr}^2_{\mathbb{F}_{q^4}\setminus\mathbb{F}_q}\right)\right) \ge 2q^3+2q^2+6q+8.$$

□

6 Conclusion

We improved the minimum distance bound of Trace Goppa codes $C(L,\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q})$ using the fact that $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ takes values over the subfield $\mathbb{F}_q$. This improves the minimum distance bound of the Trace Goppa code is significantly from $q^{m-1}+1$ to $q^{m-1}+q^{m-2}+\cdots+q+1$.

In the binary case, we found additional consecutive parity check equations of the form $ev_L\left(\frac{X^i}{\mathbf{Tr}^2_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}}\right)$. These additional equations improve the minimum distance bound from $2q^{m-1}+2$ to $2\frac{q^m-1}{q-1}+\frac{q^{m-2}-1}{q-1}+2$. For binary Trace Goppa codes with $m=3$ and $m=4$ we have further improved the minimum distance bound by finding additional consecutive parity check equations. For $m=3$, the distance bound increases from $2q^2+2q+4$ to $2q^2+2q+8$. For $m=4$, the distance bound increases from $2q^3+2q^2+4q+6$ to $2q^3+2q^2+6q+8$. If $m\ge 5$ then Lemma 12 can be applied further to increase the distance bound.

Our results imply that Trace Goppa codes can provide better distance bounds compared to the binary code obtained from puncturing and shortening the corresponding BCH codes in some cases. For example, the Trace Goppa code over $\mathbb{F}_{512}$ is a binary $[448,58,152]$ code which is better than any code obtained from puncturing or shortening BCH codes of length 511. As proven in [9] the Trace Goppa code over $\mathbb{F}_{256}$, $C(L,x^{16}+x)$ is the best known $[240,123,36]$ binary code. Thus for Trace Goppa codes and related Alternant codes using the trace function $\mathbf{Tr}_{\mathbb{F}_{q^m}\setminus\mathbb{F}_q}$ and its quasi–cyclic structure may

improve the minimum distance and decoding algorithms of BCH codes of larger lengths, perhaps over $\mathbb{F}_{2^{14}}$, $\mathbb{F}_{2^{15}}$ or $\mathbb{F}_{2^{16}}$.

Acknowledgements

The authors would like to thank the anonymous reviewers, whose input and insight have improved this article.

References

[1] V. D. Goppa, "A new class of linear error-correcting codes", Probl. Peredach. Inform., vol. 6, no. 3, pp. 24-30, Sept. 1970.

[2] E. Berlekamp, "Goppa codes," in IEEE Transactions on Information Theory, vol. 19, no. 5, pp. 590-592, September 1973, doi: 10.1109/TIT.1973.1055088.

[3] P. Veron, "Goppa codes and trace operator," in IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 290-294, Jan. 1998, doi: 10.1109/18.65104

[4] P. Véron, True Dimension of Some Binary Quadratic Trace Goppa Codes. Designs, Codes and Cryptography 24, 81–97 (2001). https://doi.org/10.1023/A:1011281431366

[5] P. Véron, Proof of Conjectures on the True Dimension of Some Binary Goppa Codes. Des Codes Crypt 36, 317–325 (2005). https://doi.org/10.1007/s10623-004-1722-4

[6] A. Couvreur, A. Otmani, J-P. Tillich, 'New identities relating wild Goppa codes" in Finite Fields and Their Applications, Volume 29, 2014, Pages 178-197, ISSN 1071-5797, https://doi.org/10.1016/j.ffa.2014.04.007.

[7] A. Canteaut and F. Chabaud, "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511," in IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 367-378, Jan. 1998, doi: 10.1109/18.651067.

[8] M. Loeloeian and J. Conan, "A [55,16,19] binary Goppa code (Corresp.)," in IEEE Transactions on Information Theory, vol. 30, no. 5, pp. 773-773, September 1984, doi: 10.1109/TIT.1984.1056946.

[9] S. Bezzateev and N.A. Shekhunova, "Chain of Separable Binary Goppa Codes and Their Minimal Distance" in IEEE Transactions on Information Theory vol 54, pp 5773 - 5778. doi: 10.1109/TIT.2008.2006442.

[10] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa, "Further results on Goppa codes and their applications to constructing efficient binary codes," in IEEE Transactions on Information Theory, vol. 22, no. 5, pp. 518-526, September 1976, doi: 10.1109/TIT.1976.1055610.

[11] M. Grassl,"Bounds on the minimum distance of linear codes and quantum codes." Online available at http://www.codetables.de. Accessed on 2023-03-15.