Chain of Separable Binary Goppa Codes and their Minimal Distance

Sergey Bezzateev and Natalia Shekhunova

Abstract—It is shown that subclasses of separable binary Goppa codes, \( \Gamma(L, G) \)-codes, with \( L = \{ \alpha \in GF(2^l): G(\alpha) \neq 0 \} \) and special Goppa polynomials \( G(x) \) can be presented as a chain of embedded codes. The true minimal distance has been obtained for all codes of the chain.

Index Terms—Goppa codes, quasi-cyclic Goppa codes, minimal distance of separable binary codes.

I. INTRODUCTION

Any \( q \)-ary Goppa code \( \Gamma(L, G) \)-code can be defined by two objects: Goppa polynomial \( G(x) \) where \( G(x) \) is a polynomial of a degree \( t \) over \( GF(q^m) \) and location set \( L \) where \( L = \{ \alpha \in GF(q^m): G(\alpha) \neq 0 \} \).

Definition 1: A \( q \)-ary vector \( a = (a_1, \ldots , a_n) \) of a length \( n \) where \( n \) is a cardinality of the set \( L = \{ \alpha_1, \ldots , \alpha_n \}, \alpha_i \in GF(q^m) \) is a codeword of the \( \Gamma(L, G) \) Goppa code if and only if the following equation is satisfied:

\[
\sum_{i=1}^{n} a_i \frac{1}{G(\alpha_i)} \equiv 0 \mod G(x).
\]

The parity check matrix of the \( \Gamma(L, G) \)-code can be presented in the following form:

\[
H = \begin{bmatrix}
\frac{1}{G(\alpha_1)} & \cdots & \frac{1}{G(\alpha_n)} \\
\alpha_1^{-1} & \cdots & \alpha_n^{-1}
\end{bmatrix}.
\]

It is known that the \( \Gamma(L, G) \)-code has following parameters [1]:
- the length of the code is equal to the cardinality \( n \) of the location set \( L \), \( n \leq q^m \)
- the dimension is \( k \geq n - tn \)
- the true minimal distance is \( d \geq t + 1 \)

The \( \Gamma(L, G) \)-code is a binary Goppa code if \( q = 2 \).

The \( \Gamma(G, L) \)-code is a separable Goppa code if all roots of its Goppa polynomial \( G \) are different.

The following estimation of the true minimal distance for binary separable \( (L,G) \)-codes is valid [1]:

\[
d \geq 2t + 1.
\]

Binary separable Goppa codes have been studied by many authors. The binary separable codes with the location set over \( GF(2^{2l}) \) where \( s = 2, 3, \ldots \) are of the greatest interest.

M. Loeloeian and J. Conan were the first who considered the code of this class. In 1984 they presented [2] the best known \((55,16,19)\)-Goppa code with the Goppa polynomial:

\[
G(x) = (x - \alpha^9)(x - \alpha^{12})(x - \alpha^{30})(x - \alpha^{34})(x - \alpha^{43})(x - \alpha^{50})(x - \alpha^{54})
\]

where \( \alpha \) is a primitive element of \( GF(2^6) \).

In 1986 we considered [3] this code as a code from a subclass of Goppa codes with the Goppa polynomial:

\[
G(x) = x^{t+1} + V_t x^t + V x + 1
\]

where \( V \in GF(2^l) \), \( t = 2^l \), \( L \subset GF(2^{2l}) \) and \( n = 2^{2l} - t - 1 \).

We have proved [3], [4] that the dimension of these codes is

\[
k \geq n - 2(t - \frac{t}{3} - 1).
\]

The same estimation for the dimension of these codes was obtained by A.M. Roseiro, J.I. Hall, J.E. Adney and M. Siegel in [6] by using the kernel of an associated trace map. In this paper, the subclass of codes with polynomial \( G(x) = x^t + x \) was called as quadratic trace Goppa codes.

In 1995 we described [7] the subclass of Goppa codes with the polynomial \( G(x) = x^{t-1} + 1 \) and we have proved that the minimal distance of these codes is equal to their design distance.

In 2001 P. Veron [8] investigated the structure of trace Goppa codes and proved that the true dimension for these codes is equal to the estimation obtained previously:

\[
k \geq n - 2(t - \frac{t}{3} - 1)
\]

In 2005 P. Veron [9] proved that the estimation of the code dimension for Goppa codes with \( G(x) = x^{t+1} + V_t x^t + V x + 1 \) and \( G(x) = x^{t-1} + 1 \) is the true dimension for the codes from this subclasses [10].

In [11] and also in [12] (G. Bonmer and F. Blanchet) and in [13] (P. Veron) it was proved that all the mentioned above codes are a quasi-cyclic binary Goppa codes.

In 2007 G. Maatouk, A. Shokrollahi and M. Cheraghchi [14] tried to prove that the class of codes which was described in [7] achieved the GV bound.

In this paper, we present all codes that were mentioned above as a chain of embedded codes. We obtain the true minimal distance for these codes. The rest of the paper is organized as follows.

Section 2 describes the chain of Goppa codes subclasses.

Section 3 gives several Lemmas for the true minimal distance for subfield subcodes:

\[
G_5(x) = C x^{t+1} + A^t x^t + Ax,
\]

S. Bezzateev and N. Shekhunova are with the Department of Information Systems and Security, Saint Petersburg State University of Airspace Instrumentation, Saint-Petersburg, Russia, e-mail: bsv@aanet.ru, sn@defa.net
$G_6(x) = R x^{t+1} + V^t x^t + V x + 1$
where $R \in GF(2^l), V \in GF(2^l)$ and $G_7(x) = x^{t+1} + 1$.

In Section 4 similar Lemmas are presented for quadratic trace Goppa codes:
$G_2(x) = A^t x^t + A x$ and
$G_3(x) = A^t x^t + A x + C$,
where $A \in GF(2^l)$ and $C \in GF(2^l)$.

In Section 5 we obtain the true minimal distance for codes that are not subfield or trace codes; these new codes with a Goppa polynomial
$G_4(x) = A^t x^t + A^{-1} x^{-1} + 1$

have not been described before.

In Conclusion a table with parameters of codes from the code chain and table of binary quasi-cyclic codes from this chain are presented.

II. CODE CHAIN

Let us show how to obtain one code from another and to create a family of embedded codes, a so-called chain of codes.

**Definition 2:** Let matrix $H_1^*$ be a parity check matrix of the binary Goppa code with a location set $L_1^* = \{ \alpha_1, \alpha_2, ..., \alpha_n \}$ of different nonzero elements from $GF(2^l)$ such that $\alpha_i^{-1} \neq 1$ for all $j = 1, ..., n$ and Goppa polynomial $G_1(x) = x^{t-1} + 1, t = 2^l$.

$$H_1^* = \begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_{i1}} & \cdots & \frac{1}{\alpha_{in}}
\frac{\alpha_1^{t-1}+1}{\alpha_{i1}^{t-1}+1} & \frac{\alpha_{i1}^{t-1}+1}{\alpha_{i2}^{t-1}+1} & \cdots & \frac{\alpha_{in}^{t-1}+1}{\alpha_{in}^{t-1}+1}
\end{bmatrix}.$$

**Lemma 1:** A row \[ \frac{1}{\alpha_1} \ldots \frac{1}{\alpha_n} \] can be represented as a linear combination of corresponding rows from the matrix $H_1^*$.

**Proof:**
For any $\alpha \in L_1^*$
$$\frac{1}{\alpha^{t-1}+1} = \frac{1}{\alpha^{t-1}(1+1)} = \frac{1}{\alpha^{t-1}(\alpha^{-1}+1)} = \frac{1}{\alpha^{t-1}(\alpha^{-1}+1)\alpha^{t-1}(\alpha^{-1}+1)} = \frac{1}{\alpha^{t-1}(\alpha^{-1}+1)^2}.$$ 
Therefore the row \[ \frac{1}{\alpha_1^{t-1}+1} \ldots \frac{1}{\alpha_{in}^{t-1}+1} \] can be obtained from the row \[ \frac{\alpha_1^{t-1}}{\alpha_{i1}} \ldots \frac{\alpha_{in}^{t-1}}{\alpha_{in}} \] of the matrix $H_1^*$.

For any $\alpha \in L_1^*$
$$\frac{1}{\alpha^{t-1}+1} = \frac{1}{\alpha^{t-1}+1} \frac{1}{\alpha^{t-1}+1} = \frac{1}{\alpha^{t-1}(\alpha^{-1}+1)}.$$ 
Therefore the row \[ \frac{\alpha_1^{t-1}}{\alpha_{i1}} \ldots \frac{\alpha_{in}^{t-1}}{\alpha_{in}} \] can be obtained from the row \[ \frac{1}{\alpha_1^{t-1}+1} \ldots \frac{1}{\alpha_{in}^{t-1}+1} \] of the matrix $H_1^*$.

**Corollary 1:** By using the result of **Lemma 1** we can rewrite the matrix $H_1^*$ in the following form:

$$H_1^* = \begin{bmatrix}
\frac{1}{\alpha_1} & \alpha_1 & \cdots & \alpha_n
\frac{\alpha_1^{t-1}+1}{\alpha_1^{t-1}+1} & \frac{\alpha_1^{t-1}+1}{\alpha_2^{t-1}+1} & \cdots & \frac{\alpha_1^{t-1}+1}{\alpha_{in}^{t-1}+1}
\end{bmatrix}.$$

Now let us obtain the parity check matrix $H_1$ for a code $\Gamma(L_1, G_1)$ with $G_1(x) = x^{t-1} + 1, t = 2^l$ and $L_1 = \{ \alpha_1, \alpha_2, ..., \alpha_{n-1}, 0 \}$, $n_1 = 2^l - 2^l + 1$.

$$H_1 = \begin{bmatrix}
\frac{1}{\alpha_1} & \alpha_1 & \cdots & \alpha_n
\frac{\alpha_1^{t-1}+1}{\alpha_1^{t-1}+1} & \frac{\alpha_1^{t-1}+1}{\alpha_2^{t-1}+1} & \cdots & \frac{\alpha_1^{t-1}+1}{\alpha_{n-1}^{t-1}+1}
\end{bmatrix} = \begin{bmatrix}
1 & 1 & \cdots & 1
0 & 0 & \cdots & 0
\end{bmatrix}.$$

By using the power $2^l$ of the first row from $H_1$ we obtain:

$$\begin{bmatrix}
\frac{1}{\alpha_1^{t-1}+1} & \alpha_1^{t-1} & \cdots & \alpha_{n-1}^{t-1} + 1
\end{bmatrix}.$$

The sum of this row and the first row from the matrix $H_1$ gives us

$$\begin{bmatrix}
\frac{1}{\alpha_1^{t-1}+1} & \alpha_1^{t-1} & \cdots & \alpha_{n-1}^{t-1} + 1
\end{bmatrix} + \begin{bmatrix}
1 & 1 & \cdots & 1
0 & 0 & \cdots & 0
\end{bmatrix}.$$

Therefore the parity check matrix $H_1$ can be rewritten:

$$H_1 = \begin{bmatrix}
\frac{1}{\alpha_1^{t-1}+1} & \alpha_1^{t-1} & \cdots & \alpha_{n-1}^{t-1} + 1
\end{bmatrix}.$$

Let us define a parity check matrix for a subcode $\Gamma(L_1^*, G_1)$ of the code $\Gamma(L_1, G_1)$, $L_1^* = L_1 \setminus (0) = \{ \alpha_1, \alpha_2, ..., \alpha_{n-1} \}$, $n_1^* = n_1 - 1$.

$$H_1^* = \begin{bmatrix}
\frac{1}{\alpha_1^{t-1}+1} & \alpha_1^{t-1} & \cdots & \alpha_{n-1}^{t-1} + 1
\end{bmatrix}.$$

**Lemma 2:** $\Gamma(L_1^*, G_1) \equiv \Gamma(L_2, G_2)$ where $G_1(x) = x^{t-1} + 1$ and $G_2(x) = A^t x^t + A x$, $t = 2^l, A \in GF(2^l)$.

**Proof:**
Obviously, $\Gamma(L_1, G_2) \equiv \Gamma(L_2, G_2)$ where $G_2(x) = x^t + x = x \ast G_1(x)$ and the Goppa polynomial $G_2(x) = A^t x^t + A x$ can be obtained from $G_1(x)$ by using the $A x$ substitution for a variable $x, A \in GF(2^l)$.

A parity check matrix $H_2$ for the code $\Gamma(L_2, G_2^*)$ with $G_2^*(x) = x^t + x, t = 2^l$ and $L_2 = \{ \alpha_1, \alpha_2, ..., \alpha_{n_2} \}, n_2 = 2^l - 2^l$ is:
It is easy to see that this matrix can be rewritten in the following form:

$$H_2 = \begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \cdots & \frac{1}{\alpha_{n_2}}
\alpha_1^{-1} + 1 & \alpha_2^{-1} + 1 & \cdots & \alpha_{n_2}^{-1} + 1
\end{bmatrix}.$$ 

From Corollary 1, the matrix $H_2$ is equal to the matrix $H_1^*$, therefore $\Gamma(L_1^*, G_1) \equiv \Gamma(L_2^*, G_2^*) \equiv \Gamma(L_2, G_2)$. (This statement has been proved by P. Veron in [13], [9] by using another approach.)

Lemma 3: $\Gamma(L_2, G_2) \equiv \Gamma(L_3, G_3)$ where $G_3(x) = A^t x^t + A x + C$, $C \in GF(2^t)$ and $A \in GF(2^l)$.

Proof: Using the $x + \beta$ substitution for a variable $x$ where $\beta \in GF(2^l)$ and $\beta \neq A^{-(t-1)}$ we obtain:

$$G_2(x + \beta) = A^t (x + \beta)^t + A(x + \beta) = A^t x^t + A x + (A^t \beta^t + A \beta),$$

where $(A^t \beta^t + A \beta)^t =$ $(A \beta + A^t \beta^t)$ follows from the conditions of Lemma 3. Therefore, $C = A^t \beta^t + A \beta$, $C \in GF(2^t)$ and $G_2(x + \beta) = A^t x^t + A x + C = G_3(x)$. 

Lemma 4: All codewords of the code $\Gamma(L_4, G_4)$ with $G_4(x) = A^t x^t + A^t x^t - 1 + 1$ have the zero value on the position corresponding to the element $0$ from $L_4 = \{\alpha_1, \alpha_2, \ldots, \alpha_{n_4-1}, 0\}$.

Proof: Obviously, by substituting $x$ to $A^{-1} x$ in $G_4(x)$ we obtain the same $\Gamma(L_4, G_4)$ code with a more simple Goppa polynomial: $G_4(x) = x^t + x^t - 1 + 1$.

Let us consider the parity check matrix of this code:

$$H_4 = \begin{bmatrix}
\frac{1}{\alpha_1} + 1 & \frac{1}{\alpha_2} + 1 & \cdots & \frac{1}{\alpha_{n_4-1} + 1} & 0
\alpha_1^{-1} + 1 & \alpha_2^{-1} + 1 & \cdots & \alpha_{n_4-1}^{-1} + 1 & 0
\end{bmatrix}.$$ 

By using the $i$-th degree of the first row of this parity check matrix we can obtain the following parity check row for $\Gamma(L_4, G_4)$:

$$r = \begin{bmatrix}
\alpha_1^{-1} + 1 & \alpha_2^{-1} + 1 & \cdots & \alpha_{n_4-1}^{-1} + 1 & 1
\end{bmatrix}.$$ 

For this row and for the last row of the parity check matrix $H_4$ and parity check row $r$ for any codeword $a = (a_1 \ldots a_{n_4})$ of the code $\Gamma(L_4, G_4)$ the following expressions are valid:

$$\sum_{i=1}^{n_4-1} a_i \alpha_i^{-1} + 1 = 0 \quad \sum_{i=1}^{n_4-1} a_i \alpha_i^{-1} + 1 = a_{n_4}.$$ 

It is possible only in case when $a_{n_4} = 0$ for all codewords of the code $\Gamma(L_4, G_4)$.

Corollary 2: The code $\Gamma(L_4, G_4)$ is equal to the code $\Gamma(L_4^*, G_4^*)$ with $n_4^* = n_4 - 1$, $k_4^* = k_4$ and $L_4^* = \{\alpha_1, \alpha_2, \ldots, \alpha_{n_4-1}\}$.

The parity check matrix $H_4^*$ of the code $\Gamma(L_4^*, G_4^*)$ is:

$$H_4^* = \begin{bmatrix}
\frac{1}{\alpha_1} + 1 & \frac{1}{\alpha_2} + 1 & \cdots & \frac{1}{\alpha_{n_4-1} + 1} & 1
\alpha_1^{-1} + 1 & \alpha_2^{-1} + 1 & \cdots & \alpha_{n_4-1}^{-1} + 1 & 1
\end{bmatrix}.$$ 

Lemma 5: A row

$$\begin{bmatrix}
\alpha_1(x_1 + \alpha_1^{-1} + 1) & \alpha_2(x_2 + \alpha_2^{-1} + 1) & \cdots & \alpha_{n_4}(x_{n_4} + \alpha_{n_4}^{-1} + 1)
\end{bmatrix}$$ 

can be represented as a linear combination of the corresponding rows from the matrix $H_4^*$.

Proof: For any $\alpha \in L_4^*$

$$\frac{1}{\alpha^2 + \alpha^{-1} + 1} = \frac{1}{\alpha^2 + \alpha^{-1} + 1} + \frac{1}{\alpha \alpha^2 + \alpha^{-1} + 1}. \quad \frac{1}{\alpha^2 + \alpha^{-1} + 1} = \frac{1}{\alpha^2 + \alpha^{-1} + 1} + \frac{1}{\alpha \alpha^2 + \alpha^{-1} + 1}.$$ 

Therefore a row

$$\begin{bmatrix}
\frac{1}{\alpha_1(x_1 + \alpha_1^{-1} + 1)} & \frac{1}{\alpha_2(x_2 + \alpha_2^{-1} + 1)} & \cdots & \frac{1}{\alpha_{n_4}(x_{n_4} + \alpha_{n_4}^{-1} + 1)}
\end{bmatrix}$$ 

can be obtained from the row

$$\begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \cdots & \frac{1}{\alpha_{n_4}}
\alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{n_4}^{-1}
\end{bmatrix}.$$ 

Lemma 5: A row

$$\begin{bmatrix}
\alpha_1(x_1 + \alpha_1^{-1} + 1) & \alpha_2(x_2 + \alpha_2^{-1} + 1) & \cdots & \alpha_{n_4}(x_{n_4} + \alpha_{n_4}^{-1} + 1)
\end{bmatrix}$$ 

can be represented as a linear combination of the corresponding rows from the matrix $H_4^*$.

Proof: For any $\alpha \in L_4^*$

$$\frac{1}{\alpha^2 + \alpha^{-1} + 1} = \frac{1}{\alpha^2 + \alpha^{-1} + 1} + \frac{1}{\alpha \alpha^2 + \alpha^{-1} + 1}. \quad \frac{1}{\alpha^2 + \alpha^{-1} + 1} = \frac{1}{\alpha^2 + \alpha^{-1} + 1} + \frac{1}{\alpha \alpha^2 + \alpha^{-1} + 1}.$$ 

Therefore a row

$$\begin{bmatrix}
\frac{1}{\alpha_1(x_1 + \alpha_1^{-1} + 1)} & \frac{1}{\alpha_2(x_2 + \alpha_2^{-1} + 1)} & \cdots & \frac{1}{\alpha_{n_4}(x_{n_4} + \alpha_{n_4}^{-1} + 1)}
\end{bmatrix}$$ 

can be obtained from the row

$$\begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \cdots & \frac{1}{\alpha_{n_4}}
\alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{n_4}^{-1}
\end{bmatrix}.$$ 

Corollary 3: By using the result of Lemma 5 we can rewrite matrix $H_4^*$ in the following form:

$$H_4^* = \begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \cdots & \frac{1}{\alpha_{n_4}}
\alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{n_4}^{-1}
\alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{n_4}^{-1}
\end{bmatrix}.$$ 

Now consider a code $\Gamma(L_3, G_3)$ with $G_3(x) = A^t x^t + A x + C$, $t = 2^l$ and $L_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_{n_3-1}\}$, $n_3 = 2^l - 2$. Obviously, by substituting $x$ to $A^{-1} C x$ in $G_3(x)$ we obtain the same $\Gamma(L_3, G_3)$ code with a more simple Goppa polynomial $G_3(x) = x^t + x + 1$. The parity check matrix for this code is:

$$H_5 = \begin{bmatrix}
\frac{1}{\alpha_1} & \frac{1}{\alpha_2} & \cdots & \frac{1}{\alpha_{n_3}}
\alpha_1^{-1} & \alpha_2^{-1} & \cdots & \alpha_{n_3}^{-1}
\end{bmatrix}.$$
Definition 3: Let us define a subcode $\Gamma(L_3, G_3)$ of the code $\Gamma(L_3, G_3)$ as shortened by a position corresponding to the element 0 from $L_3 = \{0, 1, 2, \ldots, n_3-1, 0\}$. Hence $\Gamma(L_3, G_3) \subset \Gamma(L_3, G_3)$ and $n_3 = n_3 - 1$, $k_3 = k_3 - 1$ and $L_3^* = L_3 \setminus \{0\}$.

Lemma 6: $\Gamma(L_3^*, G_3^*) \subset \Gamma(L_4, G_4)$ where $G_4(x) = A^t x^t + A^{t-1} x^{t-1} + 1$, $A \in GF(2^t)$.

Proof:

It follows directly from the above presentation of the matrix $H_3^*$. ■

Corollary 4:

$$
\begin{bmatrix}
1 & 1 & \ldots & 1 \\
1 & \ldots & 1 & 1
\end{bmatrix}
= \begin{bmatrix}
H_4^* & 0 \\
0 & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & \ddots \\
0 & \ddots & \ddots & \ddots
\end{bmatrix}
$$

Proof:

It follows directly from Lemma 3 where we have proved the equivalence of two codes: $\Gamma(L_2, G_2)$ and $\Gamma(L_3, G_3)$.

Lemma 7: $\Gamma(L_4, G_4) \equiv \Gamma(L_5, G_5)$ where $G_5(x) = C x^{t+1} + A^t x^t + A x$, $C \in GF(2^t)$, and $A \in GF(2^t)$.

Proof:

It is easy to show that $G_5(x) = x G_4(x)$ and $L_5 = L_4 \setminus \{0\}$. Obviously, by substituting $x$ to $A^{-1} C x$ in $G_5(x)$ we obtain the same $\Gamma(L_5, G_5^*)$ code with a more simple $G_5^*(x) = x^{t+1} + x^t + x$.

The parity-check matrix for this code is:

$$
H_5 = \begin{bmatrix}
1 & 1 & \ldots & 1 & 1 \\
1 & \ldots & 1 & 1 & 1 \\
1 & \ldots & 1 & 1 & 1 \\
1 & \ldots & 1 & 1 & 1
\end{bmatrix}
$$

Therefore $H_5 = H_4^*$ according to Corollary 2. ■

Lemma 8: $\Gamma(L_5, G_5) \equiv \Gamma(L_6, G_6)$ where $G_6(x) = R x^{t+1} + V_1 x^t + V x + 1$, $R \in GF(2^t)$, and $V \in GF(2^t)$.

Proof:

Using the $x + \beta$ substitution for a variable $x$ we obtain:

$$
G_5(x + \beta) = C x^{t+1} + (A^t + A C \beta) x^t + (A + C \beta) x + (C^{t+1} + A^t x^t + A x) \beta
$$

where $\beta : \beta \in GF(2^t)$ and $\beta \neq \frac{1}{A}$. Notice that $(A + C \beta^t) = (A^t + C \beta)^t$ and $(C^{t+1} + A^t x^t + A x) \beta = C^{t+1} + A \beta + A^t \beta$. Therefore

$$
G_6(x) = \frac{1}{C} \left( C x^{t+1} + A^t x^t + A x \right) \beta
$$

where $R = \frac{C (C^{t+1} + A^t x^t + A x)}{(C^{t+1} + A^t x^t + A x) \beta}$ and $V = \frac{(C^{t+1} + A^t x^t + A x) \beta}{(C^{t+1} + A^t x^t + A x) \beta}$. This means that $\Gamma(L_6, G_6) \equiv \Gamma(L_6, G_6)$.

Lemma 9: $\Gamma(L_6, G_6) \equiv \Gamma(L_7, G_7)$ where $G_7(x) = B x^{t+1} + 1$, $B = \alpha^{t-1}$, and $\alpha$ is a primitive element of $GF(2^t)$.

Proof:

It can be proved in the same way as the previous Lemma by using the $x + \beta$ substitution for a variable $x$ where $\beta = \frac{V}{R}$.

In Figure 1 we present the structure of the code chain. It is possible to define the similar code chain for the codes described in paper [15].
III. MINIMAL DISTANCE OF SUBFIELD SUBCODES

Lemma 10: The minimal distance of the last Goppa code in the chain $\Gamma (L_7, G_7)$ exactly equals to its design distance, i.e. $d = 2(t + 1) + 1$.

Proof:
It is easy to show that a polynomial $x^{2^l+1} - 1$ can be presented as a product $\prod_{i=1}^{2^l+1} (x - \alpha_i^{(2^l+1)})$ where $\alpha$ is a primitive element of $GF(2^{2l})$. Choose some element $A$ from $GF(2^l)$ such that $A^{2^l+1} \neq 1$ and let $B = A^{-1}$. Thus we can calculate two polynomials with all different roots $\{A\alpha_i^{(2^l+1)}\}$ and $\{B\alpha_i^{(2^l+1)}\}$ $i = 1,..,2^l+1$.

\[
x^{2^l+1} - A^{2^l+1} = \prod_{i=1}^{2^l+1} (x - A\alpha_i^{(2^l+1)}),
\]

\[
x^{2^l+1} - B^{2^l+1} = \prod_{i=1}^{2^l+1} (x - B\alpha_i^{(2^l+1)}).
\]

The result of the multiplication of these two polynomials and $x$ :

\[
x(x^{2^l+1} - A^{2^l+1})(x^{2^l+1} - B^{2^l+1}) = x^{2^l+3} - (A^{2^l+1} + B^{2^l+1})x^{2^l+2} - x.
\]

A formal derivative of result of this multiplication:

\[
x^{2^l+2} - 1.
\]

Now consider a binary vector $a = (a_0a_1...a_n)$ with nonzero elements on and only on positions $\beta_j$, $(j = 1,..,(2^l+1))$ from the following subset of $L$:

\[
\{A\alpha_i^{(2^l+1)}\}, i = 1,..,2^l+1 \cup \{B\alpha_i^{(2^l+1)}\}, i = 1,..,2^l+1 \cup \{0\}.
\]

From the definition of the Goppa code, this vector will be a codeword of $\Gamma (L_7, G_7)$ :

\[
\sum_{j=1}^{2^l+3} a_i x^{2^l+3}(A\alpha_i^{(2^l+1)} + B\alpha_i^{(2^l+1)}) = 0
\]

where $\beta_j \in \{A\alpha_i^{(2^l+1)}\}, i = 1,..,2^l+1 \cup \{B\alpha_i^{(2^l+1)}\}, i = 1,..,2^l+1 \cup \{0\}$.

Therefore the minimal distance of the Goppa code $\Gamma (L_7, G_7)$ is equal to the design distance $2^l+1 + 3$.

Corollary 5: The minimal distance of the equivalent Goppa codes $\Gamma (L_6, G_6)$ and $\Gamma (L_5, G_5)$ is exactly equal to its design distance, i.e. $d = 2(t + 1) + 1$.

IV. MINIMAL DISTANCE OF QUADRATIC TRACE SUBCODES

Lemma 11: The minimal distance of the equivalent Goppa codes $\Gamma (L_2, G_2)$ and $\Gamma (L_3, G_3)$ is exactly equal to the minimal even weight of a codeword of the code $\Gamma (L_5, G_5) \equiv \Gamma (L_6, G_6) \equiv \Gamma (L_7, G_7)$, i.e. $d \geq 2(t + 1) + 2$.

Proof:
It follows directly from the parity check matrices $H_3, H_2$ and $H_5$.

It is necessary to note that P Veron in [13] has proved that the Hamming weight of all codewords of these codes is even.

V. MINIMAL DISTANCE OF THE NEW CODE

Lemma 12: The minimal distance of the $\Gamma (L_4, G_4)$ and $\Gamma (L_6, G_4)$ Goppa codes is exactly equal to its design distance, i.e. $d = 2(t + 1) + 1$.

Proof: It follows directly from the equivalence of codes $\Gamma (L_4, G_4)$ and $\Gamma (L_6, G_5)$ (Lemma 7).

VI. CONCLUSION

Parameters of the codes forming a chain are presented in Table 1.

In Table 2 we present the quasi-cyclic Goppa codes from our chain. It is easy to see that by substituting $x$ by $\beta x + \gamma$ we will obtain the same code if the Goppa polynomial is invariant to this substitution: $\alpha G(x) = G(\beta x + \gamma)$ where $\alpha, \beta, \gamma \in GF(2^d)$.

In Table 2 we present such values of $\gamma$ and $\beta$ for the Goppa codes from our chain.

Therefore these quasi-cyclic codes have indexes $2^l - 1$ and $2^l + 1$.

REFERENCES

[1] V. D. Goppa, A new class of linear error correcting codes. Probl. Inform. Transm., Vol. 6, No. 3 , pp. 24-30, 1970
[2] M.Loeleian and J.Conan, A (55,16,19) binary code IEEE Trans. on Information Theory, vol. 30, p.773, 1984.
[3] S. V. Bezzateev, E. T. Mironchikov and N. A. Shekhunova, One subclass of binary Goppa codes, Proc. XI Simp. Po Probl. Izbit. v Inform. Syst. pp. 140-141, 1986.
[4] S.N. Bezzateev and N.A. Shekhunova, On the designed distance of the best known (55,16,19) Goppa code. Probl.Inform.Transm., vol. 23, No 4, p.352, 1987.
Table 1 Parameters of the code chain

| Code chain | Parity check matrix | Code length | Number of information symbols | Minimal distance |
|------------|---------------------|-------------|-------------------------------|------------------|
| $\Gamma(L_1, G_1)$, where $G_1(x) = x^{t-1} + 1$ | $H_1$ | $n_1 = 2^t - t + 1$ | $k_1 = 2^t - t - 2l(t - \frac{3}{2})$ | $d_1 = 2t - 1$ |
| $\Gamma(L_1^*, G_1^*)$ | $H_1^*$ | $n_1^* = 2^t - t$ | $k_1^* = k_1 - 1$ | $d_1^*$ |
| $\Gamma(L_2, G_2)$, where $G_2(x) = A^t x^t + Ax$ | $H_1^*$ | $n_2 = 2^t - t$ | $k_2 = k_1 - 1$ (Lemma 2) | $d_2 = d_1^*$ |
| $\Gamma(L_3, G_3)$, where $G_3(x) = A^t x^t + Ax + C$ | $H_1^* \begin{bmatrix} 0 \\ 1^{t-1} \end{bmatrix}$ | $n_3 = 2^t - t$ | $k_3 = k_2$ (Lemma 3) | $d_3 = d_1^*$ |
| $\Gamma(L_4, G_4)$, where $G_4(x) = A^t x^t + A^{-1} x^{t-1} + 1$ | $H_1^*$ | $n_4 = 2^t - t$ | $k_4 = k_3^*$ (Corollary 2) | $d_4 = d_7$ |
| $\Gamma(L_5, G_5)$, where $G_5(x) = C x^{t+1} + A^t x^t + Ax$ | $H_1^*$ | $n_5 = 2^t - t - 1$ | $k_5 = k_4$ (Lemma 7) | $d_5 = d_7$ |
| $\Gamma(L_6, G_6)$, where $G_6(x) = R x^{t+1} + V^t x^t + V x + 1$ | $H_1^*$ | $n_6 = 2^t - t - 1$ | $k_6 = k_4$ (Lemma 8) | $d_6 = d_7$ |
| $\Gamma(L_7, G_7)$, where $G_7(x) = x^{t+1} + 1$ | $H_1^*$ | $n_7 = 2^t - t - 1$ | $k_7 = k_4$ (Lemma 9) | $d_7 = 2t + 3$ (Lemma 11) |

Table 2 Quasi cyclic Goppa codes

| Code chain | $G(x)$ | $\gamma$ | $\beta$ |
|------------|--------|----------|---------|
| $\Gamma(L_1, G_1)$ | $x^{t-1} + 1$ | 0 | any nonzero element from $GF(2^t)$ |
| $\Gamma(L_2, G_2)$ | $A^t x^t + Ax$ | $A^{-1} \text{or } 0$ | any nonzero element from $GF(2^t)$ |
| $\Gamma(L_3, G_3)$ | $A^t x^t + Ax + C$ | $\gamma \in GF(2^t); \gamma^t = 1 + \beta C(1 + \beta)$ | any nonzero element from $GF(2^t)$ |
| $\Gamma(L_5, G_5)$ | $C x^{t+1} + A^t x^t + Ax$ | $\gamma \in GF(2^t); \gamma^t = 1 + \beta C$ | $\beta = \frac{\gamma^t}{C}$ |
| $\Gamma(L_7, G_7)$ | $x^{t+1} + 1$ | 0 | $\left(\alpha^{2^i - 1}\right)^i, i = 1, ..., 2^t + 1$ |

$\alpha$ is a primitive element of $GF(2^t)$ and $A \in GF(2^t)$. 

\[ \]
[5] M. Loeloeian and J. Conan, A transform approach in Goppa codes, *IEEE Trans. on Information Theory*, vol. 35, pp.105-115, 1987.
[6] A.M. Roseiro, J.I. Hall, J.E. Adney and M. Siegel, The trace operator and redundancy of Goppa codes, *IEEE Trans. on Information Theory*, vol. 38, No. 3, pp. 1130-1133, 1992.
[7] S. Bezzateev and N. Shekhunova, Subclass of binary Goppa codes with minimal distance equal to the design distance, *IEEE Trans. on Information Theory*, vol. 41, pp. 554-555, 1995.
[8] P. Veron, True dimension of some binary quadratic trace Goppa codes, Designs, Codes and Cryptography, 24, pp. 81-97, 2001.
[9] P. Veron, Proof of conjectures on the true dimension of some binary Goppa codes, Designs, Codes and Cryptography, 36, pp. 317-325, 2005.
[10] N.A. Shekhunova, S.V. Bezzateev and E.T. Mironchikov, A subclass of binary Goppa codes, Probl. Inform. Transm., vol. 25, no. 3, pp. 98-102, 1989.
[11] S.V. Bezzateev and N.A. Shekhunova, Quasi-cyclic Goppa codes, IEEE International Symposium on Information Theory, Canada, p. 499, 1995.
[12] G. Bommer and F. Blanchet, Binary quasicyclic Goppa codes, Designs, Codes and Cryptography, 20, pp. 107-124, 2000.
[13] P. Veron, Goppa codes and trace operator, *IEEE Trans. on Information Theory*, vol. 44, No. 1, pp. 290-295, 1998.
[14] G. Maatouk, A. Shokrollahi and M. Cheraghchi, Good Ensembles of Goppa Codes, *Ecole Polytechnique Federale De Lausanne, ALGO Lab*, 2007, www.algo.epfl.ch/contents/output/semp/Imud_MAATOUK.pdf
[15] S.V. Bezzateev and N.A. Shekhunova, A subclass of binary Goppa codes with improved estimation of the code dimension, Designs, Codes and Cryptography, 14, pp. 23-38, 1998.